

# **Fundamentos de Informática**



# Fundamentos de Informática

Horst H. von Brand



13 de octubre de 2015

Departamento de Informática  
Universidad Técnica Federico Santa María

© 2008-2015 Horst H. von Brand  
Todos los derechos reservados.

Compuesto por el autor en  $\text{\LaTeX}2\epsilon$  con Utopia para textos y Fourier-GUTenberg para matemáticas.

Versión 0.80-12-g27897cb

Se autoriza el uso de esta versión preliminar para cualquier fin educacional en una institución de enseñanza superior, en cuyo caso solo se permite el cobro de una tarifa razonable de reproducción. Se prohíbe todo uso comercial.

Agradezco a mi familia, a quienes he descuidado demasiado durante el desarrollo del presente texto.

El Departamento de Informática de la Universidad Técnica Federico Santa María provee el ambiente ideal de trabajo.

Dedico este texto a mis estudiantes, que sufrieron versiones preliminares del mismo. Sus sugerencias y preguntas ayudaron inmensamente a mejorarlo.



# Índice general

---

<b>Índice general</b>	<b>VII</b>
<b>Índice de figuras</b>	<b>XV</b>
<b>Índice de cuadros</b>	<b>XVIII</b>
<b>Índice de listados</b>	<b>XX</b>
<b>Índice de algoritmos</b>	<b>XXI</b>
<b>1 Preliminares</b>	<b>1</b>
1.1. Notación de lógica matemática . . . . .	1
1.1.1. Proposiciones . . . . .	1
1.1.2. Conectivas lógicas . . . . .	2
1.1.3. Lógica de predicados . . . . .	3
1.1.4. Cuantificadores . . . . .	4
1.2. Conjuntos . . . . .	4
1.3. Tuplas . . . . .	7
1.4. Multiconjuntos . . . . .	8
1.5. Sumatorias, productorias y yerbas afines . . . . .	8
1.6. Potencias factoriales . . . . .	11
1.7. Cálculo de diferencias finitas . . . . .	12
1.8. Funciones <i>floor</i> y <i>ceil</i> . . . . .	14
1.9. Otros resultados de interés . . . . .	16
1.10. Notación asintótica . . . . .	18
1.11. Notación asintótica en algoritmos . . . . .	23
<b>2 Relaciones y funciones</b>	<b>25</b>
2.1. Relaciones . . . . .	25
2.2. Funciones . . . . .	30
2.3. Operaciones . . . . .	33
<b>3 Demostraciones</b>	<b>35</b>
3.1. Razonamiento matemático . . . . .	35
3.2. Desenrollar definiciones . . . . .	37
3.3. Implicancias . . . . .	38
3.3.1. Primer método – Demostración directa . . . . .	38
3.3.2. Segundo método – Demostrar el contrapositivo . . . . .	39

3.4.	Demostrando un “Si y solo si” . . . . .	40
3.4.1.	Primer método – Cada una implica la otra . . . . .	40
3.4.2.	Segundo método – Cadena de equivalencias . . . . .	40
3.5.	Demostración por casos . . . . .	42
3.6.	Demostración por contradicción . . . . .	43
3.7.	Inducción . . . . .	49
3.7.1.	El caso más común . . . . .	49
3.7.2.	Otro punto de partida . . . . .	51
3.7.3.	Paso diferente . . . . .	51
3.7.4.	Ida y vuelta . . . . .	52
3.7.5.	Múltiples variables . . . . .	54
3.7.6.	Inducción fuerte . . . . .	56
3.7.7.	Inducción estructural . . . . .	61
3.8.	Demostrar existencia . . . . .	63
3.9.	Refutaciones . . . . .	64
3.9.1.	Refutar aseveraciones universales: Contraejemplo . . . . .	64
3.9.2.	Refutar existencia . . . . .	64
3.9.3.	Refutar por contradicción . . . . .	65
3.10.	Conjetura a teorema . . . . .	65
<b>4</b>	<b>Correctitud de programas</b>	<b>71</b>
4.1.	Lógica de Hoare . . . . .	71
4.2.	Búsqueda binaria . . . . .	73
4.2.1.	Escribiendo el programa . . . . .	73
4.3.	Exponenciación . . . . .	76
4.4.	Algunos principios . . . . .	77
<b>5</b>	<b>Números reales</b>	<b>81</b>
5.1.	Axiomas de los reales . . . . .	81
<b>6</b>	<b>Numerabilidad</b>	<b>85</b>
6.1.	Cardinalidad . . . . .	85
<b>7</b>	<b>Teoría de números</b>	<b>89</b>
7.1.	Algunas herramientas . . . . .	89
7.2.	Propiedades básicas . . . . .	89
7.3.	Máximo común divisor . . . . .	91
7.3.1.	Obtener los coeficientes de Bézout . . . . .	94
7.3.2.	Números primos . . . . .	95
7.4.	Congruencias . . . . .	98
7.5.	Aritmética en $\mathbb{Z}_m$ . . . . .	100
7.5.1.	Curvas elípticas . . . . .	108
7.5.2.	Anillos cuadráticos . . . . .	110
7.5.3.	Cuaterniones . . . . .	114
7.6.	Los teoremas de Lagrange, Euler y Fermat . . . . .	114
<b>8</b>	<b>Estructura de <math>\mathbb{Z}_m</math> y <math>\mathbb{Z}_m^\times</math></b>	<b>117</b>
8.1.	Descomposiciones . . . . .	117
8.1.1.	Homomorfismos e isomorfismos . . . . .	117
8.1.2.	Sumas directas . . . . .	119

8.1.3. Sumas directas externas . . . . .	121
8.1.4. Comentarios finales . . . . .	122
8.2. Estructura de $\mathbb{Z}_m^\times$ . . . . .	129
<b>9 Anillos de polinomios</b>	<b>139</b>
9.1. Algunas herramientas . . . . .	139
9.2. Dominios euclidianos . . . . .	142
9.3. Factorización de polinomios . . . . .	146
9.4. Raíces primitivas . . . . .	149
<b>10 Campos finitos</b>	<b>153</b>
10.1. Propiedades básicas . . . . .	153
10.2. Espacios vectoriales . . . . .	154
10.3. Estructura de los campos finitos . . . . .	156
10.4. Códigos de detección y corrección de errores . . . . .	164
10.4.1. Códigos de Hamming . . . . .	164
10.4.2. Verificación de redundancia cíclica . . . . .	164
<b>11 Algoritmos aritméticos</b>	<b>167</b>
11.1. Referencias detalladas . . . . .	167
11.2. Máximo común divisor . . . . .	167
11.3. Potencias . . . . .	171
11.4. Factorizar . . . . .	171
11.5. Factorización con curvas elípticas . . . . .	176
11.6. Determinar primalidad . . . . .	176
11.7. Números de Carmichael . . . . .	177
<b>12 Criptología</b>	<b>181</b>
12.1. Referencias adicionales . . . . .	181
12.2. Nomenclatura . . . . .	182
12.3. Protocolo Diffie-Hellman de intercambio de claves . . . . .	182
12.4. Sistema de clave pública de Rivest, Shamir y Adleman (RSA) . . . . .	183
12.4.1. Firma digital usando RSA . . . . .	185
12.5. El estándar de firma digital (DSS) . . . . .	185
12.5.1. Selección de parámetros . . . . .	185
12.5.2. Generar claves para un usuario . . . . .	186
12.5.3. Firmar y verificar firma . . . . .	186
12.5.4. Correctitud del algoritmo . . . . .	186
12.5.5. Ataques a DSS . . . . .	187
12.6. Otras consideraciones . . . . .	187
12.7. Criptografía de curvas elípticas . . . . .	187
12.7.1. Intercambio de claves . . . . .	188
12.7.2. Firmas digitales . . . . .	188
<b>13 Combinatoria elemental</b>	<b>189</b>
13.1. Técnicas básicas . . . . .	189
13.2. Situaciones recurrentes . . . . .	192
13.3. Manos de poker . . . . .	198
13.3.1. Royal Flush . . . . .	199
13.3.2. Straight Flush . . . . .	199

13.3.3. Four of a Kind . . . . .	199
13.3.4. Full House . . . . .	200
13.3.5. Flush . . . . .	200
13.3.6. Manos con dos pares . . . . .	201
13.3.7. Manos con todas las pintas . . . . .	202
13.3.8. Manos con valores diferentes . . . . .	202
13.4. El tao de BOOKKEEPER . . . . .	203
13.5. Juegos completos de poker . . . . .	203
13.6. Secuencias con restricciones . . . . .	204
<b>14 Funciones generatrices</b>	<b>207</b>
14.1. No son funciones, y nada generan . . . . .	207
14.2. Funciones generatrices . . . . .	209
14.3. Algunas series útiles . . . . .	211
14.3.1. Serie geométrica . . . . .	211
14.3.2. Teorema del binomio . . . . .	211
14.3.3. Otras series . . . . .	214
14.4. Notación para coeficientes . . . . .	215
14.5. Decimar . . . . .	216
14.6. Algunas aplicaciones combinatorias . . . . .	217
14.7. Manipulación de series . . . . .	221
14.7.1. Reglas OGF . . . . .	221
14.7.2. Reglas EGF . . . . .	225
14.8. El truco <i>zDlog</i> . . . . .	226
14.9. Ejemplos de manipulación de series . . . . .	226
14.10. Funciones generatrices en combinatoria . . . . .	229
14.11. Múltiples índices . . . . .	236
14.12. Aceite de serpiente . . . . .	236
<b>15 Principio de inclusión y exclusión</b>	<b>241</b>
15.1. El problema general . . . . .	241
15.2. Desarreglos . . . . .	246
15.3. El problema de ménages . . . . .	248
<b>16 Rudimentos de probabilidades discretas</b>	<b>251</b>
16.1. Probabilidades . . . . .	251
16.2. Distribuciones discretas . . . . .	252
16.2.1. Función generatriz de probabilidad . . . . .	254
16.2.2. Función generatriz de momentos . . . . .	255
16.2.3. Problemas de urna . . . . .	256
16.2.4. Distribuciones multivariadas . . . . .	257
16.2.5. Diagramas de árbol . . . . .	257
16.3. Probabilidad condicional . . . . .	258
16.4. Regla de Bayes . . . . .	260
16.5. Independencia . . . . .	260
16.6. Las principales distribuciones discretas . . . . .	261
16.7. Valor esperado . . . . .	264
<b>17 Series formales de potencias</b>	<b>267</b>
17.1. Un primer ejemplo . . . . .	267

17.2. Definición de serie formal . . . . .	268
17.3. Unidades y recíprocos . . . . .	269
17.4. Secuencias de series . . . . .	270
17.5. El principio de transferencia . . . . .	273
17.6. Derivadas e integrales formales . . . . .	274
17.7. Series en múltiples variables . . . . .	275
<b>18 La fórmula de Euler-Maclaurin</b>	<b>279</b>
18.1. Relación entre suma e integral . . . . .	279
18.2. Desarrollo de la fórmula . . . . .	280
18.3. Suma de potencias . . . . .	283
18.4. Números harmónicos . . . . .	283
18.5. Fórmula de Stirling . . . . .	284
18.6. Propiedades de los polinomios y números de Bernoulli . . . . .	287
18.7. El resto . . . . .	292
<b>19 Aplicaciones</b>	<b>293</b>
19.1. Números harmónicos . . . . .	293
19.2. Funciones generatrices con logaritmos . . . . .	294
19.3. Potencias factoriales . . . . .	296
19.4. Números de Fibonacci . . . . .	296
19.4.1. Solución mediante funciones generatrices ordinarias . . . . .	297
19.4.2. Solución mediante funciones generatrices exponenciales . . . . .	298
19.4.3. Números de Fibonacci y fuentes . . . . .	299
19.4.4. Búsqueda de Fibonacci . . . . .	299
19.5. Coeficientes binomiales . . . . .	301
19.6. Otras recurrencias de dos índices . . . . .	304
19.7. Dividir y conquistar . . . . .	307
19.7.1. Análisis de división fija . . . . .	308
19.7.2. Quicksort . . . . .	312
<b>20 Recurrencias</b>	<b>317</b>
20.1. Definición del problema . . . . .	317
20.2. Recurrencias lineales . . . . .	317
20.3. Recurrencias lineales de primer orden . . . . .	318
20.4. Recurrencias lineales de coeficientes constantes . . . . .	320
20.5. Método de repertorio . . . . .	321
20.6. Recurrencia de Riccati . . . . .	325
20.6.1. Vía recurrencia de segundo orden . . . . .	325
20.6.2. Reducción a una recurrencia de primer orden . . . . .	326
20.6.3. Transformación de Möbius . . . . .	327
<b>21 El método simbólico</b>	<b>329</b>
21.1. Un primer ejemplo . . . . .	329
21.2. Objetos sin rotular . . . . .	331
21.2.1. Algunas aplicaciones . . . . .	333
21.2.2. Palabras que no contienen un patrón dado . . . . .	336
21.2.3. Construcción ciclo . . . . .	339
21.2.4. Polinomios irreductibles en $\mathbb{F}_q$ . . . . .	342
21.3. Objetos rotulados . . . . .	343

21.3.1. Rotulado o no rotulado, esa es la cuestión... . . . . .	346
21.3.2. Algunas aplicaciones de objetos rotulados . . . . .	347
21.3.3. Operaciones adicionales . . . . .	350
21.4. Un problema de Moser y Lambek . . . . .	351
21.5. Contando secuencias . . . . .	352
<b>22 Familias de números famosas</b>	<b>355</b>
22.1. Subconjuntos y multiconjuntos . . . . .	355
22.2. Números de Fibonacci y de Lucas . . . . .	355
22.3. Números de Catalan . . . . .	356
22.4. Números de Motzkin . . . . .	357
22.5. Números de Schröder . . . . .	358
22.6. Números de Stirling de segunda especie . . . . .	360
22.7. Números de Stirling de primera especie . . . . .	361
22.8. Números de Lah . . . . .	363
22.9. Potencias, números de Stirling y de Lah . . . . .	364
22.10. Desarreglos . . . . .	366
22.11. Resultados de competencias con empate . . . . .	367
22.12. Particiones de enteros . . . . .	369
22.12.1. Particiones en general . . . . .	369
22.12.2. Sumandos diferentes e impares . . . . .	369
<b>23 Propiedades adicionales</b>	<b>371</b>
23.1. Funciones generatrices cumulativas . . . . .	371
23.2. Generatrices multivariadas . . . . .	379
<b>24 Grafos</b>	<b>387</b>
24.1. Algunos ejemplos de grafos . . . . .	387
24.2. Representación de grafos . . . . .	389
24.2.1. Lista de adyacencia . . . . .	390
24.2.2. Matriz de adyacencia . . . . .	390
24.2.3. Representación enlazada . . . . .	390
24.2.4. Representación implícita . . . . .	390
24.3. Isomorfismo entre grafos . . . . .	391
24.4. Algunas familias de grafos especiales . . . . .	392
24.5. Algunos resultados simples . . . . .	393
24.6. Secuencias gráficas . . . . .	394
24.7. Árboles . . . . .	402
24.8. Árboles con raíz . . . . .	405
24.9. Árboles ordenados . . . . .	406
24.9.1. Árboles de decisión . . . . .	406
24.9.2. Análisis de algoritmos de ordenamiento . . . . .	407
24.9.3. Generar código . . . . .	408
24.10. Grafos planares . . . . .	410
24.11. Algoritmos de búsqueda en grafos . . . . .	413
24.11.1. Búsqueda en profundidad . . . . .	413
24.11.2. Búsqueda a lo ancho . . . . .	415
24.11.3. Búsqueda a lo ancho versus búsqueda en profundidad . . . . .	416
24.12. Colorear vértices . . . . .	417
24.12.1. El algoritmo voraz para colorear grafos . . . . .	420

24.13. Colorear arcos . . . . .	421
24.14. Grafos bipartitos . . . . .	422
24.14.1. Matchings . . . . .	426
24.14.2. Transversales de familias de conjuntos finitos . . . . .	430
24.15. Grafos rotulados . . . . .	432
24.15.1. Árboles rotulados . . . . .	432
24.15.2. Costo mínimo para viajar entre vértices . . . . .	432
24.15.3. Árbol recubridor mínimo . . . . .	436
<b>25 Digrafos, redes, flujos</b>	<b>441</b>
25.1. Definiciones básicas . . . . .	441
25.2. Orden topológico . . . . .	442
25.3. Redes y rutas críticas . . . . .	444
25.4. Redes y flujos . . . . .	446
25.4.1. Trabajando con flujos . . . . .	448
25.4.2. Método de Ford-Fulkerson . . . . .	449
25.4.3. Redes residuales . . . . .	449
25.4.4. Caminos aumentables . . . . .	451
25.4.5. Cortes . . . . .	453
<b>26 Permutaciones</b>	<b>455</b>
26.1. Definiciones básicas . . . . .	455
<b>27 Teoría de colores de Pólya</b>	<b>463</b>
27.1. Grupos de permutaciones . . . . .	463
27.2. Órbitas y estabilizadores . . . . .	464
27.3. Número de órbitas . . . . .	468
27.4. Índice de ciclos . . . . .	471
27.5. Número de colores distinguibles . . . . .	471
<b>28 Introducción al análisis complejo</b>	<b>481</b>
28.1. Aritmética . . . . .	481
28.2. Un poquito de topología del plano . . . . .	483
28.3. Límites y derivadas . . . . .	485
28.4. Funciones elementales . . . . .	487
28.5. Logaritmos y potencias . . . . .	489
28.6. Integrales . . . . .	490
28.6.1. Integrales y antiderivadas . . . . .	491
28.6.2. El teorema de Cauchy . . . . .	493
28.6.3. La fórmula integral de Cauchy . . . . .	494
28.7. Secuencias y series . . . . .	498
28.7.1. Series . . . . .	500
28.8. Series de Taylor y Laurent . . . . .	504
28.8.1. Serie de Taylor . . . . .	505
28.8.2. Singularidades . . . . .	506
28.8.3. Series de Laurent . . . . .	510
28.8.4. Residuos . . . . .	513
28.8.5. Principio del argumento . . . . .	515
28.9. Aplicaciones discretas . . . . .	516
28.9.1. Sumas infinitas . . . . .	516

28.9.2. Números de Fibonacci . . . . .	519
28.10. La función $\Gamma$ . . . . .	520
<b>29 Estimaciones asintóticas</b>	<b>525</b>
29.1. Estimar sumas . . . . .	525
29.2. Estimar coeficientes . . . . .	526
29.2.1. Cota trivial . . . . .	526
29.2.2. Singularidades dominantes . . . . .	527
29.2.3. Número de palabras sin $k$ símbolos repetidos . . . . .	529
29.2.4. Singularidades algebraicas . . . . .	531
29.2.5. Singularidades algebraico-logarítmicas . . . . .	534
29.2.6. El método de Hayman . . . . .	535
<b>Bibliografía</b>	<b>539</b>
<b>Índice alfabético</b>	<b>559</b>

# Índice de figuras

---

1.1.	Diagramas de Venn para operaciones entre conjuntos . . . . .	6
1.2.	Desigualdad triangular . . . . .	17
1.3.	Relación entre $f(n)$ y $g(n)$ en notaciones de Bachmann-Landau . . . . .	20
2.1.	Funciones compuestas inyectivas y sobreyectivas . . . . .	32
3.1.	Diagrama para demostrar que $\sqrt{2}$ es irracional . . . . .	44
3.2.	Forma de una losa . . . . .	58
3.3.	Intento fallido de inducción . . . . .	58
3.4.	División del patio de $2^{n+1} \times 2^{n+1}$ en cuatro de $2^n \times 2^n$ . . . . .	59
3.5.	Análisis del patio de $4 \times 4$ . . . . .	59
3.6.	Inducción dejando libre cualquier cuadradito . . . . .	60
3.7.	Chapas posibles con $n = 3$ . . . . .	66
3.8.	Chapas posibles con $n = 5$ . . . . .	66
3.9.	Chapa de $7 \times 7$ como chapa de $5 \times 5$ con borde . . . . .	67
7.1.	Un cuadrado . . . . .	102
7.2.	Curvas elípticas . . . . .	109
7.3.	Sumas en curvas elípticas . . . . .	109
10.1.	Elementos de circuitos lógicos . . . . .	166
10.2.	Circuito para $x^8 + x^4 + x^3 + x^2 + 1$ . . . . .	166
13.1.	Una distribución de 6 elementos en 4 grupos . . . . .	194
14.1.	52 centavos en monedas . . . . .	218
14.2.	Colección de monedas como producto . . . . .	218
14.3.	Series para 1 o 5 centavos . . . . .	218
14.4.	Serie para combinaciones de 1 y 5 centavos . . . . .	218
14.5.	Una fuente de bloque . . . . .	234
15.1.	Intersecciones entre tres conjuntos . . . . .	241
15.2.	Dominós no traslapados en ciclo . . . . .	248
16.1.	Diagrama de árbol para lanzamiento de tres monedas . . . . .	258
16.2.	Árbol para el dilema de Monty Hall . . . . .	259
18.1.	Suma e integral como áreas . . . . .	279
18.2.	Polinomios de Bernoulli en $[0, 1]$ (escalados de mínimo a máximo) . . . . .	291

19.1.	Búsqueda de Fibonacci . . . . .	300
19.2.	Búsqueda de Fibonacci: Juego final . . . . .	301
19.3.	Idea de Quicksort . . . . .	312
19.4.	Particionamiento en Quicksort . . . . .	312
21.1.	Ciclos de largo seis . . . . .	340
21.2.	Una función de [21] a [21] . . . . .	349
22.1.	División del pentágono en triángulos . . . . .	357
22.2.	Cuerdas entre cinco puntos sobre la circunferencia . . . . .	358
24.1.	Diagrama de circuito de un filtro de paso bajo de tercer orden . . . . .	387
24.2.	Esquema del metro de Londres (1908) . . . . .	388
24.3.	Un grafo . . . . .	389
24.4.	Ejemplo de isomorfismo entre grafos . . . . .	391
24.5.	Dos formas de dibujar el grafo de Petersen . . . . .	391
24.6.	Algunos grafos $P_n$ . . . . .	392
24.7.	Algunos grafos $C_n$ . . . . .	392
24.8.	Algunos grafos $K_n$ . . . . .	393
24.9.	Algunos grafos $W_n$ . . . . .	393
24.10.	Algunos cubos . . . . .	393
24.11.	Un grafo con grados 1, 2, 2, 3 y 4 . . . . .	394
24.12.	La operación 2-switch entre los arcos $uv$ y $xy$ . . . . .	395
24.13.	Un grafo con vértices de grados $\langle 8, 8, 6, 5, 4, 3, 3, 3, 1, 1 \rangle$ . . . . .	397
24.14.	Un grafo con dos componentes conexos . . . . .	398
24.15.	Puentes de Königsberg . . . . .	400
24.16.	Dibuja una casita . . . . .	401
24.17.	Queso cortado en nueve cubitos . . . . .	402
24.18.	Cubitos de queso de colores . . . . .	402
24.19.	Esquema de vértices en la parte T3 el teorema 24.9 . . . . .	403
24.20.	Los 6 árboles con 6 vértices . . . . .	404
24.21.	Ejemplos de árbol con raíz . . . . .	405
24.22.	Vértice del árbol de decisión al pesar monedas . . . . .	407
24.23.	Árbol de decisión al ordenar 3 objetos . . . . .	407
24.24.	Árbol sintáctico de una expresión . . . . .	408
24.25.	Ilustración de la demostración de la fórmula de Euler . . . . .	410
24.26.	El grafo $K_{3,3}$ . . . . .	411
24.27.	El grafo del dodecaedro . . . . .	412
24.28.	Grafo para ejemplos de recorrido . . . . .	414
24.29.	El grafo de la figura 24.28 recorrido en profundidad . . . . .	414
24.30.	El grafo de la figura 24.28 recorrido a lo ancho . . . . .	415
24.31.	Grafo representando charlas . . . . .	417
24.32.	Asignación de horas a charlas como colores . . . . .	417
24.33.	Otra asignación de horas a charlas . . . . .	418
24.34.	Grafo a colorear . . . . .	418
24.35.	Un ciclo de largo impar en el grafo de la figura 24.34 . . . . .	419
24.36.	Un coloreo con tres colores del grafo de la figura 24.34 . . . . .	419
24.37.	Otro grafo a colorear . . . . .	419
24.38.	Subgrafos del grafo de la figura 24.37 . . . . .	419
24.39.	Coloreo con cuatro colores del grafo de la figura 24.37 . . . . .	420

24.40. Un coloreo de arcos del grafo de Frucht . . . . .	422
24.41. Algunas estrellas . . . . .	423
24.42. Algunos grafos bipartitos completos . . . . .	424
24.43. Un ciclo de largo $2l+1$ si hay conexiones cruzadas . . . . .	424
24.44. Cómo operar en el teorema 24.17 . . . . .	425
24.45. Matchings en un grafo bipartito . . . . .	426
24.46. Aumentando un matching . . . . .	429
24.47. Matching resultante . . . . .	430
24.48. Comités de la Universidad de Miskatonic . . . . .	431
24.49. Ejemplo de grafo para árbol recubridor mínimo . . . . .	436
24.50. El algoritmo de Prim aplicado al grafo de la figura 24.49 . . . . .	437
24.51. El algoritmo de Kruskal aplicado al grafo de la figura 24.49 . . . . .	438
24.52. Esquema de redes interconectadas por <i>bridges</i> . . . . .	439
24.53. La red de la figura 24.52 como grafo . . . . .	440
25.1. Ejemplos de digrafos . . . . .	442
25.2. Restricciones al vestirse . . . . .	442
25.3. Una red de actividades . . . . .	445
25.4. Una red, sus capacidades y un flujo en la red . . . . .	446
25.5. Una red . . . . .	451
25.6. Flujo y red residual en la red de la figura 25.5 . . . . .	452
25.7. El flujo aumentado según el camino aumentable de la figura 25.6b . . . . .	452
25.8. Un corte en la red de la figura 25.5 con el flujo de la figura 25.6a . . . . .	453
26.1. Ordenamiento de cartas . . . . .	457
26.2. ¿Puede hacerse? . . . . .	461
27.1. Un cuadrado y sus simetrías . . . . .	464
27.2. Un grafo de seis vértices y sus automorfismos . . . . .	464
27.3. Un ejemplo de grafo y los generadores de su grupo de automorfismos . . . . .	465
27.4. Rotaciones de un tetraedro . . . . .	467
27.5. Icosaedro trunco . . . . .	467
27.6. Ejemplos de tarjetas de identidad . . . . .	468
27.7. Configuraciones fijas bajo rotación en $\pi$ . . . . .	469
27.8. Configuraciones fijas bajo reflexión en la vertical . . . . .	469
27.9. Configuraciones fijas bajo reflexión en la diagonal . . . . .	470
27.10. Las ocho tarjetas distinguibles . . . . .	470
27.11. Efecto de la permutación $\hat{g}$ sobre un coloreo $\omega$ . . . . .	472
27.12. Algunos compuestos aromáticos . . . . .	475
27.13. Los tres isómeros del xileno . . . . .	476
27.14. Operaciones de simetría (rotaciones) de un tetraedro . . . . .	477
27.15. Un árbol binario completo . . . . .	477
27.16. Un cubo visto desde un vértice . . . . .	479
28.1. Operaciones entre complejos . . . . .	482
28.2. Dominio alternativo de $\log z$ . . . . .	490
28.3. Ejemplos de homotopía . . . . .	493
28.4. Curva para integral ejemplo . . . . .	496
28.5. Secuencia de funciones continuas con límite discontinuo . . . . .	498

# Índice de cuadros

---

1.1.	Tablas de verdad para conectivas básicas . . . . .	2
1.2.	Identidades adicionales . . . . .	3
1.3.	Propiedades importantes de las operaciones lógicas . . . . .	3
1.4.	Valores de $n^2 + n + 41$ para $1 \leq n \leq 39$ . . . . .	4
1.5.	Propiedades de las operaciones entre conjuntos . . . . .	7
1.6.	Notaciones de Bachmann-Landau . . . . .	18
7.1.	Traza del algoritmo extendido de Euclides . . . . .	95
7.2.	El grupo $D_8$ . . . . .	103
7.3.	Multiplicación de cuaterniones . . . . .	114
7.4.	La tabla de multiplicación en $\mathbb{Z}_{12}$ . . . . .	116
8.1.	El grupo $D_8$ . . . . .	117
8.2.	Los grupos $\mathbb{Z}_8^\times$ y $\mathbb{Z}_{12}^\times$ . . . . .	118
8.3.	Los grupos $\mathbb{Z}_5^\times$ y $\mathbb{Z}_4$ . . . . .	118
8.4.	Potencias en $\mathbb{Z}_{21}^\times$ . . . . .	121
9.1.	Órdenes de los elementos en $\mathbb{Z}_8^\times$ . . . . .	149
10.1.	Paridades para el código de Hamming (15,4) . . . . .	164
11.1.	Traza del algoritmo binario para máximo común divisor . . . . .	170
11.2.	Cálculo de $3^{10}$ por el método binario . . . . .	171
11.3.	Condiciones a $x$ e $y$ al factorizar 8616460799 . . . . .	172
11.4.	Ejemplo de Pollard $\rho$ . . . . .	175
13.1.	Número de alumnos por curso . . . . .	191
14.1.	Tabla para calcular $p_{50}$ . . . . .	220
15.1.	Posibilidades con un número par de ceros . . . . .	245
18.1.	Polinomios y números de Bernoulli . . . . .	282
19.1.	Triángulo de Pascal . . . . .	304
19.2.	Complejidad de algunos algoritmos . . . . .	310
20.1.	Familia para $(n-1)^{\frac{s}{2}}$ . . . . .	322
20.2.	Familia para $(n-1)^{\frac{L}{2}} H_n$ . . . . .	324

21.1. Cálculo de $c_{xy}(t) = t^4 + t$ . . . . .	338
21.2. Combinando los ciclos (1 2) y (1 3 2) . . . . .	343
22.1. Las 7 particiones de 4 elementos en 2 clases . . . . .	360
22.2. Números de Stirling de segunda especie . . . . .	361
22.3. Números de Stirling de primera especie . . . . .	362
22.4. Números de Lah . . . . .	364
24.1. Lista de adyacencia para el grafo de la figura 24.3 . . . . .	390
24.2. Matriz de adyacencia del grafo de la figura 24.3 . . . . .	390
24.3. Código óptimo para la expresión ejemplo . . . . .	409
24.4. Poliedros regulares . . . . .	412
25.1. Actividades y dependencias . . . . .	444
25.2. Términos más tempranos por actividad para la red de la figura 25.3 . . . . .	444
25.3. Inicio más tardío por actividad para la red 25.3 . . . . .	445
25.4. Holguras para las actividades de la figura 25.3 . . . . .	446
27.1. Los subgrupos de $S_3$ . . . . .	463
27.2. Pares $(\gamma, y)$ para demostración del teorema 27.4 . . . . .	466
27.3. Número de configuraciones de tarjetas respetadas por cada simetría del cuadrado . . . . .	470
27.4. Elementos del grupo para pulseras . . . . .	473
27.5. Las operaciones sobre tarjetas y sus tipos . . . . .	475
27.6. Rotaciones de un tetraedro . . . . .	476
27.7. El grupo de operaciones del árbol . . . . .	478
27.8. Operaciones de simetría rotacional de caras de un cubo . . . . .	478
29.1. Números de Bell ordenados . . . . .	528
29.2. Números de Bernoulli pares . . . . .	529
29.3. Números de Motzkin . . . . .	532
29.4. Números de Motzkin nuevamente . . . . .	535

## Índice de listados

---

1.1.	Ordenamiento por inserción . . . . .	23
4.1.	Búsqueda binaria en C . . . . .	75
19.1.	Versión simple de Quicksort . . . . .	313
23.1.	Ordenamiento por inserción . . . . .	373
23.2.	Hallar el máximo . . . . .	381

# Índice de algoritmos

---

4.1.	Secuencia . . . . .	72
4.2.	Selección . . . . .	72
4.3.	Ciclo . . . . .	73
4.4.	Esbozo de búsqueda binaria . . . . .	74
4.5.	Búsqueda binaria: Segundo esbozo . . . . .	74
4.6.	Búsqueda binaria: Pseudocódigo final . . . . .	75
4.7.	Exponenciación binaria recursiva . . . . .	76
4.8.	Exponenciación binaria no recursiva . . . . .	77
4.9.	Cálculo de $\lfloor \sqrt{n} \rfloor$ . . . . .	78
7.1.	Algoritmo de Euclides para calcular $\gcd(a, b)$ . . . . .	93
7.2.	Algoritmo extendido de Euclides . . . . .	95
11.1.	Algoritmo de Euclides para calcular $\gcd(a, b)$ . . . . .	168
11.2.	Máximo común divisor binario . . . . .	170
11.3.	Cálculo binario de potencias . . . . .	171
11.4.	Factorizar según Fermat . . . . .	172
11.5.	Detectar ciclos (Floyd) . . . . .	173
11.6.	$\rho$ de Pollard . . . . .	174
11.7.	Prueba de primalidad de Miller-Rabin . . . . .	178
19.1.	Búsqueda de Fibonacci . . . . .	302
24.1.	Recorrer árboles con raíz . . . . .	406
24.2.	Búsqueda en profundidad, versión recursiva . . . . .	414
24.3.	Búsqueda en profundidad, versión no recursiva . . . . .	415
24.4.	Búsqueda a lo ancho . . . . .	416
24.5.	Coloreo voraz . . . . .	421
24.6.	Costos mínimos desde el vértice $v$ (Dijkstra) . . . . .	433
24.7.	Costos mínimos desde el vértice $v$ (Bellman-Ford) . . . . .	434
24.8.	Costos mínimos entre todos los vértices (Floyd-Warshall) . . . . .	435
25.1.	Ordenamiento topológico de Kahn . . . . .	443
25.2.	Ordenamiento topológico de Tarjan . . . . .	443
25.3.	El método de Ford-Fulkerson . . . . .	449



## Prefacio

---

Este documento presenta (y extiende substancialmente) la materia de los ramos *Fundamentos de Informática I*, *Fundamentos de Informática II* y *Estructuras Discretas* como dictados durante los años 2009 a 2014 en la Casa Central de Universidad Técnica Federico Santa María por el autor. El tratamiento de algunos temas es definitivamente no tradicional, y en algunas áreas el autor sigue líneas de razonamiento que le parecen interesantes, aún si no son directamente parte del curso. Así hay material adicional a la materia oficial del curso en estos apuntes, que no se vio en clase. Se notan resultados que están fuera del temario donde ayudan a iluminar los temas tratados. Se ha hecho el intento de juntar todo al material relevante, en forma accesible para el no especialista. Intentamos también seguir la exhortación de Knuth de no perderse en abstracción excesiva.

Veremos una colección de temas que en conjunto se conocen bajo el nombre de *matemáticas discretas*. Trataremos de razonamiento matemático, y nos ocuparemos más que nada de fenómenos discretos, en contraposición de lo continuo que es el ámbito del cálculo. Siendo un área menos conocida, encontraremos en ella resultados sorprendentes y técnicas ingeniosas. La importancia en la informática es que en computación no se tratan fenómenos continuos. El aprender a razonar en el ámbito de objetos discretos, y las técnicas que veremos durante el curso de estos ramos, serán útiles a la hora de diseñar sistemas y evaluar su desempeño. El análisis complejo ofrece herramientas poderosas, particularmente para derivar estimaciones asintóticas de muchas de las cantidades de interés. Al no ser materia cubierta en el currículum tradicional de las carreras de ingeniería, se incluye una breve reseña de los resultados requeridos.

La razón de fondo de preocuparse de cómo razonar, en particular en el ámbito de la informática, es que cada día dependemos más de sistemas informáticos, que han dejado de ser accesorios para transformarse en parte indispensable de nuestra vida diaria. Fallas en tales sistemas pueden tener consecuencias desastrosas. Ejemplos de estas situaciones abundan, lamentablemente. Particularmente preocupantes son cuando errores lógicos son los causantes. En este sentido, parte del objetivo de los presentes ramos en el currículum de informática es entrenar en el arte de enfrentar problemas en forma estructurada, y de reconocer cuándo se tiene una solución correcta.



# 1 Preliminares

---

El capítulo resume algunas nociones y notaciones que usaremos en el resto del texto. No debiera presentar material realmente nuevo para el lector.

El rango de nociones manejados en matemáticas es muy amplio, y la notación bastante variada. La notación (y la nomenclatura) usada por distintos autores no es uniforme, por tanto servirá también para definir la notación que usaremos. Donde hay diversas notaciones en uso más o menos común, se anotarán las alternativas.

Repasaremos lógica matemática, conjuntos y notaciones para sumatorias y productorias. Introducimos potencias factoriales, las funciones piso (*floor*) y techo (*ceil*), que se usan frecuentemente en matemáticas discretas. Definiremos notaciones asintóticas, que usaremos más adelante al discutir algunos algoritmos.

## 1.1. Notación de lógica matemática

Usaremos la notación de la lógica matemática con frecuencia en lo que sigue, la introduciremos informalmente acá.

### 1.1.1. Proposiciones

**Definición 1.1.** Una *proposición* es una aseveración que puede ser verdadera o falsa.

Algunos ejemplos son:

**Proposición 1.1.** *Está lloviendo en Valparaíso.*

**Proposición 1.2.** *El número  $2^{32} + 1$  es primo*

**Proposición 1.3.** *El número real*

$$\zeta(5) = \sum_{k \geq 1} k^{-5}$$

*es irracional.*

La verdad de 1.1 depende del momento, 1.2 es falsa (es  $2^{32} + 1 = 641 \cdot 6700417$ ), y nadie sabe si 1.3 es cierta o no.

Gran parte de nuestro lenguaje no son proposiciones, con lo que la lógica no es capaz de representarlo todo. Por ejemplo, a una pregunta, a una orden o a una interjección no se le puede asignar verdad o falsedad.

### 1.1.2. Conectivas lógicas

Comúnmente combinamos proposiciones como “Si llueve, uso paraguas”, “Se puede viajar a Concepción en bus o en avión”, “No traje mis documentos”, “Apruebo el ramo solo si obtengo al menos 35 en la prueba” o “El cartel es rojo y azul”. Para precisar el significado de estas combinaciones usamos *tablas de verdad*. Al combinar proposiciones  $P$  y  $Q$  mediante las operaciones indicadas

$P$	$\neg P$
F	V
V	F

(a) Negación

$P$	$Q$	$P \vee Q$	$P \wedge Q$	$P \Rightarrow Q$	$P \Leftrightarrow Q$
F	F	F	F	V	V
F	V	V	F	V	F
V	F	V	F	F	F
V	V	V	V	V	V

(b) Conectivas

Cuadro 1.1 – Tablas de verdad para conectivas básicas

obtenemos el cuadro 1.1, donde falso se indica mediante  $F$  y verdadero mediante  $V$ . Se anota  $\vee$  para *o* (disyunción), usamos  $\wedge$  para *y* (conjunción), para *si ... entonces* escribimos  $\Rightarrow$  (implicancia), y para expresar *si y solo si* usamos  $\Leftrightarrow$  (equivalencia). Estas operaciones no son todas necesarias, por ejemplo  $P \Rightarrow Q$  es equivalente a  $\neg P \vee Q$ , y  $P \Leftrightarrow Q$  no es más que  $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ . Nótese que la tabla de verdad para  $P \Rightarrow Q$  coincide con  $\neg Q \Rightarrow \neg P$ , su *contrapositivo*.

En castellano (como en la mayoría de los lenguajes modernos) hay ambigüedad, en que “A o B” puede entenderse como *A o B, o ambos* (inclusivo), o también como *A o B, pero no ambos* (exclusivo). Un mito [184] bastante extendido entre los lógicos es que en el latín hay dos disyunciones; *vel*, que expresa el sentido inclusivo, y *aut*, que expresa el exclusivo. En realidad, ambas son ambiguas como en los lenguajes modernos. La noción empleada en lógica matemática es inclusiva, y nuestra notación sugiere el latín *vel*.

Suele decirse “A es suficiente para B” si  $A \Rightarrow B$  (si la implicancia es cierta, saber que A es cierto asegura que B es cierto, si A es falso B puede ser cierto como no serlo), y que “A es necesario para B” o “A solo si B” si  $B \Rightarrow A$  (saber que A es cierto permite concluir que debe serlo B). Así suele decirse “A es necesario y suficiente para B” o “A si y solo si B” para expresar  $A \Leftrightarrow B$ . Note que hay diversas formas de expresar lo mismo, y es fácil confundirse.

Al decir “Hoy almorzaré bife a lo pobre o pescado frito con ensalada” se entiende que es uno o el otro, no ambos; en “Leo novelas policiales o históricas” se subentiende que son ambas; mientras “Sus mascotas son perros o gatos” no queda claro si es solo uno o el otro, o posiblemente ambas. De la misma forma, “Si llueve, llevo paraguas” puede entenderse como que llevo paraguas exclusivamente cuando llueve, nuestra conectiva implica incluye la posibilidad de llevarlo incluso si no llueve. La aseveración sobre hábitos de lectura se interpretaría como que no leo nada más que novelas policiales o históricas, nuestra formalización no es así de excluyente. Hay cosas que se subentienden u omiten en el lenguaje cotidiano, si se quiere lograr precisión eso no es aceptable.

Identidades útiles reseña el cuadro 1.2, propiedades importantes da el cuadro 1.3. Nótese que la segunda columna del cuadro 1.2 se obtiene de la primera intercambiando  $\wedge$  con  $\vee$  y  $V$  con  $F$ . Esto es lo que se conoce como *dualidad*, obtenemos dos equivalencias por el precio de una. A  $Q \Rightarrow P$  se le llama el *recíproco* de  $P \Rightarrow Q$  (en inglés, *converse*). No hay relación entre los valores de verdad de una implicancia y su recíproca, como es fácil demostrar. Las identidades de los cuadros 1.2 y 1.3 debieran memorizarse.

Leyes	Nombre(s)
$\neg\neg P \equiv P$	Doble negación
$P \vee \neg P \equiv V$	Medio excluido/contradicción
$P \vee F \equiv P$	Identidad
$P \vee V \equiv V$	Dominación
$P \vee P \equiv P$	Idempotencia
$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$	de Morgan
$P \vee Q \equiv Q \vee P$	Commutatividad
$(P \vee Q) \vee R \equiv P \vee (Q \vee R)$	Asociatividad
$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$	Distributividad
$P \vee (P \wedge Q) \equiv P$	Absorción
$P \wedge \neg P \equiv F$	
$P \wedge V \equiv P$	
$P \wedge F \equiv F$	
$P \wedge P \equiv P$	
$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$	
$P \wedge Q \equiv Q \wedge P$	
$(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$	
$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$	
$P \wedge (P \wedge Q) \equiv P$	
$P \wedge (P \vee Q) \equiv P$	

Cuadro 1.2 – Identidades adicionales

Nombre	Propiedad
Definición de implicancia	$P \Rightarrow Q \equiv \neg P \vee Q$
Definición de si y solo si	$P \iff Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$
Contrapositivo	$P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$
Reducción al absurdo	$P \Rightarrow Q \equiv P \wedge \neg Q \Rightarrow F$
Transitividad de implicancia	$(P \Rightarrow Q) \wedge (Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$

Cuadro 1.3 – Propiedades importantes de las operaciones lógicas

### 1.1.3. Lógica de predicados

Queremos razonar sobre individuos de un conjunto, no solo de proposiciones que son verdaderas o falsas. Usaremos la convención que letras mayúsculas representan variables, y letras minúsculas constantes.

**Definición 1.2.** Un *predicado* es una función cuyo valor es verdadero o falso.

Usaremos la convención que letras mayúsculas denotan constantes, y letras minúsculas variables. Por ejemplo, tenemos el predicado prime( $x$ ) que es verdadero exactamente cuando  $x$  es un número primo. Así, tanto prime(2) como prime( $2^{16} + 1$ ) son verdaderos, mientras prime(2743) es falso ( $2743 = 13 \cdot 211$ ).

Podemos considerar la expresión:

$$a = 3b$$

como un predicado de dos argumentos ( $a$  y  $b$ ) que es verdadero exactamente cuando  $a = 3b$ . Asimismo,

$$17 = 3x$$

es un predicado que es falso para todos los naturales  $x$  y es cierto para el racional  $17/3$ .

Usamos las conectivas lógicas para combinar predicados, construyendo predicados más complejos. Por ejemplo,

$$ax^2 + bx + c = 0 \Rightarrow x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

resulta ser cierto si consideramos  $a$ ,  $b$ ,  $c$  y  $x$  como números complejos. Está claro que es importante indicar de qué conjunto toman valores las variables indicadas.

### 1.1.4. Cuantificadores

Desearemos expresar que un predicado es cierto para todos los posibles valores de las variables involucradas, o que es cierto al menos para uno de ellos. Esto se expresa mediante *cuantificadores*. Los que usaremos son  $\forall$  (para todo) y  $\exists$  (existe). Una proposición expresada concisamente es

$$\forall n: \text{prime}(n^2 + n + 41)$$

donde  $\text{prime}(x)$  es el predicado discutido antes. La variable usada queda atada al cuantificador y no tiene significado fuera. Explicitando el conjunto al que pertenecen las variables, escribiremos por ejemplo:

$$\forall n \in \mathbb{N}: \text{prime}(n^2 + n + 41) \quad (1.1)$$

Veamos diferentes valores de  $n$ , como resume el cuadro 1.4. Hasta  $n = 39$  vamos bien. Pero resulta

<b><math>n</math></b>	<b>Valor</b>	<b>¿Primo?</b>
0	41	Si
1	43	Si
2	47	Si
:	:	:
39	1 601	Si

Cuadro 1.4 – Valores de  $n^2 + n + 41$  para  $1 \leq n \leq 39$

$40^2 + 40 + 41 = 1681 = 41 \cdot 41$ , con lo que la proposición 1.1 es falsa. Si nos preguntamos que valores de  $n$  dan un valor compuesto, caemos en cuenta que para  $n = 41$  todos los términos son divisibles por 41. En efecto, se reduce a  $41^2$ , que no es primo. Al polinomio (1.1) se le conoce como polinomio de Euler, hay una variedad de polinomios que dan primos para sus primeros valores.

## 1.2. Conjuntos

Una de las nociones más importantes en las matemáticas actuales es la de conjunto. En términos simples, un conjunto es una colección de elementos bien definida, vale decir, para cada elemento se puede determinar claramente si pertenece o no al conjunto. Para indicar que el elemento  $a$  pertenece al conjunto  $\mathcal{A}$ , se escribe  $a \in \mathcal{A}$ , para indicar que no pertenece se anota  $a \notin \mathcal{A}$ . A veces resulta más cómodo escribir estas relaciones al revés, o sea anotar  $\mathcal{A} \ni a$  o  $\mathcal{A} \not\ni a$ , respectivamente.

Ciertos conjuntos tienen notación especial por su frecuente uso. El conjunto especial que no tiene elementos se llama el *conjunto vacío* y se anota  $\emptyset$ . Otros son el conjunto de los *números naturales*,  $\mathbb{N} = \{1, 2, 3, \dots\}$ ; el de los *números enteros*,  $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ ; los *números racionales*,  $\mathbb{Q}$ ; los *reales*,  $\mathbb{R}$ ; y los *complejos*,  $\mathbb{C}$ . El conjunto de los naturales más el cero lo anotaremos  $\mathbb{N}_0$ . Anotaremos  $\mathbb{Q}^+$  para los números racionales mayores a cero, y similarmente  $\mathbb{R}^+$  para los reales.

Una manera de describir un conjunto es por *extensión*, nombrando cada uno de sus elementos:

$$\mathcal{A} = \{1, 2, 3, 4, 5\}$$

Esto resulta incómodo para conjuntos grandes, por lo que suele usarse alguna notación como la siguiente para no dar explícitamente todos los elementos:

$$\mathcal{B} = \{1, 2, \dots, 128\}$$

Esto también se usa si estamos frente a conjuntos infinitos:

$$\mathcal{C} = \{1, 2, 4, 8, \dots\}$$

El problema es que no queda claro exactamente cuáles son los elementos a incluir. Una forma alternativa de describir conjuntos es por *intención*, describiendo de alguna forma los elementos que lo componen. Haciendo referencia a los conjuntos definidos antes:

$$\mathcal{B} = \{x: 1 \leq x \leq 128\} \quad (\text{aunque tal vez es } \mathcal{B} = \{2^k: 0 \leq k < 8\})$$

$$\mathcal{C} = \{2^k: k \geq 0\}$$

Es importante tener presente que un elemento pertenece o no al conjunto, no puede pertenecer más de una vez a él. Otro detalle es que no hay ningún orden entre los elementos de un conjunto. El conjunto  $\{1, 2, 3, 4, 5\}$  es exactamente el mismo que  $\{4, 2, 1, 5, 3\}$ , o que  $\{2, 1, 2, 5, 4, 2, 3\}$ , donde hemos mencionado el mismo elemento varias veces.

Operaciones comunes entre conjuntos se describen mediante diagramas de Venn en la figura 1.1.

**Unión:** Los elementos que pertenecen a  $\mathcal{A}$  o a  $\mathcal{B}$  o a ambos se anota  $\mathcal{A} \cup \mathcal{B}$ . Es fácil ver que  $\mathcal{A} \cup \mathcal{B} = \mathcal{B} \cup \mathcal{A}$ . Como  $(\mathcal{A} \cup \mathcal{B}) \cup \mathcal{C} = \mathcal{A} \cup (\mathcal{B} \cup \mathcal{C})$ , se suele omitir el paréntesis en tales expresiones.

**Intersección:** Aquellos elementos que pertenecen a  $\mathcal{A}$  y a  $\mathcal{B}$  se anotan  $\mathcal{A} \cap \mathcal{B}$ . Es  $\mathcal{A} \cap \mathcal{B} = \mathcal{B} \cap \mathcal{A}$ . Nuevamente,  $(\mathcal{A} \cap \mathcal{B}) \cap \mathcal{C} = \mathcal{A} \cap (\mathcal{B} \cap \mathcal{C})$ , y convencionalmente se omiten los paréntesis. Si tienen intersección vacía (o sea,  $\mathcal{A} \cap \mathcal{B} = \emptyset$ ), se dice que son *disjuntos*.

**Resta:** Los elementos de  $\mathcal{A}$  que no pertenecen a  $\mathcal{B}$  se anotan  $\mathcal{A} \setminus \mathcal{B}$ .

**Diferencia simétrica:** Los que pertenecen a  $\mathcal{A}$  o a  $\mathcal{B}$ , pero no a ambos, se escriben  $\mathcal{A} \Delta \mathcal{B}$ . También tenemos  $\mathcal{A} \Delta \mathcal{B} = \mathcal{B} \Delta \mathcal{A}$ . Considerando las diferentes áreas del diagrama de Venn para  $(\mathcal{A} \Delta \mathcal{B}) \Delta \mathcal{C}$  vemos que incluye los elementos de exactamente uno o tres de los conjuntos, con lo que  $(\mathcal{A} \Delta \mathcal{B}) \Delta \mathcal{C} = \mathcal{A} \Delta (\mathcal{B} \Delta \mathcal{C})$ .

**Complemento:** Si estamos considerando un conjunto de elementos como ámbito de discusión, lo tomamos como *universo* (comúnmente anotado  $\mathcal{U}$ ), y tenemos el *complemento* del conjunto  $\mathcal{A}$  como aquellos elementos de  $\mathcal{U}$  que no pertenecen a  $\mathcal{A}$ . Esto lo anotaremos  $\overline{\mathcal{A}}$ .

Resulta importante comparar conjuntos.

**Igualdad:** Dos conjuntos son *iguales* cuando tienen los mismos elementos. Esto se anota  $\mathcal{A} = \mathcal{B}$ .

**Subconjunto:** Si todos los elementos de  $\mathcal{A}$  pertenecen a  $\mathcal{B}$  se anota  $\mathcal{A} \subseteq \mathcal{B}$ , y se dice que  $A$  es *subconjunto* de  $\mathcal{B}$ . Si queremos excluir la posibilidad  $\mathcal{A} = \mathcal{B}$ , escribimos  $\mathcal{A} \subset \mathcal{B}$  (a veces se le llama *subconjunto propio*). Para indicar que  $\mathcal{A}$  no es subconjunto de  $\mathcal{B}$  se anota  $\mathcal{A} \not\subseteq \mathcal{B}$ . Nótese que algunos usan la notación  $\mathcal{A} \subset \mathcal{B}$  para lo que anotamos  $\mathcal{A} \subseteq \mathcal{B}$ , y usan  $\mathcal{A} \subsetneq \mathcal{B}$  para lo que llamamos  $\mathcal{A} \subset \mathcal{B}$ .

**Superconjunto:** Si  $\mathcal{A} \subseteq \mathcal{B}$ , también anotamos  $\mathcal{B} \supseteq \mathcal{A}$ , y similarmente si  $\mathcal{A} \subset \mathcal{B}$  anotamos también  $\mathcal{B} \supset \mathcal{A}$ . Decimos que  $\mathcal{B}$  es *superconjunto* de  $\mathcal{A}$ .

Las operaciones entre conjuntos pueden expresarse usando notación lógica:

$$\mathcal{A} \cup \mathcal{B} = \{x: x \in \mathcal{A} \vee x \in \mathcal{B}\} \tag{1.2}$$

$$\mathcal{A} \cap \mathcal{B} = \{x: x \in \mathcal{A} \wedge x \in \mathcal{B}\} \tag{1.3}$$

$$\mathcal{A} \subseteq \mathcal{B} \equiv x \in \mathcal{A} \implies x \in \mathcal{B} \tag{1.4}$$

$$\mathcal{A} = \mathcal{B} \equiv x \in \mathcal{B} \iff x \in \mathcal{A} \tag{1.5}$$

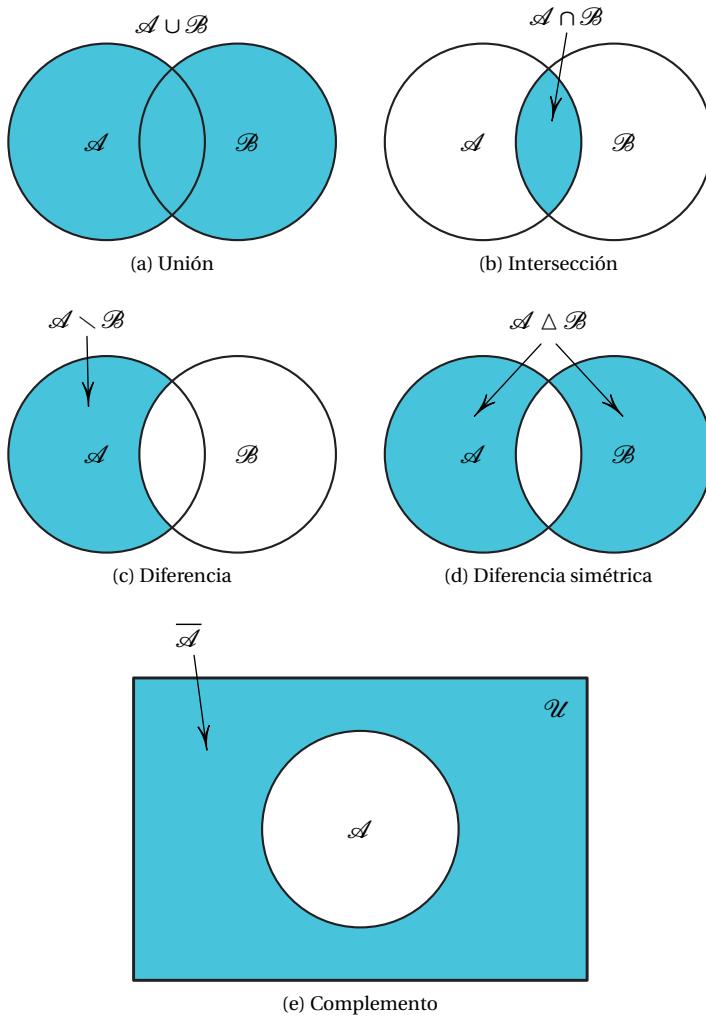


Figura 1.1 – Diagramas de Venn para operaciones entre conjuntos

La forma de la unión y la intersección sugieren la forma de la conectiva lógica en (1.2) y en (1.3). La dirección de la implicancia en (1.4) puede recordarse como ambas apuntando en la misma dirección.

Podemos definir diferencia y diferencia simétrica en términos de las operaciones tradicionales:

$$\begin{aligned}\mathcal{A} \setminus \mathcal{B} &= \mathcal{A} \cap \overline{\mathcal{B}} \\ \mathcal{A} \Delta \mathcal{B} &= (\mathcal{A} \cup \mathcal{B}) \setminus (\mathcal{A} \cap \mathcal{B}) \\ &= (\mathcal{A} \cap \overline{\mathcal{B}}) \cup (\overline{\mathcal{A}} \cap \mathcal{B})\end{aligned}$$

Algunas propiedades simples de las anteriores son las dadas en el cuadro 1.5, donde  $\mathcal{A}$ ,  $\mathcal{B}$  y  $\mathcal{C}$  representan conjuntos cualquiera. Compárese con el cuadro 1.2. También tenemos que si  $\mathcal{A} \subset \mathcal{B}$  y  $\mathcal{B} \subset \mathcal{C}$  entonces  $\mathcal{A} \subset \mathcal{C}$ . Una manera de demostrar igualdad entre conjuntos es usar el hecho que si  $\mathcal{A} \subseteq \mathcal{B}$  y  $\mathcal{B} \subseteq \mathcal{A}$ , entonces  $\mathcal{A} = \mathcal{B}$ .

Otra noción importante es el número de elementos del conjunto, su *cardinalidad*. La cardinalidad del conjunto  $\mathcal{A}$  se anotará  $|\mathcal{A}|$ . Para conjuntos finitos, es simplemente el número de elementos

Leyes		Nombre(s)
$\overline{\overline{A}} = A$		Doble complemento
$A \cup \overline{A} = U$	$A \cap \overline{A} = \emptyset$	Complemento
$A \cup \emptyset = A$	$A \cap U = A$	Identidad
$A \cup U = U$	$A \cap \emptyset = \emptyset$	Dominación
$\overline{A \cup B} = \overline{A} \cap \overline{B}$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$	de Morgan
$A \cup B = B \cup A$	$A \cap B = B \cap A$	Comutatividad
$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$	Asociatividad
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributividad
$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$	Absorción

Cuadro 1.5 – Propiedades de las operaciones entre conjuntos

del conjunto. Si  $A = \{1, 2, 4, 8, 16, 32\}$ , tenemos  $|A| = 6$ . Sólo para  $\emptyset$  se cumple  $|\emptyset| = 0$ . También tenemos que si  $A \subseteq B$  entonces  $|A| \leq |B|$ . Más adelante (capítulo 6) consideraremos conjuntos infinitos también.

Es común referirse a rangos de elementos de algún conjunto ordenado, típicamente  $\mathbb{R}$  y ocasionalmente  $\mathbb{N}$ . Para ello usaremos las notaciones siguientes.

$$\begin{aligned}(a, b) &= \{x: a < x < b\} \\ [a, b) &= \{x: a \leq x < b\} \\ (a, b] &= \{x: a < x \leq b\} \\ [a, b] &= \{x: a \leq x \leq b\}\end{aligned}$$

Si un extremo es abierto (no incluye el elemento del caso) usamos paréntesis, en caso que el extremo es cerrado (el elemento indicado está incluido) usamos corchetes (paréntesis cuadrados). En el caso especial de un rango de los primeros naturales anotaremos:

$$[1, n] = [n]$$

Al conjunto de todos los subconjuntos de algún conjunto  $A$  (el *conjunto potencia* de  $A$ ) lo anotaremos  $2^A$ . También es común notación como  $\mathcal{P}(A)$ . Por ejemplo:

$$2^{\{1,2,3\}} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

### 1.3. Tuplas

A objetos que combinan varios elementos se les llama *tuplas*. Escribimos las componentes de la tupla separados por comas y la tupla completa encerrada entre paréntesis. El caso más común es el de pares de elementos, como  $(1, 2)$ , pero también podemos tener tríos como  $(x, y, z)$ , y así sucesivamente. Es lamentable que esta notación para pares pueda confundirse con rangos abiertos, como descritos antes. Deberá quedar claro del contexto lo que se está discutiendo.

El orden importa, el par  $(1, 2)$  no es lo mismo que  $(2, 1)$ . Pueden repetirse elementos,  $(5, 2, 1, 5)$  es una tupla válida. Nada dice que los elementos deban ser tomados del mismo conjunto, podemos tener pares formados por un polinomio y un número complejo, como  $(3x^2 - 5x + 2, 3 + 5i)$ .

Una manera de construir tuplas es mediante producto cartesiano entre conjuntos:

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}$$

Podemos construir tríos vía  $\mathcal{A} \times \mathcal{B} \times \mathcal{C}$  y así sucesivamente, donde interpretamos  $\mathcal{A} \times \mathcal{B} \times \mathcal{C}$  como  $(\mathcal{A} \times \mathcal{B}) \times \mathcal{C}$ , y la tupla  $(a, b, c)$  como una abreviatura del par  $((a, b), c)$ , y de forma similar para largos mayores (llamaremos *largo* al número de elementos de la tupla). Usaremos potencias para indicar tuplas de un largo dado tomando elementos de un conjunto. Formalmente, para cualquier conjunto  $\mathcal{A}$  definimos:

$$\begin{aligned}\mathcal{A}^1 &= \mathcal{A} \\ \mathcal{A}^{n+1} &= \mathcal{A}^n \times \mathcal{A} \quad \text{si } n \geq 1\end{aligned}\tag{1.6}$$

Tuplas de elementos de un mismo conjunto, particularmente si son de largos posiblemente diferentes, se llaman *secuencias*. En una secuencia interesa el largo (que para la secuencia  $\sigma$  anotaremos  $|\sigma|$ ) y el elemento en cada posición. Hay una única secuencia de largo 0, que generalmente llamaremos  $\epsilon$ . Si las secuencias son finitas y de elementos atómicos (*símbolos*) se les suele llamar *palabras* o *strings* (por el término en inglés). Más adelante trataremos extensamente con secuencias infinitas.

## 1.4. Multiconjuntos

Un elemento puede pertenecer varias veces a un *multiconjunto*. Anotamos las repeticiones mediante exponentes. Un ejemplo es  $\{a, b, a, c, b, a\} = \{a, a, a, b, b, c\} = \{a^3, b^2, c^1\}$ .

Las operaciones entre multiconjuntos son afines a las de conjuntos: La unión es juntar todos los elementos de los multiconjuntos que se unen, la intersección es lo que tienen en común. Por ejemplo:

$$\begin{aligned}\{a^2, b^5, c^2\} \cup \{b^2, c^3, d^1\} &= \{a^2, b^7, c^5, d^1\} \\ \{a^2, b^5, c^2\} \cap \{b^2, c^3, d^1\} &= \{b^2, c^2\}\end{aligned}$$

En forma similar a las demás operaciones entre conjuntos definimos las operaciones respectivas para multiconjuntos. Para multiconjuntos tiene sentido hablar del universo del que se toman los elementos, pero no la idea de complemento. Por ejemplo:

$$\begin{aligned}\{a^2, b^5, c^2\} \setminus \{b^2, c^3, d^1\} &= \{a^2, b^3\} \\ \{a^2, b^5, c^2\} \Delta \{b^2, c^3, d^1\} &= \{a^2, b^3, c^3, d^1\}\end{aligned}$$

Un multiconjunto es subconjunto de otro si todos sus elementos (con las repeticiones respectivas) aparecen en el segundo:

$$\begin{aligned}\{a^2, b^5, c^2\} &\subseteq \{a^3, b^5, c^6, d^1\} \\ \{a^4, b^5, c^2\} &\not\subseteq \{a^3, b^5, d^3\}\end{aligned}$$

Una manera de asimilar las operaciones con las de conjuntos es que la unión considera sumar los elementos de ambos, la intersección es el mínimo.

## 1.5. Sumatorias, productorias y yerbas afines

Es común referirse a sumas de términos parecidos, como:

$$a + a^2 + \cdots + a^{16}$$

La notación indicada es sugestiva, pero no queda realmente claro cuáles son los términos a incluir. Esto lo anotamos mediante sumatoria:

$$\sum_{1 \leq k \leq 16} a^k$$

Aunque podríamos también referirnos a

$$\sum_{0 \leq k \leq 4} a^{2^k}$$

Nótese que la variable índice es irrelevante:

$$\sum_{1 \leq k \leq 16} a^k = \sum_{1 \leq r \leq 16} a^r$$

Además, esa variable queda atada a la suma, de forma que no tiene significado fuera:

$$\sum_{1 \leq r \leq 10} a^r + \sum_{1 \leq s \leq 10} b^s = \sum_{1 \leq k \leq 10} a^k + \sum_{1 \leq k \leq 10} b^k = \sum_{1 \leq i \leq 10} (a^i + b^i)$$

Un caso típico es cuando tenemos un conjunto  $\mathcal{A}$ , y queremos sumar sobre los  $k \in \mathcal{A}$ , como en:

$$\sum_{k \in \mathcal{A}} a^k$$

Incluso podemos tener varias condiciones, en cuyo caso se entiende que estamos sumando sobre el valor del índice que cumple con todas ellas:

$$\sum_{\substack{0 \leq k \leq 10 \\ k \text{ múltiplo de } 3}} a^k = a^0 + a^3 + a^6 + a^9$$

Ocasionalmente usaremos un único signo de suma para indicar suma sobre varias variables, como por ejemplo:

$$\begin{aligned} \sum_{\substack{0 \leq r \leq 2 \\ 1 \leq s \leq 3}} a^{2r+s} &= a^1 + a^2 + a^3 + a^3 + a^4 + a^5 + a^5 + a^6 + a^7 \\ &= a + a^2 + 2a^3 + a^4 + 2a^5 + a^6 + a^7 \end{aligned}$$

Un problema con esta notación es que no explicita las variables sobre las que se suma. Esto deberá quedar claro del contexto.

Con esta convención, expresamos sumas infinitas como por ejemplo la del problema de Basilea:

$$\sum_{k \geq 1} \frac{1}{k^2} = \frac{\pi^2}{6}$$

Una notación útil es la convención de Iverson [183], uno de cuyos campeones es Knuth [150, 213]. Se anota una condición entre corchetes para indicar el valor 0 si la condición es falsa, y 1 si es verdadera. Sirve, entre otras cosas, para eliminar condiciones de las sumas, transformándolas en sumas infinitas y llevando las condiciones a una posición más visible y manipulable. Una aplicación simple es:

$$\sum_{k \in \mathcal{A}} f(k) + \sum_{k \in \mathcal{B}} f(k) = \sum_k f(k)[k \in \mathcal{A}] + \sum_k f(k)[k \in \mathcal{B}] = \sum_k f(k)([k \in \mathcal{A}] + [k \in \mathcal{B}])$$

Como estamos incluyendo dos veces los elementos en la intersección:

$$[k \in \mathcal{A}] + [k \in \mathcal{B}] = [k \in \mathcal{A} \cup \mathcal{B}] + [k \in \mathcal{A} \cap \mathcal{B}]$$

O sea:

$$\sum_k f(k)([k \in \mathcal{A}] + [k \in \mathcal{B}]) = \sum_k f(k)[k \in \mathcal{A} \cup \mathcal{B}] + \sum_k f(k)[k \in \mathcal{A} \cap \mathcal{B}]$$

Nuestra suma original en notación más tradicional es:

$$\sum_{k \in \mathcal{A}} f(k) + \sum_{k \in \mathcal{B}} f(k) = \sum_{k \in \mathcal{A} \cup \mathcal{B}} f(k) + \sum_{k \in \mathcal{A} \cap \mathcal{B}} f(k) \quad (1.7)$$

También ayuda al intercambiar órdenes de sumas. El multiplicar símbolos de Iverson corresponde a que ambas condiciones sean ciertas:

$$\begin{aligned} \sum_{1 \leq j \leq n} \sum_{1 \leq k \leq j} f(j, k) &= \sum_{j, k} f(j, k) [1 \leq j \leq n] [1 \leq k \leq j] \\ &= \sum_{j, k} f(j, k) [1 \leq k \leq j \leq n] \\ &= \sum_{j, k} f(j, k) [1 \leq k \leq n] [k \leq j \leq n] \\ &= \sum_{1 \leq k \leq n} \sum_{k \leq j \leq n} f(j, k) \end{aligned} \quad (1.8)$$

Otro ejemplo interesante es:

$$\begin{aligned} \sum_{2 \leq k \leq n} \sum_{1 \leq j \leq k-1} \frac{1}{k-j} &= \sum_k [2 \leq k \leq n] \sum_j [1 \leq j \leq k-1] \cdot \frac{1}{k-j} \\ &= \sum_{k, j} [2 \leq k \leq n] \cdot [1 \leq j \leq k-1] \cdot \frac{1}{k-j} \end{aligned} \quad (1.9)$$

Podemos reorganizar:

$$[2 \leq k \leq n] \cdot [1 \leq j \leq k-1] = [1 \leq j < k \leq n] = [1 \leq j \leq n-1] \cdot [j+1 \leq k \leq n] \quad (1.10)$$

Introduciendo la nueva variable  $m = k - j$ , tenemos:

$$[j+1 \leq k \leq n] = [j+1 \leq m + j \leq n] = [1 \leq m \leq n-j] \quad (1.11)$$

Usando (1.10) con (1.11) en (1.9) permite cambiar el orden de las sumas:

$$\begin{aligned} \sum_{2 \leq k \leq n} \sum_{1 \leq j \leq k-1} \frac{1}{k-j} &= \sum_{k, j} [1 \leq j \leq n-1] \cdot [j+1 \leq k \leq n] \cdot \frac{1}{k-j} \\ &= \sum_{1 \leq j \leq n-1} \sum_{1 \leq m \leq n-j} \frac{1}{m} \end{aligned} \quad (1.12)$$

$$= \sum_{1 \leq j \leq n-1} H_{n-j} \quad (1.13)$$

Acá usamos la definición de los *números harmónicos*:

$$H_n = \sum_{1 \leq k \leq n} \frac{1}{k} \quad (1.14)$$

La suma (1.13) es sobre  $n-j$  entre 1 y  $n-1$  en reversa, que es lo mismo que sumar sobre  $j$  de 1 a  $n-1$ :

$$\sum_{2 \leq k \leq n} \sum_{1 \leq j \leq k-1} \frac{1}{k-j} = \sum_{1 \leq j \leq n-1} H_j \quad (1.15)$$

De forma similar a las sumas podemos expresar productos, por ejemplo factoriales:

$$\prod_{1 \leq k \leq n} k = n!$$

También productos infinitos, como el producto de Wallis (lo demostraremos en el teorema 18.2):

$$\prod_{k \geq 1} \frac{2k}{2k-1} \cdot \frac{2k}{2k+1} = \frac{2}{1} \cdot \frac{2}{3} \cdot \frac{4}{3} \cdot \frac{4}{5} \cdot \frac{6}{5} \cdot \frac{6}{7} \cdot \frac{8}{7} \cdot \frac{8}{9} \cdots = \frac{\pi}{2}$$

Esta idea es aplicable a toda operación asociativa y commutativa, ya que implícitamente estamos obviando completamente el orden en que se efectúan las operaciones entre los elementos considerados. Claro que tal cosa solo es válida en sumas (o productos, etc) finitas o sumas infinitas que convergen en forma incondicional. Podemos expresar uniones e intersecciones:

$$\bigcup_{1 \leq k \leq 10} \mathcal{A}_k \quad \bigcap_{1 \leq k \leq 10} \mathcal{A}_k$$

Hace falta definir qué se entenderá por una suma sin términos, un producto sin factores, etc. La convención general es que el resultado es el valor neutro para la operación indicada. Vale decir, con  $\mathcal{U}$  el conjunto universo:

$$\begin{aligned} \sum_{k \in \emptyset} t_k &= 0 && \text{porque } t + 0 = t \\ \prod_{k \in \emptyset} t_k &= 1 && \text{porque } t \cdot 1 = t \\ \bigcup_{k \in \emptyset} t_k &= \emptyset && \text{porque } t \cup \emptyset = t \\ \bigcap_{k \in \emptyset} t_k &= \mathcal{U} && \text{porque } t \cap \mathcal{U} = t \end{aligned}$$

Podemos partir con esto y extender la suma (o el producto, etc) un elemento a la vez. La definición completa de la sumatoria es:

$$\sum_{k \in \emptyset} t_k = 0 \quad \sum_{k \in \mathcal{A} \cup \{n\}} t_k = \sum_{k \in \mathcal{A}} t_k + t_n \quad \text{si } n \notin \mathcal{A}$$

El caso más común, claro está, es extender un rango. Expresamos  $k \in \emptyset$  mediante el rango  $0 \leq k \leq -1$ :

$$\sum_{0 \leq k \leq -1} t_k = 0 \quad \sum_{0 \leq k \leq n+1} t_k = \sum_{0 \leq k \leq n} t_k + t_{n+1}$$

## 1.6. Potencias factoriales

Siguiendo a Knuth (ver por ejemplo [150]) usamos las siguientes notaciones para  $x$  cualquiera y entero no negativo  $n$ :

$$\begin{aligned} x^n &= \prod_{0 \leq k < n} (x - k) && (1.16) \\ &= x \cdot (x - 1) \cdots (x - (n - 1)) \\ &= x \cdot (x - 1) \cdots (x - n + 1) \end{aligned}$$

$$\begin{aligned} x^{\bar{n}} &= \prod_{0 \leq k < n} (x + k) && (1.17) \\ &= x \cdot (x + 1) \cdots (x + n - 1) \end{aligned}$$

Nótese que son exactamente  $n$  factores, como en las potencias convencionales. Siguiendo la convención de que productos vacíos son 1:

$$x^0 = x^{\bar{0}} = 1 \quad (1.18)$$

Les llamamos *potencias factoriales en bajada* y *en subida* (en inglés *falling factorial power* y *rising factorial power*), respectivamente. Hay una variedad de otras notaciones en uso para esto; particularmente común es  $(x)_k$  (*símbolo de Pochhammer*) para la potencia en bajada (aunque ocasionalmente se usa para potencias factoriales en subida). Se usa también  $x^{(n)}$  para la potencia factorial en subida. Algunos autores usan  $(x)_n^+$  y  $(x)_n^-$  para potencias factoriales en subida y bajada, respectivamente.

Una de las razones que hacen útil esta notación es lo siguiente:

$$\frac{d^n}{du^n} u^x = x(x-1)(x-2) \cdots (x-n+1) u^{x-n} = x^n u^{x-n}$$

Esto vale para  $x \in \mathbb{C}$ , y con la convención que la 0-ésima derivada es no hacer nada, vale para todo  $n \in \mathbb{N}_0$ .

Nótese que si  $m, n$  y  $k$  son enteros no negativos:

$$m^{\underline{n+k}} = m^n \cdot (m-n)^k \quad (1.19)$$

$$m^{\overline{n+k}} = m^{\overline{n}} \cdot (m+n)^{\overline{k}} \quad (1.20)$$

En particular:

$$(m+n)^{\underline{n}} \cdot m! = (m+1)^{\overline{n}} \cdot m! = (m+n)! \quad (1.21)$$

Esto porque:

$$(m+n)^{\underline{n}} \cdot m! = (m+n)(m+n-1) \cdots (m+1) \cdot m! = (m+n)!$$

$$(m+1)^{\overline{n}} \cdot m! = (m+1)(m+2) \cdots (m+n) \cdot m! = (m+n)!$$

Tenemos también:

$$n^{\underline{n}} = 1^{\overline{n}} = n! \quad (1.22)$$

Otra relación notable es la siguiente:

$$x^k = (-1)^k (-x)^{\overline{k}} \quad (1.23)$$

## 1.7. Cálculo de diferencias finitas

Si definimos el operador  $\Delta$ :

$$\Delta f(n) = f(n+1) - f(n) \quad (1.24)$$

El operador es claramente lineal:

$$\Delta(\alpha f(n) + \beta g(n)) = \alpha \Delta f(n) + \beta \Delta g(n) \quad (1.25)$$

Tenemos el operador inverso, que también es lineal:

$$\Sigma f(n) = \sum_{0 \leq k < n} f(k) + c \quad (1.26)$$

El límite inferior de la suma es arbitrario, pero hay que fijar alguno. Como  $\Delta c = 0$  vale para cualquier constante  $c$ :

$$\begin{aligned} \Delta \Sigma f(n) &= f(n) \\ \Sigma \Delta f(n) &= f(n) + c \end{aligned} \quad (1.27)$$

para alguna constante arbitraria  $c$ . Tenemos:

$$\begin{aligned}\Delta n^k &= (n+1)^k - n^k \\ &= (n+1)n^{k-1} - n^{k-1} \cdot (n-k+1) \\ &= (n+1 - (n-k+1))n^{k-1} \\ &= kn^{k-1}\end{aligned}\tag{1.28}$$

De (1.27) y (1.28) tenemos también:

$$\Sigma n^k = \frac{n^{k+1}}{k+1} + c\tag{1.29}$$

Otras relaciones de interés son:

$$\Delta c = 0 \quad (c \text{ es una constante})\tag{1.30}$$

$$\Delta c^n = (c-1)c^n\tag{1.31}$$

En particular:

$$\Delta 2^n = 2^n\tag{1.32}$$

Demostrar relaciones similares a (1.28) y (1.29) para potencias factoriales en subida queda de ejercicio.

Un resultado interesante es la *suma por partes*, afín a la integración por partes. Comenzamos con:

$$\begin{aligned}\Delta x_k y_k &= x_{k+1}y_{k+1} - x_k y_k \\ &= x_{k+1}y_{k+1} - x_k y_{k+1} + x_k y_{k+1} - x_k y_k \\ &= y_{k+1}\Delta x_k + x_k \Delta y_k\end{aligned}\tag{1.33}$$

De (1.33) reorganizando y sumando tenemos:

$$\sum_{0 \leq k \leq n} x_k \Delta y_k = x_{n+1}y_{n+1} - x_0 y_0 - \sum_{0 \leq k \leq n} y_{k+1}\Delta x_k\tag{1.34}$$

La relación (1.34) permite completar la suma (1.9). En (1.15) habíamos llegado a:

$$\sum_{2 \leq k \leq n} \sum_{1 \leq j \leq k-1} \frac{1}{k-j} = \sum_{1 \leq j \leq n-1} H_j$$

Podemos considerar:

$$x_j \Delta y_j = H_j \cdot 1 \quad \Delta x_j = H_{j+1} - H_j = \frac{1}{j+1} \quad y_j = j$$

Substituyendo en (1.34), con ajustes de índices:

$$\sum_{1 \leq j \leq n-1} H_j = nH_n - 1 \cdot H_1 - \sum_{1 \leq j \leq n-1} (j+1) \frac{1}{j+1} = nH_n - n$$

y finalmente:

$$\sum_{2 \leq k \leq n} \sum_{1 \leq j \leq k-1} \frac{1}{k-j} = nH_n - n\tag{1.35}$$

Las relaciones (1.25), (1.27), (1.29) y (1.34) recuerdan a las del cálculo infinitesimal, y son base del *cálculo de diferencias finitas*, con aplicaciones en la aproximación de funciones mediante polinomios y la interpolación. Referencia obligada es Milne-Thomson [256], una visión más moderna ofrecen Graham, Knuth y Patashnik [150]. Extensiones de las paralelas indicadas dan pie al *cálculo umbral*, formalizado por Roman y Rota [307], una visión general dan Bucchianico y Loeb [58].

### 1.8. Funciones *floor* y *ceil*

Siguiendo nuevamente a Knuth, usaremos la notación  $\lfloor x \rfloor$  para el entero inmediatamente inferior a  $x$  (en inglés le llaman *floor*, piso) y  $\lceil x \rceil$  para el entero inmediatamente superior (le llaman *ceil*, por *ceiling*, techo en inglés). La notación es mnemónica en que indica el entero inferior a través de marcar un “piso”, y el entero superior mediante un “techo”. Fue Gauß quien introdujo la noción de *floor* con la notación  $[x]$ , que se mantuvo como estándar indiscutible hasta que Iverson [183] introdujera las usadas acá en 1962. La notación de Gauß sigue siendo común en teoría de números. Algunos usan  $\lfloor x \rfloor$  para  $\lceil x \rceil$ , y hay quienes interpretan  $\lfloor x \rfloor$  como la “parte entera”, el entero más cercano en dirección al cero. Nuestra definición es más regular, no depende del signo. Por ejemplo:

$$\begin{aligned}\left\lfloor -\frac{2}{3} \right\rfloor &= -1 \\ \lfloor \pi \rfloor &= 3 \\ \lceil \pi \rceil &= 4 \\ \lfloor -3 \rfloor &= \lceil -3 \rceil = -3\end{aligned}$$

Una función relacionada es la *parte fraccional*, o *función diente de sierra* (en inglés *sawtooth*):

$$\{x\} = x - \lfloor x \rfloor \quad (1.36)$$

Se cumplen las siguientes relaciones básicas para estas funciones:

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1 \quad (1.37)$$

$$\lceil x \rceil - 1 < x \leq \lceil x \rceil \quad (1.38)$$

Expresado de otra forma:

$$x - 1 < \lfloor x \rfloor \leq x \quad (1.39)$$

$$x \leq \lceil x \rceil < x + 1 \quad (1.40)$$

$$0 \leq \{x\} < 1 \quad (1.41)$$

Es claro que:

$$\lfloor x \rfloor = -\lceil -x \rceil \quad (1.42)$$

$$\lceil x \rceil = -\lfloor -x \rfloor \quad (1.43)$$

De la definición, ecuación (1.36), tenemos directamente:

$$\lfloor x \rfloor = x - \{x\} \quad (1.44)$$

Usando las relaciones para cambio de signo tenemos:

$$x = \lceil x \rceil + (x - \lceil x \rceil) = \lceil x \rceil - (-x - \lfloor -x \rfloor)$$

y resulta

$$\lceil x \rceil = x + \{-x\} \quad (1.45)$$

Si  $n$  es un entero y  $x$  un real cualquiera, se cumplen:

$$\lfloor x + n \rfloor = \lfloor x \rfloor + n \quad (1.46)$$

$$\lceil x + n \rceil = \lceil x \rceil + n \quad (1.47)$$

$$\{x + n\} = \{x\} \quad (1.48)$$

En cambio, para  $x$  e  $y$  reales cualquiera tenemos:

$$\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1 \quad (1.49)$$

$$\lceil x \rceil + \lceil y \rceil - 1 \leq \lceil x + y \rceil \leq \lceil x \rceil + \lceil y \rceil \quad (1.50)$$

Algunas identidades más interesantes con  $x$  real,  $m$  entero y  $n$  natural son [150]:

$$\left\lfloor \frac{x+m}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor + m}{n} \right\rfloor \quad (1.51)$$

$$\left\lceil \frac{x+m}{n} \right\rceil = \left\lceil \frac{\lceil x \rceil + m}{n} \right\rceil \quad (1.52)$$

La primera servirá de ejemplo de demostración con estas nociones:

$$\left\lfloor \frac{x+m}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor + \{x\} + m}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor + m}{n} + \frac{\{x\}}{n} \right\rfloor$$

Como  $\{x\} < 1$ , el término final no influye.

Con  $m$  positivo:

$$n = \left\lfloor \frac{n}{m} \right\rfloor + \left\lfloor \frac{n+1}{m} \right\rfloor + \left\lfloor \frac{n+2}{m} \right\rfloor + \dots + \left\lfloor \frac{n+m-1}{m} \right\rfloor \quad (1.53)$$

$$n = \left\lceil \frac{n}{m} \right\rceil + \left\lceil \frac{n-1}{m} \right\rceil + \left\lceil \frac{n-2}{m} \right\rceil + \dots + \left\lceil \frac{n-m+1}{m} \right\rceil \quad (1.54)$$

Para demostrar la primera de éstas, llamemos  $n = q \cdot m + r$ , con  $0 \leq r < m$ . Escribamos:

$$\sum_{0 \leq k < m} \left\lfloor \frac{n+k}{m} \right\rfloor = \sum_{0 \leq k < m} \left\lfloor q + \frac{r+k}{m} \right\rfloor = m \cdot q + \sum_{0 \leq k < m} \left\lfloor \frac{r+k}{m} \right\rfloor$$

Los términos de la última suma son 0 si  $r+k < m$  y 1 si  $r+k \geq m$ , que es el rango  $m-r \leq k < m$  con exactamente  $r$  elementos, y resulta lo indicado.

Más generalmente, con  $x \in \mathbb{R}$ :

$$\lfloor mx \rfloor = \lfloor x \rfloor + \left\lfloor x + \frac{1}{m} \right\rfloor + \left\lfloor x + \frac{2}{m} \right\rfloor + \dots + \left\lfloor x + \frac{m-1}{m} \right\rfloor \quad (1.55)$$

$$\lceil mx \rceil = \lceil x \rceil + \left\lceil x - \frac{1}{m} \right\rceil + \left\lceil x - \frac{2}{m} \right\rceil + \dots + \left\lceil x - \frac{m-1}{m} \right\rceil \quad (1.56)$$

A la relación (1.55) se le conoce como *identidad de Hermite*. La siguiente demostración es debida a Matsuoka [250]. Sea:

$$f(x) = \lfloor mx \rfloor - \lfloor x \rfloor - \left\lfloor x + \frac{1}{m} \right\rfloor - \left\lfloor x + \frac{2}{m} \right\rfloor - \dots - \left\lfloor x + \frac{m-1}{m} \right\rfloor$$

Entonces, como para  $\alpha, \beta$  reales siempre es  $\lfloor \alpha + 1 \rfloor - \lfloor \beta + 1 \rfloor = \lfloor \alpha \rfloor - \lfloor \beta \rfloor$  tenemos:

$$\begin{aligned} f\left(x + \frac{1}{m}\right) &= \lfloor mx + 1 \rfloor - \left\lfloor x + \frac{1}{m} \right\rfloor - \left\lfloor x + \frac{2}{m} \right\rfloor - \dots - \left\lfloor x + \frac{m-1}{m} \right\rfloor - \lfloor x + 1 \rfloor \\ &= \lfloor mx \rfloor - \lfloor x \rfloor - \left\lfloor x + \frac{1}{m} \right\rfloor - \left\lfloor x + \frac{2}{m} \right\rfloor - \dots - \left\lfloor x + \frac{m-1}{m} \right\rfloor \\ &= f(x) \end{aligned}$$

Por el otro lado, para  $0 \leq x < 1/m$  tenemos  $f(x) = 0$ , con lo que  $f(x) = 0$  para todo  $x$ , que es lo que queríamos probar. La relación (1.56) se demuestra de forma similar.

Alternativamente, para la identidad de Hermite por (1.51) podemos escribir:

$$\left\lfloor \frac{\lfloor mx \rfloor + k}{m} \right\rfloor = \left\lfloor \frac{mx + k}{m} \right\rfloor = \left\lfloor x + \frac{k}{m} \right\rfloor$$

Por (1.53) resulta lo indicado.

Para  $m$  positivo, las siguientes permiten transformar pisos en techos y viceversa:

$$\left\lfloor \frac{n}{m} \right\rfloor = \left\lceil \frac{n-m+1}{m} \right\rceil = \left\lceil \frac{n+1}{m} \right\rceil - 1 \quad (1.57)$$

$$\left\lceil \frac{n}{m} \right\rceil = \left\lceil \frac{n+m-1}{m} \right\rceil = \left\lceil \frac{n-1}{m} \right\rceil + 1 \quad (1.58)$$

Para demostrar (1.57), sea  $n = qm + r$  con  $0 \leq r < m$ . Entonces:

$$\begin{aligned} n - m + 1 &= (q-1)m + r + 1 \\ n + 1 &= qm + r + 1 \end{aligned}$$

Como  $1 \leq r + 1 \leq m$ , resultan las relaciones indicadas en (1.57).

A veces resultan útiles:

$$\left\lfloor \frac{\lfloor x/m \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{mn} \right\rfloor \quad (1.59)$$

$$\left\lceil \frac{\lceil x/m \rceil}{n} \right\rceil = \left\lceil \frac{x}{mn} \right\rceil \quad (1.60)$$

Estas son reflejo de lo siguiente: Sea  $f(x)$  una función continua monótona creciente con la propiedad especial que si  $f(x)$  es entero entonces  $x$  es entero. Entonces:

$$\begin{aligned} \lfloor f(\lfloor x \rfloor) \rfloor &= \lfloor f(x) \rfloor \\ \lceil f(\lceil x \rceil) \rceil &= \lceil f(x) \rceil \end{aligned}$$

Veremos el primer caso, el otro es análogo. Cuando  $x = \lfloor x \rfloor$  no hay nada que demostrar. Supongamos entonces que  $\lfloor x \rfloor < x$ , con lo que  $f(\lfloor x \rfloor) < f(x)$  ya que  $f$  es monótona, y  $\lfloor f(\lfloor x \rfloor) \rfloor \leq \lfloor f(x) \rfloor$ . Si fuera  $\lfloor f(\lfloor x \rfloor) \rfloor < \lfloor f(x) \rfloor$ , habría un número  $y$  tal que  $\lfloor x \rfloor < y \leq x$  con  $f(y) = \lfloor f(x) \rfloor$  dado que  $f$  es continua. Pero entonces  $f(y)$  es entero, luego por la propiedad especial  $y$  es entero también. Como no hay enteros  $y$  que cumplen  $\lfloor x \rfloor < y \leq x$ , debe ser  $\lfloor f(\lfloor x \rfloor) \rfloor = \lfloor f(x) \rfloor$ .

Como ejemplo, esto da:

$$\lfloor \sqrt{\lfloor x \rfloor} \rfloor = \lfloor \sqrt{x} \rfloor$$

## 1.9. Otros resultados de interés

En esta sección recogeremos la demostración de algunos resultados que usaremos más adelante.

**Teorema 1.1** (Desigualdad de Cauchy-Schwarz). *Sean vectores de números reales  $\mathbf{a} = (a_1, a_2, \dots, a_n)$  y  $\mathbf{b} = (b_1, b_2, \dots, b_n)$ . Definimos:*

$$p = \sum_{1 \leq k \leq n} a_k^2 \quad q = \sum_{1 \leq k \leq n} a_k b_k \quad r = \sum_{1 \leq k \leq n} b_k^2$$

Entonces  $q^2 \leq pr$ .

*Demostración.* Sea  $x \in \mathbb{R}$ , y consideremos la suma

$$s(x) = \sum_{1 \leq k \leq n} (a_k x + b_k)^2$$

Siendo  $s(x)$  una suma de cuadrados de números reales,  $s(x) \geq 0$ . Expandiendo los cuadrados y agrupando términos la suma se expresa:

$$s(x) = px^2 + 2qx + r$$

Este polinomio tiene a lo más un cero real ya que nunca es negativo, por lo que su discriminante no es positivo:

$$4q^2 - 4pr \leq 0$$

Esto equivale a lo anunciado.  $\square$

**Teorema 1.2** (Desigualdad triangular). *Sean  $a$  y  $b$  números complejos. Entonces  $|a + b| \leq |a| + |b|$ .*

Se le llama “desigualdad triangular” porque si se consideran  $a$  y  $b$  como los lados de un triángulo,  $a + b$  es el tercer lado (vea la figura 1.2), y el teorema dice que la suma de los largos de dos lados del

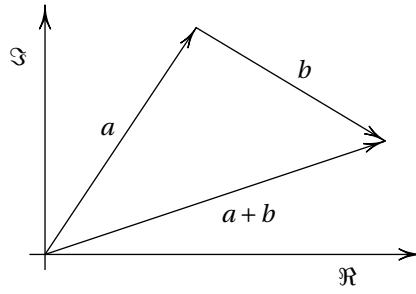


Figura 1.2 – Desigualdad triangular

triángulo es mayor que el largo del tercero (salvo cuando el triángulo es en realidad una única línea, en cuyo caso la suma de los largos de dos de los lados es igual al largo del tercero).

*Demostración.* Sean  $a = u + iv$  y  $b = x + iy$ . En estos términos, anotando  $\bar{a}$  para el conjugado de  $a$ :

$$\begin{aligned} |a|^2 &= u^2 + v^2 = a \cdot \bar{a} \\ |a + b|^2 &= (a + b) \cdot \overline{(a + b)} \\ &= (a + b) \cdot (\bar{a} + \bar{b}) \\ &= a \cdot \bar{a} + b \cdot \bar{b} + a \cdot \bar{b} + \bar{a} \cdot b \\ &= |a|^2 + |b|^2 + a \cdot \bar{b} + \bar{a} \cdot b \end{aligned}$$

Por otro lado:

$$a \cdot \bar{b} + \bar{a} \cdot b = (u + iv) \cdot (x - iy) + (u - iv) \cdot (x + iy) = 2ux + 2vy$$

Por la desigualdad de Cauchy-Schwarz es  $(ux + vy)^2 \leq (u^2 + v^2) \cdot (x^2 + y^2)$ , así que  $ux + vy \leq |a| \cdot |b|$  y resulta:

$$|a + b|^2 = |a|^2 + |b|^2 + a \cdot \bar{b} + \bar{a} \cdot b \leq |a|^2 + 2|a| \cdot |b| + |b|^2 = (|a| + |b|)^2$$

Tomando raíces cuadradas obtenemos lo prometido.  $\square$

Es obvio que esto puede extenderse a sumas finitas:

$$\left| \sum_{1 \leq k \leq n} a_k \right| \leq \sum_{1 \leq k \leq n} |a_k| \quad (1.61)$$

Una observación simple es lo que llaman el *principio del palomar* (en inglés *pigeonhole principle*): Si hay  $n$  palomares, y hay más de  $n$  palomas, hay al menos un palomar con más de una paloma. Si hay infinitas palomas, al menos uno de los palomares tiene infinitos huéspedes.

**Teorema 1.3** (Principio extendido del palomar). *Si hay  $n$  palomares, y  $r$  palomas, hay un palomar con al menos  $\lceil r/n \rceil$  palomas.*

*Demostración.* La demostración es por contradicción. Supongamos que todos los palomares tienen menos de  $\lceil r/n \rceil$  palomas. Entonces el número total de palomas cumple:

$$r \leq n \cdot \left( \left\lceil \frac{r}{n} \right\rceil - 1 \right) < n \cdot \frac{r}{n} = r$$

Concluimos  $r < r$ , lo que es absurdo.  $\square$

Para un ejemplo, considere los números  $1, 2, \dots, 2n$ , y elija  $n+1$  de ellos formando el conjunto  $\mathcal{A}$ . Entonces hay dos números relativamente primos en  $\mathcal{A}$ , porque hay dos números que difieren en 1 (considere los  $n$  “palomares” formados por pares adyacentes  $(1, 2), (3, 4), \dots, (2n-1, 2n)$ , al menos uno contiene dos números).

Considere nuevamente la situación anterior. Entonces entre los números de  $\mathcal{A}$  hay uno que divide a otro. Acá podemos escribir cada uno de los  $2n$  elementos como  $2^k m$ , con  $m$  impar en el rango  $1 \leq m \leq 2n-1$ . Como hay  $n+1$  números, pero solo  $n$  posibles partes impares, alguna debe repetirse, y en consecuencia tenemos un par que solo difiere en la potencia de 2.

## 1.10. Notación asintótica

Con frecuencia interesa comparar la tasa de crecimiento de dos funciones, o acotar un error. En tales casos una expresión exacta puede ser imposible de obtener, o sencillamente demasiado complicada. Una solución a este tipo de problemática ofrecen distintas notaciones asintóticas. El caso típico de interés es considerar las funciones conforme el argumento crece sin límite, pero son perfectamente aplicables al acercarse el argumento a un valor arbitrario. Trataremos el caso de argumento tendiendo a infinito, las modificaciones para la situación general son simples. A la familia del

Notación	Definición
$f(n) \underset{n \rightarrow \infty}{=} O(g(n))$	$\exists k > 0, n_0 \forall n > n_0 :  f(n)  \leq k \cdot g(n)$
$f(n) \underset{n \rightarrow \infty}{=} \Omega(g(n))$	$\exists k > 0, n_0 \forall n > n_0 :  f(n)  \geq k \cdot g(n)$
$f(n) \underset{n \rightarrow \infty}{=} \Theta(g(n))$	$\exists k_1 > 0, k_2 > 0, n_0 \forall n > n_0 : k_1 \cdot g(n) \leq  f(n)  \leq k_2 \cdot g(n)$
$f(n) \underset{n \rightarrow \infty}{=} o(g(n))$	$\forall \epsilon > 0 \exists n_0 \forall n > n_0 :  f(n)  \leq \epsilon \cdot g(n)$
$f(n) \underset{n \rightarrow \infty}{=} w(g(n))$	$\forall \epsilon > 0 \exists n_0 \forall n > n_0 :  f(n)  \geq \epsilon \cdot g(n)$
$f(n) \underset{n \rightarrow \infty}{\sim} g(n)$	$\lim_{n \rightarrow \infty} f(n)/g(n) = 1$

Cuadro 1.6 – Notaciones de Bachmann-Landau

cuadro 1.6 se le llama *notaciones de Bachmann-Landau*, aunque en realidad fue Knuth [210] quien

las definió como las damos acá. Por convención se escriben las cosas de la forma más simple posible, vale decir no se escribe  $O(\pi)$  sino  $O(1)$ , tampoco  $O(3n^2 + 17)$  sino simplemente  $O(n^2)$ . Aunque acá esto se ha anotado en términos de la variable  $n$ , lo que hace subentender  $n \in \mathbb{N}$ , la notación tiene perfecto sentido para  $n \in \mathbb{R}$ .

Intuitivamente:

$f(n) \underset{n \rightarrow \infty}{=} O(g(n))$ : Indica que  $f$  crece a lo más como (una constante por)  $g$  cuando  $n \rightarrow \infty$ , que  $g$  acota a  $f$  por arriba. Se aplica cuando  $\lim_{n \rightarrow \infty} f(n) = \infty$ .

$f(n) \underset{n \rightarrow \infty}{=} \Omega(g(n))$ : Significa que  $f$  crece a lo menos como (una constante por)  $g$  cuando  $n \rightarrow \infty$ , que  $g$  acota a  $f$  por abajo. Al igual que el caso anterior, se aplica más que nada cuando  $\lim_{n \rightarrow \infty} f(n) = \infty$ .

$f(n) \underset{n \rightarrow \infty}{=} \Theta(g(n))$ : En este caso  $f$  está acotada por arriba y abajo por  $g$ , ambas crecen a la misma tasa (dentro de un factor constante) cuando  $n \rightarrow \infty$ . Resume el caso en que  $f(n) \underset{n \rightarrow \infty}{=} O(g(n))$  y también  $f(n) \underset{n \rightarrow \infty}{=} \Omega(g(n))$ .

$f(n) \underset{n \rightarrow \infty}{=} o(g(n))$ : Acá  $f$  es dominada asintóticamente por  $g$ ,  $f$  disminuye más rápidamente que  $g$  cuando  $n \rightarrow \infty$ . Esto se usa más que nada para comparar funciones tales que  $\lim_{n \rightarrow \infty} f(n) = 0$ .

$f(n) \underset{n \rightarrow \infty}{=} \omega(g(n))$ : La situación acá es la inversa de la anterior,  $f$  domina asintóticamente a  $g$ ,  $g$  disminuye más rápidamente que  $f$  cuando  $n \rightarrow \infty$ . Útil principalmente cuando  $\lim_{n \rightarrow \infty} f(n) = 0$ .

$f(n) \underset{n \rightarrow \infty}{\sim} g(n)$ : Asintóticamente, ambas funciones son iguales.

Más que nada usaremos las primeras tres, las otras se mencionan por completitud.

Es común el caso de considerar el caso en que  $x \rightarrow 0$  (o alguna otra constante), no  $n \rightarrow \infty$ , y por ejemplo la definición de  $O()$  se debe leer como:

$$f(x) \underset{x \rightarrow a}{=} O(g(x)) \text{ si } \exists k \forall \epsilon > 0 \ \forall x: |x - a| \leq \epsilon \implies |f(x)| \leq k \cdot g(x)$$

Para las demás notaciones se definen en forma afín.

Nótense las similitudes con las definiciones de los límites respectivos:

$$\lim_{n \rightarrow \infty} f(n) = a \text{ cuando } \forall \epsilon > 0 \ \exists N: n \geq N \implies |f(n) - a| \leq \epsilon$$

$$\lim_{x \rightarrow x_0} f(x) = a \text{ cuando } \forall \epsilon > 0 \ \exists \delta: 0 < |x - x_0| \leq \delta \implies |f(x) - a| \leq \epsilon$$

Lejos las más usadas son  $n \rightarrow \infty$ , y se suele solo indicar explícitamente en otros casos. Si la variable es real normalmente se estará frente a la situación  $x \rightarrow 0$ .

Podemos deducir relaciones entre las distintas situaciones, suponiendo que  $f(n)$  y  $g(n)$  no se anulan. Las definiciones inmediatamente indican que  $f(n) = \Theta(g(n))$  si  $f(n) = \Omega(g(n))$  y también  $f(n) = O(g(n))$ . Es fácil ver que si  $f(n) = O(g(n))$  entonces  $g(n) = \Omega(f(n))$ , y viceversa. Similarmente,  $f(n) = o(g(n))$  si y solo si  $g(n) = \omega(f(n))$ . Vemos también que si  $f(n) = o(g(n))$  no puede ser simultáneamente  $f(n) = \Omega(g(n))$ . Si  $f(n) \sim g(n)$ , es claro que  $f(n) = \Theta(g(n))$ , pero por ejemplo  $3n = \Theta(n)$  y  $3n \not\sim n$ . La figura 1.3 resume las relaciones indicadas.

Las notaciones dadas son abusivas. Por ejemplo,  $n^{1/2} = O(n^2)$  y  $3n^2 - 17 = O(n^2)$  definitivamente no permiten concluir que  $n^{1/2} = 3n^2 - 17$ . Una notación más ajustada sería considerar  $O(g(n))$  como el *conjunto* de funciones que cumplen lo indicado, y decir  $f(n) \in O(g(n))$ . La forma más simple de evitar problemas es considerar siempre que el lado derecho de igualdades que usan estas notaciones es una versión menos precisa del lado izquierdo.

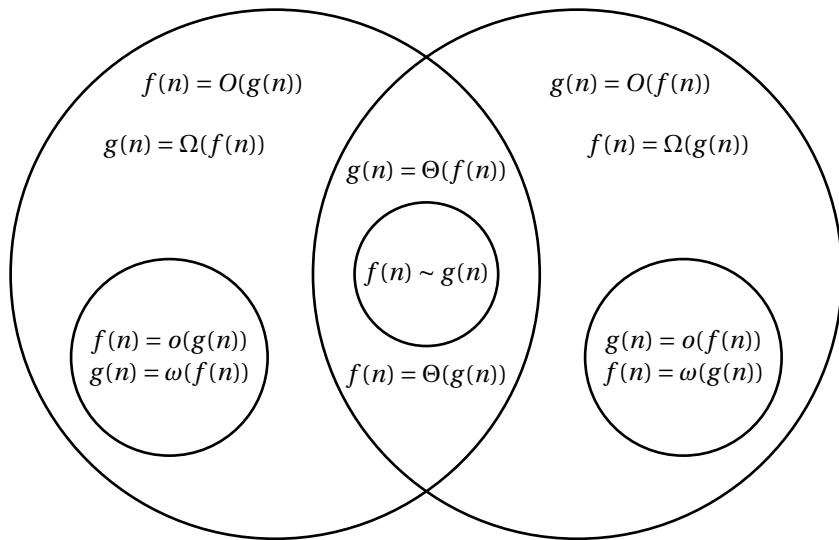


Figura 1.3 – Relación entre  $f(n)$  y  $g(n)$  en notaciones de Bachmann-Landau

También se usa notación como:

$$f(n) = 3n^3 + 2n^2 + O(n)$$

con la intención de indicar que hay una función  $g(n)$  que da:

$$f(n) = 3n^3 + 2n^2 + g(n)$$

donde  $g(n) = O(n)$ . Este uso hace preferible el no considerar las notaciones como conjuntos de funciones.

Recordemos la definición:

$$\lim_{n \rightarrow \infty} f(n) = a$$

si para todo  $\epsilon > 0$  existe  $n_0$  tal que para todo  $n \geq n_0$  se cumple  $|f(n) - a| \leq \epsilon$ . Considerar los límites suele ser útil para determinar relaciones asintóticas. Incluso hay quienes usan resultados como el teorema siguiente para definirlas.

**Teorema 1.4.** *Dadas funciones  $f(n)$  y  $g(n)$ , si  $\lim_{n \rightarrow \infty} f(n)/g(n)$  es finito, entonces  $f(n) = O(g(n))$ . Si además el límite es positivo, entonces  $f(n) = \Theta(g(n))$  (en particular, tenemos  $f(n) = \Omega(g(n))$ ). Si  $\lim_{n \rightarrow \infty} f(n)/g(n) = \infty$ , entonces  $f(n) = \Omega(g(n))$ .*

*Demostración.* Por definición

$$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = a$$

con  $a$  finito cuando para todo  $\epsilon > 0$  hay  $n_0$  tal que siempre que  $n \geq n_0$  tenemos  $|f(n)/g(n) - a| \leq \epsilon$ . Esto puede expresarse como:

$$(a - \epsilon)g(n) \leq f(n) \leq (a + \epsilon)g(n) \text{ cuando } n \geq n_0$$

La segunda desigualdad corresponde a la definición de  $f(n) = O(g(n))$ .

Si el límite  $a > 0$ , podemos elegir  $\epsilon < a$ , lo que da constantes positivas en ambas desigualdades, y corresponde a  $f(n) = \Theta(g(n))$ . La definición de  $f(n) = \Omega(g(n))$  es simplemente una de las desigualdades del caso anterior.

Por definición,

$$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = \infty$$

significa que para todo  $c > 0$  hay  $n_0$  tal que si  $n \geq n_0$ :

$$\frac{f(n)}{g(n)} \geq c \quad f(n) \geq cg(n)$$

En esto basta elegir  $c$  con su correspondiente  $n_0$  para satisfacer la definición de  $f(n) = \Omega(g(n))$ .  $\square$

Nótese que hay situaciones en las cuales esto no es aplicable. Por ejemplo, sea

$$f(n) = 3n^2 \sin^2 n + n/2$$

Sabemos que  $0 \leq \sin^2 n \leq 1$ , con lo que para todo  $n > 1$ :

$$\begin{aligned} f(n) &\geq \frac{1}{2} n \\ f(n) &\leq 3n^2 + \frac{1}{2} n \leq \frac{7}{2} n^2 \end{aligned}$$

Estas corresponden directamente a  $f(n) = \Omega(n)$  y  $f(n) = O(n^2)$ . Pero los límites a los que hace referencia el teorema 1.4 no ayudan:  $\lim_{n \rightarrow \infty} f(n)/n^2$  no existe (la razón oscila entre 0 y 3) y tampoco existe  $\lim_{n \rightarrow \infty} f(n)/n$  (la razón oscila entre 1/2 y 3n). No hay  $\alpha$  tal que  $f(n) = \Theta(n^\alpha)$ .

Sabemos del teorema de Taylor (para condiciones sobre la función y otros véase un texto de cálculo, por ejemplo el de Stein y Barcellos [338]) que si  $a \leq x$  y  $x$  está dentro del radio de convergencia podemos escribir:

$$f(x) = \sum_{0 \leq r \leq k} \frac{f^{(r)}(a)}{r!} (x - a)^r + R_k(x)$$

La forma de Lagrange del residuo es:

$$R_k(x) = \frac{f^{(k+1)}(\xi)}{(k+1)!} (x - a)^{k+1}$$

donde  $a \leq \xi \leq x$ . Si  $f^{(k+1)}(x)$  es acotado en el rango de interés, podemos decir:

$$f(x) = \sum_{0 \leq r \leq k} \frac{f^{(r)}(a)}{r!} (x - a)^r + O((x - a)^{k+1})$$

Por ejemplo:

$$\frac{n}{n-1} = \frac{1}{1-1/n}$$

Aplicando el teorema de Maclaurin:

$$\frac{1}{1-x} = 1 + x + O(x^2)$$

porque

$$\frac{d^2}{dx^2} \frac{1}{1-x} = \frac{2}{(1-x)^3}$$

En el rango de interés (digamos  $n \geq 2$ , que se traduce en  $0 < 1/n \leq 1/2$ , donde lo único que realmente interesa es que  $1/n < 1$ ) la derivada está acotada. Resulta:

$$\frac{n}{n-1} = \frac{1}{1-1/n} = 1 + \frac{1}{n} + O(n^{-2})$$

Suponiendo que  $a_r \neq 0$ , tenemos que:

$$a_r n^r + a_{r-1} n^{r-1} + \cdots + a_0 = \Theta(n^r)$$

Esto porque:

$$\lim_{n \rightarrow \infty} \frac{a_r n^r + a_{r-1} n^{r-1} + \cdots + a_0}{n^r} = a_r$$

También:

$$a_r n^r + a_{r-1} n^{r-1} + \cdots + a_0 \sim a_r n^r$$

Para demostrar esto debemos calcular:

$$\lim_{n \rightarrow \infty} \frac{a_r n^r + a_{r-1} n^{r-1} + \cdots + a_0}{a_r n^r} = \lim_{n \rightarrow \infty} \left( 1 + \frac{a_{r-1} n^{r-1} + \cdots + a_0}{a_r n^r} \right) = 1$$

Es fácil demostrar que para valores reales de  $a < b$ :

$$n^a = O(n^b) \quad n^b = \Omega(n^a)$$

Porque tenemos:

$$\lim_{n \rightarrow \infty} \frac{n^b}{n^a} = \lim_{n \rightarrow \infty} n^{b-a} = \infty$$

Por el teorema 1.4 se cumple lo indicado. Lo otro se demuestra de forma similar.

También resulta para  $a \geq 0$  y  $b > 1$ :

$$n^a = O(b^n)$$

Si  $a = 0$ , el resultado es inmediato. Si  $a > 0$ , hacemos:

$$\lim_{n \rightarrow \infty} \frac{n^a}{b^n} = \exp \left( \lim_{n \rightarrow \infty} (a \ln n - n \ln b) \right) = 0$$

El teorema 1.4 entrega lo aseverado. Nótese que esto significa, por ejemplo, que  $n^{100} = O(1,01^n)$ , aunque las constantes involucradas son gigantescas.

Hay que tener cuidado de no interpretar  $f(n) = O(g(n))$  en el sentido que  $g(n)$  es de alguna forma “mejor posible”. Por ejemplo,  $\sqrt{5n^2 + 2} = O(n^3)$ , como es fácil demostrar, y eso está lejos de ser ajustado. Como:

$$\lim_{n \rightarrow \infty} \frac{\sqrt{5n^2 + 2}}{n} = \sqrt{5}$$

sabemos del teorema 1.4 que  $\sqrt{5n^2 + 2} = \Theta(n)$ . Pero también, dado que para  $x \geq 0$  es  $1 + x \leq (1 + x)^2$ , o  $(1 + x)^{1/2} \leq 1 + x$ , lo que es lo mismo que  $(1 + x)^{1/2} = 1 + O(x)$ :

$$\sqrt{5n^2 + 2} = n\sqrt{5} \cdot \sqrt{1 + \frac{2}{5n^2}} = n\sqrt{5} \cdot (1 + O(1/n^2)) = n\sqrt{5} + O(1/n)$$

Acá usamos que  $f(n) \cdot O(g(n)) = O(f(n) \cdot g(n))$ , como se demuestra fácilmente. Este tipo de ideas pueden extenderse bastante, hasta obtener reglas para manipular y simplificar toda variedad de expresiones asintóticas. Para mayores detalles refiérase por ejemplo a Graham, Knuth y Patashnik [150] o a Sedgewick y Flajolet [320, capítulo 4]. En resumen, se aplican las reglas básicas del álgebra, con algún cuidado: Hay que recordar que las notaciones de Bachmann-Landau representan cotas, no valores exactos. Debemos siempre ponernos en el peor caso, en particular no podemos contar con cancelaciones en sumas. Así:

$$\begin{aligned} O(f(n)) \pm O(g(n)) &= O(f(n) + g(n)) \\ O(f(n)) \cdot O(g(n)) &= O(f(n) \cdot g(n)) \end{aligned}$$

Como un ejemplo obtengamos una aproximación para  $e^{1/n}\sqrt{n^2 - 2n}$ . Primeramente, por el teorema de Maclaurin:

$$\begin{aligned} e^{1/n} &= 1 + \frac{1}{n} + O(n^{-2}) \\ \sqrt{n^2 - 2n} &= n\sqrt{1 - 2/n} \\ &= n\left(1 - \frac{1}{n} - \frac{1}{2n^2} + O(n^{-3})\right) \end{aligned}$$

Multiplicando directamente tenemos:

$$e^{1/n}\sqrt{n^2 - 2n} = \left(1 + \frac{1}{n} + O(n^{-2})\right) \cdot n\left(1 - \frac{1}{n} - \frac{1}{2n^2} + O(n^{-3})\right) = n - \frac{1}{n} + O(n^{-2})$$

Suele ocurrir que la cota para el resultado es mucho peor que las cotas que entran. Si la cota  $O(n^{-2})$  que resulta no fuera suficiente, deberemos volver atrás y obtener mejores aproximaciones de partida. Normalmente deben entrar cotas de la misma precisión para no desperdiciarla en el proceso.

## 1.11. Notación asintótica en algoritmos

Comúnmente se usa notación asintótica para expresar tiempos de ejecución de algoritmos. En este tipo de aplicación el que  $O(g(n))$  “oculte” factores constantes es cómodo, así los resultados no dependen de detalles de la máquina ni de cómo se programó el algoritmo. Para obtener esta clase de estimaciones basta fijarse en alguna operación clave, tal que el costo de las demás operaciones sean proporcionales (o menos) que las operaciones claves. Por ejemplo, en el listado 1.1 aparece una rutina de ordenamiento por inserción codificada en C [202].

---

```

1 void sort(double a[], const int n)
2 {
3     int i, j;
4     double tmp;
5
6     for(i = 1; i < n; i++) {
7         tmp = a[i];

```

```

8           for (j = i - 1; j >= 0 && tmp < a[j]; j--)
9               a[j + 1] = a[j];
10              a[j + 1] = tmp;
11      }
12  }

```

---

Listado 1.1 – Ordenamiento por inserción

Acá las líneas 6, 7 y 10 se ejecutan  $n - 1$  veces, mientras las líneas 8 y 9 se ejecutan entre  $n - 1$  y  $n(n - 1)/2$  veces, respectivamente cuando el arreglo ya está ordenado y si viene exactamente en orden inverso. Si simplemente contamos “líneas de C ejecutadas” (lo que es válido bajo el supuesto que cada línea toma un tiempo máximo, independiente de los valores de las variables involucradas) para un valor dado de  $n$ , el tiempo de ejecución será alguna expresión de la forma

$$\begin{aligned} T_{\min}(n) &= 3(n - 1) + 2(n - 1) \\ &= 5n - 5 \\ T_{\max}(n) &= 3(n - 1) + 2 \frac{n(n - 1)}{2} \\ &= n^2 + 2n - 3 \end{aligned}$$

Podemos decir que para el tiempo de ejecución  $T(n)$  del programa tenemos una cota superior dado que los ciclos anidados de las líneas 6 a 11 dan que la línea 9 se ejecuta a lo más  $n^2$  veces, mientras que en el mejor caso se ejecuta solo  $n$  veces, lo que da:

$$\begin{aligned} T(n) &= O(n^2) \\ T(n) &= \Omega(n) \end{aligned}$$

Esto coincide con lo obtenido antes. Puede verse que esta clase de estimaciones son simples de obtener, y son más sencillas de usar que funciones detalladas. Además tienen la ventaja de obviar posibles diferencias en tiempos de ejecución entre instrucciones. Cabe notar que las anteriores cotas son las mejores posibles, y en este caso no se puede obtener la misma función como cota inferior y superior ( $\Theta$ ). De todas formas, es útil contar con valores asintóticos del tiempo de ejecución [320], el que un  $O(\cdot)$  o incluso  $\Theta(\cdot)$  oculte constantes hace fácil obtener la cota, pero poder decir que el tiempo de ejecución (o el número de ciertas operaciones) cumple  $T(n) \sim ag(n)$  es mucho más valioso.

Está claro que se puede hacer un análisis mucho más detallado, contabilizando cada tipo de operación que ejecuta el programa, y considerando el tiempo que demanda en una implementación particular. El ejemplo clásico es el monumental trabajo de Knuth [216–219] en análisis de algoritmos. Esto es mucho más trabajo, y en caso de cambiar de plataforma (diferente compilador, cambian opciones de compilación, otro lenguaje o nuevo computador) gran parte del análisis hay que repetirlo. Para la mayor parte de los efectos basta con nuestro análisis somero. Si tenemos que elegir entre un algoritmo con tiempo de ejecución  $O(n^2)$  y otro con tiempo de ejecución  $O(n^3)$ , para valores suficientemente grandes de  $n$  ganará el primero. Sin embargo, puede ocurrir que los valores de  $n$  de interés práctico sean más importantes los factores constantes ocultados por la notación. Mucho más detalle de cómo lograr esta clase de estimaciones se encuentra en textos sobre algoritmos o estructuras de datos, por ejemplo en [4, 82, 320, 326]. Otros algoritmos son mucho más complejos de manejar, el desarrollo de mejores algoritmos y el análisis de su desempeño son áreas de investigación activa. En [36, 37, 201] se discute cómo llevar algoritmos a buenos programas.

Los algoritmos efectúan operaciones discretas sobre estructuras de datos discretas, evaluar su rendimiento es estudiar esas estructuras y contar las operaciones efectuadas sobre ellas. Esta es una de las razones que hacen que las matemáticas discretas sean fundamentales en la informática.

## 2 Relaciones y funciones

---

Conceptos básicos de todas las matemáticas son los de *relación* y *función*. A pesar de su simplicidad, ofrecen aspectos de bastante interés. Nuevamente, la mayor parte del material presentado debe considerarse como sistematización de conocimientos previos. Una buena sistematización del área es el texto de Düntsche y Gediga [107].

### 2.1. Relaciones

**Definición 2.1.** Sean  $\mathcal{A}$  y  $\mathcal{B}$  conjuntos. Una *relación*  $R$  entre  $\mathcal{A}$  y  $\mathcal{B}$  es un subconjunto de  $\mathcal{A} \times \mathcal{B}$ .

Si  $(a, b) \in R$ , se anota  $a R b$ . Similarmente, para  $(a, b) \notin R$  se anota  $a \not R b$ .

Esto en rigor solo describe *relaciones binarias*, es perfectamente posible considerar relaciones de un solo elemento, de dos, tres o más elementos. Las relaciones binarias son lejos las más importantes, así que nos restringiremos a ellas acá.

Según esta definición son relaciones “menor a” entre números naturales, “pololea con” entre personas, “precio de” entre libros y sus precios en las librerías de la ciudad. Nótese que perfectamente pueden haber varios elementos relacionados, como por ejemplo  $1 < 2, 1 < 17, 1 < 31$ . De la misma forma, el mismo libro puede tener precios diferentes en distintas librerías, pueden haber varias ediciones, o una librería tiene copias usadas más o menos deterioradas.

Relacionado a lo anterior están los siguientes conceptos:

**Definición 2.2.** Sea  $R$  una relación entre  $\mathcal{A}$  y  $\mathcal{B}$ . A la relación:

$$R^{-1} = \{(y, x) : x R y\}$$

se le llama la *transpuesta* de  $R$ .

**Definición 2.3.** Sea  $R_1$  una relación entre  $\mathcal{A}$  y  $\mathcal{B}$ , y  $R_2$  una relación entre  $\mathcal{B}$  y  $\mathcal{C}$ . A la relación  $R$  definida mediante:

$$R = \{(x, z) : \exists y \in \mathcal{B} : x R_1 y \wedge y R_2 z\}$$

se le llama la *composición* de  $R_1$  y  $R_2$ , y se anota  $R = R_2 \circ R_1$

Si consideramos que  $x R_1 y$  como que la relación  $R_1$  lleva de  $x$  a  $y$ , y de la misma forma  $y R_2 z$  que  $R_2$  lleva de  $y$  a  $z$ , entonces  $R_2 \circ R_1$  es una relación que lleva de  $x$  a  $z$ .

El caso más común de relación es el en que ambos conjuntos son el mismo. Si  $R \subseteq \mathcal{U} \times \mathcal{U}$  se habla de una relación sobre  $\mathcal{U}$ . Algunas propiedades de relaciones entre elementos del mismo conjunto tienen nombres especiales:

**Definición 2.4.** Sea  $R$  una relación sobre  $\mathcal{U}$ . Entonces:

- Si para todo  $a \in \mathcal{U}$  se cumple  $a R a$ , la relación se llama *reflexiva*.
- Si para ningún  $a \in \mathcal{U}$  se cumple  $a R a$ , la relación se llama *irreflexiva*.
- Si para todo  $a, b, c \in \mathcal{U}$  se cumple que si  $a R b$  y  $b R c$  entonces  $a R c$  la relación se dice *transitiva*.
- Si para todo  $a, b \in \mathcal{U}$  siempre que  $a R b$  se tiene que  $b R a$ , a la relación se le llama *simétrica*.
- Si para todo  $a, b \in \mathcal{U}$ , siempre que  $a R b$  y  $b R a$  entonces  $a = b$  se dice que la relación es *antisimétrica*.
- Si para todo  $a, b \in \mathcal{U}$ , se cumple  $a R b$  o  $b R a$ , se le llama relación *total*.

Ejemplos de relaciones reflexivas son  $=$  y  $\leq$  sobre  $\mathbb{Z}$ . La relación  $\neq$  no es reflexiva ni transitiva ni antisimétrica, pero es simétrica, la relación  $<$  en  $\mathbb{R}$  es irreflexiva, es transitiva, no es simétrica y es antisimétrica (en forma vacía, ya que no hay  $a, b \in \mathbb{R}$  con  $a < b$  y  $b < a$ ). La relación “pololea con” es simétrica, y definitivamente no es antisimétrica. La relación  $\geq$  en  $\mathbb{Z}$  es antisimétrica, y no es simétrica. Tanto  $\leq$  como  $\geq$  sobre  $\mathbb{R}$  son totales (para cada par  $a, b$  se cumple una de  $a \leq b$  o  $b \leq a$ , incluso cuando  $a = b$ ). La relación “conoce a” entre personas no es total (hay gente que no se conoce entre sí).

Consideremos dados marcados como sigue:

- A: 1, 1, 3, 5, 5, 6  
 B: 2, 3, 3, 4, 4, 5  
 C: 1, 2, 2, 4, 6, 6

Al lanzar dos dados hay 36 posibles resultados, dados normales dan 15 veces ganador cada uno y 6 empates. Los dados considerados acá son no transitivos en el sentido que si se lanzan A y B, A tiene mayor probabilidad de dar el valor mayor (A gana 17 veces, hay 4 empates y pierde 15 veces). Anotaremos  $A > B$  para indicar que A tiene ventaja frente a B. Resulta que  $B > C$ , pero sorprendentemente también  $C > A$ , en los tres casos con las mismas proporciones. Vale decir, en contra de la intuición la relación “le gana a” entre estos dados no es transitiva. Finkelstein [120] desarrolla la teoría de este tipo de juegos de dados no transitivos.

Es notable que estos dados estén marcados con valores entre 1 y 6, y que las sumas de los valores de todas las caras es siempre 21, como en los dados normales.

Nótese que una relación total sobre un conjunto no vacío necesariamente es reflexiva, ya que la definición exige que para cualquier par  $a, b$  (incluyendo el caso  $a = b$ ) debe darse una de  $a R b$  o  $b R a$ .

Algunas combinaciones de las propiedades se repiten frecuentemente y llevan a propiedades interesantes de la relación, con lo que merecen nombres especiales.

**Definición 2.5.** Sea  $R$  una relación sobre  $\mathcal{U}$ . Si  $R$  es reflexiva, simétrica y transitiva se le llama *relación de equivalencia*.

El caso clásico de relación de equivalencia es la igualdad. Otros ejemplos son la congruencia y semejanza geométricas. Veremos (y usaremos) muchas más en lo que sigue.

La característica más importante de las relaciones de equivalencia está dada por el siguiente teorema.

**Teorema 2.1.** *Sea  $R \subseteq \mathcal{U}^2$  una relación de equivalencia. Entonces los conjuntos definidos por:*

$$[a]_R = \{x \in \mathcal{U} : a R x\}$$

*son disjuntos y su unión es todo  $\mathcal{U}$ .*

*Demostración.* Hay dos cosas que demostrar acá:

$$1. \bigcup_{a \in \mathcal{U}} [a]_R = \mathcal{U}$$

$$2. [a]_R \cap [b]_R = \emptyset \text{ o } [a]_R = [b]_R$$

Para el primer punto, por reflexividad  $x \in [x]_R$ , con lo que todo elemento  $x \in \mathcal{U}$  aparece al menos en la clase  $[x]_R$ , y la unión de todas las clases es  $\mathcal{U}$ .

Para el segundo punto consideremos dos elementos distintos  $a, b \in \mathcal{U}$ , y veamos las clases  $[a]_R$  y  $[b]_R$ . Si estos conjuntos son disjuntos, no hay nada que demostrar. Si no son disjuntos, habrá  $x \in \mathcal{U}$  en la intersección, o sea  $x \in [a]_R$  y  $x \in [b]_R$ . Tenemos:

$$x R a \quad \text{por suposición} \tag{2.1}$$

$$x R b \quad \text{por suposición} \tag{2.2}$$

$$a R x \quad \text{por simetría de } R \text{ y (2.2)} \tag{2.3}$$

$$a R b \quad \text{por transitividad de } R \text{ con (2.2) y (2.3)} \tag{2.4}$$

Ahora bien, si elegimos  $y \in [a]_R$ :

$$y \in [a]_R \quad \text{por suposición} \tag{2.5}$$

$$y R a \quad \text{por definición de } [a]_R \tag{2.6}$$

$$y R b \quad \text{por transitividad, de (2.6) con (2.4)} \tag{2.7}$$

$$y \in [b]_R \quad \text{por definición de } [b]_R \tag{2.8}$$

Vale decir  $[a]_R \subseteq [b]_R$ . Por simetría, también  $[b]_R \subseteq [a]_R$ , y así  $[a]_R = [b]_R$ .  $\square$

**Definición 2.6.** A los conjuntos  $[a]_R$  les llamamos *clases de equivalencia de R*, al conjunto  $[a]_R$  le llamamos la *clase de equivalencia de a (en R)*.

Omitiremos la relación en la notación de clases de equivalencia cuando se subentienda cuál es la relación considerada.

A la situación del teorema 2.1 se le dice que las clases *particionan* el conjunto  $\mathcal{U}$ . Las clases corresponden precisamente a los conjuntos de elementos que la relación considera “equivalentes”.

**Ejemplo 2.1.** Una relación  $R$  tal que si  $a R b$  y  $a R c$  entonces  $b R c$  se llama *euclíadiana*. Demuestre que toda relación euclíadiana reflexiva es una relación de equivalencia.

Para demostrar que  $R$  es relación de equivalencia, debemos demostrar que es reflexiva, simétrica y transitiva. La relación dada es reflexiva por hipótesis, falta demostrar las otras dos propiedades.

**Simetría:** Supongamos que  $a R b$ . Por reflexividad de  $R$ , sabemos que  $a R a$ ; y de  $a R b$  y  $a R a$  deducimos  $b R a$ .

**Transitividad:** Supongamos  $a R b$  y  $b R c$ . Por simetría, es  $b R a$ ; y de  $b R a$  y  $b R c$  concluimos  $a R c$ .

**Ejemplo 2.2.** Consideremos las siguientes relaciones. Nótese que para demostrar que una de las propiedades *no vale*, basta encontrar un único caso en que falla; para demostrar que *sí vale* hay que cubrir todos los casos.

**$a R_1 b$  si  $ab = 100$ , sobre  $\mathbb{N}$ :** Analizamos las distintas propiedades en turno:

- No es reflexiva, ya que por ejemplo  $5 \cdot 5 \neq 100$ .
- Es simétrica (si  $ab = 100$ , entonces  $ba = 100$ ).

- No es transitiva, ya que  $ab = 100$  y  $bc = 100$  no significa  $ac = 100$ . Por ejemplo, tenemos  $5 \cdot 20 = 100$  y  $20 \cdot 5 = 100$ , pero  $5 \cdot 5 \neq 100$ .
- No es antisimétrica, ya que por ejemplo  $5 R_1 20$  y  $20 R_1 5$ , pero  $5 \neq 20$ .
- No es total, ya que por ejemplo el natural 3 no tiene ningún natural relacionado.

**$a R_2 b$  si  $a + b$  es par, sobre  $\mathbb{N}$ :** Esta es una relación de equivalencia. Las clases son los números pares y los impares. No es total.

**$x R_3 y$  siempre que  $x - y$  es racional, sobre  $\mathbb{R}$ :** Es relación de equivalencia. En detalle:

**Reflexiva:**  $x R_3 x$  corresponde a  $x - x$  racional, y 0 es racional.

**Transitiva:** Si  $x R_3 y$  y también  $y R_3 z$ , quiere decir que  $x - y$  e  $y - z$  son racionales, con lo que  $x - z = (x - y) + (y - z)$  también es racional.

**Simétrica:** Si  $x R_3 y$ , entonces  $x - y$  es racional, y lo es  $-(x - y) = y - x$ , o sea,  $y R_3 x$ .

Sabemos que hay clases de equivalencia de  $R_3$ , aunque no son fáciles de describir.

**$(x_1, y_1) R_4 (x_2, y_2)$  cuando  $x_1^2 + y_1^2 = x_2^2 + y_2^2$ , sobre  $\mathbb{R}^2$ :** Equivalencia en  $\mathbb{R}^2$ . Las clases de equivalencia son circunferencias de radio  $r$  alrededor del origen, definidas por  $x^2 + y^2 = r^2$ .

Considere una relación  $R$  y su transpuesta  $R^{-1}$  sobre algún universo  $\mathcal{U}$ . Veamos qué podemos decir acerca de  $R^{-1}$  si sabemos que:

**$R$  es simétrica:** Que  $R$  sea simétrica significa que siempre que  $a R b$  también  $b R a$ . Expresando esto en términos de  $R^{-1}$ , es que  $b R^{-1} a$  siempre que  $a R^{-1} b$ , y la transpuesta también lo es.

**$R$  es antisimétrica:** Similar al caso anterior, se ve que en tal caso  $R^{-1}$  también es antisimétrica.

**$R$  es transitiva:** Si  $R$  es transitiva,  $R^{-1}$  también lo es (“caminando en la dirección contraria”).

**$R$  es reflexiva:** Si  $a R a$ , entonces  $a R^{-1} a$ , y  $R^{-1}$  también es reflexiva.

**$R$  es total:** Si  $a R b$  o  $b R a$  entonces también  $a R^{-1} b$  o  $b R^{-1} a$ , y  $R^{-1}$  también es total.

Se recomienda al lector analizar en detalle estas observaciones, algunas no son tan simples como parecen.

**Definición 2.7.** Sea  $R$  una relación sobre un conjunto  $\mathcal{U}$ . Si  $R$  es reflexiva, transitiva y antisimétrica se le llama *relación de orden*. A una relación de orden que es total se le llama *relación de orden total*, en caso contrario es *parcial*.

Ejemplos clásicos de relaciones de orden son  $\leq$  y  $\geq$ . En  $\mathbb{Z}$  ambas son totales. Otra relación de orden es  $\subseteq$  entre conjuntos. No es total, ya que dos conjuntos no necesariamente se relacionan uno como subconjunto del otro.

Otro ejemplo es la relación “divide a”, definida sobre  $\mathbb{N}$  mediante:

$$a | b \text{ si y solo si existe } c \in \mathbb{N} \text{ tal que } b = a \cdot c$$

Como es tradicional, anotamos  $a \nmid b$  si  $a$  no divide a  $b$ . Veamos en detalle esta relación:

**Reflexividad:**  $a | a$  ya que  $a = a \cdot 1$  y  $1 \in \mathbb{N}$ .

**Transitividad:**  $a | b$  y  $b | c$  significa que existen  $m, n \in \mathbb{N}$  tales que:

$$b = a \cdot m \quad c = b \cdot n$$

con lo que:

$$c = b \cdot n = (a \cdot m) \cdot n = a \cdot (m \cdot n)$$

que es decir  $a | c$ .

**Antisimetría:** Supongamos  $a | b$  y  $b | a$ . Entonces existen  $m, n \in \mathbb{N}$  tales que:

$$b = a \cdot m \quad a = b \cdot n$$

Esto lleva a:

$$a = (a \cdot m) \cdot n$$

$$a \cdot 1 = a \cdot (m \cdot n)$$

$$1 = m \cdot n$$

Si ahora demostramos  $m = 1$ , tenemos  $b = a \cdot m = a \cdot 1 = a$ . Esto lo haremos por contradicción. Sabemos que  $1 \leq m$ ; supongamos entonces que  $1 < m$ , vale decir que para algún  $c \in \mathbb{N}$ :

$$1 + c = m$$

$$1 \cdot n + c \cdot n = m \cdot n$$

$$n + c \cdot n = 1$$

Esto significa que  $n < 1$ , y tal  $n$  no existe.

Este no es un orden total, ya que por ejemplo no se da ni  $6 | 15$  ni  $15 | 6$ .

Otros ejemplos dan las notaciones asintóticas de Bachmann-Landau definidas en la sección 1.10. Consideremos la relación entre funciones  $f$  y  $g$  dada cuando  $f(n) = \Theta(g(n))$ . Si  $f(n) = \Theta(g(n))$ , hay  $n_0$  y constantes positivas  $c_1$  y  $c_2$  tales que para todo  $n \geq n_0$  se cumple  $c_1 g(n) \leq f(n) \leq c_2 g(n)$ . Esta relación es reflexiva (podemos tomar  $n_0 = 1$ ,  $c_1 = 1/2$  y  $c_2 = 2$ ), con lo que  $f(n) = \Theta(f(n))$ . Es simétrica, ya que para  $n \geq n_0$  tenemos:

$$\frac{1}{c_2} f(n) \leq g(n) \leq \frac{1}{c_1} f(n)$$

vale decir,  $g(n) = \Theta(f(n))$ . También es transitiva, ya que si  $f(n) = \Theta(g(n))$  y además  $g(n) = \Theta(h(n))$ , existen constantes  $n'_0$  y  $c'_1$  y  $c'_2$  con  $c'_1 h(n) \leq g(n) \leq c'_2 h(n)$  cuando  $n \geq n'_0$ . Al tomar  $n \geq \max(n_0, n'_0)$ , combinando resulta  $c_1 c'_1 h(n) \leq f(n) \leq c_2 c'_2 h(n)$ . Esto corresponde a la definición de  $f(n) = \Theta(g(n))$ .

Si consideramos  $f(n) = \Theta(g(n))$  como una especie de “igualdad” entre funciones, un desarrollo similar hará considerar  $f(n) = O(g(n))$  como un “menor o igual que”, y similarmente  $f(n) = \Omega(g(n))$  como “mayor o igual a”. Nótese eso sí que estas relaciones *no* son totales. Tómense por ejemplo las funciones:

$$f(n) = \begin{cases} 1 & \text{si } n \text{ es par} \\ n & \text{caso contrario} \end{cases}$$

$$g(n) = \begin{cases} n & \text{si } n \text{ es par} \\ 1 & \text{caso contrario} \end{cases}$$

No se cumple  $f(n) = \Omega(g(n))$  ni  $f(n) = O(g(n))$ , y tampoco  $g(n) = \Omega(f(n))$  ni  $g(n) = O(f(n))$ . Estas funciones resultan ser no comparables.

## 2.2. Funciones

Históricamente, en los inicios del análisis se hablaba de “curvas” (ver por ejemplo incluso el título del texto de l’Hôpital [180]), el que Euler hablaría de “funciones” (que inicialmente definiera esencialmente como expresiones algebraicas, para más adelante acercarse al concepto actual) fue un importante avance. El concepto se refinó, llegando a hacerse central en matemática en su forma actual, en que la función  $f$  asigna exactamente un valor  $f(x)$  a cada  $x$ .

Una *función* es simplemente un tipo especial de relación. Para ser más precisos:

**Definición 2.8.** Sean  $\mathcal{D}$  y  $\mathcal{R}$  conjuntos. Decimos que una relación  $f$  es una *función de  $\mathcal{D}$  a  $\mathcal{R}$*  si a cada  $x \in \mathcal{D}$  le relaciona exactamente un elemento  $z$  de  $\mathcal{R}$ . Se anota  $f: \mathcal{D} \rightarrow \mathcal{R}$ , llamamos *dominio* a  $\mathcal{D}$  y *codominio* o *recorrido* a  $\mathcal{R}$ . Si  $(x, z) \in f$  llamamos a  $z$  el *valor de  $f$  en  $x$* , o *imagen* de  $x$ , y anotamos  $f(x)$ . Al conjunto de todos los valores de la función se le llama su *rango*. Se le llama *preimagen de  $z$*  a cualquier  $x$  tal que  $f(x) = z$ .

Los puntos centrales de la definición son:

1.  $f(x)$  está definido para todos los  $x \in \mathcal{D}$ .
2. A cada  $x \in \mathcal{D}$  la función le asigna exactamente un valor en  $\mathcal{R}$ .

En vez de escribir  $f(x) = x^2 + 2$  anotaremos también  $f: x \mapsto x^2 + 2$ .

El caso más común de funciones en matemática elemental tiene dominio y rango conjuntos de números, por ejemplo  $\mathbb{N}$ . Si rango y dominio son conjuntos de números, el método más simple de especificar la función es mediante una fórmula, como:

$$f(n) = n^2 + n + 41$$

No siempre es posible llegar a una fórmula cerrada. En el caso particular en que el dominio es  $\mathbb{N}$  una alternativa es usar una definición recursiva. Un ejemplo importante es:

$$f(1) = 1, \quad f(2) = 1, \quad f(n+2) = f(n+1) + f(n) \quad (n \geq 1)$$

Esta función es la secuencia de los números de Fibonacci, que comienza:

$$\langle 1, 1, 2, 3, 5, 8, 13, 21, 34, \dots \rangle$$

Nuevamente, hay clasificaciones:

**Definición 2.9.** Sea  $f: \mathcal{D} \rightarrow \mathcal{R}$  una función. Entonces:

- Si para todo  $x, y \in \mathcal{D}$  con  $x \neq y$ ,  $f(x) \neq f(y)$ , se dice *inyectiva* (o *uno a uno*).
- Si para todo  $y \in \mathcal{R}$  hay  $x \in \mathcal{D}$  tal que  $f(x) = y$  se le llama *sobreyectiva* (o simplemente *sobre*).
- Si la función es inyectiva y sobreyectiva se dice *biyectiva*, también se le llama *biyección*.

Para demostrar que una función  $f: \mathcal{X} \rightarrow \mathcal{Y}$  es inyectiva, debemos demostrar que si  $a \neq b$  entonces  $f(a) \neq f(b)$ . La manera más sencilla de hacer esto suele ser demostrar el contrapositivo: Si  $f(a) = f(b)$ , entonces  $a = b$ . Para demostrar que una función  $f: \mathcal{X} \rightarrow \mathcal{Y}$  es sobreyectiva, hay que demostrar que para cada  $y \in \mathcal{Y}$  hay al menos un  $x \in \mathcal{X}$  tal que  $f(x) = y$ . Para demostrar que una función es biyectiva hay que demostrar las dos anteriores.

Como un ejemplo, anotamos para  $a, b \in \mathbb{R}$  con  $a < b$  el intervalo abierto  $(a, b) = \{x: a < x < b\}$ , y  $\mathbb{R}^+$  para los reales positivos. Definimos la función  $f: (a, b) \rightarrow \mathbb{R}^+$  mediante:

$$f(t) = \frac{t-a}{b-t}$$

Primeramente,  $f$  es una función, ya que a cada  $t \in (a, b)$  le asigna un único valor en  $\mathbb{R}^+$ . También es inyectiva, ya que:

$$\begin{aligned} f(t) &= z \\ &= \frac{t-a}{b-t} \\ t &= \frac{a+zb}{z+1} \end{aligned}$$

Así, a un valor dado de  $z > 0$  le corresponde a un único valor de  $t$ . Además es sobreyectiva, ya que si  $z > 0$  la última expresión siempre está definida. Como hay una biyección entre  $\mathbb{R}$  y un rango, podemos concluir que hay tantos números reales en un rango cualquiera como el total de los reales. Volveremos sobre este punto en el capítulo 6.

Un truco útil para demostrar que una relación  $R$  es de equivalencia es buscar una función  $f$  tal que  $a R b$  si y solo si  $f(a) = f(b)$ , porque en tal caso:

- $f(a) = f(a)$  para todo  $a$  (reflexividad)
- $f(a) = f(b) \implies f(b) = f(a)$  (simetría)
- $f(a) = f(b) \wedge f(b) = f(c) \implies f(a) = f(c)$  (transitividad)

En tal caso las clases de equivalencia son *fibras* de  $f$ , conjuntos de la forma:

$$[a] = \{b \in \mathcal{A} : f(b) = f(a)\}$$

El número de clases de equivalencia es simplemente la cardinalidad del rango de  $f$ .

Podemos construir nuevas funciones partiendo de funciones dadas, dado que son simplemente relaciones:

**Definición 2.10.** Sean  $f: \mathcal{A} \rightarrow \mathcal{B}$  y  $g: \mathcal{B} \rightarrow \mathcal{C}$  funciones. La *composición* de  $f$  y  $g$  está definida ya que son relaciones. La *función inversa de  $f$* ,  $f^{-1}: \mathcal{B} \rightarrow \mathcal{A}$  se define como la transpuesta de la relación,  $f^{-1}(z) = x$  siempre que  $f(x) = z$ .

La función inversa solo puede existir si el rango de  $f$  es su recorrido  $\mathcal{B}$  ( $f$  es sobreyectiva), y además un elemento de  $\mathcal{B}$  tiene una única preimagen ( $f$  es inyectiva). Combinando ambas,  $f$  es biyectiva. Además es fácil ver que en tal caso  $(f^{-1})^{-1} = f$ .

Si  $f, g, h$  son funciones, es simple demostrar que  $(f \circ g) \circ h = f \circ (g \circ h)$  (acá los paréntesis indican en qué orden se componen las funciones).

**Teorema 2.2.** Sean  $f: \mathcal{A} \rightarrow \mathcal{B}$  y  $g: \mathcal{B} \rightarrow \mathcal{C}$  funciones. Entonces:

1. Si  $f$  y  $g$  son inyectivas, lo es  $g \circ f$ .
2. Si  $f$  y  $g$  son sobreyectivas, lo es  $g \circ f$ .
3. Si  $f$  y  $g$  son biyectivas, lo es  $g \circ f$ . La función inversa de la composición es  $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ .
4. Si  $g \circ f$  es inyectiva,  $f$  es inyectiva ( $g$  puede no serlo).
5. Si  $g \circ f$  es sobreyectiva,  $g$  es sobreyectiva ( $f$  puede no serlo).

*Demostración.* Demostramos cada punto por turno.

1. Supongamos  $(g \circ f)(x) = (g \circ f)(y)$ . Esto es  $g(f(x)) = g(f(y))$ , y como supusimos  $g$  inyectiva, quiere decir que  $f(x) = f(y)$ , y esto a su vez que  $x = y$  ya que  $f$  es inyectiva.

2. Si  $f$  y  $g$  son sobreyectivas, quiere decir que para cada  $c \in \mathcal{C}$  hay algún  $b \in \mathcal{B}$  tal que  $g(b) = c$ , y también que para cada  $b \in \mathcal{B}$  hay  $a \in \mathcal{A}$  tal que  $f(a) = b$ . Combinando estas, para cada  $c \in \mathcal{C}$  hay algún  $a \in \mathcal{A}$  tal que  $g(f(a)) = c$ , que es decir  $(g \circ f)(a) = c$ , y  $g \circ f$  es sobreyectiva también.
3. Esto se obtiene combinando las partes (1) y (2). La función  $g \circ f$  lleva (vía  $f$ ) de  $\mathcal{A}$  a  $\mathcal{B}$ , y luego (vía  $g$ ) de  $\mathcal{B}$  a  $\mathcal{C}$ .

Para la inversa de  $g \circ f$  usamos asociatividad y la definición de inversa:

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ f = \iota$$

Terminamos con la función identidad, y componer por la derecha se trata de forma análoga resultando la identidad también. Concluimos que  $f^{-1} \circ g^{-1}$  es la inversa prometida.

4. Sean  $x, y \in \mathcal{A}$  tales que  $f(x) = f(y)$ . Entonces  $g(f(x)) = g(f(y))$ , y como suponemos  $g \circ f$  inyectiva,  $x = y$ , con lo que  $f$  es inyectiva. Mostraremos más adelante que  $g$  no tiene porqué ser inyectiva.
5. Como  $g \circ f$  es sobreyectiva, para cada  $c \in \mathcal{C}$  hay  $a \in \mathcal{A}$  para el cual  $(g \circ f)(a) = g(f(a)) = c$ , y podemos elegir  $b = f(a)$  para demostrar que para todo  $c \in \mathcal{C}$  hay  $b \in \mathcal{B}$  tal que  $g(b) = c$ . Mostraremos más adelante que  $f$  no tiene porqué ser sobreyectiva.  $\square$

Nótese que en la demostración de la parte (4) nada podemos concluir sobre  $g$ , puede ser que en lo anterior no “usamos” valores de  $g$  que hacen fallar la inyección. Ver figura 2.1a. De forma similar, en la parte (5) nada podemos decir sobre  $f$ , ver figura 2.1b.

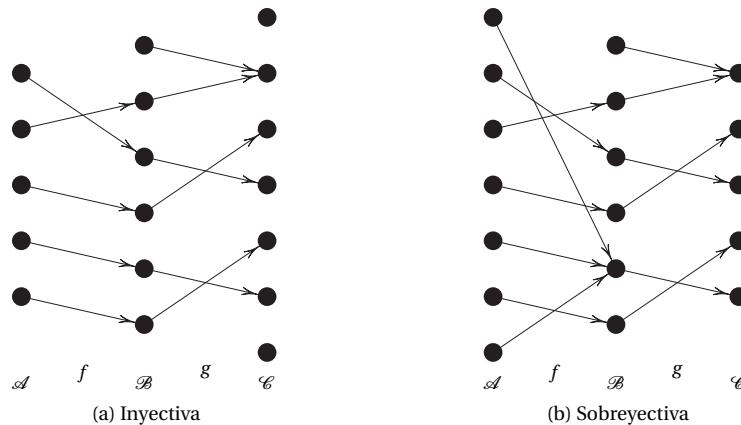


Figura 2.1 – Funciones compuestas inyectivas y sobreyectivas

En el caso especial en que dominio y codominio son iguales, podemos hacer algunas cosas adicionales:

- La *función identidad*,  $\iota: \mathcal{A} \rightarrow \mathcal{A}$ , se define mediante  $\iota(x) = x$  para todo  $x \in \mathcal{A}$ . Claramente cumple con  $\iota \circ f = f \circ \iota = f$  para toda función  $f$ . Además,  $\iota^{-1} = \iota$ .
- Es obvio de la definición que  $f \circ f^{-1} = f^{-1} \circ f = \iota$  si  $f$  es biyectiva.

En el caso de una función  $f: \mathcal{X} \rightarrow \mathcal{Z}$ , con  $\mathcal{A} \subseteq \mathcal{X}$  se usa la notación  $f(\mathcal{A}) = \{f(x): x \in \mathcal{A}\}$  para la imagen de un subconjunto del dominio. Igualmente, para  $\mathcal{B} \subseteq \mathcal{Z}$  se anota  $f^{-1}(\mathcal{B}) = \{x: f(x) \in \mathcal{B}\}$  para la preimagen de un conjunto. En el último caso la función inversa no tiene porqué existir para que la notación tenga sentido.

## 2.3. Operaciones

Un caso particular importante de funciones son las *operaciones* sobre un conjunto  $\mathcal{A}$ , que formalmente no son más que funciones  $\text{op}: \mathcal{A}^n \rightarrow \mathcal{A}$ . Nótese que esta definición trae implícito que la operación entrega un valor en  $\mathcal{A}$  para todos sus posibles argumentos, cosa que suele indicarse diciendo que la operación es *cerrada*. Se suelen distinguir operaciones *unarias* si tienen un único argumento, y *binarias* si tienen dos. Pueden considerarse operaciones de más de dos argumentos, pero son raras en la práctica. Nótese también que por ejemplo la división entre números reales no es una operación según nuestra definición ( $a/b$  no está definido si  $b = 0$ ). Tampoco lo son las relaciones, ya que por ejemplo  $a < b$  toma dos reales y entrega verdadero o falso.

Las operaciones de uso común suelen anotarse en forma especial, por ejemplo para la operación binaria de suma de  $a$  y  $b$  anotamos  $a + b$ . Esto se conoce como *notación infijo*. Para operaciones unarias es posible la notación *prefijo* (como en  $-a$  o  $\tan a$ ) o *postfijo* (es el caso del factorial, como en  $n!$ ).

En rigor, una expresión como  $a + b + c$  no tiene sentido, debiera indicarse el orden en que se efectúan las operaciones mediante paréntesis. Para ahorrar notación, se suelen adoptar convenciones: Si  $a \circ b \circ c$  ha de interpretarse como  $(a \circ b) \circ c$  se dice que la operación *asocia hacia la izquierda* (o que es *asociativa izquierda*), si en cambio  $a \circ b \circ c$  significa  $a \circ (b \circ c)$  se dice que *asocia hacia la derecha* o es *asociativa derecha*. En caso que  $a \circ b \circ c$  no se le dé sentido, se le llama *no asociativa*. Las operaciones comunes se consideran todas asociativas izquierdas; salvo las potencias, que son asociativas derechas (o sea,  $2^{3^4} = 2^{(3^4)}$ ).

Si tenemos dos operaciones  $\circ$  y  $\oplus$ , y se interpretan  $a \circ b \oplus c$  como  $(a \circ b) \oplus c$  y  $a \oplus b \circ c$  como  $a \oplus (b \circ c)$  (siempre se efectúa  $\circ$  antes de  $\oplus$ ) se dice que  $\circ$  tiene *mayor precedencia* que  $\oplus$ . En caso que ambas operaciones sean asociativas izquierdas, y  $a \circ b \oplus c$  se interpreta como  $(a \circ b) \oplus c$  y  $a \oplus b \circ c$  como  $(a \oplus b) \circ c$  (siempre se efectúan las operaciones de izquierda a derecha), se dice que tienen la *misma precedencia*.

Hay ciertas propiedades de las funciones mismas que son de interés también.

- Si  $a \circ b = b \circ a$  la operación se dice *comutativa*.
- Si  $(a \circ b) \circ c = a \circ (b \circ c)$ , la operación se llama *asociativa*. Esto no debe confundirse con las convenciones de notación mencionadas antes.
- De existir un elemento  $e$  tal que  $a \circ e = e \circ a = a$  para todos los  $a$ , a  $e$  se le llama *elemento neutro* de la operación.
- Si siempre se cumple  $(a \oplus b) \circ c = (a \circ c) \oplus (b \circ c)$ , se dice que  $\circ$  *distribuye sobre  $\oplus$  por la derecha*, en forma similar si  $a \circ (b \oplus c) = (a \circ b) \oplus (a \circ c)$  *por la izquierda*. Si  $\circ$  distribuye sobre  $\oplus$  tanto por la derecha como por la izquierda, se dice simplemente que distribuye sobre ella.



## 3 Demostraciones

---

La forma general de funcionar de las matemáticas es deducir nuevos resultados partiendo de cosas ya demostradas. Se busca tener una cadena sólida de deducciones, no se aceptan “cosas obvias” ni razonamientos por analogía. Lo que se entiende como prueba es mucho más riguroso que lo aceptado en otras áreas, lo que se busca es que no quede ningún espacio posible de duda. En este capítulo comentaremos del razonamiento matemático y discutiremos técnicas de demostración comunes, mostrando algunas aplicaciones interesantes de las mismas.

### 3.1. Razonamiento matemático

Aun insistiendo sobre demostraciones rigurosas que no dejan espacio a dudas, las matemáticas son una actividad humana, repleta de errores y paradojas, como relatan Kleiner y Movshovitz-Hadar [207]. Incluso Barbeau [28] se dedicó durante más de una década a recopilar errores, desde desarrollos completamente incorrectos que llevan a la solución correcta a razonamientos cuyo rango de validez no es simple de determinar, y los discute en detalle.

Entre otros, Wigner ha dicho que la efectividad de las matemáticas en las ciencias naturales no es para nada razonable [361]. Hamming considera que simplicidad de las matemáticas y la aplicabilidad de los mismos conceptos en áreas totalmente diferentes no tiene explicación racional [163]. Renz expone que el papel de una demostración en las matemáticas ha ido cambiando, junto con lo que se considera una demostración válida [299]. Thurston [350] da su visión como matemático profesional. Precisamente el siglo XX vio profundas controversias sobre el significado de las matemáticas y las demostraciones en particular (ver Kleiner [206] para una perspectiva histórica; de Millo [87] arguye que debe considerarse como una actividad social, en las líneas de la definición de “ciencia” de Kuhn [226]).

La idea de que los resultados deben demostrarse se atribuye a Tales de Mileto, que así es el primer matemático como entendemos hoy el término. Para construir una cadena sólida de conclusiones debemos comenzar con alguna base, que asumimos verdadera sin demostración. Esto (que fue el aporte más importante de Euclides) es lo que se conoce como el *método axiomático*, y los puntos de partida son los *axiomas*. Claro que Euclides y sus sucesores hasta la época de Gauß (1777–1855) consideraban un axioma como una verdad simple, indiscutible. La visión actual (desde alrededor de 1900, de manos particularmente de Hilbert) es que un axioma simplemente describe la relación entre los términos no definidos de la teoría entre manos, y se usan como punto de partida para deducir nuevas relaciones. Cuando los axiomas se cumplen, estamos resolviendo problemas en áreas diversas de una sola vez.

Nótese que en matemática (como en las demás ciencias) “teoría” es un cuerpo organizado de conocimiento aplicable a un rango relativamente amplio de situaciones. No se refiere, como suele usarse el término coloquialmente, a una sospecha que puede o no ser cierta. Por ejemplo, al hablar de grupos (cosa que haremos en mayor detalle en la sección 7.5) partimos con un conjunto de

elementos y una operación que cumplen ciertos axiomas. Estas propiedades simples se cumplen en una gran variedad de situaciones, y la teoría es de amplia aplicación.

Algunos términos para indicar el papel que una proposición tiene en un cuerpo mayor son los siguientes:

- Un *teorema* es una proposición importante, un resultado central.
- Un *corolario* es un resultado (teorema) que se obtiene casi inmediatamente de alguna proposición anterior.
- Un *lema* es un resultado preliminar, un paso para demostrar proposiciones más adelante.

Esto no es para nada una división precisa, hay lemas que resultaron mucho más importantes que los teoremas que se demostraron usándolos. Un poco en broma se dice que el sueño de todo matemático no es ser conocido por algún teorema, sino por un lema. No es uniforme el uso de esta nomenclatura, hay autores que llaman “proposición” a todos los resultados que demuestran, independiente de su importancia o de cuán fácil resultan de demostrar de proposiciones anteriores. Usaremos la división tradicional, y nombraremos simplemente “proposición” a un resultado independiente, sin mayor relevancia posterior.

Los teoremas y lemas suelen nombrarse por quienes los demostraron por primera vez, aunque hay bastantes excepciones a esta regla. Por ejemplo, el importante resultado conocido como *lema de Burnside* el mismo Burnside se lo atribuye a Frobenius, aunque mucho antes lo había demostrado Cauchy. Burnside demostró su utilidad en una influyente publicación [59]. Algunos lo llaman “el lema que no es de Burnside” por esta enrevesada historia. El *teorema de Borges* es llamado así en honor al cuento *La biblioteca de Babel* [50], del ilustre escritor argentino por Flajolet y Sedgewick [126].

La conocida *regla de l'Hôpital* para calcular límites en realidad se debe a Johann Bernoulli, a quien el marqués de l'Hôpital había contratado como tutor en matemáticas, con un contrato que decía en parte “*darle sus resultados, para usarlos a gusto*”. El marqués publicó anónimamente el primer texto impreso de cálculo diferencial [180], basado en gran medida en el trabajo de Bernoulli. En el prefacio de su libro l'Hôpital indica que usó libremente resultados de otros y que felizmente daría el crédito a quienes los reclamaran como suyos. Igual Bernoulli se quejó amargamente que sus aportes no eran reconocidos como debían. Y la regla quedó con el nombre del marqués. Truesdell [354] discute esta curiosa situación en detalle.

Otro caso interesante lo provee el *postulado de Bertrand*, que dice que entre los naturales  $n$  y  $2n$  siempre hay un número primo, cosa que notó Bertrand en 1845 y verificó hasta 3 000 000 [45]; pero fue demostrado por primera vez por Chebyshev [69]. Luego Ramanujan [297] dio una demostración mucho más sencilla, que a su vez fue mejorada por Erdős [114] en su primera publicación (tenía 19 años). Y este resultado se conoce como “postulado”, no como teorema. También se conoce por los nombres de *teorema de Bertrand-Chebyshev* o *teorema de Chebyshev*.

Tal vez el caso más famoso es el del *último* (o gran) *teorema de Fermat*, quien en 1637 anotó en el margen de un libro que tenía una maravillosa demostración de que  $x^n + y^n = z^n$  no tiene soluciones en números naturales  $x, y, z$  si  $n > 2$ , pero que la demostración no cabía en ese margen. Este resultado se demostró recién en 1995 [362], usando técnicas muy nuevas. Se le llamó “último teorema” porque de muchos resultados anunciados sin demostración por Fermat fue el último en ser resuelto.

Es común que resultados importantes tengan muchas demostraciones diferentes. Se ha dicho que el teorema de Pitágoras es el que más demostraciones tiene, Loomis [243] lista 367 demostraciones distintas. Hay que considerar que un teorema (u otro resultado) tiene interés como herramienta a ser aplicada, pero su demostración también sirve para iluminar relaciones entre distintos resultados. Seleccionar la demostración más simple de entender es vital a la hora de elegir cómo enseñar a nuevas generaciones, muchas de las demostraciones que veremos son radicalmente diferentes a

las demostraciones originales de los mismos resultados (a veces incluso cubren el tema en forma mucho más amplia). Contar con varias demostraciones independientes de resultados importantes además ayuda a aumentar la confianza en ellos.

Hay varios esquemas de demostración con las que uno debe familiarizarse. En el resto del texto usaremos estos esquemas con frecuencia. Algunas pistas adicionales sobre cómo estructurar una demostración da Cusick [86]. Una discusión mucho más detallada de técnicas de demostración que la que puede darse en este exiguo espacio ofrece Hammack [161], incluyendo un amplio rango de ejercicios. Zeitz [369] distingue entre *ejercicios*, en los cuales el plan de ataque está claro (aunque llevarlo adelante puede incluir desarrollos complejos) y *problemas*, en los cuales no está claro de antemano cuál es el camino más adecuado, y tal vez siquiera si hay una solución. Nos interesa entrenar en resolución de problemas más que en solución de ejercicios. Taylor [347] da las siguientes recomendaciones:

- **Conozca y entienda las definiciones** – Razonamiento preciso requiere saber sobre qué estamos razonando. Si un término no es familiar, busque su definición.
- **Desarrolle ejemplos** – Asegúrese que lo que intenta demostrar tiene alguna posibilidad de ser cierto. Son pocas las instancias en que exhibir un ejemplo es demostración suficiente (salvo que queramos demostrar que algo existe). Igualmente, un par de ejemplos ayudan a familiarizarse con el terreno. Es un buen momento para verificar que aplica correctamente las definiciones. Por lo demás, en el desarrollo de ejemplos puede tropezar con una idea o relación útil para demostrar el caso general. La inspiración nace en los lugares más extraños.
- **Busque contraejemplos** – Si sospecha que lo que intenta demostrar es falso, busque un contraejemplo. Incluso si es cierto, buscar contraejemplos y analizar porqué la búsqueda falla puede indicar métodos de ataque.
- **Intente usar las técnicas estándar de demostración** – Las técnicas que discutiremos más abajo han sido probadas y refinadas por generaciones. Hay situaciones en que ninguna de ellas es aplicable, pero son muy raras. No se encasille en una técnica, intente variantes.
- **Parta con un esqueleto** – Escriba lo que quiere demostrar, y un esbozo a llenar para la demostración. Vaya completando detalles. Puede ser útil trabajar desde ambos extremos (desde las hipótesis hacia la conclusión, y desde la conclusión hacia las hipótesis), en la esperanza que se encuentren al medio.
- **Sea persistente** – No se desanime si el primer intento no funciona, pruebe otro camino.
- **Navaja de Ockham** – Si todo lo demás es igual, la solución más simple es mejor.

## 3.2. Desenrollar definiciones

Una estrategia básica, aplicable siempre que no se conozcan relaciones directas que ayuden, es reducir términos a sus definiciones.

**Definición 3.1.** Un número se dice *algebraico* si es un cero de un polinomio con coeficientes enteros.

**Proposición 3.1.** *La suma de un número racional y uno algebraico es algebraico.*

No tenemos nada que relacione números racionales y algebraicos, así que partimos de las definiciones.

*Demostración.* Sea  $\alpha$  un número algebraico, y  $\rho$  un número racional. Por definición de número algebraico, hay un polinomio  $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$  tal que  $p(\alpha) = 0$ . Por la definición de número racional,  $\rho = a/b$ , con  $a$  y  $b$  enteros y  $b \neq 0$ . Vemos que  $b^n(x - \rho)^k = b^{n-k}(bx - a)^k$ , si  $k \leq n$  esto último es un polinomio con coeficientes enteros. Así  $q(x) = b^n \cdot p(x - \rho)$  es un polinomio de coeficientes enteros. Pero  $q(\alpha + \rho) = b^n \cdot p(\alpha) = 0$ , con lo que  $\alpha + \rho$  es un cero de un polinomio de coeficientes enteros, y  $\alpha + \rho$  es algebraico.  $\square$

Esta técnica la usaremos con mucha frecuencia en lo que sigue.

Se suele marcar el comienzo de la demostración mediante algo como la palabra “Demostración”, y el fin de la misma mediante algo como  $\square$  o Q.E.D. (abreviatura del latín “quod erat demonstrandum”, que es decir “lo que se quería demostrar”).

### 3.3. Implicancias

Interesan proposiciones de la forma “Si  $P$ , entonces  $Q$ ”. También se expresan como “ $P$  implica  $Q$ ”, diciendo “ $Q$  es necesario para  $P$ ”, mediante “ $P$  solo si  $Q$ ” o también “ $P$  es suficiente para  $Q$ ”. Esta nomenclatura se aclara si se revisa la tabla de verdad de nuestra relación “implica”. Si  $P \Rightarrow Q$  es verdadero, y  $Q$  es falso, definitivamente es falso  $P$ ; por lo que  $P$  verdadero es posible solo si  $Q$  es verdadero. Por otro lado, si  $P$  es verdadero, siempre es verdadero  $Q$ ; pero  $Q$  puede ser verdadero siendo  $P$  falso.

Proposiciones relacionadas a  $P \Rightarrow Q$  son su *recíproco*  $Q \Rightarrow P$ , su *inverso*  $\neg P \Rightarrow \neg Q$  y su *contrapositivo*  $\neg Q \Rightarrow \neg P$ . Es importante distinguirlas; la implicancia y su contrapositivo son equivalentes, y el recíproco y el inverso son equivalentes (el inverso es el contrapositivo del recíproco). Note que en inglés el recíproco se llama *converse*.

El recíproco no siempre se cumple. Por ejemplo, los primos de la forma  $a^n - 1$  deben tener  $n = 1$  o  $a = 2$  (por la factorización  $a^n - 1 = (a - 1)(a^{n-1} + \dots + 1)$ ). Además, con  $a = 2$  debe ser primo  $n$ , porque si fuera  $n = uv$  entonces:

$$2^{uv} - 1 = (2^u - 1)(2^{(v-1)u} + 2^{(v-2)u} + \dots + 1)$$

A estos primos se les llama *primos de Mersenne*, en honor a quien los estudió por primera vez. Sin embargo, el recíproco ( $2^p - 1$  es primo si  $p$  es primo) no se cumple, el primer contraejemplo es  $2^{11} - 1 = 2047 = 23 \cdot 89$ .

#### 3.3.1. Primer método – Demostración directa

Para demostrar que  $P$  implica  $Q$ :

1. Escriba “Supongamos  $P$ ”
2. Demuestre que  $Q$  es una consecuencia lógica.

Por ejemplo:

**Proposición 3.2.** Si  $0 \leq x \leq 2$ , entonces  $-x^3 + 4x + 1 > 0$

Antes de demostrar esto, haremos algún trabajo de borrador para ver porqué es cierto. La desigualdad es cierta si  $x = 0$ , el lado izquierdo es 1 y 1  $> 0$ . Al aumentar  $x$ , el término  $4x$  (que es positivo) inicialmente es de mayor magnitud que  $-x^3$  (que es negativo). Por ejemplo, para  $x = 1$  tenemos  $4x = 4$ , mientras  $-x^3 = -1$ . Considerando estos dos términos, da la impresión que  $-x^3$  recién comienza a dominar cuando  $x > 2$ . O sea,  $-x^3 + 4x + 1$  no será negativo para todo  $x$  entre 0 y 2, lo que significaría que  $-x^3 + 4x + 1$  es positivo.

Hasta acá vamos bien. Necesitamos reemplazar los “da la impresión” y “parece” en lo anterior por pasos lógicos sólidos. Una manera de enfrentar el término  $-x^3 + 4x$  es factorizando:

$$-x^3 + 4x = x(2 - x)(2 + x) \quad (3.1)$$

¡Bien! Para  $0 \leq x \leq 2$ , ninguno de los factores del lado izquierdo de (3.1) es negativo, y por tanto el producto no es negativo.

Formalmente, esto queda expresado en la siguiente demostración. Probablemente alguien que se encuentre con ella quedará convencido que el resultado es correcto, pero igual se preguntará de dónde salió este razonamiento.

*Demostración.* Por hipótesis  $0 \leq x \leq 2$ . Entonces ninguno de  $x$ ,  $2 - x$  o  $2 + x$  es negativo, y su producto no es negativo. Sumando 1 al producto de estos tres factores da un resultado positivo:

$$x(2 - x)(2 + x) + 1 = -x^3 + 4x + 1 > 0$$

□

Un par de puntos acá que son aplicables a toda demostración.

- Frecuentemente habrá que hacer trabajo en borrador mientras se construye la demostración. El trabajo en borrador puede ser todo lo desorganizado que se quiera, lleno de ideas que no resultaron, diagramas extraños, palabrotas, lo que sea.
- La versión definitiva de la demostración debe ser concisa y clara. Las matemáticas tienen sus propias reglas de estética, y una demostración elegante es altamente apreciada. Un ejemplo es la colección de demostraciones hermosas dadas por Aigner y Ziegler [6]. Dunham ha comparado algunos de los grandes teoremas de las matemáticas con las máximas obras de arte [103, 104], que debieran apreciarse como tales.
- Organizar una demostración compleja tiene mucho en común con escribir un programa: Hay que dividirla en trozos digeribles, particularmente en lemas fáciles de usar (y reusables). Si alguna parte de la demostración es repetitiva, tal vez vale la pena abstraerla, y explicarla una vez solamente.

### 3.3.2. Segundo método – Demostrar el contrapositivo

Una implicación “ $P$  implica  $Q$ ”, es lógicamente equivalente a su contrapositiva, “No  $Q$  implica no  $P$ ”, como puede verse de las tablas de verdad correspondientes. Demostrar una es tan bueno como demostrar la otra, y puede ser mucho más fácil demostrar el contrapositivo. De ser así, el esquema es:

1. Escriba “Demostraremos el contrapositivo”, luego enuncie éste.
2. Aplique alguna de las otras técnicas.

**Proposición 3.3.** *Si  $r$  es irracional, entonces  $\sqrt{r}$  también es irracional.*

Recuerde que un número es racional si es la razón entre números enteros, e irracional en caso contrario.

*Demostración.* Demostraremos el contrapositivo: Si  $\sqrt{r}$  es racional, entonces  $r$  es racional.

Supongamos que  $\sqrt{r}$  es racional. Esto significa que existen enteros  $a$  y  $b$  tales que:

$$\sqrt{r} = \frac{a}{b} \quad (3.2)$$

Entonces, elevando (3.2) al cuadrado:

$$r = \frac{a^2}{b^2} \quad (3.3)$$

Como en (3.3)  $a^2$  y  $b^2$  son enteros,  $r$  es racional.  $\square$

### 3.4. Demostrando un “Si y solo si”

Muchos teoremas aseguran que dos proposiciones son lógicamente equivalentes; vale decir, una vale si y solo si vale la otra. A esto también se le llama “necesario y suficiente”, como habíamos indicado antes; a veces lo expresaremos mediante “exactamente cuando”. También se dice que “ $P$  implica  $Q$  y a la inversa”. La frase “si y solo si” aparece tan comúnmente que se suele abbreviar *ssi* (en inglés, “*if and only if*” se abrevia *iff*). Nos abstendremos de usar estas abreviaturas, es demasiado fácil omitir una letra (o no verla al leer).

#### 3.4.1. Primer método – Cada una implica la otra

La proposición “ $P$  si y solo si  $Q$ ” equivale a la conjunción de las dos proposiciones “ $P$  implica  $Q$ ” y “ $Q$  implica  $P$ ”. Así demostramos dos implicancias:

1. Escriba “Demostraremos que  $P$  implica  $Q$ , y viceversa”.
2. Escriba “Primero demostraremos  $P$  implica  $Q$ ”. Hágalo usando alguna de las técnicas para demostrar implicancias.
3. Escriba “Ahora demostraremos que  $Q$  implica  $P$ ”. Nuevamente, aplique una de las técnicas para demostrar implicancias.

Una variante de esto se da cuando se quiere demostrar que una colección de proposiciones son equivalentes entre sí. Por ejemplo, para demostrar que  $P$ ,  $Q$  y  $R$  son equivalentes, podemos demostrar que  $P$  implica  $Q$ , que  $Q$  implica  $R$ , y finalmente que  $R$  implica  $P$ .

Una situación a primera vista sorprendente se da cuando se demuestra el contrapositivo de la conversa. O sea, demostramos  $P \implies Q$  y  $\neg P \implies \neg Q$ .

#### 3.4.2. Segundo método – Cadena de equivalencias

Otra alternativa es demostrar una cadena de equivalencias. Para demostrar que  $P$  si y solo si  $Q$ :

1. Escriba “Construimos una cadena de si y solo si”.
2. Demuestre que  $P$  es equivalente a una segunda proposición, que es equivalente a una tercera, y así sucesivamente hasta llegar a  $Q$ .

Esto muchas veces requiere más ingenio que el primer método, pero suele dar una demostración simple y clara.

La desviación estándar  $\sigma$  de un conjunto de valores reales  $x_1, x_2, \dots, x_n$  se define como:

$$\sigma = \sqrt{\frac{(x_1 - \mu)^2 + (x_2 - \mu)^2 + \dots + (x_n - \mu)^2}{n}} \quad (3.4)$$

donde la media  $\mu$  está dada por:

$$\mu = \frac{x_1 + x_2 + \dots + x_n}{n} \quad (3.5)$$

**Proposición 3.4.** *La desviación estándar de un conjunto de valores  $x_1, x_2, \dots, x_n$  es cero si y solo si todos los valores son iguales.*

*Demostración.* Construiremos una cadena de “si y solo si”, comenzando con la proposición de que la desviación estándar es cero:

$$\sqrt{\frac{(x_1 - \mu)^2 + (x_2 - \mu)^2 + \dots + (x_n - \mu)^2}{n}} = 0 \quad (3.6)$$

Como el único número cuya raíz cuadrada es cero es cero, la ecuación (3.6) vale si y solo si:

$$(x_1 - \mu)^2 + (x_2 - \mu)^2 + \dots + (x_n - \mu)^2 = 0 \quad (3.7)$$

Como el cuadrado de un número real nunca es negativo, cada término del lado izquierdo de (3.7) es no-negativo. Luego, el lado izquierdo de (3.7) es cero si y solo si cada término es cero. Pero el término  $(x_i - \mu)^2$  es cero si y solo si  $x_i = \mu$ , o sea, todos son iguales a la media.  $\square$

Requeriremos lo que viene, que es un resultado sin particular importancia por sí mismo, en la demostración de la proposición siguiente. Excusa perfecta para un lema. Usaremos demostración por inducción, que se discute en mayor detalle en la sección 3.7.

**Lema 3.1.** *El entero  $10^k - 1$  es divisible por 9 para todo  $k \geq 0$ .*

*Demostración.* Por inducción sobre  $k$ .

**Base:** Para  $k = 0$ , dice que 0 es divisible por 9, lo que es cierto.

**Inducción:** Suponemos que  $10^k - 1 = 9c$  para  $c \in \mathbb{N}_0$ . Entonces:

$$\begin{aligned} 10^{k+1} - 1 &= ((10^k - 1) + 1) \cdot 10 - 1 \\ &= (9c + 1) \cdot 10 - 1 \\ &= 90c + 9 \end{aligned}$$

Como ambos términos son divisibles por 9, lo es la suma.

Por inducción, vale para  $k \in \mathbb{N}_0$ .  $\square$

**Proposición 3.5.** *El entero  $m$  es divisible por 9 si y solo si la suma de sus dígitos es divisible por 9.*

*Demostración.* Sea  $s$  la suma de los dígitos de  $m$ , o sea si  $\langle d_k \rangle_{k \geq 0}$  son los dígitos de  $m$ , con lo que  $0 \leq d_k < 10$ , tenemos:

$$m = d_n \cdot 10^n + d_{n-1} \cdot 10^{n-1} + \dots + d_1 \cdot 10 + d_0 \quad (3.8)$$

$$s = d_n + d_{n-1} + \dots + d_1 + d_0 \quad (3.9)$$

$$m - s = d_n \cdot (10^n - 1) + d_{n-1} \cdot (10^{n-1} - 1) + \dots + d_1 \cdot (10 - 1) + d_0 \cdot (1 - 1) \quad (3.10)$$

Cada uno de los factores  $10^k - 1$  en (3.10) es divisible por 9 por el lema 3.1, con lo que  $m - s$  es siempre divisible por 9; y  $m$  es divisible por 9 si y solo si  $s$  lo es.  $\square$

### 3.5. Demostración por casos

Acá la idea es dividir una demostración complicada en casos más simples, y luego demostrar cada caso en turno. Es importante asegurarse que los casos resulten exhaustivos, vale decir, que no queden cabos sueltos.

Muchas veces los casos aparecen en el problema mismo, típicamente en forma de una disyunción. Si alguno de los conceptos involucrados está definido por casos puede ser necesario considerarlos por separado.

**Proposición 3.6.** *Para  $x \in \mathbb{R}$ , se cumple  $x \leq |x|$ .*

Simplemente seguimos la definición:

$$|x| = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x < 0 \end{cases}$$

*Demostración.* Consideramos por separado los casos  $x \geq 0$  y  $x < 0$ .

**$x \geq 0$ :** En este caso es  $|x| = x$ , y lo anunciado se cumple.

**$x < 0$ :** En este caso  $|x| = -x > 0$ , y  $x < 0 < -x = |x|$ . También se cumple.

Estas son todas las posibilidades. □

En otras ocasiones conviene introducir casos de manera de tener más con qué trabajar.

**Proposición 3.7.** *Si  $n$  es un entero, entonces  $n^2 + n$  es par.*

*Demostración.* Conviene separar la demostración en dos casos:

**$n$  es par:** En este caso,  $n^2$  y  $n$  son ambos pares, y su suma es par.

**$n$  es impar:** Acá  $n^2$  y  $n$  son ambos impares, y su suma es par.

Como estos casos cubren todas las posibilidades de  $n$ , vale para todo entero. □

Como en este ejemplo, suele ser útil considerar casos de enteros pares e impares. También es común separar en menor, igual o mayor a cero.

Dadas dos personas, estas se han encontrado o no. A un conjunto de personas en el que cada par de personas se han encontrado lo llamaremos *club*, a un conjunto de personas en el que ningún par se ha encontrado lo llamaremos *extraños*.

**Teorema 3.2.** *Toda colección de 6 personas incluye un club de 3 personas o un grupo de 3 extraños.*

Claramente si esto se cumple con 6 personas, se cumplirá con todo grupo mayor también. Al decir que hay un club de 3 personas, estamos indicando que hay un club de *al menos* tres personas (podemos tomar tres cualquiera de ellas como un club de tres).

*Demostración.* La demostración es por casos. Sea  $x$  una de las 6 personas. Hay dos posibilidades:

1. Entre las 5 personas restantes, al menos 3 se han encontrado con  $x$ .
2. Entre las 5 personas restantes, al menos 3 no se han encontrado con  $x$ .

Tenemos que asegurarnos que debe darse uno de los dos casos. Pero esto es fácil: Hemos dividido el grupo de 5 en dos, los que se han encontrado con  $x$  y los que no; uno de los dos grupos debe tener al menos 3 miembros. Ahora consideraremos cada caso por turno:

1. Consideremos el caso en que hay al menos 3 personas se han encontrado con  $x$ , y tomemos 3 de ellas. Tenemos dos casos, que nuevamente son exhaustivos:

- a) Ningún par de estas 3 personas se han encontrado. Tenemos un grupo de 3 extraños, con lo que el teorema vale en este caso.
- b) Algún par de estas 3 personas se han encontrado, con lo que este par con  $x$  forman un club, y el teorema vale en este caso.

O sea, el teorema vale si hay 3 personas que se han encontrado con  $x$ .

2. Supongamos que a lo menos 3 personas nunca se han encontrado con  $x$ , y consideremos 3 de ellas. Este caso también se divide en dos:

- a) Cada par de estas personas se han encontrado entre sí. Entonces forman un club, y el teorema vale en este caso.
- b) Algún par de estas 3 personas no se han encontrado nunca, con lo que forman un grupo de 3 extraños con  $x$ , y en este caso el teorema vale.

Así el teorema también vale en caso que hayan 3 que no se han encontrado con  $x$ .

Hemos cubierto todas las distintas alternativas, y en todas ellas hemos demostrado que el teorema se cumple.  $\square$

En general no seremos tan detallistas en nuestras demostraciones. En particular, se ve que los distintos casos son todos muy similares, y en la práctica bastaría detallar uno e indicar que los demás se manejan de forma afín. De todas maneras nuestras demostraciones serán más detalladas que las usuales entre matemáticos profesionales. Es común usar la frase “sin pérdida de generalidad” (en inglés *without loss of generality*, comúnmente abreviado *wlog*) para indicar que solo se tratará uno de varios casos muy similares.

**Proposición 3.8.** *Si dos enteros son de paridad opuesta, su suma es impar.*

*Demostración.* Sean  $m$  y  $n$  enteros de paridad opuesta. Sin pérdida de generalidad, sea  $m$  par y  $n$  impar. Vale decir  $m = 2a$  y  $n = 2b + 1$  con  $a$  y  $b$  enteros. Entonces  $m + n = 2a + 2b + 1 = 2(a + b) + 1$ , que es impar.  $\square$

Las demostraciones por casos se consideran poco elegantes, particularmente si los casos a considerar son muchos. Pero por ejemplo para el famoso problema de los cuatro colores (bastan cuatro colores para colorear un mapa de manera que no hayan áreas vecinas del mismo color) la demostración más simple a la fecha [304] involucra analizar alrededor de 630 casos. Para este famoso problema hay una demostración completamente formal escrita en Coq [81] por Gonthier [143]. Lo interesante es que un problema tan simple requiera una solución tan compleja.

## 3.6. Demostración por contradicción

A veces una demostración toma la forma a la que alude la famosa cita de Sherlock Holmes: «How often have I said to you that when you have eliminated the impossible, whatever remains, however improbable, must be the truth?» (Conan Doyle [75]). A esta importante técnica también se le llama “demostración indirecta” o “por reducción al absurdo” (en inglés se suele usar la frase del latín *reductio ad absurdum*). La idea básica es partir con lo contrario de lo que se quiere demostrar, y llegar a una contradicción. Suele ser una manera fácil de demostrar algo; pero la descripción como

“indirecta” es bastante adecuada, puede llevar a demostraciones complejas, difíciles de entender. Por esta razón Knuth, Larrabee y Roberts [220] recomiendan evitarla en lo posible.

Partimos de la negación de lo que se quiere demostrar, y deducimos algo que se sabe es falso (una contradicción). Sabemos que si  $P$  implica falso, la única manera en que esta proposición puede ser verdadera es que  $P$  sea falso. Debe tenerse cuidado de no usar los resultados intermedios de tales demostraciones fuera de ellas, como de ellos se deduce algo falso son falsos.

La forma de construir una demostración según este esquema es como sigue:

1. Escriba “La demostración es por contradicción”. Enuncie la negación de lo que se desea demostrar, indicando que se supone que esto es cierto.
2. Deduzca de lo anterior algo que se sabe es falso. Concluya “Esta contradicción demuestra el teorema”.

Ya vimos un ejemplo de esta técnica al demostrar el principio extendido del palomar, teorema 1.3. El ejemplo clásico es la demostración de que  $\sqrt{2}$  es irracional. Dice la leyenda que Pitágoras se enojó tanto con la demostración de la existencia de irracionales (que echaba por tierra su filosofía de “todo se expresa en números”, donde “números” hay que entenderlo como números naturales y sus razones) que hizo ahogar a quien descubrió esto. En realidad, este resultado produjo un escándalo mayúsculo en la matemática: Gran parte de la teoría de semejanza de figuras se basaba en que “obviamente” todas las proporciones podían expresarse como razones entre enteros. Fue el genio de Eudoxo de Cnido quien resolvió el tema mediante su teoría de proporciones, precursor de la actual definición de límite.

**Teorema 3.3 (Hipasso de Metaponto).**  $\sqrt{2}$  es irracional

La demostración original se perdió, pero todo indica que debe haber sido a lo largo de las líneas de esta.

*Demostración.* La demostración es por contradicción. Consideremos el triángulo  $ABC$  (véase la figura 3.1), tal que  $AC = a$  y  $AB = BC = b$ , con el ángulo  $ABC$  recto. Por el teorema de Pitágoras,

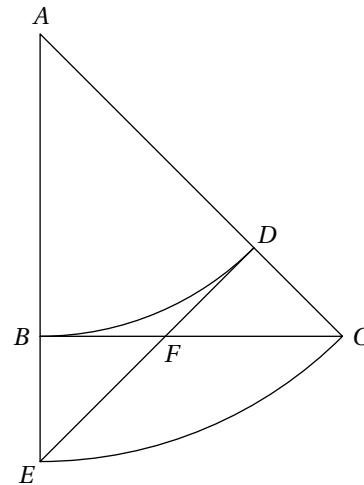


Figura 3.1 – Diagrama para demostrar que  $\sqrt{2}$  es irracional

$a^2 = 2b^2$ , o sea  $\sqrt{2} = a/b$ . Claramente  $b < a < 2b$  (la desigualdad triangular). Supongamos ahora que  $a$  y  $b$  son múltiplos enteros de una unidad, elegida tal que  $b$  es el mínimo de los enteros que dan la

relación dada. Extendemos la recta  $AB$ , y con centro en  $A$  dibujamos los arcos  $BD$  y  $CE$ , y dibujamos la recta  $ED$  que corta  $BC$  en  $F$ . Por construcción los triángulos  $ABC$  y  $ADE$  son congruentes (tienen el ángulo  $ABC$  en común, y respectivamente iguales los lados  $AD = AB$  y  $AC = AE$ ). En particular, el ángulo  $ADE$  es recto, con lo que es recto  $CDE$ . El triángulo  $CDF$  es semejante a  $ABC$  (comparten el ángulo  $ACB$ , y ambos son triángulos rectos), así que  $DC = DF$ . De la misma forma,  $EBF$  es semejante a  $ABC$ , y como  $BE = DC$ ,  $CDF$  es congruente a  $EBF$ . Ahora bien,  $BF = BE = a - b$ , y  $CF = BC - BF = b - (a - b) = 2b - a$ . Si  $a$  y  $b$  son enteros, también lo son  $a - b$  y  $2b - a$ , que son menores que  $a$  y  $b$  y están en la misma relación por similitud. Esto es absurdo, habíamos supuesto que  $b$  era el mínimo entero que sirve de denominador en esta razón.  $\square$

Las demostraciones corrientes actualmente son algebraicas, hay que recordar que en tiempos de Pitágoras no había nada parecido a nuestra álgebra. Precisamente el problema que planteaban los irracionales hizo que desde los griegos se usara casi exclusivamente la geometría como lenguaje matemático para expresar cantidades continuas, recién por la época de Newton se retomó la idea de expresiones numéricas.

*Demostración.* La demostración es por contradicción. Supongamos que  $\sqrt{2}$  fuera racional. Entonces existen números naturales  $a$  y  $b$  tales que:

$$\sqrt{2} = \frac{a}{b} \quad (3.11)$$

En (3.11) podemos suponer que la fracción está expresada en mínimos términos, vale decir,  $a$  y  $b$  no tienen factores en común. En particular, a lo más uno de los dos es par. Ahora bien, elevando (3.11) al cuadrado tenemos:

$$a^2 = 2b^2 \quad (3.12)$$

De (3.12) sabemos que  $a^2$  es par, por lo que  $a$  debe ser par, digamos  $a = 2c$ . Pero esto lleva a:

$$\begin{aligned} 4c^2 &= 2b^2 \\ 2c^2 &= b^2 \end{aligned}$$

con lo que también  $b$  es par. Esta contradicción de números de los cuales a lo más uno puede ser par pero que resultan ser ambos pares demuestra que tales  $a$  y  $b$  no pueden existir, y  $\sqrt{2}$  es irracional.  $\square$

Una demostración alternativa es la siguiente:

*Demostración.* La demostración es por contradicción. Supongamos que  $\sqrt{2}$  es racional, y sea  $q$  el menor natural tal que  $q' = (\sqrt{2} - 1)q$  es entero. Entonces  $0 < q' < q$ , pero  $(\sqrt{2} - 1)q' = q - 2q' > 0$  es entero. Esto contradice la anterior elección de  $q$ .  $\square$

Una demostración que no hace uso de divisibilidad se debe a Leo Moser [260].

*Demostración.* Suponga  $\sqrt{2} = a/b$ , con  $b$  lo más pequeño posible, con lo que  $0 < b < a$  ya que  $\sqrt{2} > 1$ . Entonces:

$$\frac{2ab}{ab} = 2 \quad (3.13)$$

$$\frac{a^2}{b^2} = 2 \quad (3.14)$$

De (3.13) y (3.14) por propiedades de las proporciones, como  $b < a < 2b$ :

$$2 = \frac{2ab - a^2}{ab - b^2} = \frac{a(2b - a)}{b(a - b)} \quad (3.15)$$

Simplificando (3.15) usando la definición de  $a$  y  $b$  resulta:

$$\sqrt{2} = \frac{2b - a}{a - b}$$

Como  $b < a < 2b$  tenemos  $0 < a - b < b$ , obtenemos una fracción con un denominador menor que el mínimo, lo que es imposible.  $\square$

Vimos en la sección 1.1.4 el polinomio de Euler, que da números primos como valores para  $0 \leq n \leq 39$ .

**Proposición 3.9.** *Ningún polinomio no constante con coeficientes enteros da sólo números primos en los enteros no negativos.*

*Demuestra*ción. La demostración es por contradicción. Sea  $p(x)$  un polinomio no constante cuyo valor es primo para todo  $n \geq 0$ . En particular,  $q = p(0)$  es primo. Si consideramos  $p(aq)$  para  $a \in \mathbb{N}$ , vemos que todos sus términos, incluyendo el término constante, son divisibles por  $q$ . Como el primo  $q$  divide al primo  $p(aq)$ , es  $p(aq) = q$ . Pero entonces  $p(x) = q$  para infinitos valores de  $x$ , y  $p$  es constante, contradiciendo la hipótesis.  $\square$

Muchas veces la forma más cómoda de demostrar una desigualdad es por contradicción.

**Proposición 3.10.** *Sean  $x, y$  reales mayores a cero. Si  $y(y+1) \leq (x+1)^2$  entonces  $y(y-1) \leq x^2$ .*

*Demuestra*ción. La demostración es por contradicción. Sean  $y(y+1) \leq (x+1)^2$  y  $y(y-1) > x^2$ . En tal caso claramente  $y > 1$ .

La primera condición se traduce en:

$$y^2 + y \leq x^2 + 2x + 1$$

Con la suposición  $x^2 < y(y-1)$ :

$$\begin{aligned} y^2 + y &< y^2 - y + (2x + 1) \\ y &< x + \frac{1}{2} \\ y - 1 &< x - \frac{1}{2} \end{aligned}$$

Como  $y > 1$ , el lado izquierdo es positivo, y podemos multiplicar las últimas dos desigualdades:

$$y(y-1) < x^2 - \frac{1}{4}$$

Esto último contradice a  $x^2 < y(y-1)$ .  $\square$

Otro buen ejemplo de demostración por contradicción es debido a Fourier de un resultado que Euler originalmente demostró en 1737.

**Teorema 3.4.** *El número  $e$  es irracional.*

*Demostración.* La demostración es por contradicción. Supongamos que  $e$  es racional. Entonces existen enteros  $a$  y  $b$  tales que:

$$e = \frac{a}{b} \quad (3.16)$$

También sabemos:

$$e = \sum_{k \geq 0} \frac{1}{k!} \quad (3.17)$$

Consideremos la siguiente expresión, que debiera ser entera bajo nuestra suposición:

$$\begin{aligned} b!e &= \sum_{k \geq 0} \frac{b!}{k!} \\ &= \sum_{0 \leq k \leq b} \frac{b!}{k!} + \sum_{k > b} \frac{b!}{k!} \end{aligned} \quad (3.18)$$

La primera suma en (3.18) es un entero, nos concentraremos en acotar la segunda, a la que llamaremos  $S$ , para demostrar que no es un entero. Más precisamente, mostraremos que  $0 < S < 1$ :

$$\begin{aligned} S &= \sum_{k > b} \frac{b!}{k!} \\ &= \sum_{k > b} \frac{1}{(b+1)(b+2)\cdots k} \\ &= \sum_{r \geq 1} \frac{1}{(b+1)(b+2)\cdots(b+r)} \end{aligned} \quad (3.19)$$

Cada término de la suma (3.19) es positivo, y es una fracción cuyo denominador son  $r$  factores, cada uno mayor o igual a  $b+1$ , con lo que:

$$\frac{1}{(b+1)(b+2)\cdots(b+r)} \leq \frac{1}{(b+1)^r} \quad (3.20)$$

En consecuencia, como los términos después del primero son menores que  $(b+1)^{-r}$ :

$$\begin{aligned} 0 < S &< \sum_{r \geq 1} (b+1)^{-r} \\ &= (b+1)^{-1} \sum_{r \geq 0} (b+1)^{-r} \\ &= \frac{1}{b+1} \cdot \frac{1}{1 - 1/(b+1)} \\ &= \frac{1}{b} \\ &\leq 1 \end{aligned} \quad (3.21)$$

Resulta por (3.21) que  $b!e$  no es entero, cuando por nuestra suposición debiera serlo. Esta contradicción completa la demostración que  $e$  es irracional.  $\square$

Una interesante demostración alternativa es la siguiente:

*Demostración.* Si  $e^{-1}$  es irracional, también lo es  $e$ . Demostraremos por contradicción que  $e^{-1}$  es irracional.

Sabemos que:

$$e^{-1} = \sum_{n \geq 0} \frac{(-1)^n}{n!} \quad (3.22)$$

Al ser (3.22) una serie de términos no nulos, que disminuyen en valor absoluto con signos alternantes, las sumas parciales son alternativamente mayores y menores que el límite. O sea, para  $m$  cualquiera es:

$$\sum_{0 \leq n \leq 2m-1} \frac{(-1)^n}{n!} < e^{-1} < \sum_{0 \leq n \leq 2m} \frac{(-1)^n}{n!} \quad (3.23)$$

Pero la diferencia entre las dos sumas de (3.23) es el último término, que es  $1/(2m)!$ , y así  $e^{-1}$  no puede ser expresado como una fracción con  $(2m)!$  de denominador, con lo que su denominador no puede ser divisor de esto. Pero al ser  $m$  arbitrariamente grande,  $e^{-1}$  no puede ser expresado como fracción, y  $e$  debe ser irracional.  $\square$

Otro bonito ejemplo es la demostración de Niven [266]:

**Teorema 3.5.** *El número  $\pi$  es irracional.*

*Demostración.* Por contradicción. Supongamos  $\pi = a/b$ , con  $a$  y  $b$  enteros positivos. Definamos los polinomios:

$$f(x) = \frac{x^n(a - bx)^n}{n!}$$

$$F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) - \dots + (-1)^n f^{(2n)}(x)$$

El entero  $n$  lo fijaremos más adelante.

El coeficiente de  $x^k$  en  $f(x)$  es  $f^{(k)}(0)/k!$  (teorema de Maclaurin). Por otro lado, como  $f(x) = x^n(a - bx)^n/n!$  el coeficiente de  $x^k$  puede escribirse  $c_k/n!$  para un entero  $c_k$ . O sea:

$$f^{(k)}(0) = \frac{k!}{n!} c_k$$

Para  $0 \leq k < n$ , el coeficiente  $c_k = 0$ ; para  $k \geq n$  es entero  $k!/n!$ . En resumen, las derivadas  $f^{(k)}(0)$  son todas enteras. Como  $f(a/b - x) = f(x)$ , lo mismo vale para  $x = \pi = a/b$ .

Por cálculo elemental:

$$\frac{d}{dx} (F'(x) \sin x - F(x) \cos x) = F''(x) \sin x + F(x) \sin x = f(x) \sin x$$

por lo que:

$$\int_0^\pi f(x) \sin x \, dx = (F'(x) \sin x - F(x) \cos x) \Big|_0^\pi = F(\pi) + F(0) \quad (3.24)$$

Ahora  $F(\pi) + F(0)$  es un *entero*, dado que las derivadas de  $f$  en 0 y  $\pi$  lo son. Pero para  $0 < x < \pi$  claramente ambos factores son positivos, y tenemos la cruda cota superior resultante de tomar el valor máximo de cada factor de  $f(x)$ :

$$0 < f(x) \sin x < \frac{\pi^n a^n}{n!}$$

con lo que la integral de (3.24) es positiva, pero arbitrariamente pequeña para  $n$  suficientemente grande. Esto es absurdo, no hay enteros positivos arbitrariamente pequeños.  $\square$

### 3.7. Inducción

Una técnica importante para demostrar un número infinito de casos es *inducción*. Algunos puntos de lo que sigue se tomaron del resumen de Tuffley [356]. Esta importante técnica de demostración se ha usado implícitamente desde épocas antiguas. Lambrou [229, 230] da una breve reseña de su historia, y plantea muchos ejemplos.

Supongamos que queremos demostrar que una proposición es válida para todo  $n \in \mathbb{N}$ . La manera de hacer esto es:

1. Escribir “Usamos inducción”.
2. Escribir: “Caso base:” Plantear la proposición para  $n = 1$ , y demostrarla.
3. Escribir “Inducción.” Asumiendo que la proposición es verdadera para  $n = k$ , demostrar que vale para  $n = k + 1$ .

La validez de esto se deduce de los axiomas de los números naturales, tema sobre el que volveremos en el capítulo 5. Hay algunas variantes que vale la pena distinguir.

#### 3.7.1. El caso más común

A una secuencia  $\langle r^n \rangle_{r \geq 0}$  se le llama *geométrica* (con razón  $r$ ), nuestro resultado es la suma de la serie geométrica.

**Teorema 3.6.**

$$\sum_{0 \leq k \leq n} r^k = 1 + r + r^2 + \cdots + r^n = \frac{1 - r^{n+1}}{1 - r}$$

*Demostración.* Usamos inducción.

**Caso base:** Cuando  $n = 1$ , tenemos:

$$\sum_{0 \leq k \leq n} r^k = 1 + r = \frac{(1 - r)(1 + r)}{1 - r} = \frac{1 - r^2}{1 - r}$$

Esto demuestra el caso base.

**Inducción:** Suponemos que para  $n = m$  vale:

$$\sum_{0 \leq k \leq m} r^k = \frac{1 - r^{m+1}}{1 - r}$$

Entonces:

$$\begin{aligned} \sum_{0 \leq k \leq m+1} r^k &= \sum_{0 \leq k \leq m} r^k + r^{m+1} \\ &= \frac{1 - r^{m+1}}{1 - r} + r^{m+1} \\ &= \frac{1 - r^{m+1} + r^{m+1} - r^{m+2}}{1 - r} \\ &= \frac{1 - r^{m+2}}{1 - r} \end{aligned}$$

que es precisamente la proposición para  $n = m + 1$ .

Por inducción, lo aseverado es verdadero para todo  $n$  natural.

En realidad, el resultado también se cumple para  $n = 0$ , y por tanto vale para todo  $n \in \mathbb{N}_0$ .  $\square$

Hay que tener cuidado en la demostración del paso de inducción. La tentación de trabajar “a ambos lados” suele ser fuerte, pero conlleva el riesgo de terminar en una identidad que no demuestra lo que se desea obtener. La forma más simple de evitar problemas es partir del lado izquierdo y derivar el lado derecho. El desarrollo debe ser estrictamente “hacia adelante”, lo que debemos demostrar es la implicancia  $P(n) \implies P(n+1)$ .

Del teorema 3.6 sigue que si  $|r| < 1$  entonces:

$$\lim_{n \rightarrow \infty} \sum_{0 \leq k \leq n} r^k = \lim_{n \rightarrow \infty} \frac{1 - r^{n+1}}{1 - r} = \frac{1}{1 - r} \quad (3.25)$$

Esto lo usamos antes en nuestra primera demostración que  $e$  es irracional (teorema 3.4).

Otro caso importante es el siguiente:

**Teorema 3.7.** Para  $m \in \mathbb{N}_0$  tenemos:

$$\sum_{1 \leq k \leq n} k^{\overline{m}} = \frac{n^{\overline{m+1}}}{m+1}$$

*Demostración.* La demostración es por inducción sobre  $n$ .

**Base:** Cuando  $n = 1$  el lado izquierdo de lo planteado se reduce a:

$$1^{\overline{m}} = m!$$

mientras el lado derecho da:

$$\frac{1^{\overline{m+1}}}{m+1} = \frac{(m+1)!}{m+1} = m!$$

Esto coincide, incluso en el caso  $m = 0$ .

**Inducción:** Suponiendo que vale para  $n$ , demostramos que vale para  $n + 1$ . Tenemos:

$$\sum_{1 \leq k \leq n+1} k^{\overline{m}} = \sum_{1 \leq k \leq n} k^{\overline{m}} + (n+1)^{\overline{m}}$$

Por la hipótesis:

$$\begin{aligned} \sum_{1 \leq k \leq n+1} k^{\overline{m}} &= \frac{n^{\overline{m+1}}}{m+1} + (n+1)^{\overline{m}} \\ &= \frac{n \cdot (n+1)^{\overline{m}} + (m+1) \cdot (n+1)^{\overline{m}}}{m+1} \\ &= \frac{(n+m+1) \cdot (n+1)^{\overline{m}}}{m+1} \\ &= \frac{(n+1)^{\overline{m+1}}}{m+1} \end{aligned}$$

Por inducción vale para todo  $n \in \mathbb{N}$ . Pero vale también para  $n = 0$ , como es simple verificar.  $\square$

Una relación similar se cumple para potencias factoriales en bajada, cuya demostración quedará de ejercicio. Es interesante el paralelo entre el teorema 3.7 y la integral de  $x^m$ .

### 3.7.2. Otro punto de partida

Es común querer demostrar que un predicado vale no desde 1, sino desde algún otro valor  $m$ . En tal caso formalmente tenemos dos maneras de proceder:

- Definir un nuevo predicado:

$$P'(n) = \begin{cases} \text{Verdadero} & \text{si } n < m \\ P(n) & \text{caso contrario} \end{cases}$$

- Definir un nuevo predicado:

$$P''(n) = P(n - m + 1)$$

y aplicar inducción a  $P'(n)$  o  $P''(n)$ , según corresponda. En la práctica, esto se reduce a indicar que la inducción comienza con otra base. Podemos también trabajar en  $\mathbb{N}_0$ , iniciando la inducción con 0. Incluso puede comenzar la inducción en un valor negativo.

### 3.7.3. Paso diferente

Otra variante se da cuando no es claro obtener el caso  $n + 1$  directamente del caso  $n$ , pero sí podemos obtener el caso  $n + 2$  de  $n$  (y  $n + 3$  de  $n + 1$ ). Más en general, hay algún  $k$  tal que  $P(n)$  permite concluir  $P(n + k)$ . En tal caso debemos tener  $k$  puntos de partida, y razonar las distintas secuencias entrelazadas.

Un ejemplo es el siguiente:

**Proposición 3.11.** *Para ningún  $n$  natural es  $n^2 + n + 1$  divisible por 5.*

*Demostración.* La demostración es por inducción.

**Casos base:** Para los casos base:

$$0^2 + 0 + 1 = 1$$

$$1^2 + 1 + 1 = 3$$

$$2^2 + 2 + 1 = 7$$

$$3^2 + 3 + 1 = 13$$

$$4^2 + 4 + 1 = 21$$

Ninguno es divisible por 5.

**Inducción:** Demostramos que si  $n^2 + n + 1$  no es divisible por 5, tampoco lo es  $(n + 5)^2 + (n + 5) + 1$ .

Vemos que:

$$\begin{aligned} (n + 5)^2 + (n + 5) + 1 &= n^2 + 10n + 25 + n + 5 + 1 \\ &= (n^2 + n + 1) + (10n + 30) \end{aligned} \tag{3.26}$$

En (3.26) el segundo término es divisible por 5; como el primer término no lo es, la suma no es divisible por 5.  $\square$

El lector podrá entretenerte demostrando que si contamos con estampillas de 5 y 8 centavos podemos franquear cualquier cantidad mayor a 27 centavos.

### 3.7.4. Ida y vuelta

La *media aritmética* de  $a_1, a_2, \dots, a_n$  (suponemos todos positivos) es:

$$\frac{a_1 + a_2 + \dots + a_n}{n}$$

La *media geométrica* de estos mismos valores es:

$$\sqrt[n]{a_1 a_2 \cdots a_n}$$

Un caso especial de inducción se da en la demostración de Cauchy [65] de la relación entre las medias aritmética y geométrica. Resulta simple demostrar el caso  $2^{k+1}$  a partir del caso  $2^k$ , y usamos inducción en reversa (de  $n$  concluimos  $n - 1$ ) para llenar los espacios.

**Teorema 3.8** (Desigualdad entre las medias geométrica y aritmética). *Para números reales no negativos  $a_1, a_2, \dots, a_n$  se cumple:*

$$(a_1 a_2 \cdots a_n)^{1/n} \leq \frac{a_1 + a_2 + \dots + a_n}{n}$$

*Demostración.* Usamos una forma especial de inducción. Primeramente demostramos por inducción sobre  $k$  que si la desigualdad se cumple para  $2^k$  vale para  $2^{k+1}$ ; y luego completamos los casos faltantes a través de demostrar que si vale para  $n$  también vale para  $n - 1$ .

Primero para potencias de dos. Es claro que la desigualdad se cumple para  $2^0$ .

**Base:** Para el caso  $2^1 = 2$ , consideremos  $a$  y  $b$  positivos:

$$\begin{aligned} (a - b)^2 &\geq 0 \\ a^2 + b^2 &\geq 2ab \end{aligned}$$

Si substituimos  $a \mapsto \sqrt{a_1}$ ,  $b \mapsto \sqrt{a_2}$ , resulta:

$$\frac{a_1 + a_2}{2} \geq \sqrt{a_1 a_2}$$

que es el caso  $n = 2$ .

**Inducción:** Del caso  $2^k$  concluimos el caso  $2^{k+1}$ . Para ello dividimos los  $2^{k+1}$  valores en dos grupos de  $2^k$ , y combinamos. De la hipótesis de inducción:

$$\begin{aligned} \frac{a_1 + \dots + a_{2^k}}{2^k} &\geq (a_1 \cdots a_{2^k})^{1/2^k} \\ \frac{a_{2^k+1} + \dots + a_{2^{k+1}}}{2^k} &\geq (a_{2^k+1} \cdots a_{2^{k+1}})^{1/2^k} \end{aligned}$$

Aplicando el caso  $n = 2$  a las anteriores:

$$\begin{aligned} \frac{\frac{a_1 + \dots + a_{2^k}}{2^k} + \frac{a_{2^k+1} + \dots + a_{2^{k+1}}}{2^k}}{2} &\geq \left( \frac{a_1 + \dots + a_{2^k}}{2^k} \cdot \frac{a_{2^k+1} + \dots + a_{2^{k+1}}}{2^k} \right)^{1/2} \\ \frac{a_1 + \dots + a_{2^{k+1}}}{2^{k+1}} &\geq \left( (a_1 \cdots a_{2^k})^{1/2^k} \cdot (a_{2^k+1} \cdots a_{2^{k+1}})^{1/2^k} \right)^{1/2} \\ &= (a_1 \cdots a_{2^{k+1}})^{1/2^{k+1}} \end{aligned}$$

Por inducción vale para todo  $n = 2^k$  con  $k \in \mathbb{N}_0$ .

Resta demostrar que si vale para  $n$ , vale para  $n - 1$ , inducción en reversa. Supongamos que vale para  $n$ :

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq (a_1 a_2 \cdots a_n)^{1/n}$$

y consideremos:

$$\alpha = \frac{a_1 + a_2 + \cdots + a_{n-1}}{n-1}$$

Entonces:

$$\frac{a_1 + a_2 + \cdots + a_{n-1} + \alpha}{n} = \frac{(n-1)\alpha + \alpha}{n} = \alpha$$

Por el otro lado, usando la hipótesis de inducción:

$$\frac{a_1 + a_2 + \cdots + a_{n-1} + \alpha}{n} \geq (a_1 a_2 \cdots a_{n-1} \alpha)^{1/n}$$

con lo que

$$\begin{aligned} \alpha^n &\geq a_1 a_2 \cdots a_{n-1} \alpha \\ \alpha^{n-1} &\geq a_1 a_2 \cdots a_{n-1} \end{aligned}$$

esto último equivale a lo anunciado.

Uniendo ambos casos, tenemos que la desigualdad vale para todo  $n \in \mathbb{N}$ .  $\square$

La tercera media que reconocía Pitágoras es la *media harmónica*:

$$\frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}} \quad (3.27)$$

Tenemos:

**Teorema 3.9** (Desigualdad entre las medias geométrica y harmónica). *Para números reales positivos  $a_1, a_2, \dots, a_n$  se cumple:*

$$\frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}} \leq (a_1 a_2 \cdots a_n)^{1/n}$$

*Demostración.* Usemos el teorema 3.8 con los recíprocos:

$$\begin{aligned} \frac{\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}}{n} &\geq \left( \frac{1}{a_1} \cdot \frac{1}{a_2} \cdots \frac{1}{a_n} \right)^{1/n} \\ &= (a_1 a_2 \cdots a_n)^{-1/n} \end{aligned}$$

$$\frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}} \leq (a_1 a_2 \cdots a_n)^{1/n}$$

Hay igualdad si y solo si los  $a_i$  son todos iguales.  $\square$

### 3.7.5. Múltiples variables

Se da la situación en la cual hay varias variables involucradas. La mayoría de las veces puede resolverse vía fijar algunas de las variables y aplicar inducción sobre otra, pero en raras ocasiones realmente se requiere inducción sobre más de una variable. Suponiendo variables  $m$  y  $n$ , una opción es intentar inducción sobre alguna combinación como  $m + n$ . Sin embargo, hay situaciones en las que esto no funciona.

Un ejemplo de inducción sobre múltiples variables es demostrar que:

$$C(m, n) = \frac{(2m)!(2n)!}{n!m!(m+n)!} \quad (3.28)$$

siempre es un entero para  $m, n \geq 0$ . Nuestra estrategia es demostrar (por inducción) que  $C(m, 0)$  es siempre un entero, y luego derivar una relación entre  $C(m, n)$ ,  $C(m+1, n)$  y  $C(m, n+1)$  que demuestra que si los primeros dos son enteros lo es el tercero. Esto lo usamos para demostrar por inducción que  $C(m, n)$  es siempre entero.

El siguiente resultado es más general que lo que necesitamos, pero resulta más simple de demostrar.

**Teorema 3.10.** *Un producto de  $n$  enteros consecutivos siempre es divisible por  $n!$ .*

*Demostración.* Podemos escribir el producto de  $n$  enteros consecutivos como  $m^n$ , con lo que queremos demostrar que  $n! \mid m^n$  para todo  $m$  y  $n$ . Esto lo hacemos por inducción sobre  $n$ .

**Base:** El caso  $n = 0$  se reduce a  $0! \mid m^0$ , que es  $1 \mid 1$ , independiente del valor de  $m$ .

**Inducción:** Suponiendo que  $n! \mid k^n$  para todo  $k$ , demostramos que  $(n+1)! \mid m^{n+1}$  para todo  $m$ .

Sabemos de (1.29) que:

$$m^{n+1} = (n+1) \sum_{1 \leq k \leq m} k^n \quad (3.29)$$

Como (por inducción) cada término de la suma del lado derecho de (3.29) es divisible por  $n!$ , su lado izquierdo es divisible por  $(n+1)n! = (n+1)!$ .

Por inducción, vale para  $n \in \mathbb{N}_0$ . □

Vamos ahora a nuestro interés original.

**Proposición 3.12.** *El valor  $C(m, n)$  definido por (3.28) es un entero.*

Calculamos la suma dada en el paso de inducción en esperanza de factores comunes que resulten en una expresión simple.

*Demostración.* Por inducción sobre  $n$ .

**Bases:** Primeramente, si  $n = 0$ , se reduce a:

$$C(m, 0) = \frac{(2m)!}{m!m!} = \frac{(2m)^m}{m!} \quad (3.30)$$

que por (3.29) es un entero para todo  $m \in \mathbb{N}_0$ .

**Inducción:** Suponemos  $C(m, n)$  entero para todo  $m \in \mathbb{N}_0$ . Consideremos:

$$\begin{aligned}
 C(m+1, n) + C(m, n+1) &= \frac{(2m+2)!(2n)!}{(m+1)!n!(m+n+1)!} + \frac{(2m)!(2n+2)!}{m!(n+1)!(m+n+1)!} \\
 &= \frac{(2m)!(2n)!}{m!n!(m+n+1)!} \cdot \left( \frac{(2m+1)(2m+2)}{m+1} + \frac{(2n+1)(2n+2)}{n+1} \right) \\
 &= \frac{(2m)!(2n)!}{m!n!(m+n+1)!} \cdot 4 \cdot (m+n+1) \\
 &= 4C(m, n)
 \end{aligned} \tag{3.31}$$

Por inducción sabemos que son enteros  $C(m+1, n)$  y  $C(m, n+1)$ . Por lo tanto también es entero  $C(m, n+1) = 4C(m, n) - C(m+1, n)$ .

Por inducción es entero  $C(m, n)$  para  $m, n \in \mathbb{N}_0$ .  $\square$

A pesar de ser oficialmente inducción sobre  $n$ , también estamos usando el resultado para varios valores de  $m$ .

Otro ejemplo involucra los *números de Fibonacci*, definidos mediante la recurrencia:

$$F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n \tag{3.32}$$

y los relacionados *números de Lucas*:

$$L_0 = 2, L_1 = 1, L_{n+2} = L_{n+1} + L_n \tag{3.33}$$

Nuestro interés es la sorprendente identidad:

**Proposición 3.13.** *Para todos  $m, n \geq 0$  se cumple:*

$$2F_{m+n} = L_m F_n + L_n F_m \tag{3.34}$$

Quien descubrió esta relación o era brujo o muy ocioso...

*Demostración.* La demostración es por inducción simultánea sobre  $m$  y  $n$ ; si se cumple para  $m+n$  y para  $m+n+1$  deducimos que se cumple con  $m+n+2$ .

**Bases:** Para  $m+n=0$  la única posibilidad es  $m=n=0$ , para  $m+n=1$  están las combinaciones  $m=0$  con  $n=1$  y  $m=1$  con  $n=0$ . Por simetría, los últimos dos casos se reducen a uno solo:

$$2F_0 = L_0 F_0 + L_0 F_0 = 2 \cdot 0 + 1 \cdot 0 = 0$$

$$2F_1 = L_1 F_0 + L_0 F_1 = 1 \cdot 0 + 2 \cdot 1 = 2$$

Las dos se cumplen.

**Inducción:** Supongamos que vale para  $m$  y  $n$ , para  $m$  y  $n+1$ , y para  $m+1$  y  $n$ :

$$2F_{m+n} = L_m F_n + L_n F_m \tag{3.35}$$

$$2F_{m+n+1} = L_m F_{n+1} + L_{n+1} F_m \tag{3.36}$$

$$= L_{m+1} F_n + L_n F_{m+1} \tag{3.37}$$

Al sumar (3.35) con (3.36) obtenemos para el lado derecho:

$$2F_{m+n} + 2F_{m+n+1} = 2F_{m+n+2}$$

Al lado izquierdo resulta:

$$L_m(F_n + F_{n+1}) + (L_n + L_{n+1})F_m = L_mF_{n+2} + L_{n+2}F_m$$

O sea, para esta combinación de valores se cumple.

Para la otra combinación, sumar (3.35) con (3.37) resulta en:

$$(L_m + L_{m+1})F_n + L_n(F_m + F_{m+1}) = L_{m+2}F_n + L_nF_{m+2}$$

Nuevamente se cumple.

Por inducción simultánea sobre  $m$  y  $n$ , lo anunciado se cumple para todo  $m$  y  $n$ .  $\square$

### 3.7.6. Inducción fuerte

Una variante de la técnica de inducción es lo que se conoce como *inducción fuerte*, donde suponemos no solo la validez para  $n = k$  al demostrar el caso  $n = k + 1$ , sino la validez en todos los casos  $1 \leq k \leq n$ . Nótese que no se requiere usar todos los casos anteriores, es común que solo se necesiten algunos de ellos. En todo caso, es raro que se haga la distinción entre inducción fuerte y su variante tradicional en la literatura profesional.

Para justificar esto, recurrimos a definir un nuevo predicado  $\tilde{P}(n)$  que es cierto si  $P(k)$  es verdadero para  $1, 2, \dots, n$ . Una definición recursiva de  $\tilde{P}(n)$  en términos de  $P(n)$  es:

$$\tilde{P}(n) = \begin{cases} P(1) & \text{si } n = 1 \\ \tilde{P}(n-1) \wedge P(n) & \text{si } n > 1 \end{cases} \quad (3.38)$$

Aplicando la equivalencia  $A \implies B \equiv A \implies A \wedge B$ , a definición (3.38) de  $\tilde{P}(n)$  podemos escribir:

$$\begin{aligned} (\tilde{P}(n) \implies P(n+1)) &\implies (\tilde{P}(n) \implies \tilde{P}(n) \wedge P(n+1)) \\ &\implies (\tilde{P}(n) \wedge \tilde{P}(n+1)) \end{aligned} \quad (3.39)$$

y con (3.39) la inducción fuerte sobre  $P(n)$  no es más que inducción tradicional sobre  $\tilde{P}(n)$ .

Un ejemplo simple ofrece la proposición siguiente.

#### Proposición 3.14.

$$T(n) = \begin{cases} 0 & \text{si } n = 0 \\ n + T(0) + T(1) + \dots + T(n-1) & \text{si } n > 0 \end{cases}$$

Entonces:

$$T(n) = 2^n - 1$$

*Demostración.* Usamos inducción fuerte sobre  $n$ .

**Caso base:** Para  $n = 0$ , tenemos  $T(0) = 0 = 2^0 - 1$ , que sigue de la definición de  $T$ .

**Inducción:** Suponemos cierto el resultado para  $0 \leq k < n$ , y tenemos:

$$\begin{aligned} T(n) &= n + \sum_{0 \leq k < n} T(k) \\ &= n + \sum_{0 \leq k < n} (2^k - 1) \\ &= \sum_{0 \leq k < n} 2^k \\ &= \frac{2^n - 1}{2 - 1} \\ &= 2^n - 1 \end{aligned}$$

En esto hemos usado la suma de una serie geométrica (teorema 3.6).

Por inducción, vale para todo  $n \in \mathbb{N}$ . □

Acá tuvimos que usar todos los casos anteriores.

Otro ejemplo lo pone el juego de Nim, en el cual dos jugadores se enfrentan con dos pilas de fósforos. Por turno cada jugador saca un número de fósforos de una de las pilas. Gana quien toma el último fósforo.

**Proposición 3.15.** *En el juego de Nim, si a la partida ambas pilas tienen el mismo número de fósforos, el segundo jugador gana.*

La estrategia para el segundo jugador es crear y luego mantener esta situación, vale decir si el primer jugador saca  $m$  fósforos de una pila, el segundo saca el número adecuado de fósforos de la otra para que resulten iguales. Esto demuestra que el segundo jugador siempre puede ganar.

*Demostración.* Usamos inducción fuerte sobre el número  $n$  de fósforos en las pilas.

**Base:** Cuando  $n = 1$ , la única movida posible para el primer jugador es sacar un fósforo de una pila, y el segundo jugador se queda con el último.

**Inducción:** Supongamos que esto es válido para todos los números de fósforos en las pilas entre 1 y  $n$ , demostraremos que vale para pilas con  $n + 1$  fósforos. Consideremos el caso de dos pilas de  $n + 1$  fósforos, con el turno del primer jugador. Si este saca  $m$  fósforos de una de las pilas, el segundo puede sacar  $m$  de la otra, y quedamos en la situación con dos pilas de  $n + 1 - m \leq n$  fósforos cada una. Por hipótesis, el segundo jugador gana desde esta posición.

Por inducción, si al comienzo las dos pilas tienen el mismo número de fósforos, gana el segundo jugador. □

Recurrimos solo a uno de los casos anteriores en esta demostración, pero al no estar determinado cuál necesitamos debemos suponerlos todos.

Un ejemplo más tentador es el siguiente: Se tiene una barra de chocolate que se divide en  $n$  cuadraditos. Se pide determinar cuántas veces como mínimo se debe partir la barra para dividirla en sus cuadraditos individuales.

**Proposición 3.16.** *Para dividir una barra de chocolate de  $n$  cuadraditos en sus cuadraditos individuales se requieren exactamente  $n - 1$  cortes.*

*Demostración.* Usamos inducción fuerte.

**Base:** Cuando  $n = 1$ , claramente se requieren  $n - 1 = 0$  cortes.

**Inducción:** Suponiendo que la aseveración es cierta para  $1 \leq k \leq n$ , demostramos que es cierta para  $n + 1$ . En el primer paso dividimos la barra en dos partes, de  $n_1$  y  $n_2$  cuadraditos respectivamente, donde  $n_1 + n_2 = n + 1$ . Por hipótesis de inducción, requeriremos  $n_1 - 1$  y  $n_2 - 1$  cortes para las partes, respectivamente; en total se requieren  $(n_1 - 1) + (n_2 - 1) + 1 = (n_1 + n_2) - 1 = n$  cortes.

Por inducción queda demostrado que se requieren  $n - 1$  cortes para todo  $n \in \mathbb{N}$ . □

Nótese que esta demostración es aplicable a cualquier forma de la barra original, no solo a las tradicionales barras rectangulares que se dividen en cuadraditos. La única restricción es que cada corte divida una barra en dos partes.

En esta demostración usamos dos casos anteriores, y (como en el ejemplo precedente) no podemos determinar de antemano cuáles serían, por lo que fue necesario suponerlos todos.

Es común que no resulte posible demostrar el paso inductivo. Nuestro instinto nos dice que en tal caso lo que debe hacerse es hacer más débil lo que deseamos demostrar; pero eso no sirve, ya que (de resultar) terminamos demostrando menos de lo pedido. La solución es demostrar una proposición más fuerte (lo que también da más con que trabajar).

Un mecenas (llamémosle August) dona un pavimento para el patio de la Universidad de Miskatonic, que casualmente tiene tamaño  $2^n \times 2^n$ . Pone como condición que debe instalarse una estatua suya adyacente al centro del patio. Archer Harris (el arquitecto de la Universidad) tiene sus propias ideas, todo debe pavimentarse con losas de forma en L (ver la figura 3.2). La base de la estatua de

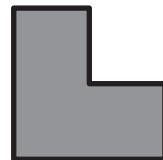


Figura 3.2 – Forma de una losa

August tiene exactamente el tamaño de uno de los tres cuadrados que forman la losa.

Lo que buscamos entonces es demostrar:

**Proposición 3.17.** *Dadas las condiciones enunciadas, es posible pavimentar un patio de tamaño  $2^n \times 2^n$  dejando un espacio adyacente al centro para la estatua de August.*

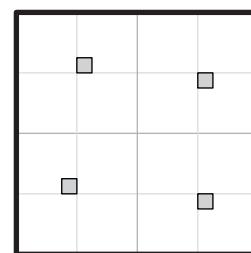


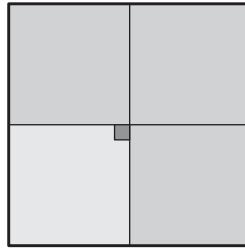
Figura 3.3 – Intento fallido de inducción

*Demostración (Intento fallido).* Usamos inducción.

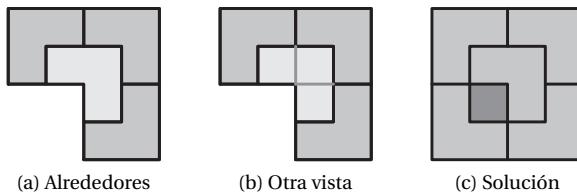
**Caso base:** Claramente se puede lograr lo pedido cuando  $n = 1$ , con una losa y la estatua ocupando la esquina faltante (queda “lo más cerca del centro posible” de esta forma).

**Inducción:** Suponiendo que se puede ubicar a August adyacente al centro para tamaño  $2^n$ , intentamos ahora demostrar que se puede hacer para  $2^{n+1}$ . Pero esto lleva a la situación de la figura 3.3, que no ayuda en nada.  $\square$

La solución es demostrar una cosa más fuerte, debemos buscar la condición que nos permita cerrar el ciclo. Es claro que  $2^{n+1} \times 2^{n+1}$  es el cuadrado en el cual la estatua de August está en la

Figura 3.4 – División del patio de  $2^{n+1} \times 2^{n+1}$  en cuatro de  $2^n \times 2^n$ 

esquina adyacente al centro rodeado por tres otros cuadrados similares llenos, como en la figura 3.4. Algunos dibujos para el caso  $4 \times 4$  muestran que la manera de cubrir excluyendo el cuadrado  $2 \times 2$  en la esquina inferior izquierda es la que da la figura 3.5a. Esto puede considerarse como tres cuadrados

Figura 3.5 – Análisis del patio de  $4 \times 4$ 

de  $2 \times 2$  con cuadraditos faltantes en esquinas que se unen al centro, como la figura 3.5b. La solución completa de  $4 \times 4$  la muestra la figura 3.5c.

Ahora tenemos dos caminos posibles:

- Notando que nuestro patio de  $4 \times 4$  lo hemos dividido como en la figura 3.4 en un área de la forma de una losa y un cuadrado del doble tamaño, podemos construir cuatro cuadrados de  $2^{n-1} \times 2^{n-1}$  con un cuadradito faltante en una esquina cada uno, unir tres de las esquinas al centro y cubrirlas con una losa, dejando la cuarta adyacente al centro como en la figura 3.5c.
- El espacio libre de la figura 3.5a en un cuadrado de  $4 \times 4$  podemos cubrirlo de forma de dejar el espacio para la estatua de August en cualquiera de las posiciones en la esquina inferior, y por simetría en cualquiera de las posiciones en el patio completo. Esto hace sospechar que se puede ubicar a August en cualquier posición en el patio.

La segunda estrategia lleva a la siguiente demostración, dejamos el detalle de la primera como entretenimiento al lector.

*Demostración.* Usamos inducción para demostrar que la estatua de August puede ubicarse en cualquier posición en un patio de  $2^n \times 2^n$ .

**Caso base:** Para  $n = 1$  es simplemente que la losa se puede ubicar en cualquier orientación.

**Inducción:** Suponiendo que es posible ubicar a August en cualquier lugar en un patio de  $2^n \times 2^n$ , podemos dividir nuestro patio de  $2^{n+1} \times 2^{n+1}$  en cuatro cuadrados de  $2^n \times 2^n$ . La posición designada de August estará en uno de los cuadrantes, y por hipótesis podemos cubrir el resto de éste. En los otros tres cuadrantes ubicamos el espacio que August ocuparía en una de las esquinas, ver la figura 3.6. También estos pavimentos son posibles, por hipótesis. Pero

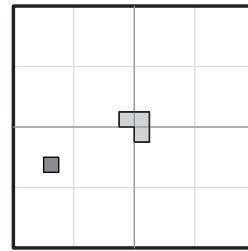


Figura 3.6 – Inducción dejando libre cualquier cuadradito

entonces podemos cubrir las tres esquinas adyacentes al centro con una losa, y es posible ubicar a August en cualquier posición en un patio de  $2^{n+1} \times 2^{n+1}$ .

Por inducción, es posible ubicar a August en cualquier posición en un patio de  $2^n \times 2^n$  para todo  $n \in \mathbb{N}$ . En particular, es posible ubicarlo adyacente al centro.  $\square$

El que resulte más fácil demostrar algo más general que lo que se busca directamente se conoce como la *paradoja del inventor*. Otro ejemplo de este fenómeno es el siguiente:

**Teorema 3.11.**

$$1 + \frac{1}{4} + \frac{1}{9} + \dots + \frac{1}{n^2} < 2$$

Esto no se puede demostrar por inducción directamente, ya que al sumar algo al lado derecho se echa a perder la condición. Para poder cerrar el ciclo con un valor menor a 2 buscamos alguna diferencia  $d_n$ , lo más simple posible, que dé:

$$2 - d_n + \frac{1}{(n+1)^2} \leq 2 - d_{n+1} \quad (3.40)$$

o, lo que es lo mismo:

$$d_n - d_{n+1} \geq \frac{1}{(n+1)^2} \quad (3.41)$$

Debe ser  $0 < d_n \leq 1$  para no meternos en problemas. Sumando (3.41) de  $n+1$  en adelante vemos que en realidad queremos que:

$$d_n > \sum_{k \geq n+1} \frac{1}{k^2} \quad (3.42)$$

Podemos estimar crudamente la suma mediante una integral:

$$\sum_{k \geq n+1} \frac{1}{k^2} \approx \int_{n+1}^{\infty} \frac{dx}{x^2} = \frac{1}{n+1} \quad (3.43)$$

La relación (3.43) hace sospechar que algo como  $d_n = 1/n$  (la expresión  $1/n$  es más simple que  $1/(n+1)$ , además que siendo mayor da mayor holgura) pueda funcionar, lo que lleva a la demostración siguiente.

*Demostración.* Por inducción demostramos un resultado más fuerte:

$$1 + \frac{1}{4} + \frac{1}{9} + \dots + \frac{1}{n^2} \leq 2 - \frac{1}{n} \quad (3.44)$$

**Caso base:** Para  $n = 1$  la ecuación (3.44) se reduce a  $1 \leq 1$ , que ciertamente es verdad.

**Inducción:** Suponiendo que (3.44) vale para  $n$ , demostramos que vale para  $n + 1$ . Partiendo de nuestra hipótesis:

$$\begin{aligned} 1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} &\leq 2 - \frac{1}{n} \\ 1 + \frac{1}{4} + \cdots + \frac{1}{n^2} + \frac{1}{(n+1)^2} &\leq 2 - \frac{1}{n} + \frac{1}{(n+1)^2} \end{aligned} \quad (3.45)$$

Consideremos los últimos dos términos de (3.45), donde como  $n \geq 1$ :

$$\begin{aligned} \frac{1}{n} - \frac{1}{(n+1)^2} &= \frac{n^2 + n + 1}{n(n+1)^2} \\ &> \frac{n^2 + n}{n(n+1)^2} \\ &= \frac{1}{n+1} \end{aligned} \quad (3.46)$$

Con (3.46) en (3.45) tenemos:

$$\begin{aligned} 1 + \frac{1}{4} + \cdots + \frac{1}{n^2} + \frac{1}{(n+1)^2} &\leq 2 - \frac{1}{n} + \frac{1}{(n+1)^2} \\ &\leq 2 - \frac{1}{n+1} \end{aligned}$$

como se prometió.

Por inducción (3.44) vale para todo  $n \in \mathbb{N}$ . Pero:

$$1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n} < 2$$

que es lo que se quería probar. □

### 3.7.7. Inducción estructural

Esta es una generalización del método de demostración por inducción. La idea es aplicable a estructuras definidas recursivamente, como árboles binarios, expresiones aritméticas o listas.

Supongamos un orden parcial bien fundado (una relación  $R$  es *bien fundada* si todo subconjunto de  $\mathcal{X}$  tiene un *mínimo* respecto de  $R$ , o sea, si todo subconjunto no vacío  $\mathcal{S}$  de  $\mathcal{X}$  contiene al menos un elemento  $m$  tal que para todo  $s \in \mathcal{S}$  es  $s R m$ ). Dicho de otra forma, toda secuencia  $x_1 > x_2 > x_3 \dots$  en  $\mathcal{X}$  termina, si anotamos  $>$  para la transpuesta de  $R$ .

Para demostrar que  $P(x)$  es cierto para todo  $x \in \mathcal{X}$ , demostramos (base) que vale para las elementos mínimos, y que (inducción) si vale para todo  $y$  tal que  $y R x$ , entonces vale para  $x$ . Esto se justifica suponiendo que algún elemento  $x \in \mathcal{X}$  es el mínimo contraejemplo. Entonces no puede ser un elemento mínimo de  $\mathcal{X}$ , ya que por la base para todos ellos se cumple  $P()$ ; y como vale para todos los  $y$  con  $y R x$  ya que  $x$  es el mínimo contraejemplo, vale para  $x$ , una clara contradicción.

Por ejemplo, consideremos listas, definidas mediante:

- $[]$  es una lista (la *lista vacía*)
- Si  $H$  es un elemento y  $T$  es una lista,  $H : T$  es una lista. Llamaremos *cabeza* a  $H$ , y *cola* a  $T$ .

Esto define un orden parcial entre listas, en que  $T \leq L$  si  $L = H : T$  o  $L = T$ .

Para listas definimos una operación *length* mediante:

**LEN1**  $\text{length}([]) = 0$

**LEN2**  $\text{length}(H : T) = 1 + \text{length}(T)$

Definimos la operación de concatenación de listas, anotada  $L_1 \cdot L_2$ , por:

**CAT1**  $[] \cdot L = L$

**CAT2**  $(H : T) \cdot L = H : (T \cdot L)$

Interesa demostrar:

**Teorema 3.12.**

$$\text{length}(L \cdot M) = \text{length}(L) + \text{length}(M) \quad (3.47)$$

*Demostración.* Esto lo demostramos por inducción estructural sobre listas.  $P(L)$  asevera que (3.47) vale para toda lista  $L$ .

**Base:** Primero demostramos que  $P([])$  es verdadero:

$$\begin{aligned} \text{length}([] \cdot M) &= \text{length}(M) && \text{por CAT1} \\ &= 0 + \text{length}(M) \\ &= \text{length}([]) + \text{length}(M) && \text{por LEN1} \end{aligned}$$

**Inducción:** Si  $L$  no es vacía, consta de cabeza y cola, o sea  $L = H : T$ . Nuestra hipótesis de inducción es que si  $P(T)$  vale para la cola  $T$  de la lista, entonces vale para la lista. En detalle, nuestra hipótesis es:

$$\text{length}(T \cdot M) = \text{length}(T) + \text{length}(M)$$

y tenemos:

$$\begin{aligned} \text{length}(L \cdot M) &= \text{length}((H : T) \cdot M) \\ &= \text{length}(H : (T \cdot M)) && \text{por CAT2} \\ &= 1 + \text{length}(T \cdot M) && \text{por LEN2} \\ &= 1 + \text{length}(T) + \text{length}(M) && \text{por hipótesis} \\ &= \text{length}(H : T) + \text{length}(M) && \text{por LEN2} \\ &= \text{length}(L) + \text{length}(M) \end{aligned}$$

Por inducción estructural, vale para todas las listas. □

Si definimos expresiones algebraicas como:

- Un *átomo* (una variable o constante)
- Una expresión entre paréntesis
- Dos expresiones unidas por un *operador*, uno de  $\{+, -, \cdot, /\}$

Esto define una relación, en la cual todas las cadenas terminan en átomos; por tanto es bien fundada.

**Teorema 3.13.** *En toda expresión con  $n$  átomos hay  $n - 1$  operadores.*

*Demostración.* Por inducción estructural.

**Base:** Si la expresión es un único átomo, tiene 1 átomo y 0 operadores.

**Inducción:** Si la expresión es una expresión entre paréntesis, tiene el mismo número de átomos y operadores que esta última.

Si la expresión consta de dos expresiones  $E_1$  y  $E_2$  unidas por un operador, por inducción si  $E_1$  tiene  $n_1$  átomos tiene  $n_1 - 1$  operadores, y si  $E_2$  tiene  $n_2$  átomos tiene  $n_2 - 1$  operadores. La expresión completa tiene  $n = n_1 + n_2$  átomos y  $n_1 - 1 + n_2 - 1 + 1 = n - 1$  operadores.

Por inducción estructural, vale para todas las expresiones.  $\square$

A esta técnica se le conoce como *inducción estructural* porque (como muestran los ejemplos) la aplicación típica es a estructuras definidas recursivamente, partiendo de estructuras mínimas y reglas para combinarlas creando estructuras más complejas. La demostración por inducción estructural en tal caso corresponde a demostrar que la propiedad vale para las estructuras mínimas, y que si la propiedad vale para las estructuras componentes también vale para la estructura que las incluye.

Las demostraciones por inducción vistas en la sección 3.7 corresponden a considerar el conjunto  $\mathbb{N}$  con la relación sucesor que relaciona a  $n$  con  $n + 1$ ; la inducción fuerte corresponde a  $\mathbb{N}$  con la relación menor que.

### 3.8. Demostrar existencia

Muchas veces interesa demostrar que algún objeto que cumple ciertas condiciones existe. La forma más simple de hacer esto es exhibir el objeto del caso (para demostrar que hay primos pares, basta exhibir el primo 2) o dar un mecanismo claro que permite construirlo. Sin embargo, se da también la situación que podemos demostrar la existencia del objeto, sin poder asirlo de forma más concreta. Esto definitivamente es bastante poco satisfactorio, pero válido de todas formas. Un ejemplo es lo siguiente:

**Proposición 3.18.** *Hay números irracionales  $\alpha$  y  $\beta$  tales que  $\alpha^\beta$  es racional.*

*Demostración.* Sabemos que  $\sqrt{2}$  es irracional. Entonces:

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$$

Ahora bien, hay dos opciones para  $\sqrt{2}^{\sqrt{2}}$ : Si es racional, entonces podemos tomar  $\alpha = \beta = \sqrt{2}$  como ejemplo. Si es irracional, tomamos  $\alpha = \sqrt{2}^{\sqrt{2}}$  y  $\beta = \sqrt{2}$  como ejemplo.  $\square$

Bonito, pero es frustrante en que no da un ejemplo concreto. Otro ejemplo clásico es la demostración de Cantor (que discutiremos en el capítulo 6) que hay infinitos números trascendentes (números irracionales que no son ceros de un polinomio con coeficientes enteros) sin dar luces de cómo obtener alguno.

Una demostración alternativa, que da ejemplos concretos, es:

*Demostración.* Sea  $\alpha = \sqrt{2}$ ,  $\beta = \log_2 9$ , con lo que  $\alpha^\beta = 3$ .

Sabemos que  $\alpha$  es irracional por el teorema 3.3. Demostramos que  $\beta$  es irracional por contradicción. Supongamos que  $\beta$  fuera racional, digamos que para naturales  $m$  y  $n$  tenemos  $\beta = m/n$ . Claramente es  $\beta = \log_2 9 > 0$ , con lo que  $m > 0$ . Entonces sería  $9^n = 2^m$ , pero  $9^n$  es impar, mientras  $2^m$  es par. Esto es imposible.  $\square$

Se ha demostrado que el número de Hilbert (también conocido como constante de Gelfond-Schneider)  $2^{\sqrt{2}}$  es irracional (incluso es trascendente), y da otro ejemplo concreto al elevar a  $\sqrt{2}$ . Por lo demás, siendo trascendente  $2^{\sqrt{2}}$ , su raíz (el número que consideramos arriba) también es trascendente. Claro que para discutir estos temas habría que profundizar mucho más...

### 3.9. Refutaciones

Nos hemos concentrado hasta acá en demostrar cosas que sabemos ciertas. En la cruda realidad de las matemáticas nos encontramos con mayor frecuencia con aseveraciones que no sabemos si son ciertas o falsas (*conjeturas*). La tarea se compone, entonces, de determinar si la conjetura es verdadera o no, y luego demostrar que es verdadera o que no se cumple. Si no somos capaces de demostrar que la conjetura es cierta, esto no demuestra que sea falsa: Puede ser cierta, simplemente no hemos sido capaces de demostrarlo.

Igual que para demostrar que una aseveración es cierta, hay ciertas técnicas para demostrar que es falsa. La forma más simple de refutar la aseveración  $P$  es demostrar  $\neg P$ . Esta última a su vez es susceptible de cualquiera de las técnicas ya discutidas. Igual hay una variedad de situaciones especiales que merecen atención, como explica Hammack en su texto [161].

#### 3.9.1. Refutar aseveraciones universales: Contraejemplo

Si debemos demostrar que la aseveración  $\forall x \in S. P(x)$  es falsa, nuestra indicación general es demostrar su negación:

$$\neg(\forall x \in S. P(x)) \equiv \exists x \in S. \neg P(x)$$

O sea, debemos hallar  $x$  tal que  $P(x)$  sea falso. Basta exhibir un solo contraejemplo para que no valga para todo  $x$ . Por ejemplo:

**Conjetura 3.1.** Si  $n^2 - n$  es par, entonces  $n$  es par.

*Refutación.* Exhibimos un contraejemplo: Para  $n = 1$  tenemos  $n^2 - n = 0$ , que es par. Pero  $n$  es impar.  $\square$

#### 3.9.2. Refutar existencia

Si queremos demostrar que es falso  $\exists x \in S. P(x)$ , nuevamente es demostrar la negación:

$$\neg(\exists x \in S. P(x)) \equiv \forall x \in S. \neg P(x)$$

Como esto es una aseveración universal, un ejemplo no es suficiente.

**Conjetura 3.2.** Hay números primos  $p$  y  $q$  tales que  $p - q = 97$ .

*Refutación.* Demostramos que si  $q$  es primo, entonces  $p = q + 97$  no es primo. Dividimos la demostración en dos casos:

**$q = 2$ :** En este caso,  $q + 97 = 99 = 3 \cdot 3 \cdot 11$ , que no es primo.

***q es un primo impar:*** Si  $q$  es impar, entonces  $q + 97$  es un par mayor a 2, y por tanto no es primo.

□

### 3.9.3. Refutar por contradicción

Ciertamente es posible aplicar la técnica de reducción al absurdo a la tarea de refutar. Sólo que en este caso lo que buscamos es obtener una contradicción de la aseveración misma, no de su negación.

**Conjetura 3.3.** *Hay un real  $x$  para el cual  $x^4 < x < x^2$ .*

*Refutación.* Por contradicción. Supongamos que la conjetura es cierta. Sea  $x$  un número real para el cual  $x^4 < x < x^2$ . Como  $x > x^4$ ,  $x$  es positivo. Partimos con:

$$x^4 < x < x^2$$

Dividiendo por  $x$ :

$$\begin{aligned} x^3 &< 1 < x \\ x^3 - 1 &< 0 < x - 1 \end{aligned}$$

Factorizamos  $x^3 - 1$ :

$$(x - 1)(x^2 + x + 1) < 0$$

Como  $x - 1 > 0$ , podemos dividir:

$$x^2 + x + 1 < 0$$

Pero esto último es imposible, ya que  $x > 0$ .

□

## 3.10. Conjetura a teorema

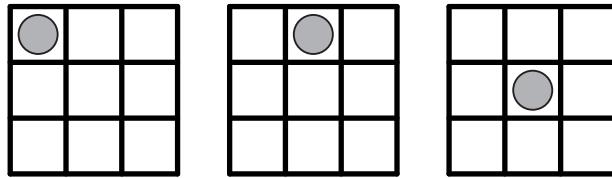
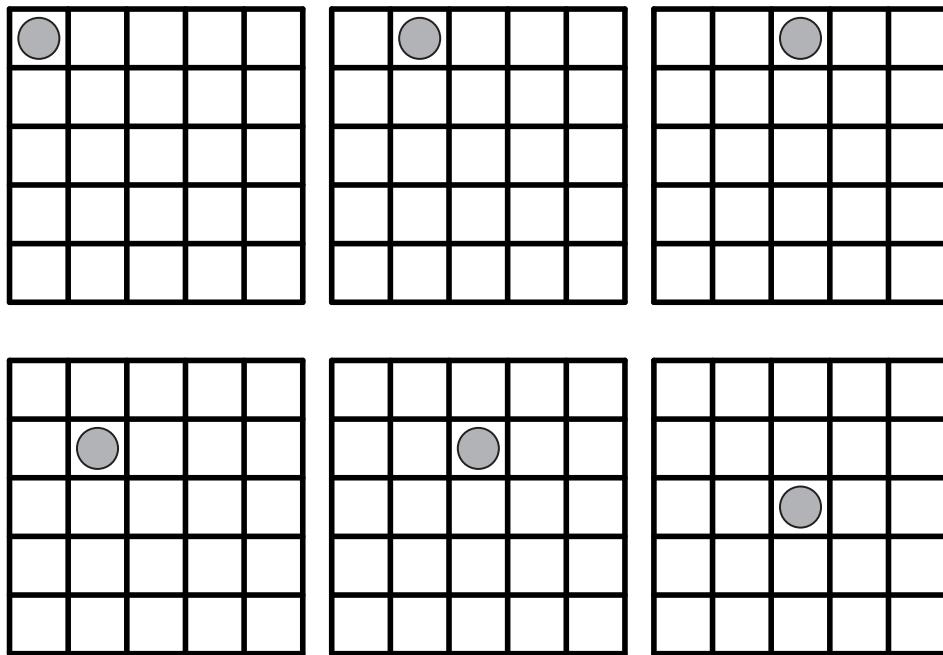
Una pregunta abierta luego de lo anterior es cómo se transforma una buena sospecha en un teorema (una solución al problema). Daremos un ejemplo simple, que más adelante servirá para ilustrar algunas de las técnicas más poderosas que presenta este texto. Ejemplos mucho más acabados muestran Bruckner, Thomson y Bruckner [57].

**Ejemplo 3.1.** En la Competencia de Ensayos de la Universidad de Miskatonic los ensayos deben entregarse anónimamente, cada uno acompañado por una tarjeta que identifica al autor. Las tarjetas codificadas son tarjetas cuadradas idénticas de  $n \times n$  [mm] ( $n$  es un número impar) divididas por ambos lados en cuadrados de 1 [mm]. En uno de estos cuadrados se perfora un agujero redondo.

Sea  $b_n$  el número de tarjetas diferentes que se pueden producir de esta forma, bajo el supuesto que las tarjetas se pueden rotar e invertir. Se pide encontrar una fórmula para  $b_n$  en términos de  $n$ , y usarla para determinar cuánto debe ser  $n$  si se esperan 100 participantes en el concurso.

**Solución** Atacaremos el problema en etapas.

**Paso 1: Experimentar.** Como nos dijeron que  $n$  es impar, analizaremos los casos  $n = 1, 3, 5$  para comenzar. En el caso  $n = 1$ , hay un único cuadradito, y por tanto es posible una única chapa.  $b_1 = 1$ .

Figura 3.7 – Chapas posibles con  $n = 3$ Figura 3.8 – Chapas posibles con  $n = 5$ 

En el caso  $n = 3$ , un par de intentos muestran que solo hay 3 posibilidades diferentes, como indica la figura 3.7. Cualquier otra alternativa puede rotarse de forma de obtener una de estas. O sea,  $b_3 = 3$ .

Algo de trabajo adicional lleva a concluir que  $b_5 = 6$ , véase la figura 3.8.

**Paso 2: Adivinar.** Hay dos estrategias posibles para adivinar la solución. La “heroica” es adivinar una fórmula para  $b_n$  directamente, en base a la información obtenida hasta acá (posiblemente complementada con valores adicionales). De ser así, se puede proceder directamente al paso 5.

La otra es usar la estrategia “segura”, que pasa por encontrar una relación recursiva entre los valores buscados. Acá la pregunta es cómo pasar de  $n = 1$  a  $n = 3$ , y de  $n = 3$  a  $n = 5$ , y así

sucesivamente. Tenemos hasta acá:

$$b_1 = 1 \quad (3.48)$$

$$b_3 = b_1 + 2 \quad (3.49)$$

$$b_5 = b_3 + 3 \quad (3.50)$$

Tal vez  $b_7 = b_5 + 4 = 10$ , y en general se cumple:

$$b_{2r+1} = b_{2r-1} + r + 1 \quad (3.51)$$

Con esto tenemos una *conjetura*.

**Paso 3: Entender.** Debemos corroborar nuestra conjetura (3.51), con el caso siguiente  $n = 7$ . Esto puede hacerse verificando  $b_7 = 10$  directamente, pero es mucho mejor analizar cómo se relacionan  $b_3$  con  $b_5$  (deben analizarse las figuras 3.7 y 3.8) y  $b_7$  con  $b_5$ . Esto último lo ilustra la figura 3.9. Puede verse que la chapa de  $7 \times 7$  puede considerarse como una de  $5 \times 5$  con un

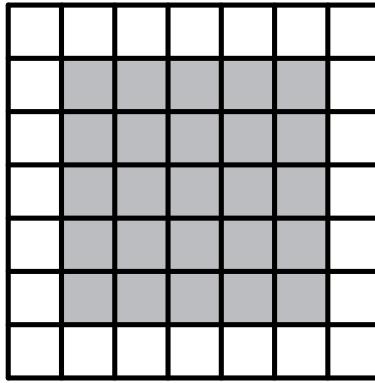


Figura 3.9 – Chapa de  $7 \times 7$  como chapa de  $5 \times 5$  con borde

borde. Si se perfora alguno de los cuadraditos del centro, se obtienen  $b_5$  posibilidades. Las otras opciones resultan de perforar el borde. Un momento de reflexión, también comparando el caso  $n = 3$  con el  $n = 5$ , muestra que solo la mitad del borde superior aporta alternativas esencialmente diferentes, o sea, aporta 4 más. Hemos demostrado que  $b_7 = b_5 + 4$ .

Con esto se completa el trabajo pesado. El mismo razonamiento confirma la conjetura (3.51) para el caso general.

**Paso 4: La fórmula.** Nos piden una fórmula para los  $b_n$ , y ahora sabemos que quedan descritos por la secuencia definida recursivamente por:

$$b_{2r+1} = \begin{cases} 1 & \text{si } r = 0 \\ b_{2r-1} + r + 1 & \text{si } r \geq 1 \end{cases} \quad (3.52)$$

Ya conocemos los valores  $b_1 = 1$ ,  $b_3 = 3$ ,  $b_5 = 6$ ,  $b_7 = 10$ , y podemos calcular valores adicionales según se requieran. Posiblemente ya hayamos dado en cuenta que:

$$1 = (1 \cdot 2)/2, \quad 3 = (2 \cdot 3)/2, \quad 6 = (3 \cdot 4)/2, \quad 10 = (4 \cdot 5)/2 \quad (3.53)$$

lo que lleva a sospechar:

$$b_{2r+1} = \frac{1}{2} (r+2)(r+1) \quad \text{para todo } r \in \mathbb{N} \quad (3.54)$$

**Paso 5: Demostración.** Resta demostrar que la fórmula (3.54) es correcta.

**Proposición 3.19.** Para todo  $r \in \mathbb{N}_0$ ,  $b_{2r+1} = \frac{1}{2}(r+2)(r+1)$

*Demostración.* Por inducción sobre  $r$ .

**Base:** La fórmula (3.54) vale cuando  $r = 0$ , ya que  $b_1 = 1$  y  $(0+2)(0+1)/2 = 1$ .

**Inducción:** Supongamos que (3.54) se cumple para  $r = k$ , vale decir,  $b_{2k+1} = \frac{1}{2}(k+2)(k+1)$ .

Usando la relación (3.51) descubierta en el paso 3:

$$\begin{aligned} b_{2(k+1)+1} &= b_{2k+1} + k + 2 \\ &= \frac{1}{2}(k+2)(k+1) + k + 2 \\ &= \frac{1}{2}(k+2)(k+3) \\ &= \frac{1}{2}((k+1)+2)((k+1)+1) \end{aligned}$$

La fórmula vale para todo  $r \in \mathbb{N}_0$  por inducción. □

**Paso 6: La respuesta.** El duro trabajo de los matemáticos se aprecia solo cuando entrega una respuesta definitiva a un problema práctico. En este caso, la “respuesta definitiva” es el tamaño de la tarjeta necesaria para 100 participantes, o sea, el valor  $r^*$  tal que  $b_{2r^*+1} \leq 100 < b_{2r^*+3}$ . Planteamos:

$$\frac{1}{2}(r+2)(r+1) \geq 100 \quad (3.55)$$

Los ceros del polinomio que corresponde a (3.55) son  $r = -3,217$  y  $r = 12,65$ . Como para  $r \geq 0$  la expresión del lado izquierdo de la desigualdad (3.55) es creciente, aproximamos al entero superior y tenemos  $r^* = 13$ . Las chapas son de  $27 \times 27$  [mm], lo que da para 105 participantes.

Para mayor detalle sobre cómo resolver problemas, particularmente en el ámbito matemático, dirigimos al lector al clásico de Pólya [289], quien plantea cuatro pasos esenciales:

1. **Entender el problema.** Muchas veces este paso se omite como obvio, pero es frecuente empatanarse por no entender completamente el problema. Como remedio se sugieren preguntas como:

- ¿Qué se busca encontrar?
- Plantee el problema en sus propias palabras.
- ¿Se le ocurre un dibujo o diagrama que ayude a entender el problema?
- ¿Hay suficiente información para resolver el problema?

2. **Idear un plan.** Hay muchas maneras razonables de resolver problemas. La habilidad de elegir la estrategia apropiada se adquiere resolviendo sistemática y ordenadamente problemas diversos. Una lista parcial de estrategias a considerar es:

- Adivine y verifique.
- Elabore una lista ordenada.
- Elimine posibilidades.

- Use simetría.
  - Considere casos especiales.
  - Razonamiento directo.
  - Busque patrones.
  - Resuelva un problema más simple.
  - Trabaje en reversa.
3. **Lleve a cabo el plan.** Esto suele ser más fácil que idear el plan. Generalmente solo requiere cuidado y paciencia, si tiene las habilidades requeridas. Persista. Si no funciona, descártelo e intente otro.
4. **Revise/extienda.** Puede ganar mucho tomándose el tiempo de reflexionar, mirando atrás para ver qué funcionó y qué no. Esto ayuda a elegir la estrategia adecuada en casos futuros relacionados con este.

Pero tal vez más importante que la habilidad de resolver problemas es hallar preguntas interesantes a resolver. Brown y Walter [56] animan a cultivar el arte de plantear problemas.



## 4 Correctitud de programas

---

Cada día dependemos más de programas computacionales. Lamentablemente, muchos programas han demostrado ser incorrectos, errores de programación han dado lugar a costos inmensos (el reporte de Calude, Calude y Marcus [62] da algunos ejemplos notorios, pero todos hemos sufrido en menor o mayor medida a causa del comportamiento erróneo de programas). Dijkstra [92] observa que la computación significa un cambio radical en nuestro mundo, al introducir artefactos cuyo funcionamiento no es continuo, y más aún dar lugar a fenómenos que abarcan órdenes de magnitud absolutamente inimaginables en otras disciplinas. Veremos cómo aplicar técnicas de razonamiento matemático a la tarea de asegurar que un programa funcione como se espera.

### 4.1. Lógica de Hoare

Formalmente, un algoritmo (o un programa, que es la representación concreta de un algoritmo en un lenguaje específico) se dice que es *correcto* si cumple con las siguientes características:

1. Produce la salida deseada para cada posible dato de entrada
2. Su tiempo de ejecución es siempre finito

Salvo en casos muy simples, es imposible indicar la salida para cada posible dato de entrada. En consecuencia, se describe la relación entre entradas y salidas mediante alguna especificación más o menos formal. Nos interesa en particular el caso en que las especificaciones pueden expresarse en lenguaje matemático, con lo que podemos razonar formalmente sobre ellas.

Ya a fines de los años 60, Floyd [131] y luego Hoare [176] propusieron demostrar formalmente que los programas cumplen con sus especificaciones, idea que fue luego desarrollada por Dijkstra [94] y de alguna manera completada por Gries [153]. Posiblemente la formalización más completa es la que da Apt [16, 17]. Una descripción formal reciente (con orientación pedagógica) dan Gordon y Collavizza [147]. Jones [187] resume la historia desde sus comienzos. Una crítica del área de demostrar correctitud da Gutmann en su tesis [156, capítulos 4 y 5].

Demostrar correctitud de programas aumenta la confianza de que funcionen correctamente, pero las técnicas formales son complejas y caras de aplicar en general. Aún con ayuda del computador hoy solo es posible verificar completamente programas relativamente pequeños. Tal vez el ejemplo más notable de verificación es la del micronúcleo seL4 [204, 205], un sistema de unas 8 700 líneas de C de las cuales se verificaron formalmente unas 7 500. Para contraste, el núcleo de un sistema operativo de uso común, como Linux, tiene casi doce millones de líneas de código.

Sigue vigente el famoso dicho: «Beware of bugs in the above code; I have only proved it correct, not tried it» (Donald E. Knuth [211]). Al efecto, Berry [44] cita el ejemplo de un programita de 25 líneas de Algol especificado y demostrado correcto informalmente en 1969 por Naur [264], publicado sin probarlo. El año siguiente, revisando la publicación de Naur Leavenworth [233] encontró un error que habría sido evidente de ejecutar el programa. Aún después, London [241] halló tres errores

adicionales que habrían sido fáciles de hallar probando el programa. Ofreció un programa corregido, acompañando esta vez una demostración formal de correctitud. Igualmente, Goodenough y Gerhart [145] hallaron tres errores adicionales en el programa de London, que nuevamente habrían sido evidentes al probar el programa. A su vez, las especificaciones dieron lugar a una comedia de errores adicional. El hecho que incluso ejemplos mínimos, de las manos de los máximos expertos del área, den lugar a tal espectáculo es prueba patente de lo complejo del tema.

Siempre debe tenerse presente el dicho: «There are two ways of constructing a software design: One way is to make it so simple that there are *obviously* no deficiencies, and the other way is to make it so complicated that there are no *obvious* deficiencies. The first method is far more difficult.» (C. A. R. Hoare [177]). En la misma línea nos advierten: «Premature optimization is the root of all evil.» (D. E. Knuth [209, 212]).

La idea tras el trabajo de Hoare y sus sucesores es que durante su ejecución un programa pasa por *estados* bien definidos, y que estos estados cambian conforme se ejecutan instrucciones. Mediante *predicados* sobre los valores de las variables se describen los aspectos de interés de cada estado, y se busca demostrar que dadas ciertas condiciones iniciales al finalizar el programa se cumple lo solicitado (*correctitud parcial*) y, generalmente en forma separada de lo anterior, que el programa siempre termina con el resultado correcto (*correctitud total*). Esto involucra relacionar los predicados antes y después de las distintas instrucciones del lenguaje empleado.

La forma general de expresar los resultados es:

$\{P\}$  programa  $\{Q\}$

para expresar que si se cumple  $P$  antes del programa, cuando éste termine se cumple  $Q$ . Esto permite componer estructuras más complejas.

Una secuencia de instrucciones queda representada como 4.1. Para demostrar que si se inicia la

---

Algoritmo 4.1: Secuencia

---

$\{P_1\}$  Instrucción 1  $\{Q_1\}$   
 $\{P_2\}$  Instrucción 2  $\{Q_2\}$

---

secuencia y se cumple  $P$  y al final se cumple  $Q$ , debemos demostrar que  $P \Rightarrow P_1$ , que dado  $P_1$  al inicio de la primera instrucción al final de ella se cumple  $Q_1$ , que  $Q_1 \Rightarrow P_2$ , dado  $P_2$  al inicio de la segunda instrucción cuando termina se cumple  $Q_2$ , y finalmente que  $Q_2 \Rightarrow Q$ .

Para selección empleamos el esquema 4.2. Acá debemos demostrar que  $P \wedge$  condición  $\Rightarrow P_i$  y

---

Algoritmo 4.2: Selección

---

```
if condición then
     $\{P_i\}$  Instrucción 1  $\{Q_i\}$ 
else
     $\{P_e\}$  Instrucción 2  $\{Q_e\}$ 
end
```

---

que  $P \wedge \neg$  condición  $\Rightarrow P_e$ ; que las instrucciones aseguran las condiciones  $Q_i$  y  $Q_e$ , respectivamente; y finalmente que  $Q_i \Rightarrow Q$  y  $Q_e \Rightarrow Q$ .

Para ciclos la construcción básica es 4.3. Acá debemos asegurar que  $P \wedge$  condición  $\Rightarrow P_w$ , que dado  $P_w$  la instrucción asegura  $Q_w$ , que  $Q_w \Rightarrow P_w$ . Además debe ser que  $P \wedge \neg$  condición  $\Rightarrow Q$ , y que  $Q_w \wedge \neg$  condición  $\Rightarrow Q$ . A la aseveración  $P_w$  se le llama *invariante del ciclo*, ya que las iteraciones la mantienen.

---

Algoritmo 4.3: Ciclo

---

```
while condición do
    { $P_w$ } Instrucción { $Q_w$ }
end
```

---

La forma de manejar funciones o procedimientos es definir precondiciones y postcondiciones, asegurar que la relación entre estas se cumpla, y luego usar esto en las invocaciones. Esto es aplicable también a llamadas recursivas.

Al agregar aseveraciones a un programa lo más difícil suele ser hallar invariantes de ciclo, que por eso debieran siempre darse como comentarios.

Nótese que lo anterior nos asegura únicamente que si la ejecución alcanza el final de la secuencia, se cumple la postcondición. A esto se le denomina *correctitud parcial*. Aparte debe demostrarse que el algoritmo termina, con lo que tenemos *correctitud total*.

## 4.2. Búsqueda binaria

La técnica esbozada anteriormente requiere un trabajo meticoloso, que generalmente no se justifica en tanto detalle. En la práctica se suele usar razonamiento más informal, lo que obviamente no asegura los resultados con la misma rigurosidad.

Como un ejemplo, desarrollaremos paso a paso una función de búsqueda binaria, siguiendo la exposición de Bentley [37, capítulo 4]. Es también de interés histórico, la primera exposición del programa fue publicada en 1946, la primera versión correcta recién en 1962. Bentley reporta haber usado el programa como ejercicio en cursos para programadores profesionales. Al cabo de una hora, revisaban sus programas durante media hora adicional, y consistentemente 90 % de ellos hallaban errores. Bentley reconoce que no está seguro si el 10 % restante era correcto.

Nuestro problema es determinar si el arreglo ordenado  $x[1..N]$  contiene el valor  $t$ . Más precisamente, sabemos que  $N \geq 0$  y que  $x[1] \leq x[2] \leq \dots \leq x[N]$ . Los tipos de  $t$  y de los elementos de  $x$  son los mismos, el pseudocódigo debiera funcionar igualmente bien para enteros, reales o strings. La respuesta es el entero  $p$ ; si  $p$  es cero  $t$  no está en  $x[1..N]$ , en caso contrario  $1 \leq p \leq N$  y  $t = x[p]$ .

Búsqueda binaria resuelve este problema siguiendo la pista a un rango dentro del arreglo en el que  $t$  tiene que estar si es que está en el arreglo. Inicialmente el rango es el arreglo completo. El rango se acorta comparando  $t$  con el elemento medio del rango y descartando la mitad que no puede contenerlo. El proceso continúa hasta que se halle el elemento o el rango esté vacío.

### 4.2.1. Escribiendo el programa

La idea clave es que siempre sabemos que si  $t$  está en alguna parte de  $x[1..N]$ , está en un cierto rango. Usaremos DebeEstar(*rango*) para significar que si  $t$  está en el arreglo, debe estar en el *rango* indicado. Con esto, la descripción informal se puede transformar en el esbozo de programa 4.4. Parte crucial de nuestro esbozo es el *invariante de ciclo*, que encerramos entre llaves. Se cumple siempre al comienzo de cada ciclo (de allí su nombre), y formaliza nuestra idea intuitiva presentada antes.

Refinamos el esbozo, asegurándonos que nuestras acciones respetan el invariante. Primeramente debemos decidir cómo representar el *rango*. Usaremos dos índices  $i$  (inferior) y  $s$  (superior) para el rango  $i..s$ . (Hay otras opciones, como inicio y largo.) El siguiente paso es la inicialización: ¿Qué valores deben tener  $i$  y  $s$  para que DebeEstar( $i, s$ ) se cumpla inicialmente? La respuesta obvia es  $i = 1$  y  $s = N$ : DebeEstar(1,  $N$ ) dice que si  $t$  está en  $x$ , está en  $x[1..N]$ , exactamente lo que sabemos al comenzar el programa. El siguiente paso es verificar si el rango es vacío, cosa que se da siempre que

---

Algoritmo 4.4: Esbozo de búsquedas binaria

---

Inicialice *rango* para designar  $x[1..N]$

**loop**

{ Invariante: DebeEstar(*rango*) }

**if** *rango* es vacío **then**

    Retorne que *t* no está en el arreglo

**end**

    Calcule *m*, el punto medio de *rango*

    Use *m* como prueba para encoger el rango, si halla *t* en el proceso retorne su posición

**end**

---

*i > s*. Hallar el punto medio del rango es:

$$m = \left\lfloor \frac{i+s}{2} \right\rfloor$$

Uniendo las piezas obtenemos el segundo esbozo 4.5. Para evitar confusiones con la relación de igualdad u otras, en nuestros algoritmos usaremos  $\leftarrow$  para indicar asignación. Resta refinar la última

---

Algoritmo 4.5: Búsquedas binaria: Segundo esbozo

---

*i*  $\leftarrow 1$ ; *s*  $\leftarrow N$

**loop**

{ Invariante: DebeEstar(*i, s*) }

**if** *i > s* **then**

*p*  $\leftarrow 0$ ; **break**

**end**

*m*  $\leftarrow \lfloor (i+s)/2 \rfloor$

    Use *m* como prueba para encoger el rango *i..s*, si halla *t* en el proceso retorne su posición

**end**

---

acción del ciclo. Correspondrá a comparar *t* con  $x[m]$  y tomar la acción apropiada:

**case** *t < x[m]*: Acción a

**case** *t = x[m]*: Acción b

**case** *t > x[m]*: Acción c

Sabemos que la acción correcta en el segundo caso es asignar *m* a *p* y quebrar el ciclo. En el primer caso el rango se reduce a *i..m - 1*, en el tercero a *m + 1..s*. Esto se logra asignando a *s* o *i*, respectivamente. Expresado en términos de las estructuras de control comunes resulta 4.6. En rigor, solo hemos demostrado (muy informalmente, claro está) que si el ciclo termina entrega el resultado correcto. Debemos asegurar además que el ciclo siempre termina, vale decir, que el largo del rango disminuye en cada paso. Como el largo es un entero, no puede disminuir indefinidamente.

Igualmente, en implementaciones en máquinas reales el algoritmo 4.6 tiene un error fatal: Si la suma de *i + s* es mayor que el máximo entero representable, el cálculo del nuevo valor de *m* falla.

---

Algoritmo 4.6: Búsqueda binaria: Pseudocódigo final

---

```

i ← 1; s ← N
loop
  { Invariante: DebeEstar(i, s) }
  if i > s then
    p ← 0; break
  end
  m ← ⌊(i + s)/2⌋
  if t < x[m] then
    s ← m – 1
  if t = x[m] then
    p ← m; break
  else
    i ← m + 1
  end
end

```

---

Esto puede sonar a sofisma, pero fue un error real en la biblioteca de Java. La solución correcta es escribir esa línea como  $m \leftarrow i + \lfloor(s - i)/2\rfloor$ . De esa forma, las variables y valores intermedios están acotados por  $n$ , y no hay rebalses.

Sea  $l$  el largo del rango al comenzar un ciclo. Llamemos  $l'$  al largo después del ciclo, suponiendo  $t \neq x[m]$ . Entonces:

$$l' = \begin{cases} (m-1) - i + 1 = (\lfloor(i+s)/2\rfloor - 1) - i + 1 \leq (s-i)/2 = (l+1)/2 & \text{si } t < x[m] \\ s - (m+1) - 1 = s - (\lfloor(i+s)/2\rfloor + 1) - 1 \leq s - (i+s)/2 - 1 = l/2 - 3/2 < l & \text{si } t > x[m] \end{cases}$$

En el caso  $t < x[m]$ , si  $l > 1$  claramente  $l' \leq (l+1)/2 < l$ , pero para  $l = 1$  resulta la cota inútil  $l' \leq 1$ . En esta última situación es  $i = s$ , y el algoritmo asigna  $s = m - 1 = i - 1$ , cumpliendo la condición de término. Cada iteración nos acerca a la condición que hace terminar el ciclo, el programa termina.

Es sencillo ahora traducir el pseudocódigo 4.6 a un lenguaje de programación como C, ver el listado 4.1. Nuestra versión incluye la precaución contra rebalses aritméticos mencionada antes.

---

```

/* @file binary-search.c */

#include "binary-search.h"

int binarysearch(const DataType t, const DataType x[], const int n)
{
    int l, u, m;

    l = 0; u = n – 1;
    while(l <= u) {
        /* If t is in x,
         * it must be in x[l .. u] */
        m = l + (u – l) / 2;
        if(x[m] < t)
            l = m + 1;
        else if(x[m] == t)
            return m;
    }
}

```

```

    else /*  $x[m] > t$  */
        u = m - 1;
    }
return -1;
}

```

Listado 4.1 – Búsqueda binaria en C

Nuestro desarrollo cuidadoso da gran confianza de que el programa resultante sea correcto. El registrar el invariante del ciclo ayudará a nuestros lectores a convencerse de ello.

Para no caer en un programa demostrado correcto que falla con el primer caso de prueba (como se narra en la introducción del presente capítulo), usamos el computador para lo que es mejor: Tareas rutinarias. Un pequeño programa bombardea esta función con casos de prueba: Se crea un arreglo de 22 elementos que se llena con los valores 0 a 21, luego se buscan los valores de 1 a  $N$  en él dando el rango de 1 a  $N$  para la búsqueda, con  $N$  variando de 1 a 20. Después se buscan los valores 0 y  $N+1$  (ambos presentes, pero fuera del rango indicado), y finalmente los valores de 0,5 a  $N+0,5$  con paso 1. Con esto cubrimos valores populares para errores: 1, 2, 3, algunas potencias de 2, números que difieren de potencias de 2 en 1. Y se cumplió lo indicado respecto de que los errores se cometan principalmente en las partes simples del programa: Algunos de los casos de prueba iniciales fallaron, estaban escritos incorrectamente...

### 4.3. Exponenciación

El calcular una potencia vía multiplicaciones sucesivas viene directamente de la definición de potencia. Sin embargo, hay métodos más eficientes. Partiendo de la identidad:

$$n = d \cdot \left\lfloor \frac{n}{d} \right\rfloor + n \bmod d$$

donde  $n \bmod d$  es el resto de la división de  $n$  por  $d$ , podemos expresar potencias:

$$x^n = (x^{\lfloor n/2 \rfloor})^2 \cdot x^{n \bmod 2} \quad (4.1)$$

Tenemos inmediatamente el algoritmo recursivo 4.7. La justificación es que suponiendo que la

Algoritmo 4.7: Exponenciación binaria recursiva

---

```

function power ( $x, n$ )
    if  $n = 0$  then
        return 1
    else
         $s \leftarrow \text{power}(x, \lfloor n/2 \rfloor)$ 
         $r \leftarrow s^2$ 
        if  $n \bmod 2 = 1$  then
             $r \leftarrow r \cdot x$ 
        end
        return  $r$ 
    end

```

---

función  $\text{power}(x, k)$  hace correctamente su trabajo para  $k < n$ , por la identidad (4.1) calcula correctamente la potencia  $n$ . Para justificar que termina, vemos que cada vez se invoca la función

recursivamente con un valor menor para el parámetro  $n$ , por lo que tarde o temprano llega al valor 0, que no involucra recursión. Esto es en esencia una demostración por inducción fuerte.

Una versión alternativa (no recursiva) del algoritmo 4.7 es el algoritmo 4.8. Usamos operaciones con bits al estilo C [202]. Estamos usando la relación:

---

Algoritmo 4.8: Exponenciación binaria no recursiva

---

```

function power ( $x, n$ )
  if  $n = 0$  then
    return 1
  end
  for  $i \leftarrow 0; n \& (1 \ll i); i \leftarrow i + 1$  do
    /* Nada
   */
  end
  /* Ahora ( $i \geq 0$ )  $\wedge (2^i \leq n < 2^{i+1})$ 
   */
   $r \leftarrow x$ 
  for ;  $i > 0; i \leftarrow i - 1$  do
    /* Invariante:  $u = \lfloor n/2^i \rfloor$ ,  $v = n \bmod 2^i$ ,  $(r = x^u) \wedge (x^n = r^{2^i} \cdot x^v)$ 
     */
     $r \leftarrow r^2$ 
    if  $n \& (1 \ll (i - 1))$  then
       $r \leftarrow r \cdot x$ 
    end
  end
  /* Del invariante con  $i = 0$  resulta  $r = x^n$ 
   */
  return  $r$ 

```

---

$$x^n = \left( x^{\lfloor n/2^i \rfloor} \right)^2 \cdot x^{n \bmod 2^i}$$

Primeramente calculamos  $i$  tal que  $2^i \leq n \leq 2^{i+1}$ , el código restante calcula  $x^n$  partiendo por la potencia de 2 más significativa en  $n$ . Las invariantes indicadas en el código servirán de explicación. En vez de calcular potencias de dos, es más eficiente considerar los bits de  $n$ .

Un ejemplo adicional es el algoritmo 4.9 para obtener la raíz cuadrada entera, vale decir, calcular  $\lfloor \sqrt{n} \rfloor$ . Todas las variables del algoritmo son enteras. Es simple verificar el invariante, y con la condición de término del ciclo tenemos que  $u^2 \leq n < (u + 1)^2$ , vale decir,  $u \leq \sqrt{n} < u + 1$ , o sea  $u = \lfloor \sqrt{n} \rfloor$ . En cada ciclo aumenta  $u$  o disminuye  $v$ , por lo que el algoritmo termina.

## 4.4. Algunos principios

El ejemplo de búsqueda binaria ilustra las fortalezas de la verificación de programas: El problema a resolver es importante y requiere código cuidadoso, lo desarrollamos guiados por ideas de verificación, y el análisis de correctitud usa herramientas generales. En todo caso, en la práctica el nivel de detalle del desarrollo será substancialmente menor. Algunos principios generales resultan de la discusión:

**Afirmaciones:** Permiten expresar las relaciones entre datos de entrada, variables internas y resultados en forma precisa.

---

**Algoritmo 4.9: Cálculo de  $\lfloor \sqrt{n} \rfloor$** 


---

```

function isqrt (n)
  u  $\leftarrow$  0
  v  $\leftarrow$  n + 1
  while u + 1  $\neq$  v do
    /* Invariante:  $u^2 \leq n \leq v^2$  y  $u + 1 \leq v$  */ 
    x  $\leftarrow$   $\lfloor (u + v)/2 \rfloor$ 
    if x2  $\leq n$  then
      u  $\leftarrow$  x
    else
      v  $\leftarrow$  x
    end
  end
  return u

```

---

**Estructuras de control secuenciales:** La estructura de control más simple es ejecutar una acción, seguida por otra. Entendemos un programa por afirmaciones entre las instrucciones y razonamos de una a la siguiente.

**Estructuras de selección:** Durante la ejecución, se toma una de varias acciones. Demostramos la correctitud de tales estructuras razonando de la afirmación antes de la estructura junto a la condición especial que nos lleva al presente caso. Lo que podemos concluir luego de cada una de las opciones se cumple al finalizar la estructura completa.

**Estructuras de iteración:** Argüir la correctitud de un ciclo tiene tres fases: Inicialización, preservación y término. Primero demostramos que el invariante del ciclo se establece antes del ciclo (inicialización), luego que si el invariante se cumple al comienzo del ciclo se cumple cuando el ciclo termina, y finalmente demostramos que el ciclo se ejecuta un número finito de veces. Después del ciclo sabemos que se cumple el invariante y la condición de término se cumplió.

**Variables:** Muchos programas modifican los valores de variables, pero interesa expresar que cierta relación se cumple respecto de los valores iniciales. Una posibilidad es usar la convención que si la variable es *n*, su valor original se representa mediante *n*<sub>0</sub>. Otra opción es definir variables fantasma que recogen valores de interés. Usamos variables fantasma en el algoritmo 4.8 para expresar el invariante en forma más sencilla.

**Subrutinas:** Para verificar una subrutina, explicitamos su propósito mediante dos afirmaciones: Su precondición describe el estado antes de ejecutarla, la postcondición describe lo que garantiza del estado una vez que finaliza. Externamente usamos estas afirmaciones para razonar sobre sus usos, internamente verificamos que dadas las precondiciones estamos garantizando las postcondiciones. Esto es válido también en el caso de rutinas recursivas: Suponemos que las llamadas recursivas “hacen lo correcto”, y en base a ello demostramos que la rutina cumple su contrato.

**Recursión:** Verificar la versión recursiva de la exponentiación binaria resulta substancialmente más sencillo que verificar la versión no recursiva. Esta observación es aplicable en general.

Hallar afirmaciones simples (particularmente invariantes de ciclos) no es nada fácil. Esta manera de enfrentar el problema de escribir un programa formaliza la manera en que entendemos un programa

(muchas veces la explicación del funcionamiento es a través de una traza de la ejecución, pero está claro que el detalle de los valores que toman las variables en esa instancia particular no es todo lo que se está transmitiendo). Por esta razón conviene familiarizarse con este enfoque.

Las partes difíciles de un programa hacen que se recurra a métodos más formales, mientras las partes simples se desarrollan de la forma tradicional. La experiencia común es que las partes difíciles luego funcionan correctamente la primera vez, las fallas están en las partes simples.

No se ha logrado el objetivo inicial de estos esfuerzos: Contar con algún artilugio que tome un programa e indique “correcto” o “incorrecto”. Igualmente logramos algo muy valioso: Una comprensión mejor del proceso de programación. Lenguajes de programación actuales se definen al menos en parte cuidando que sea fácil razonar con sus operaciones. Técnicas similares a las usadas acá para demostrar correctitud emplean los compiladores para “optimizar” código (en realidad, solo intentan mejorar características de ejecución): Dependiendo de restricciones deducidas sobre los valores, el código puede especializarse o incluso omitirse sin cambiar los resultados. Refinamientos del análisis son técnicas de ejecución simbólica, que pueden hallar errores o al menos generar automáticamente casos de prueba para la mayoría del código, un ejemplo es KLEE [60]. También hay herramientas que ayudan a construir y verificar demostraciones de correctitud, como Frama-C [84].



## 5 Números reales

---

Los números reales son fundamentales en mucha de la matemática que usamos diariamente. No nos detendremos en un estudio detallado de ellos, los exploraremos como ejemplo de campo, estructura algebraica que trataremos en algún detalle más adelante (mostrando el funcionamiento del método axiomático y algunas técnicas de demostración).

### 5.1. Axiomas de los reales

Daremos una breve introducción a los números reales y sus propiedades, siguiendo en lo general a Chen [70, capítulo 1]. Anotamos  $\mathbb{R}$  para el conjunto de números reales, con operaciones  $+$  y  $\cdot$ . Los números reales con sus operaciones cumplen los siguientes axiomas, que simplemente daremos por hechos. Estos axiomas describen lo que se conoce como un *campo* (en inglés *field*). En esta lista  $a, b, c$  son reales cualquiera.

**R1:** La suma es asociativa:  $(a + b) + c = a + (b + c)$ .

**R2:** Hay un *elemento neutro para la suma*  $0 \in \mathbb{R}$  tal que  $a + 0 = a$

**R3:** Hay un elemento  $-a \in \mathbb{R}$  tal que  $a + (-a) = 0$ . A  $-a$  se le llama *inverso aditivo* de  $a$ .

**R4:** La suma es conmutativa:  $a + b = b + a$ .

**R5:** La multiplicación es asociativa:  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

**R6:** La multiplicación distribuye sobre la suma:  $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ .

**R7:** Hay un elemento *neutro para la multiplicación*  $1 \in \mathbb{R}$  tal que  $a \cdot 1 = a$ .

**R8:** La multiplicación es conmutativa:  $a \cdot b = b \cdot a$ .

**R9:** Para  $a \neq 0$  hay un elemento  $a^{-1} \in \mathbb{R}$  tal que  $a \cdot a^{-1} = 1$ . A  $a^{-1}$  se le llama *inverso multiplicativo* de  $a$ .

Entre los reales tenemos además un orden, una relación  $<$  que cumple los siguientes axiomas adicionales, donde  $a, b$  y  $c$  nuevamente denotan números reales cualquiera. Anotamos  $a > b$  si  $b < a$ , como es convencional.

**O1:** Se cumple exactamente uno de  $a < b$ ,  $a = b$  o  $a > b$ . Esta propiedad se conoce como *tricotomía*.

**O2:** Si  $a < b$  y  $b < c$  entonces  $a < c$ .

**O3:** Si  $a < b$ , entonces  $a + c < b + c$ .

**O4:** Si  $a < b$  y  $c > 0$  entonces  $a \cdot c < b \cdot c$ .

En términos de las propiedades de relaciones, diríamos que  $<$  es transitiva e irreflexiva, y que la relación  $\leq$  en  $\mathbb{R}$ , definida mediante  $a \leq b \equiv (a < b) \vee (a = b)$ , es un orden total.

Un subconjunto de los reales es el conjunto de los números naturales,  $\mathbb{N} = \{1, 2, 3, \dots\}$ . Los siguientes axiomas dan sus principales características. Primeramente,  $\mathbb{N} \subseteq \mathbb{R}$  con las mismas operaciones y relación de orden. Enseguida:

**N1:**  $1 \in \mathbb{N}$

**N2:** Si  $n \in \mathbb{N}$ , entonces  $n + 1 \in \mathbb{N}$ . A  $n + 1$  se le llama el *sucesor* de  $n$ .

**N3:** Todo  $n \in \mathbb{N}$  tal que  $n \neq 1$  es el sucesor de un único número natural.

**N4:** Todo subconjunto no vacío de  $\mathbb{N}$  contiene un elemento mínimo. Esto se conoce como *principio de buen orden*.

Puede demostrarse que el principio de buen orden es equivalente al *principio de inducción*, acá demostraremos este último partiendo de buen orden:

**Teorema 5.1** (Principio de inducción). *Sea  $p(\cdot)$  un predicado que cumple:*

(I)  $p(1)$  es verdadero

(II)  $p(n) \Rightarrow p(n + 1)$

*Entonces  $p(n)$  es verdadero para todo  $n \in \mathbb{N}$ .*

*Demostración.* Por contradicción. Supongamos un conjunto no vacío  $\mathcal{C} \subseteq \mathbb{N}$  para el que  $p(\cdot)$  no vale. Por el principio del buen orden,  $\mathcal{C}$  contiene su elemento mínimo, llamémosle  $m$ . Sabemos que  $p(1)$  es cierto, así que  $m > 1$  y es el sucesor de un natural  $n$ . Como  $m$  es el mínimo para el que no vale  $p(\cdot)$ ,  $p(n)$  es cierto, pero entonces es cierto  $p(n + 1) = p(m)$ , contradiciendo la elección de  $m$ .  $\square$

El conjunto  $\mathbb{Z}$  de los enteros es la extensión de  $\mathbb{N}$  para incluir a 0 y los números de la forma  $-n$  para  $n \in \mathbb{N}$ . El conjunto  $\mathbb{Q}$  de los racionales es el conjunto de números de la forma  $a \cdot b^{-1}$ , con  $a \in \mathbb{Z}$  y  $b \in \mathbb{N}$ .

Los axiomas de campo y de orden valen para  $\mathbb{Q}$ . Pero vimos que  $\mathbb{Q}$  es incompleto (por el teorema 3.3,  $\sqrt{2} \notin \mathbb{Q}$ ). Veremos una propiedad que distingue a  $\mathbb{R}$  de  $\mathbb{Q}$ . Se le conoce como *axioma de completitud*, que nosotros definiremos en términos de cotas.

**Definición 5.1.** A un número  $x \in \mathbb{R} \setminus \mathbb{Q}$  se le llama *irracional*.

**Definición 5.2.** Un conjunto no vacío  $\mathcal{S}$  de números reales se dice *acotado por arriba* si hay  $C \in \mathbb{R}$  tal que  $x \leq C$  para todo  $x \in \mathcal{S}$ . A  $C$  se le llama *cota superior* de  $\mathcal{S}$ . Si hay  $c \in \mathbb{R}$  tal que  $x \geq c$  para todo  $x \in \mathcal{S}$ , se dice *acotado por abajo* y a  $c$  se le llama *cota inferior* de  $\mathcal{S}$ . Si  $\mathcal{S}$  es acotado por abajo y por arriba, se dice *acotado*.

Por ejemplo,  $\mathbb{N}$  es acotado por abajo pero no por arriba (cosa que demostraremos en el teorema 5.3), el conjunto  $\mathbb{Q}$  no tiene cota inferior ni superior, mientras  $\{x \in \mathbb{R}: 1 < x \leq 3\}$  es acotado.

**Axioma (Supremo).** *Sea  $\mathcal{S} \subseteq \mathbb{R}$  no vacío, acotado por arriba. Entonces existe  $M \in \mathbb{R}$  tal que*

(a)  $M$  es cota superior de  $\mathcal{S}$ .

(b) Para todo  $\epsilon > 0$  hay  $s \in \mathcal{S}$  tal que  $s > M - \epsilon$ .

Esto dice que no pueden haber cotas superiores menores que  $M$ , y asegura que  $M$  es un número real.

**Definición 5.3.** A  $M$  se le llama el *supremo* (o mínima cota superior) de  $\mathcal{S}$ , se anota  $M = \sup \mathcal{S}$ .

El axioma del supremo puede expresarse en la forma obviamente equivalente:

**Axioma (Ínfimo).** Sea  $\mathcal{S} \subseteq \mathbb{R}$  no vacío, acotado por abajo. Entonces existe  $m \in \mathbb{R}$  tal que

- (a)  $m$  es cota inferior de  $\mathcal{S}$ .
- (b) Para todo  $\epsilon > 0$  hay  $s \in \mathcal{S}$  tal que  $s > m + \epsilon$ .

**Definición 5.4.** A este  $m$  se le llama *ínfimo* (máxima cota inferior) de  $\mathcal{S}$ , se anota  $m = \inf \mathcal{S}$ .

Como un ejemplo, demostraremos que  $\sqrt{2}$  es real, y por tanto irracional.

**Teorema 5.2.** Hay un real positivo  $r$  que cumple  $r^2 = 2$ .

*Demostración.* Sea  $\mathcal{S} = \{x \in \mathbb{R} : x^2 < 2\}$ . Entonces  $\mathcal{S}$  no es vacío, ya que  $1^2 < 2$ ; y tiene a 2 como cota superior, ya que si  $x > 2$  entonces  $x^2 > 4 > 2$ . Por el axioma del supremo, hay  $r \in \mathbb{R}$  tal que  $r = \sup \mathcal{S}$ . Claramente  $r > 0$ , ya que  $1 \in \mathcal{S}$ . Demostraremos por contradicción que  $r^2 = 2$ . Supongamos  $r^2 \neq 2$ . Por el axioma O1, debe ser entonces  $r^2 < 2$  o  $r^2 > 2$ . Para demostrar que estas no se cumplen, basta exhibir un  $\epsilon > 0$  para cada caso para el cual falla. Por turno:

**$r^2 < 2$ :** Sea  $\epsilon > 0$  y consideremos:

$$(r + \epsilon)^2 = r^2 + 2r\epsilon + \epsilon^2 < r^2 + (2r + 1)\epsilon \quad (5.1)$$

Si ahora  $\epsilon < (2 - r^2)/(2r + 1)$ , la última expresión en (5.1) es menor a 2, lo que contradice la elección de  $r$  como supremo.

**$r^2 > 2$ :** Para  $\epsilon > 0$  calculamos:

$$(r - \epsilon)^2 = r^2 - 2r\epsilon + \epsilon^2 > r^2 - 2r\epsilon \quad (5.2)$$

Si elegimos  $\epsilon < (r^2 - 2)/(2r)$ , la última expresión de (5.2) es mayor a 2, nuevamente contradiciendo la elección de  $r$  como supremo.

En consecuencia, debe ser  $r^2 = 2$ . □

Algunas consecuencias de la completitud de los reales son las siguientes.

**Teorema 5.3** (Propiedad arquimediana). *Para todo  $x \in \mathbb{R}$  hay  $n \in \mathbb{N}$  tal que  $n > x$ .*

*Demostración.* La demostración es por contradicción. Supongamos que  $x \in \mathbb{R}$ , y que para todo  $n \in \mathbb{N}$  es  $n \leq x$ . Entonces  $x$  es una cota superior para  $\mathbb{N}$ , y el conjunto  $\mathbb{N}$  tiene un supremo por completitud, sea  $M = \sup \mathbb{N}$ . Así  $M \geq n$  para  $n \in \mathbb{N}$ , en particular es  $M \geq n$  para  $n = 2, 3, 4, \dots$ . Pero cada número natural (salvo 1) es el sucesor de un número natural, con lo que  $M \geq k + 1$  para  $k = 1, 2, 3, \dots$ , o  $M - 1 \geq k$  para todo  $k \in \mathbb{N}$ . Pero habíamos elegido  $M$  como el supremo de  $\mathbb{N}$ , no puede tener cotas superiores menores. □

Esta demostración completa nuestra aseveración anterior que  $\mathbb{N}$  no tiene cota superior.

**Teorema 5.4.** Los racionales e irracionales son densos en  $\mathbb{R}$ , o sea entre cada par de reales distintos hay un racional y un irracional.

*Demostración.* Supongamos  $x, y \in \mathbb{R}$ , con  $x < y$ . Primero hay  $r \in \mathbb{Q}$  tal que  $x < r < y$ . Supongamos  $x > 0$  por ahora. Por la propiedad arquimediana, teorema 5.3, existe  $b \in \mathbb{N}$  tal que  $b > (y - x)^{-1}$ , de manera que  $b(y - x) > 1$ . Por la propiedad arquimediana existe  $n \in \mathbb{N}$  tal que  $n > bx$ , con lo que el conjunto  $\mathcal{S} = \{n \in \mathbb{N}: n > bx\}$  no es vacío, y por el axioma N4 contiene su mínimo, llamémosle  $a$ . Entonces  $a - 1 \leq bx$ : Si fuera  $a = 1$ ,  $a - 1 = 0 < bx$ ; en caso contrario  $a - 1 > bx$  contradice la elección de  $a$  como mínimo. Se sigue:

$$bx < a = (a - 1) + 1 < bx + b(y - x) = by$$

de forma que:

$$x < a \cdot b^{-1} < y$$

Veamos ahora el caso  $x \leq 0$ . Por la propiedad arquimediana, existe  $k \in \mathbb{N}$  tal que  $k > -x$ , de manera que  $k + x > 0$ . Por lo anterior, hay  $s \in \mathbb{Q}$  tal que  $x + k < s < y + k$ , y  $x < s - k < y$  donde  $s - k \in \mathbb{Q}$ .

Para hallar un irracional entre  $x$  e  $y$ , vemos por lo anterior que hay  $r_1 \in \mathbb{Q}$  tal que  $x < r_1 < y$ ; de la misma forma hay  $r_2 \in \mathbb{Q}$  tal que  $r_1 < r_2 < y$ . Como  $1 < \sqrt{2} < 2$ , es:

$$x < r_1 < r_1 + (r_2 - r_1)/\sqrt{2} < r_2 < y$$

y  $r_1 + (r_2 - r_1)/\sqrt{2}$  claramente es irracional. □

## 6 Numerabilidad

---

La manera más básica de contar es construir una biyección entre dos conjuntos, que de esa forma tienen la misma cardinalidad (“número de elementos”). Por ejemplo, para determinar si en una sala hay tantos asistentes como sillas basta solicitar que todos se sienten. Si no sobran sillas vacías ni quedan personas de pie, hay tantas personas como sillas.

Nuestro interés está en la existencia de diferentes infinitos, en particular la demostración de Cantor de que hay más números reales que enteros. No haremos uso de esto en el texto presente, pero los conceptos y las técnicas de demostración usadas muestran ser centrales en el estudio de la computabilidad (los límites de lo que un algoritmo puede hacer).

### 6.1. Cardinalidad

Ya indicamos que la manera fundamental de asignar un “tamaño” a un conjunto es hallar una correspondencia con un conjunto prototipo. Si los conjuntos son finitos, esta operación es conocida; buscamos extender la definición a conjuntos infinitos de forma de poder razonar sobre ellos.

**Definición 6.1.** La *cardinalidad* del conjunto  $\{1, 2, \dots, n\}$  con  $n \in \mathbb{N}$  es  $n$ . La cardinalidad de  $\emptyset$  es 0. Un conjunto cuya cardinalidad es  $n \in \mathbb{N}_0$  se dice *finito*.

A partir de aquí podemos definir igualdad de cardinalidades mediante biyecciones, incluso para conjuntos infinitos. Anotaremos  $|\mathcal{A}|$  para la cardinalidad del conjunto  $\mathcal{A}$ . Formalmente:

**Definición 6.2.** Dos conjuntos  $\mathcal{A}$  y  $\mathcal{B}$  tienen la misma cardinalidad, lo que se anota  $|\mathcal{A}| = |\mathcal{B}|$ , si hay una biyección  $\phi: \mathcal{A} \rightarrow \mathcal{B}$ . Decimos que  $|\mathcal{A}| \leq |\mathcal{B}|$  si hay una inyección  $\gamma: \mathcal{A} \rightarrow \mathcal{B}$ . Si  $|\mathcal{A}| \leq |\mathcal{B}|$  pero no existe biyección entre  $\mathcal{A}$  y  $\mathcal{B}$ , decimos  $|\mathcal{A}| < |\mathcal{B}|$ .

Las notaciones indicadas son sugerentes. El lector confirmará que corresponden a las relaciones indicadas en caso que los conjuntos sean finitos. Para justificarlas en general debemos demostrar que la igualdad de cardinalidades es una relación de equivalencia. El que la función identidad es una biyección provee reflexividad, como la función inversa de una biyección es una biyección da simetría y ya que la composición de biyecciones es una biyección es transitiva. Además debemos verificar que  $|\mathcal{A}| \leq |\mathcal{B}|$  es una relación de orden (es transitiva, reflexiva y simétrica bajo el entendido de la igualdad de cardinalidades). La reflexividad es obvia, la función identidad es una inyección. La transitividad es simple, ya que la composición de inyecciones es una inyección (ver el punto 1 del teorema 2.2). Demostrar simetría es más complejo, es el tema de nuestro siguiente teorema. Como ya es costumbre, fue primeramente demostrado por Dedekind, quien no aparece entre los créditos. La demostración que mostramos se debe a Julius König.

**Teorema 6.1** (Cantor-Bernstein-Schröder). *Si hay inyecciones  $f: \mathcal{A} \rightarrow \mathcal{B}$ , y  $g: \mathcal{B} \rightarrow \mathcal{A}$ , entonces hay una biyección entre  $\mathcal{A}$  y  $\mathcal{B}$ .*

*Demostración.* Sin pérdida de generalidad podemos suponer que  $\mathcal{A}$  y  $\mathcal{B}$  son disjuntos. Partiendo de un elemento  $a \in \mathcal{A}$  cualquiera, podemos definir una secuencia en  $\mathcal{A}$  y  $\mathcal{B}$  en ambas direcciones aplicando repetidas veces  $f$  y  $g$ , y  $f^{-1}$  y  $g^{-1}$  donde estén definidas:

$$\dots \rightarrow f^{-1}(g^{-1}(a)) \rightarrow g^{-1}(a) \rightarrow a \rightarrow f(a) \rightarrow g(f(a)) \rightarrow \dots$$

Por ser inyectivas (no hay preimágenes repetidas), esta es una cadena. Cada elemento de  $\mathcal{A} \cup \mathcal{B}$  pertenece a exactamente una cadena, esto define una partición de  $\mathcal{A} \cup \mathcal{B}$  (y en consecuencia de ambos conjuntos). Uniendo biyecciones construidas para cada una de las particiones obtenemos una biyección entre  $\mathcal{A}$  y  $\mathcal{B}$ . Una cadena puede ser:

**Infinita en ambas direcciones:** En este caso,  $f$  es una biyección.

**Es un ciclo:** Nuevamente,  $f$  es una biyección.

**Termina en  $\mathcal{A}$ :** También en este caso  $f$  es una biyección

**Termina en  $\mathcal{B}$  pero no en  $\mathcal{A}$ :** En este caso  $g$  define una biyección

Tenemos la biyección prometida. □

Estudiaremos los conjuntos infinitos en algo más de detalle, partiendo por  $\mathbb{N}$ .

**Definición 6.3.** Un conjunto  $\mathcal{X}$  se dice *infinito numerable* si hay una biyección entre  $\mathcal{X}$  y  $\mathbb{N}$ . Un conjunto se llama *numerable* si es finito o es infinito numerable.

Esta definición dice que si  $\mathcal{X}$  es infinito numerable, entonces podemos escribir  $\mathcal{X} = \{x_1, x_2, \dots\}$ , bajo el entendido que existe la biyección  $\phi: \mathcal{X} \rightarrow \mathbb{N}$  con  $\phi(x_n) = n$  para cada  $n \in \mathbb{N}$ . Asimismo, un conjunto es numerable si hay una biyección entre él y un subconjunto de  $\mathbb{N}$ .

Acostumbramos distinguir objetos por un *índice*. Esto no es más que una función entre el conjunto índice  $\mathcal{I}$  y el conjunto de objetos  $\mathcal{A}$ , claro que se anota de forma particular:  $i \mapsto a_i$ . Típicamente el conjunto índice  $\mathcal{I}$  es un rango de los naturales, pero nada impide usar índices tomados de otros conjuntos.

**Teorema 6.2.** *La unión numerable de conjuntos numerables es numerable.*

*Demostración.* Sea  $\mathcal{I}$  un conjunto índice numerable, tal que para cada  $i \in \mathcal{I}$  el conjunto  $\mathcal{X}_i$  es numerable. Entonces  $\mathcal{I}$  es finito o es infinito numerable. Consideraremos solo el segundo caso, el primero requiere modificaciones menores.

Como  $\mathcal{I}$  es infinito numerable, hay una biyección entre  $\mathcal{I}$  y  $\mathbb{N}$ , con lo que podemos adoptar  $\mathbb{N}$  como conjunto índice sin pérdida de generalidad. Definamos:

$$\mathcal{X} = \bigcup_{n \in \mathbb{N}} \mathcal{X}_n$$

Si  $\mathcal{X}$  es finito, es numerable y estamos listos.

El otro caso a considerar es que  $\mathcal{X}$  sea infinito. Como para todo  $n \in \mathbb{N}$  el conjunto  $\mathcal{X}_n$  es numerable, podemos escribir  $\mathcal{X}_n = \{x_{n1}, x_{n2}, \dots\}$ . Con la convención que si  $\mathcal{X}_n$  es finito la secuencia  $\langle x_{n1}, x_{n2}, x_{n3}, \dots \rangle$  simplemente repite los elementos de  $\mathcal{X}_n$ , podemos escribir la matriz doblemente infinita:

$$\begin{array}{cccc} x_{11} & x_{12} & x_{13} & \dots \\ x_{21} & x_{22} & x_{23} & \dots \\ x_{31} & x_{32} & x_{33} & \dots \\ \vdots & \vdots & \vdots & \ddots \end{array}$$

Esta matriz podemos recorrerla diagonalmente, listando elementos  $x_{ij}$  en orden de  $i + j$  creciente: Primero  $x_{11}$ , luego  $x_{12}$  y  $x_{21}$ , después  $x_{13}$ ,  $x_{22}$  y  $x_{31}$ , y así sucesivamente, omitiendo elementos ya listados. Este recorrido numera todos los elementos de  $\mathcal{X}$ , construye una biyección entre  $\mathbb{N}$  y  $\mathcal{X}$ .  $\square$

**Teorema 6.3.** *Todo subconjunto de un conjunto numerable es numerable.*

*Demostración.* Sea  $\mathcal{X}$  un conjunto numerable. Si  $\mathcal{X}$  es finito, la conclusión es inmediata. Supongamos entonces  $\mathcal{X}$  infinito numerable, e  $\mathcal{Y} \subseteq \mathcal{X}$ . Si  $\mathcal{Y}$  es finito, estamos listos. Supongamos entonces que  $\mathcal{Y}$  es infinito. Definimos la secuencia  $\langle n_1, n_2, \dots \rangle$  mediante:

$$\begin{aligned} n_1 &= \min\{n \in \mathbb{N}: x_n \in \mathcal{Y}\} \\ n_k &= \min\{n \in \mathbb{N}: n > n_{k-1} \wedge x_n \in \mathcal{Y}\} \end{aligned}$$

La secuencia  $\langle n_k \rangle_{k \geq 1}$  define una biyección entre  $\mathbb{N}$  e  $\mathcal{Y}$  (asocia un índice  $k$  con cada elemento de  $\mathcal{Y}$ ).  $\square$

Llegamos así a los resultados más importantes que veremos acá.

**Teorema 6.4.** *El conjunto  $\mathbb{Z}$  es numerable.*

*Demostración.* Tenemos la unión de tres conjuntos numerables:

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-1, -2, -3, \dots\}$$

$\square$

**Teorema 6.5.** *El conjunto  $\mathbb{Q}$  es numerable.*

*Demostración.* Podemos representar  $r \in \mathbb{Q}$  como  $r = a/b$ , con  $a \in \mathbb{Z}$  y  $b \in \mathbb{N}$ . El conjunto de fracciones con denominador  $b$  es numerable (hay una biyección obvia con  $\mathbb{Z}$ , y por el teorema 6.4 éste es numerable), y la colección de tales conjuntos es numerable. Por el teorema 6.2, su unión  $\mathbb{Q}$  es numerable.  $\square$

**Teorema 6.6 (Cantor).** *El conjunto  $\mathbb{R}$  no es numerable.*

*Demostración.* La demostración es por contradicción. En vista del teorema 6.3, basta demostrar que  $[0, 1]$  no es numerable. Supongamos entonces que hay una biyección entre  $[0, 1]$  y  $\mathbb{N}$ . Un número  $x \in [0, 1]$  puede expresarse en notación decimal como  $0.d_1 d_2 d_3 \dots$ , donde  $0 \leq d_i \leq 9$  son los dígitos correspondientes de su expansión decimal. Ponemos la condición adicional que la expansión no es solo nueves a partir de un punto dado, para evitar ambigüedades. Con la biyección supuesta tendremos una matriz en que  $d_{ij}$  corresponde al  $j$ -ésimo dígito del  $i$ -ésimo número, llamémosle  $x_i$ :

$$\begin{aligned} 1: & \quad d_{1,1} \, d_{1,2} \, d_{1,3} \, d_{1,4} \, d_{1,5} \, d_{1,6} \, d_{1,7} \, d_{1,8} \, d_{1,9} \, d_{1,10} \dots \\ 2: & \quad d_{2,1} \, d_{2,2} \, d_{2,3} \, d_{2,4} \, d_{2,5} \, d_{2,6} \, d_{2,7} \, d_{2,8} \, d_{2,9} \, d_{2,10} \dots \\ \vdots & \quad \vdots \\ n: & \quad d_{n,1} \, d_{n,2} \, d_{n,3} \, d_{n,4} \, d_{n,5} \, d_{n,6} \, d_{n,7} \, d_{n,8} \, d_{n,9} \, d_{n,10} \dots \\ \vdots & \quad \vdots \end{aligned}$$

Consideremos el número  $y = 0.v_1 v_2 v_3 \dots$ , cuyos dígitos se definen por:

$$v_i = \begin{cases} 2 & \text{si } d_{ii} = 1 \\ 1 & \text{si } d_{ii} \neq 1 \end{cases}$$

Claramente  $y \in [0, 1]$ , no tiene solo nueves a partir de una posición dada (no es simplemente una manera alternativa de escribir un número), y difiere al menos en el dígito  $i$ -ésimo de  $x_i$ , el  $i$ -ésimo número de la lista (se definió de forma que  $v_i \neq d_{ii}$ ). Esto significa que  $y$  no está en esta lista que supuestamente los contiene a todos. Esta contradicción completa la demostración.  $\square$

Alguna variante de este argumento diagonal se usa en muchas demostraciones relacionadas a conjuntos infinitos.

Nótese que el conjunto  $\mathbb{R} \setminus \mathbb{Q}$  no es numerable, con lo que en cierto sentido hay más números irracionales que racionales. Incluso más: Un número se llama *algebraico* si es un cero de un polinomio con coeficientes enteros. Entonces:

**Teorema 6.7** (Cantor). *El conjunto de números reales algebraicos es numerable.*

*Demostración.* Dado un polinomio  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ , su *altura* es  $n + |a_n| + |a_{n-1}| + \dots + |a_0|$ . Hay un número finito de polinomios de cada altura y un polinomio de grado  $n$  tiene a lo más  $n$  raíces reales (esto lo demostraríamos en el capítulo 9), con lo que hay un número finito de números algebraicos reales de cada altura. Los números algebraicos son entonces una unión numerable de conjuntos numerables, y por tanto numerables.  $\square$

Los números reales no algebraicos se llaman *trascendentes*. Euler ya sospechó su existencia, la demostración anterior indica que hay muchos más números trascendentes que algebraicos, pero no exhibe ninguno.

Un importante teorema es el siguiente:

**Teorema 6.8** (Cantor).  $|\mathcal{A}| < |2^{\mathcal{A}}|$

*Demostración.* Por contradicción. Sea  $f: \mathcal{A} \rightarrow 2^{\mathcal{A}}$  una función cualquiera, construimos un conjunto  $\mathcal{T} \in 2^{\mathcal{A}}$  que no es imagen de ningún  $\alpha \in \mathcal{A}$ , con lo que  $f(\cdot)$  no puede ser una biyección por no ser sobre. Para todo  $\alpha \in \mathcal{A}$ , debe ser  $\alpha \in \mathcal{T}$  o  $\alpha \notin \mathcal{T}$ . Sea  $\mathcal{T} = \{\alpha \in \mathcal{A}: \alpha \notin f(\alpha)\}$ . Si  $\alpha \in \mathcal{T}$ , entonces  $\alpha \notin f(\alpha)$ , de forma que  $f(\alpha) \neq \mathcal{T}$ . Por el otro lado, si  $\alpha \notin \mathcal{T}$ , entonces  $\alpha \in f(\alpha)$ , y nuevamente  $f(\alpha) \neq \mathcal{T}$ . La función  $f$  no es sobre ya que su rango no incluye a  $\mathcal{T}$ , no puede ser biyección.  $\square$

Esto es nuevamente el argumento diagonal que usamos para demostrar el teorema 6.6. Este teorema demuestra que hay infinitas cardinalidades mayores que la de  $\mathbb{N}$ .

Resulta que el conjunto de subconjuntos *finitos* de un conjunto numerable es numerable. Si el conjunto universo es finito, el conjunto de sus subconjuntos es finito, y por tanto numerable. Si el conjunto universo es infinito, sin pérdida de generalidad podemos tomarlo como  $\mathbb{N}$ . Los conjuntos  $S_n = 2^{[1,n]}$  son todos finitos, y la unión de todos ellos es la unión numerable de conjuntos numerables.

Vemos también que rangos abiertos y cerrados de  $\mathbb{R}$  tienen la misma cardinalidad: Por ejemplo, como entre  $(0, 1)$  y  $[0, 1]$  tenemos las inyecciones  $x \mapsto x$  e  $y \mapsto (y+1)/3$ , por el teorema 6.1 tienen la misma cardinalidad. Con la biyección  $x \mapsto (x+a)/(b-a)$  entre  $[0, 1]$  y  $[a, b]$  todos los rangos finitos tienen la misma cardinalidad. La biyección  $x \mapsto \tanh x$  entre  $\mathbb{R}$  y  $(-1, 1)$  muestra que rangos infinitos comparten la misma cardinalidad de rangos finitos.

Lo que sí resulta sorprendente es que  $\mathbb{R}$  y  $\mathbb{C}$  tienen la misma cardinalidad, e incluso en general  $|\mathbb{R}| = |\mathbb{R}^n|$  para  $n \geq 1$ . Para ilustrar la demostración general, mostraremos una biyección entre  $(0, 1]$  y el cuadrado  $0 < x, y \leq 1$ . Representamos  $z \in (0, 1]$  mediante su expansión decimal que no termina (en vez de 0,5 escribimos 0,49). Dividimos  $z$  en el par  $(x, y)$  en  $(0, 1]$  por la vía de cortar la expansión de  $z$  en grupos de ceros y el dígito que sigue. Vale decir, si  $z = 0,1003049\dots$  obtenemos  $x = 0,104\dots$  e  $y = 0,0039\dots$ . Como la expansión decimal de  $z$  no termina en una secuencia infinita de ceros, siempre tendremos dónde cortar para el siguiente; las expansiones resultantes para  $x$  e  $y$  nunca terminan en secuencias infinitas de ceros. Esto provee una biyección entre un rango finito y un cuadrado finito, podemos extender ambos como antes. La misma idea puede usarse para  $n$  mayor.

## 7 Teoría de números

---

El estudio de los números enteros tiene una larga y distinguida historia, algo de la cual describe Ore [275]. La importancia de la teoría de números en informática es porque mucho de lo que se hace en el computador es trabajar con números (o cosas que se representan como tales, o debemos contar objetos con ciertas características para determinar los recursos que se requieren). Mucha de la tecnología criptográfica moderna se basa en resultados de la teoría de números y áreas afines. Nuestra presentación sigue la de Richman [300] en que explícitamente discute las estructuras algebraicas involucradas.

### 7.1. Algunas herramientas

Para calcular con números grandes resulta cómodo el programa `bc` (1), para computaciones más complejas son útiles `PARI/GP` [278] o `maxima` [251]. El sistema `Sage` [339] agrupa varios sistemas para computación numérica y simbólica (incluyendo los mencionados) de código abierto bajo una interfaz común. Para uso en programas se recomiendan las bibliotecas `GMP` [151], `CLN` [157] o `NTL` [324]. Detalles de muchos algoritmos en C++ da Arndt [19].

### 7.2. Propiedades básicas

La parte más interesante de la estructura de los números enteros viene dada por la multiplicación (y en consecuencia divisibilidad). Ya sabemos (ver el capítulo 2) que la relación “divide a” es una relación de orden en  $\mathbb{N}$  (en  $\mathbb{Z}$  no es antisimétrica, ya que por ejemplo  $-3 \mid 3$  y  $3 \mid -3$ , pero  $3 \neq -3$ ). Algunas propiedades adicionales son:

1. Si  $a \mid b$  y  $a \neq b$  entonces  $a < b$ , ya que en tal caso  $b = ma$  con  $m > 1$ .
2. Si  $a \mid b$ , entonces  $a \mid b \cdot c$
3. Si  $a \mid b$  y  $a \mid c$ , entonces  $a \mid (sb + tc)$  para todo  $s, t \in \mathbb{Z}$
4. Siempre que  $c \neq 0$ ,  $a \mid b$  si y solo si  $ac \mid bc$

Si  $a \mid b$ , decimos que  $b$  es *múltiplo* de  $a$ , o que  $a$  es un *factor* o un *divisor* de  $b$ .

Una propiedad básica de los enteros es la siguiente:

**Teorema 7.1** (Algoritmo de división). *Sean  $n, d \in \mathbb{Z}$  con  $d > 0$ . Entonces existen enteros  $q, r$  únicos tales que:*

$$n = q \cdot d + r \quad 0 \leq r < d$$

A  $d$  se le llama *divisor*, a  $q$  se le llama *cociente* mientras  $r$  es el *resto*.

*Demostración.* El conjunto de “restos” es:

$$\mathcal{R} = \{n - sd : s \in \mathbb{Z} \wedge n - sd \geq 0\} \quad (7.1)$$

Este conjunto no es vacío, siempre será  $n + (|n| + 1) \cdot d > 0$ , y esto está en  $\mathcal{R}$ . Siendo  $\mathcal{R}$  un conjunto de enteros acotado por debajo, contiene su mínimo, llamémosle  $r$ , que podemos expresar  $r = n - q \cdot d$ . Debemos demostrar que  $r < d$ . Esto lo haremos por contradicción. Si suponemos  $r \geq d$ , podemos escribir:

$$r - d = n - (q + 1) \cdot d$$

donde  $r - d \geq 0$ , pertenece a  $\mathcal{R}$  y es menor que  $r$ , contradiciendo la elección de  $r$  como el menor elemento en  $\mathcal{R}$ .

Falta demostrar que  $q$  y  $r$  son únicos. Nuevamente procedemos por contradicción. Supongamos dos soluciones diferentes  $q_1, r_1$  y  $q_2, r_2$ , donde podemos tomar  $r_2 \geq r_1$  sin pérdida de generalidad. Entonces:

$$\begin{aligned} n &= q_1 \cdot d + r_1 \\ n &= q_2 \cdot d + r_2 \\ 0 &= (q_2 - q_1) \cdot d + (r_2 - r_1) \end{aligned} \quad (7.2)$$

Sabemos que  $0 \leq r_2 < d$  por lo anterior. Como asumimos  $r_1 \leq r_2$ , tenemos que  $0 \leq r_2 - r_1$ . Pero también, dado que  $0 \leq r_1 < d$ :

$$\begin{aligned} r_2 &< d \\ r_2 - r_1 &< d - r_1 \leq d \end{aligned}$$

En resumen, resulta:

$$0 \leq r_2 - r_1 < d \quad (7.3)$$

Pero de la ecuación (7.2) tenemos:

$$(q_1 - q_2) \cdot d = r_2 - r_1 \quad (7.4)$$

Como el lado izquierdo de (7.4) es divisible por  $d$  también lo es el derecho; pero por (7.3) esto es menor que  $d$ , y la única posibilidad es que sea cero. Concluimos que  $r_1 = r_2$ . Pero siendo cero el lado derecho de (7.4), y el izquierdo el producto de  $d$  y  $q_1 - q_2$ , concluimos que  $q_1 - q_2 = 0$ , o sea  $q_1 = q_2$ . Pero habíamos supuesto que  $(q_1, r_1) \neq (q_2, r_2)$ , contradicción que demuestra que  $q$  y  $r$  son únicos.  $\square$

Es común que queramos hablar del resto de la división, para ello introducimos la notación:

$$r = a \text{ mód } b$$

El cociente respectivo puede expresarse simplemente como:

$$q = \left\lfloor \frac{a}{b} \right\rfloor$$

No se requiere una notación especial para esto, se usa con menos frecuencia que el resto.

### 7.3. Máximo común divisor

Sean  $a, b \in \mathbb{Z}$ , y consideremos  $\mathcal{I} = \{ua + vb : u, v \in \mathbb{Z}\}$ . Si  $a = b = 0$ , entonces  $\mathcal{I} = \{0\}$ . En caso contrario, este conjunto no es vacío, y contiene elementos positivos (siempre es  $a^2 + b^2 \in \mathcal{I}$ ). Si uno de  $a$  o  $b$  se anula, es simplemente el conjunto de múltiplos del otro. Consideremos el mínimo elemento positivo de  $\mathcal{I}$ , llamémosle  $m$ . Entonces hay  $s, t \in \mathbb{Z}$  tales que:

$$m = sa + tb \quad (7.5)$$

Demostraremos que  $m$  divide a todos los elementos de  $\mathcal{I}$ .

Sea  $n \in \mathcal{I}$ , que significa  $n = s'a + t'b$  para algún  $s'$  y  $t'$ . Por el algoritmo de división:

$$n = qm + r \quad 0 \leq r < m \quad (7.6)$$

Pero:

$$\begin{aligned} n &= s'a + t'b \\ &= q(sa + tb) + r \\ r &= (s' - qs)a + (t' - qt)b \end{aligned}$$

con lo que  $r \in \mathcal{I}$ . Como  $m$  es el mínimo elemento positivo de  $\mathcal{I}$ , por (7.6) solo puede ser  $r = 0$ , y  $m \mid n$ ; e  $\mathcal{I}$  es el conjunto de los múltiplos de  $m$ . Como  $a$  y  $b$  pertenecen a  $\mathcal{I}$ ,  $m$  es un divisor común de ambos. Pero por otro lado, cualquier divisor de  $a$  y  $b$  debe dividir a  $m = sa + tb$ , con lo que  $m$  es el *máximo común divisor* entre  $a$  y  $b$ . Para completar la definición de esta función, el máximo común divisor entre  $a \neq 0$  y  $0$  es simplemente  $a$ , y definimos  $\gcd(0, 0) = 0$ . Este número lo anotaremos  $\gcd(a, b)$  (por *greatest common divisor* en inglés). Otra notación común es  $(a, b)$ . De (7.5) vemos que:

$$\gcd(a, b) = sa + tb \quad (7.7)$$

A la importante relación (7.7) se le llama *identidad de Bézout*. En caso que  $\gcd(a, b) = 1$  se dice que  $a$  y  $b$  son *relativamente primos* o *coprimos*.

Nótese que si se cumple (7.7) también son soluciones a  $\gcd(a, b) = s'a + t'b$  para todo  $k \in \mathbb{Z}$ :

$$\begin{aligned} s' &= s + \frac{kb}{\gcd(a, b)} \\ t' &= t - \frac{ka}{\gcd(a, b)} \end{aligned} \quad (7.8)$$

Esto es fácil de ver substituyendo (7.8).

**Lema 7.2.** *Tenemos las siguientes propiedades del máximo común divisor:*

1.  $\gcd(a, b) = \gcd(b, a)$
2.  $\gcd(a, b) = \gcd(\pm a, \pm b)$
3. *Todo divisor común de  $a$  y  $b$  divide a  $\gcd(a, b)$ .*
4.  $\gcd(ka, kb) = |k| \cdot \gcd(a, b)$ .
5. *Si  $m = \gcd(a, b)$ , entonces  $\gcd(a/m, b/m) = 1$ . Nótese que  $a/m$  y  $b/m$  son enteros acá, la división es exacta.*

6. Si  $\gcd(a, b) = 1$  y  $\gcd(a, c) = 1$ , entonces  $\gcd(a, bc) = 1$ .
7. Si  $a \mid bc$  y  $\gcd(a, b) = 1$ , entonces  $a \mid c$ .
8. Si  $\gcd(a, b) = 1$ , y  $a \mid c$  y  $b \mid c$ , entonces  $ab \mid c$ .

*Demostración.* Demostramos cada parte por turno.

1. Los elementos de  $\mathcal{I} = \{ua + vb : u, v \in \mathbb{Z}\}$  e  $\mathcal{I}' = \{ub + va : u, v \in \mathbb{Z}\}$  son los mismos, y lo son sus mínimos elementos positivos.
2. Nuevamente, los elementos del conjunto  $\mathcal{I}$  respectivo son los mismos para ambos lados de la ecuación.
3. Esto lo vimos antes.
4. De la identidad de Bézout sabemos que, absorbiendo el signo de  $k$  en ellos, hay  $s, t \in \mathbb{Z}$  tales que:

$$\begin{aligned}\gcd(ka, kb) &= s(|k| \cdot a) + t(|k| \cdot b) \\ &= |k| \cdot (sa + tb)\end{aligned}$$

En particular, este es el mínimo de todos los valores positivos que se pueden obtener eligiendo  $s, t \in \mathbb{Z}$ , por lo que  $sa + tb$  debe también ser el mínimo positivo de esta última expresión,  $sa + tb = \gcd(a, b)$ .

5. De la identidad de Bézout sabemos que hay  $s$  y  $t$  que dan  $m = \gcd(a, b)$  como:

$$\begin{aligned}m &= sa + tb \\ 1 &= s(a/m) + t(b/m)\end{aligned}$$

con lo que  $\gcd(a/m, b/m) = 1$ . Esto también implica que  $\gcd(s, t) = 1$ .

6. Si  $\gcd(a, b) = \gcd(a, c) = 1$  existen  $s, t, u, v \in \mathbb{Z}$  tales que:

$$\begin{aligned}1 &= sa + tb \\ 1 &= ua + vc\end{aligned}$$

Entonces:

$$\begin{aligned}tb &= 1 - sa \\ vc &= 1 - ua \\ tvbc &= 1 - (s + u)a + sua^2 \\ 1 &= (s + u - sua)a + (tv)bc\end{aligned}$$

Esto es el mínimo entero positivo, y por tanto es  $\gcd(a, bc)$ .

7.  $a \mid bc$  significa que existe  $k$  tal que  $bc = ka$ . Tenemos:

$$\begin{aligned}1 &= sa + tb \\ c &= sac + tbc \\ &= (sc + tk) \cdot a\end{aligned}$$

y esto último dice que  $a \mid c$ .

8. Existen  $x, y \in \mathbb{Z}$  tales que  $c = ax = by$ . Por la identidad de Bézout existen  $u, v \in \mathbb{Z}$  con:

$$\begin{aligned} au + bv &= 1 \\ acu + bcv &= c \\ abuy + abvx &= c \\ ab(uv + vx) &= c \end{aligned}$$

con lo que  $ab | c$ . □

Como ejemplo demostramos  $\gcd(x^2, y^2) = (\gcd(x, y))^2$ . Si  $\gcd(x, y) = 1$ , aplicando la propiedad (6) con  $a = x$ ,  $b = c = y$  tenemos  $\gcd(x, y^2) = 1$ . Repitiendo esto con  $a = y^2$  y  $b = c = x$  resulta  $\gcd(x^2, y^2) = 1$ . En realidad, podemos demostrar de la misma forma que  $\gcd(x^m, y^n) = 1$ , para  $m \geq 1$  y  $n \geq 1$ . Ahora, por (4), si  $x = ku$  y  $y = kv$ , donde  $k = \gcd(u, v)$  tendremos  $\gcd(u, v) = 1$ , y  $\gcd(x^2, y^2) = \gcd(k^2 u^2, k^2 v^2) = k^2 \cdot \gcd(u^2, v^2) = (\gcd(x, y))^2$ . Queda como ejercicio demostrar de forma similar que  $\gcd(x^m, y^m) = (\gcd(x, y))^m$ .

El máximo común divisor es muy importante, interesa obtener una forma de calcularlo eficientemente. De partida, sabemos que si  $m = \gcd(a, b)$ , entonces  $m | u \cdot a + v \cdot b$  para todo par  $u, v$ . En particular,  $m | a$  mód  $b$ , ya que  $a$  mód  $b = a - q \cdot b$ . Al revés, cualquier divisor común de  $a$  mód  $b$  y  $b$  divide a  $a = a$  mód  $b + qb$  y a  $b$ , y por lo tanto a su máximo común divisor. Así  $\gcd(a, b) = \gcd(b, a \text{ mód } b)$ . Esto lleva directamente al algoritmo de Euclides 7.1 (los 13 tomos de los *Elementos* de este alejandrino del siglo III AC incluyen teoría de números en los tomos 7 a 9). El algoritmo de Euclides de interés histórico también, es el algoritmo más antiguo que involucra ciclos, y fue el primer algoritmo cuyo rendimiento se analizó matemáticamente (por Gabriel Lamé en 1844). El análisis lo discutiremos en la sección 11.2.

---

Algoritmo 7.1: Algoritmo de Euclides para calcular  $\gcd(a, b)$

---

```
function gcd(a, b)
  while b > 0 do
    (a, b)  $\leftarrow$  (b, a mód b)
  end
  return a
```

---

Una función íntimamente relacionada con el máximo común divisor es el *mínimo común múltiplo*, que anotaremos  $\text{lcm}(a, b)$  (por *least common multiple* en inglés). Sea  $m$  un múltiplo común de  $a$  y  $b$ , vale decir  $m = ha = kb$ . Sean  $a = a_1 \gcd(a, b)$  y  $b = b_1 \gcd(a, b)$ , dividiendo la relación para  $m$  por  $\gcd(a, b)$  resulta  $ha_1 = kb_1$ . Como por el lema 7.2 parte 5 es  $\gcd(a_1, b_1) = 1$ , por la parte 7 debe ser  $a_1 | k$ , y obtenemos el mínimo cuando  $a_1 = k$ , vale decir:

$$\text{lcm}(a, b) = \frac{|ab|}{\gcd(a, b)} \tag{7.9}$$

Una aplicación simple de lo anterior es el siguiente teorema:

**Teorema 7.3** (Criterio de cero racional). *Sea  $p(x) = a_n x^n + \dots + a_0$  un polinomio de coeficientes enteros. Todo cero racional  $r = u/v$ , expresado en términos mínimos, de  $p(x)$  cumple  $u | a_0$  y  $v | a_n$ .*

*Demostración.* Sin pérdida de generalidad podemos suponer que los  $a_i$  no tienen factores en común, que  $a_n \neq 0$  y que  $a_0 \neq 0$ . Substituyendo  $u/v$  en  $p(x) = 0$ , y multiplicando por  $v^n$ , resulta:

$$a_n u^n + a_{n-1} u^{n-1} v + \dots + a_1 u v^{n-1} + a_0 v^n = 0$$

Observamos que todos los términos, salvo posiblemente el primero, son divisibles por  $v$ . En consecuencia, como la expresión completa es divisible por  $v$ , tiene que serlo el primer término, o sea  $v \mid a_n$ , ya que supusimos que  $u$  y  $v$  no tienen factores en común. Asimismo, todos los términos, salvo posiblemente el último, son divisibles por  $u$ . Por el mismo razonamiento anterior, la única forma que esto se puede cumplir es que  $u \mid a_0$ .  $\square$

El teorema 7.3 restringe los posibles ceros racionales del polinomio a un número finito. En el caso de polinomios mónicos (cuyo coeficiente del término de mayor grado es uno) vemos que los ceros son enteros de ser racionales. Esto da una manera adicional de demostrar que  $\sqrt{2}$  es irracional: Es cero de  $x^2 - 2$ , como  $\sqrt{2}$  no es entero, es irracional. Incluso más, toda raíz de un entero o es entera o es irracional, por un razonamiento similar.

### 7.3.1. Obtener los coeficientes de Bézout

Sabemos por la identidad de Bézout que existen enteros  $s, t$  tales que:

$$\gcd(a, b) = sa + tb$$

y encontrar estos es de interés también. Una manera de proceder es ir registrando paso a paso los valores en el algoritmo de Euclides, y luego ir reemplazando en reversa. Por ejemplo, para calcular  $\gcd(40902, 24140)$  hacemos:

$$\begin{aligned} 40902 &= 24140 \cdot 1 + 16762 \\ 24140 &= 16762 \cdot 1 + 7378 \\ 16762 &= 7378 \cdot 2 + 2006 \\ 7378 &= 2006 \cdot 3 + 1360 \\ 2006 &= 1360 \cdot 1 + 646 \\ 1360 &= 646 \cdot 2 + 68 \\ 646 &= 68 \cdot 9 + 34 \\ 68 &= 34 \cdot 2 + 0 \end{aligned}$$

Sabemos entonces que  $\gcd(40902, 24140) = 34$ . De lo anterior también tenemos que:

$$\begin{aligned} 34 &= 646 - 68 \cdot 9 \\ 68 &= 1360 - 646 \cdot 2 \\ 646 &= 2006 - 1360 \cdot 1 \\ 1360 &= 7378 - 2006 \cdot 3 \\ 2006 &= 16762 - 7378 \cdot 2 \\ 7378 &= 24140 - 16762 \cdot 1 \\ 16762 &= 40902 - 24140 \cdot 1 \end{aligned}$$

Substituyendo las expresiones para los restos finalmente obtenemos  $34 = 337 \cdot 40902 - 571 \cdot 24140$ .

Una manera de organizar mejor el trabajo es el algoritmo 7.2, debido a Blankinship [46]. Usa vectores auxiliares  $(x_1, x_2, x_3), (y_1, y_2, y_3)$  y  $(t_1, t_2, t_3)$ , que manipula de forma que siempre se cumple que:

$$\begin{aligned} x_1 a + x_2 b &= x_3 \\ y_1 a + y_2 b &= y_3 \\ t_1 a + t_2 b &= t_3 \end{aligned}$$

El algoritmo 7.2 es exactamente el mismo que el algoritmo 7.1 respecto de la manipulación de  $x_3$  e

---

Algoritmo 7.2: Algoritmo extendido de Euclides

---

```

function xgcd( $a, b$ )
   $(x_1, x_2, x_3) \leftarrow (1, 0, a)$ 
   $(y_1, y_2, y_3) \leftarrow (0, 1, b)$ 
  while  $y_3 \neq 0$  do
     $q \leftarrow \lfloor x_3 / y_3 \rfloor$ 
     $(t_1, t_2, t_3) \leftarrow (x_1, x_2, x_3) - q \cdot (y_1, y_2, y_3)$ 
     $(x_1, x_2, x_3) \leftarrow (y_1, y_2, y_3)$ 
     $(y_1, y_2, y_3) \leftarrow (t_1, t_2, t_3)$ 
  end
  return  $x_3 = x_1 \cdot a + x_2 \cdot b$ 

```

---

$y_3$ , con lo que calcula  $\text{gcd}(a, b)$  correctamente; por la relación que se mantiene entre  $a, b, x_1, x_2$  y  $x_3$  obtenemos los coeficientes de Bézout.

Podemos eliminar buena parte de la computación del algoritmo 7.2 si omitimos  $x_2, y_2$  y  $t_2$ , y obtenemos  $x_2$  de la relación  $x_1a + x_2b = x_3$  al final. Manejar los casos de  $a$  o  $b$  negativos queda de ejercicio.

La traza del algoritmo 7.2 para  $\text{gcd}(40\,902, 24\,140)$  da el cuadro 7.1. Tenemos nuevamente:

$x_1$	$x_2$	$x_3$	$y_1$	$y_2$	$y_3$	$q$
1	0	40902	0	1	24140	1
0	1	24140	1	-1	16762	1
1	-1	16762	-1	2	7378	2
-1	2	7378	3	-5	2006	3
3	-5	2006	-10	17	1360	1
-10	17	1360	13	-22	646	2
13	-22	646	-36	61	68	9
-36	61	68	337	-571	34	2
337	-571	34	-710	1203	0	

Cuadro 7.1 – Traza del algoritmo extendido de Euclides

$$\text{gcd}(40902, 24140) = 34 = 337 \cdot 40902 - 571 \cdot 24140$$

### 7.3.2. Números primos

Habíamos indicado que es de interés más que nada la factorización. Esto lleva a números que se comportan en forma especial con ella.

**Definición 7.1.** Un entero positivo  $p \geq 2$  se llama *primo* si siempre que  $p \mid ab$  es  $p \mid a$  o  $p \mid b$ .

Esto lo usamos al demostrar antes que  $\sqrt{2}$  es irracional (teorema 3.3): Si  $2 \mid a^2$ , debe ser  $2 \mid a$  ya que 2 es primo.

La definición más tradicional es que  $p$  es primo si sus únicos divisores positivos son 1 y  $p$ :

**Definición 7.2.** A un entero  $e$  se le llama *irreducible* si siempre que  $e = ab$  es  $a = \pm 1$  o  $b = \pm 1$ .

Resulta:

**Teorema 7.4.** *Si  $p$  es primo,  $p$  es irreducible.*

*Demostración.* Por contradicción. Supongamos  $p$  primo y reducible, con lo que podemos escribir  $p = ab$  para  $a \neq \pm 1$  y  $b \neq \pm 1$ . Así  $p \mid ab$ , con lo que por definición de primo  $p \mid a$  o  $p \mid b$ . Sin pérdida de generalidad, si  $p \mid a$  es  $a = mp$  para un entero  $m$ . Pero entonces:

$$p = ab = mpb$$

con lo que:

$$p(1 - mb) = 0$$

Como  $p \neq 0$ , esto significa que  $mb = 1$ , y  $b \mid 1$ , con lo que  $b = \pm 1$ , lo que contradice nuestra suposición sobre la factorización de  $p$ .  $\square$

El resultado converso, que los naturales irreducibles son primos, es más profundo.

**Teorema 7.5** (Lema de Euclides). *Si  $e$  es irreducible, es primo.*

*Demostración.* Por contradicción. Supongamos que  $e$  es irreducible, y que  $e$  divide a  $ab$ , pero no divide ni  $a$  ni  $b$ . Esto es:

$$\begin{aligned} \gcd(e, a) &= 1 \\ \gcd(e, b) &= 1 \end{aligned}$$

Sabemos que en tal caso hay enteros  $u, v, x, y$  tales que:

$$\begin{aligned} ue + va &= 1 \\ xe + yb &= 1 \end{aligned}$$

Multiplicando las últimas dos:

$$\begin{aligned} (ue + va)(xe + yb) &= uxe^2 + uybe + vaxe + vyab \\ &= 1 \end{aligned}$$

Todos los términos de la suma son divisibles por  $e$ , con lo que  $e \mid 1$ , lo que es absurdo en  $\mathbb{Z}$ .  $\square$

Esto justifica la definición tradicional de número primo, que realmente corresponde a irreducibles positivos.

Todo número natural se puede escribir como un producto de primos. Para demostrarlo usamos un truco bastante común: Nos fijamos en el mínimo supuesto contraejemplo y usamos contradicción.

**Teorema 7.6.** *Todo número natural se puede expresar como producto de números primos.*

*Demostración.* Por convención, 1 es el producto de cero primos.

Para números mayores a 1, la demostración es por contradicción. Llamémosle  $m$  al mínimo número que no es un producto de primos. Entonces  $m$  no puede ser primo, ya que de serlo sería el producto de primos (uno solo); así podemos escribir  $m = a \cdot b$ , donde  $1 < a, b < m$  y por tanto  $a$  y  $b$  son productos de primos. Pero entonces podemos escribir  $m$  como producto de primos, contrario a nuestra suposición de que tal cosa no era posible.  $\square$

Nuestro siguiente objetivo es demostrar que la factorización en primos es única. Un paso clave en esa dirección es:

**Lema 7.7.** Sea  $p$  primo y  $x_1, x_2, \dots, x_n$  enteros tales que  $p \mid x_1 x_2 \cdots x_n$ . Entonces  $p \mid x_i$  para algún  $i$ .

*Demostración.* Usamos inducción.

**Base:** Cuando  $n = 1$ , el supuesto se reduce a  $p \mid x_1$ , y el resultado es inmediato.

**Inducción:** Supongamos que el resultado es cierto para  $n$ , y queremos demostrar que es válido para  $n + 1$ . Tenemos  $p \mid x_1 \cdots x_n \cdot x_{n+1}$ . Por la definición de primo, es  $p \mid x_1 \cdots x_n$  o  $p \mid x_{n+1}$ . En el primer caso (por inducción)  $p \mid x_i$  para algún  $1 \leq i \leq n$ , en el segundo  $p \mid x_{n+1}$ . En resumen,  $p \mid x_i$  para algún  $1 \leq i \leq n + 1$ .  $\square$

**Teorema 7.8** (Teorema fundamental de la aritmética). *Todo entero positivo tiene una factorización única en números primos, salvo el orden de los factores.*

*Demostración.* El número 1 es un caso especial, se factoriza en cero primos.

Para los demás procedemos por contradicción, aplicando el mismo truco anterior. Si hay enteros para los que esto no es cierto, hay uno mínimo, llamémosle  $N$ . Vale decir, podemos escribir  $N = p_1 p_2 \cdots p_k$  y también  $N = q_1 q_2 \cdots q_l$ , donde los  $p_i$  son primos (no necesariamente distintos), y similarmente los  $q_j$ . Ahora bien, como  $p_1 \mid N$ , sabemos que  $p_1 \mid q_1 q_2 \cdots q_l$ , y por tanto  $p_1 \mid q_j$  para algún  $1 \leq j \leq l$ . Como  $q_j$  es primo, es irreducible y esto significa que  $p_1 = q_j$ . Pero entonces tenemos

$$N' = p_2 p_3 \cdots p_k = q_1 q_2 \cdots q_{j-1} q_{j+1} \cdots q_l$$

y  $N' < N$  también tendría dos factorizaciones diferentes, contrario a la elección de  $N$  como el mínimo natural con esa característica.  $\square$

Otro hecho fundamental fue demostrado primeramente por Euclides. De este importante resultado se da una variedad de bonitas demostraciones, basadas en conceptos totalmente diferentes, en Aigner y Ziegler [6]. Nuestra variante de la demostración clásica de Euclides se debe a Ernst Kummer.

**Teorema 7.9.** *Hay infinitos números primos.*

*Demostración.* Procedemos por contradicción. Supongamos que hay un número finito de primos,  $p_1, p_2, \dots, p_r$  en orden creciente, donde sabemos que  $r > 1$ . Consideremos:

$$N = p_1 p_2 \cdots p_r$$

El número  $N - 1$  es compuesto, ya que es mayor que  $p_r$  y no es primo (no aparece en nuestra lista). Luego tiene un factor primo  $p$ , y este factor lo tiene en común con  $N$ . Entonces  $p$  divide tanto a  $N$  como a  $N - 1$ , y divide a su diferencia, que es decir  $p \mid 1$ , lo que es absurdo.  $\square$

Incluso se puede demostrar más. El siguiente resultado se debe a Leonhard Euler, la brillante demostración siguiente es de Paul Erdős [115]. La importancia del mismo radica en que la divergencia de la serie da un indicio de la tasa de crecimiento de los números primos. Como dijo el mismo Euler, “hay más primos que cuadrados” (por el teorema 3.11 la serie de recíprocos de los cuadrados converge).

**Teorema 7.10.** *La serie*

$$\sum_p \frac{1}{p}$$

(donde la suma es sobre los números primos) *diverge*.

*Demostración.* Por contradicción. Enumeremos los primos como  $p_1, p_2, \dots$  en orden creciente. Si la serie converge, hay un punto a partir del cual la suma es menor que  $1/2$ , con lo que podemos escribir:

$$\sum_{i \geq k+1} \frac{1}{p_i} < \frac{1}{2}$$

Llamaremos *primos chicos* a  $p_1, p_2, \dots, p_k$  y *primos grandes* a  $p_{k+1}, p_{k+2}, \dots$ . Tomemos algún  $N > p_k$  a determinar más adelante, y llamemos  $N_1$  a la cantidad de números hasta  $N$  divisibles solo por primos chicos, y similarmente  $N_2$  los que tienen divisores grandes. Debe ser  $N = N_1 + N_2$ , pero dada la suposición de arriba veremos que podemos elegir  $N$  tal que al acotar  $N_1$  y  $N_2$  de forma suficientemente precisa concluimos que  $N_1 + N_2 < N$ .

Como  $\lfloor N/p \rfloor$  de los números entre 1 y  $N$  son divisibles por el primo  $p$  y  $\lfloor x \rfloor \leq x$ , tenemos que:

$$\begin{aligned} N_2 &\leq \sum_{i \geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor \\ &\leq \sum_{i \geq k+1} \frac{N}{p_i} \\ &= N \sum_{i \geq k+1} \frac{1}{p_i} \\ &< \frac{N}{2} \end{aligned} \tag{7.10}$$

Consideremos ahora los números menores que  $N$  que solo tienen factores primos chicos. Si tomamos uno cualquiera de ellos y le llamamos  $x$ , podemos escribir  $x = y \cdot z^2$ , donde  $y$  no es divisible por el cuadrado de ningún primo. Obviamente  $z^2 \leq N$ , con lo que hay a lo más  $\sqrt{N}$  valores posibles de  $z$ . Como hay  $k$  primos chicos, hay a lo más  $2^k$  posibles valores distintos de  $y$ . Esto da una sobre estimación bastante burda, pero suficiente para nuestras necesidades presentes:

$$N_1 \leq 2^k \cdot \sqrt{N} \tag{7.11}$$

Ahora queremos elegir  $N$  de forma que  $N_1 < N/2$ , o sea por la cota (7.11):

$$\begin{aligned} 2^k \cdot \sqrt{N} &< \frac{N}{2} \\ 2^{2k+2} &< N \end{aligned} \tag{7.12}$$

Combinando (7.12) con nuestra estimación (7.10), para el valor elegido de  $N$  tenemos:

$$N = N_1 + N_2 < \frac{N}{2} + \frac{N}{2} = N$$

Esto es ridículo. □

Nuevamente, si la serie diverge no puede tener finitos términos y hay infinitos números primos.

## 7.4. Congruencias

El concepto de *congruencia* está íntimamente relacionado con el resto de la división, e incluso usan notaciones similares. De todas formas es importante distinguirlos.

**Definición 7.3.** Sean  $a, b, m \in \mathbb{Z}$ , con  $m \neq 0$ . Definimos:

$$a \equiv b \pmod{m}$$

si  $m | a - b$ . Esto se expresa diciendo que  $a$  es congruente con  $b$  módulo  $m$ .

Esta es una relación de equivalencia:

**Reflexiva:** Si  $a = b$ , la definición se reduce a  $m | 0$ , lo que siempre es cierto.

**Simétrica:**  $a \equiv b$  (mód  $m$ ) significa que  $m | a - b$ , pero entonces  $m | b - a$ , que es decir  $b \equiv a$  (mód  $m$ ).

**Transitiva:**  $a \equiv b$  (mód  $m$ ) y  $b \equiv c$  (mód  $m$ ) significan  $m | a - b$  y  $m | b - c$ , que es  $a - b = k_1 m$  y  $b - c = k_2 m$ ; pero entonces  $a - c = (k_1 + k_2)m$ , o sea  $m | a - c$ , que es decir  $a \equiv c$  (mód  $m$ ).

Los siguientes teoremas dan algunas propiedades importantes.

**Teorema 7.11.** Sea  $m$  un entero positivo y sean  $x_1, x_2, y_1, y_2$  enteros tales que:

$$x_1 \equiv x_2 \pmod{m}$$

$$y_1 \equiv y_2 \pmod{m}$$

Entonces:

$$x_1 + y_1 \equiv x_2 + y_2 \pmod{m}$$

$$x_1 \cdot y_1 \equiv x_2 \cdot y_2 \pmod{m}$$

*Demostración.* Nos dieron que  $x_1 - x_2 = ma$ ,  $y_1 - y_2 = mb$ , para algunos  $x, y \in \mathbb{Z}$ . Entonces para la suma

$$\begin{aligned} (x_1 + y_1) - (x_2 + y_2) &= (x_1 - x_2) + (y_1 - y_2) \\ &= ma + mb \\ &= m(a + b) \end{aligned}$$

lo que es decir

$$x_1 + y_1 \equiv x_2 + y_2 \pmod{m}$$

Similarmente, para el producto:

$$\begin{aligned} x_1 y_1 - x_2 y_2 &= x_1 y_1 - x_2 y_1 + x_2 y_1 - x_2 y_2 \\ &= (x_1 - x_2) y_1 + x_2 (y_1 - y_2) \\ &= may_1 + x_2 mb \\ &= m(ay_1 + bx_2) \end{aligned}$$

con lo que

$$x_1 \cdot y_1 \equiv x_2 \cdot y_2 \pmod{m}$$

□

**Teorema 7.12.** Sean  $m, n$  enteros positivos. Entonces, si

$$a \equiv b \pmod{mn}$$

tenemos

$$a \equiv b \pmod{m}$$

$$a \equiv b \pmod{n}$$

Además, si

$$a \equiv b \pmod{m}$$

$$a \equiv b \pmod{n}$$

entonces

$$a \equiv b \pmod{\text{lcm}(m, n)}$$

En particular, si  $\gcd(m, n) = 1$ , entonces:

$$a \equiv b \pmod{mn}$$

*Demostración.* Para la primera aseveración, tenemos por definición que  $mn \mid a - b$ , pero en tal caso  $m \mid a - b$  y también  $n \mid a - b$ .

Para la segunda, tenemos que:

$$m \mid a - b$$

$$n \mid a - b$$

Como tanto  $m$  y  $n$  dividen a  $a - b$ , el mínimo común múltiplo lo divide:

$$\text{lcm}(m, n) \mid a - b$$

y obtenemos nuestro resultado. □

## 7.5. Aritmética en $\mathbb{Z}_m$

Para cualquier entero  $x$  y un entero positivo  $m$  anotaremos  $[x]_m$  para la clase de equivalencia de  $x$  en la relación de congruencia módulo  $m$ . Vale decir,  $[x]_m$  es el conjunto de todos los enteros  $x'$  tales que  $x - x'$  es múltiplo de  $m$ :

$$[5]_3 = \{\dots, -4, -1, 2, 5, 8, \dots\}$$

$$[-3]_7 = \{\dots, -10, -3, 4, 11, \dots\}$$

Sabemos que las clases de equivalencia partitionan  $\mathbb{Z}$ . Por ejemplo:

$$\mathbb{Z} = [0]_3 \cup [1]_3 \cup [2]_3$$

Para cualquier  $m$  dado, las clases son  $[0]_m, [1]_m, \dots, [m-1]_m$ , lo que sigue del algoritmo de división, ya que cualquier entero  $x$  puede expresarse como:

$$x = q \cdot m + r$$

con  $0 \leq r < m$ , y  $x \in [r]_m$  en tal caso. Esto motiva:

**Definición 7.4.** Sea  $m$  un entero positivo. El *conjunto de enteros módulo  $m$* , anotado  $\mathbb{Z}_m$ , es el conjunto de las clases de equivalencia  $[x]_m$ .

Vale decir,  $\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$ .

Cabe enfatizar que los elementos de  $\mathbb{Z}_m$  son subconjuntos de  $\mathbb{Z}$ , pero muchas veces resulta conveniente considerarlos como los enteros  $0, 1, \dots, m-1$  (aunque podríamos elegir otro conjunto de representantes si resulta conveniente) con una estructura aritmética diferente. A los elementos de  $\mathbb{Z}_m$  se les suele llamar *residuos* (módulo  $m$ ).

Definimos las operaciones:

$$[x]_m \oplus [y]_m = [x + y]_m$$

$$[x]_m \odot [y]_m = [x \cdot y]_m$$

Por nuestro teorema 7.11 estas operaciones están bien definidas.

**Teorema 7.13.** Sea  $m$  un entero positivo, y sean  $a, b, c \in \mathbb{Z}_m$  cualquiera. Para simplificar anotaremos  $0 = [0]_m$ ,  $1 = [1]_m$ . Entonces:

**G1:**  $a \oplus (b \oplus c) = (a \oplus b) \oplus c$

**G2:** Hay  $0 \in \mathbb{Z}_m$  tal que para todo  $a \in \mathbb{Z}_m$  se cumple  $a \oplus 0 = a$

**G3:** Para todo  $a \in \mathbb{Z}_m$  existe  $-a \in \mathbb{Z}_m$  tal que  $a \oplus (-a) = 0$

**G4:**  $a \oplus b = b \oplus a$

**R1:**  $(a \odot b) \odot c = a \odot (b \odot c)$

**R2:**  $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$  y  $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$

**R3:** Hay  $1 \in \mathbb{Z}_m$  tal que para todo  $a \in \mathbb{Z}_m$  se cumple  $a \odot 1 = 1 \odot a = a$

**R4:**  $a \odot b = b \odot a$

Hay una curiosa simetría entre G2 y R3, la definición de anillo generalmente indica también que  $a \oplus 0 = 0 \oplus a = a$ . Demostraremos esto en el teorema 7.17. Asimismo, suele agregarse que  $a \oplus (-a) = (-a) \oplus a = 0$ , lo que también sigue de las anteriores (teorema 7.16).

*Demostración.* Demostraremos algunas cosas, dejamos el resto a la imaginación del lector.

Para G4, sean  $a = [x]_m$  y  $b = [y]_m$ . Entonces:

$$\begin{aligned} a \oplus b &= [x]_m \oplus [y]_m \\ &= [x + y]_m \quad (\text{definición de } \oplus) \\ &= [y + x]_m \quad (\text{en } \mathbb{Z}) \\ &= [y]_m \oplus [x]_m \quad (\text{definición de } \oplus) \\ &= b \oplus a \end{aligned}$$

Para G3, tomamos  $-[x]_m = [-x]_m$ , que cumple lo solicitado. □

Si un conjunto  $G$  con una operación  $\oplus$  cumple G1 a G3 para algún elemento 0 se le llama *grupo*, y se anota  $\langle G, \oplus \rangle$ . Un grupo que cumple G4 es un *grupo conmutativo* o *abeliano*. Si es un grupo abeliano con  $\oplus$  y hay una segunda operación  $\odot$  y un elemento 1 que cumple con R1 hasta R3 se le llama *anillo*, y se anota  $\langle G, \oplus, \odot \rangle$ . Si además cumple R4 es un *anillo conmutativo*. Nuestro teorema afirma entonces que  $\mathbb{Z}_m$  con las operaciones  $\oplus$  y  $\odot$  es un anillo conmutativo. Cuidado, hay quienes omiten el axioma R3 al definir anillos, y le llaman *anillos con unidad* a lo que nosotros llamamos anillos.

En inglés algunos usan el nombre *ring* para nuestros anillos, y usan *rng* (por *ring* sin identidad). Asimismo, exigiremos que  $0 \neq 1$ , para evitar los casos especiales que produce un anillo con un único elemento. Para abreviar, generalmente solo se nombra el conjunto, omitiendo las operaciones como obvias. Así, en vez de hablar del grupo  $\langle \mathbb{Z}_m, \oplus \rangle$  o de los anillos  $\langle \mathbb{Z}_m, \oplus, \odot \rangle$  o  $\langle \mathbb{C}, +, \cdot \rangle$  se habla simplemente de  $\mathbb{Z}_m$  o  $\mathbb{C}$ , subentendiendo las operaciones tradicionales. Esto no debiera llevar a confusión. Temas como este son el ámbito del álgebra abstracta, para profundizar en ellos se recomienda el texto de Pinter [285] o el de Judson [190].

En el caso de grupos abelianos por convención se le llama o anota como “suma” a la operación, y al neutro se le designa con 0. Al inverso  $-a$  de la “suma” se le llama *inverso aditivo* en tal caso. Escribiremos  $a \ominus b = a \oplus (-b)$  para grupos abelianos. Por convención se anota como “multiplicación” la operación en grupos generales, al neutro se le llama 1 o  $e$  y el inverso de  $a$  en tal caso se anota  $a^{-1}$ .

Los elementos que llamamos 0 y 1 arriba (axiomas G2 y R3) no son necesariamente los enteros cero y uno, simplemente los usamos como nombres convenientes. Nótese que en el caso de grupos y anillos las operaciones son esenciales, debiera anotarse  $\langle R, + \rangle$  y  $\langle R, +, \cdot \rangle$  para explicitar las operaciones. Los elementos especiales resultan de las operaciones, no vale la pena nombrarlos. En anillos se anota  $-a$  para el inverso aditivo de  $a$  y  $a^{-1}$  para su inverso multiplicativo (si existe).

Generalmente se indica únicamente el conjunto.

Al número de elementos de un grupo o de un anillo  $R$  se le llama su *orden*, anotado  $|R|$ . Si un subconjunto del grupo es a su vez un grupo con la operación del caso se le llama *subgrupo*. De la misma forma podemos definir *subanillos*, claro que insistiremos en que incluyan a 1 para evitar que el subanillo tenga estructura incompatible con el anillo. Por ejemplo, en  $\mathbb{Z}_6$ , el subconjunto  $\{0, 3\}$  es cerrado respecto de suma y multiplicación, con neutro multiplicativo 3. Pero en  $\mathbb{Z}_6$  3 ni siquiera tiene inverso multiplicativo. Si  $A$  es subgrupo (o subanillo) de  $B$ , se anota  $A \leq B$ .

Un caso es el conjunto de un único elemento  $e$ , y definimos  $e = e \circ e$ . Por razones obvias se le llama el *grupo trivial*.

Otro grupo es el de las operaciones en el cubo de Rubik, que intercambian las posiciones de las caras de colores de los cubitos. Joyner [189] usa este juguete como excusa para introducir la teoría de grupos, y muestra cómo aplicarla para resolver este puzzle y otros similares.

Un ejemplo importante lo proveen las simetrías de objetos al moverse en el espacio. Por ejemplo, si consideramos un cuadrado (como el de la figura 7.1), tenemos las siguientes operaciones que lo

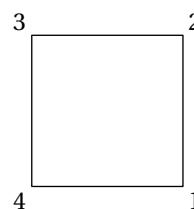


Figura 7.1 – Un cuadrado

hacen coincidir con su posición original. Podemos componer estas operaciones vía efectuar una y luego la otra. En otras palabras,  $ba$  describe aplicar  $a$  y luego  $b$ . Como una combinación de operaciones vuelve el cuadrado a su posición original (aunque intercambiando vértices), la composición es cerrada. Podemos describir las simetrías del cuadrado mediante dos operaciones básicas, rotación en  $\pi/4$  (la llamamos  $r$ ) y reflejo en el eje vertical (denominada  $s$ ). En total:

- No hacer nada (identidad,  $e$ ). Vemos que  $e = r^4 = s^2$ .
- Girar en sentido contra reloj en  $\pi/2, \pi, 3\pi/2$  ( $r, r^2$  y  $r^3 = r^{-1}$ ).

- Reflejar verticalmente ( $s$ ), horizontalmente ( $r^2 s$ ), y a través de las diagonales 1 3 y 2 4 ( $rs$  y  $r^3 s$ ).

Los elementos  $r$  y  $s$ , con los cuales podemos construir el grupo completo, se llaman sus *generadores*. Vemos en particular que  $srs = r^{-1}$ , o lo que es lo mismo  $sr = r^3 s$ . Esto ayuda a construir el cuadro 7.2, que describe al grupo conocido como  $D_8$ . Es D por *diedro*, el 8 por el número de operaciones del

$\circ$	$e$	$r$	$r^2$	$r^3$	$s$	$rs$	$r^2 s$	$r^3 s$
$e$	$e$	$r$	$r^2$	$r^3$	$s$	$rs$	$r^2 s$	$r^3 s$
$r$	$r$	$r^2$	$r^3$	$e$	$rs$	$r^2 s$	$r^3 s$	$s$
$r^2$	$r^2$	$r^3$	$e$	$r$	$r^2 s$	$r^3 s$	$s$	$rs$
$r^3$	$r^3$	$e$	$r$	$r^2$	$r^3 s$	$s$	$rs$	$r^2 s$
$s$	$s$	$r^3 s$	$r^2 s$	$rs$	$e$	$r^3$	$r^2$	$r$
$rs$	$rs$	$s$	$rs$	$r^2 s$	$r$	$e$	$r^3$	$r^2$
$r^2 s$	$r^2 s$	$rs$	$s$	$r^3 s$	$r^2$	$r$	$e$	$r$
$r^3 s$	$r^3 s$	$r^2 s$	$rs$	$s$	$r^3$	$r^2$	$r$	$e$

Cuadro 7.2 – El grupo  $D_8$

grupo. En general, el polígono regular de  $n$  lados da lugar al grupo denominado  $D_{2n}$ , hay  $n$  rotaciones y  $n$  reflexiones para un total de  $2n$  operaciones. Estos grupos no son comutativos.

Un poco más de la teoría elemental de grupos provee Chen [73, capítulo 4]. En particular, construye sistemáticamente todos los grupos de orden hasta 7. Resultados importantes son los siguientes:

**Teorema 7.14.** *El elemento neutro de un grupo es único.*

*Demostración.* Supongamos que en el grupo  $(G, \odot)$  los elementos  $a$  y  $b$  son ambos neutros. Entonces:

$$a = a \odot b = b$$

□

**Teorema 7.15** (Ley de cancelación). *Si  $a, b, c \in G$  son tales que  $a \odot c = b \odot c$ , entonces  $a = b$ .*

*Demostración.* Tenemos:

$$a = a \odot 1 = a \odot (c \odot c^{-1}) = (a \odot c) \odot c^{-1} = (b \odot c) \odot c^{-1} = b \odot (c \odot c^{-1}) = b$$

□

Puede aplicarse exactamente la misma técnica para demostrar cancelación a la izquierda.

**Teorema 7.16** (Mutualidad). *Si en un grupo  $a \odot b = 1$ , entonces  $b \odot a = 1$ .*

*Demostración.* Escribamos:

$$1 \odot b = b \odot 1 = b \odot (a \odot b) = (b \odot a) \odot b$$

Luego aplicamos la ley de cancelación.

□

Esto nos dice que  $(a^{-1})^{-1} = a$ , vale decir,  $a$  y  $a^{-1}$  siempre comutan.

**Teorema 7.17.** *En un grupo,  $1 \odot a = a$*

*Demostración.* Por mutualidad podemos escribir:

$$1 \odot a = (a \odot a^{-1}) \odot a = a \odot (a^{-1} \odot a) = a \odot 1 = a$$

□

Vale decir, en un grupo el neutro siempre commuta con todos los elementos.

**Teorema 7.18.** *El inverso de un elemento es único.*

*Demostración.* Sea  $a \in G$  un elemento cualquiera, y supongamos que se cumplen  $a \odot b = 1$  y  $a \odot c = 1$ . Por cancelación por la izquierda,  $b = c$ . Por mutualidad, si  $a \odot b = 1$  entonces  $b \odot a = 1$ , y  $b = a^{-1}$ .  $\square$

En lo que sigue consideraremos un grupo  $G$  con operación  $\odot$  (o simplemente se omite). El elemento neutro de  $G$  lo denotaremos 1. Para simplificar notación, en un grupo con operación multiplicación usaremos la definición para potencias enteras, donde  $a$  es un elemento cualquiera del grupo:

$$a^n = \underbrace{a \odot a \odot \cdots \odot a}_{n \text{ veces}}$$

Formalmente:

$$a^0 = 1 \tag{7.13}$$

$$a^{k+1} = a^k \odot a \quad \text{si } k \geq 0 \tag{7.14}$$

Es fácil ver que si definimos:

$$a^{-k} = (a^{-1})^k \tag{7.15}$$

se cumplen las propiedades tradicionales de las potencias:

$$a^{m+n} = a^m \odot a^n \tag{7.16}$$

$$(a^m)^n = a^{mn} \tag{7.17}$$

Si la operación es suma usamos la notación  $n \cdot a$  (o simplemente  $na$ ) con  $n \in \mathbb{Z}$ ; si anotamos 0 para el neutro aditivo:

$$n \cdot a = \underbrace{a + a + \cdots + a}_{n \text{ veces}}$$

Formalmente:

$$0 \cdot a = 0$$

$$(k+1) \cdot a = k \cdot a + a \quad \text{si } k \geq 0$$

$$-k \cdot a = k \cdot (-a)$$

Nótese que  $ma + na = (m+n)a$  si  $m, n \in \mathbb{Z}$ , que no es más que (7.16) en esta notación, y que  $m(na) = (mn)a$  corresponde a (7.17).

Sea  $a$  un elemento de un grupo  $G$ , en el cual usamos notación de multiplicación. Los elementos  $a^k$  con  $k \in \mathbb{Z}$  forman un subgrupo abeliano de  $G$ . Si  $G$  es finito, el conjunto de los  $a^n$  para  $n \in \mathbb{N}$  tiene que contener repeticiones, ya que son todos elementos de  $G$ . Si resulta que  $a^m = a^n$  con  $m > n$ , tendremos  $a^{m-n} = 1$ . El mínimo  $n > 0$  tal que  $a^n = 1$  (siempre existe si  $G$  es finito, aunque incluso hay grupos infinitos todos cuyos elementos son de orden finito) se llama el *orden de a*, que se anota  $\text{ord}_G(a)$  (o simplemente  $\text{ord}(a)$ , si el grupo se subentiende). Más aún, si  $a^k = 1$ , entonces  $\text{ord}_G(a) | k$ .

Para demostrar esto, usamos el algoritmo de división. Con  $n = \text{ord}_G(a)$  podemos escribir  $k = qn + r$ , donde  $0 \leq r < n$ , y:

$$\begin{aligned} a^k &= a^{qn+r} \\ 1 &= a^{qn} \odot a^r \\ &= (a^n)^q \odot a^r \\ &= a^r \end{aligned} \tag{7.18}$$

Como  $0 \leq r < n$ , por la definición de orden la única opción en (7.18) es  $r = 0$ , y  $n \mid k$ .

**Definición 7.5.** Sea  $G$  un grupo. Si todos los elementos de  $G$  se pueden escribir como  $g^k$  para algún elemento  $g \in G$  y  $k \in \mathbb{Z}$  a  $G$  se le llama *grupo cíclico*, y a  $g$  se le llama *generador* del grupo.

Si  $a$  tiene orden finito  $n$ , los elementos  $1 = a^0, a, \dots, a^{n-1}$  forman un grupo cíclico de orden  $n$ , llamado *el grupo generado por a*, que se anota  $\langle a \rangle$ . Tenemos  $a^{n-1} = a^{-1}$ , lo que completa la condición de subgrupo que dimos antes en el teorema 7.21.

Vamos ahora a anillos, que son las estructuras que realmente nos interesan acá.

**Definición 7.6.** En un anillo  $R$ , si para  $r$  hay un  $x$  tal que  $r \odot x = x \odot r = 1$ , se dice que  $r$  es *invertible*, que  $x$  es su *inverso* y escribimos  $x = r^{-1}$ . Nótese que también es  $x^{-1} = r$ . A los elementos invertibles del anillo  $R$  se les llama *unidades*, y su conjunto se denota  $R^\times$ .

Notaciones alternativas para el grupo de unidades de  $R$  son  $U(R)$ ,  $R^*$  y  $E(R)$ .

**Teorema 7.19.** *El conjunto de unidades de un anillo forma un grupo con la multiplicación.*

*Demuestra*ción. La multiplicación es asociativa en  $R$ , así que lo es en el subconjunto  $R^\times$ . Toda unidad tiene inverso por definición, y 1 siempre es una unidad. Si  $a$  y  $b$  son invertibles, entonces  $a \odot b$  tiene inverso  $b^{-1} \odot a^{-1}$ , y la multiplicación es cerrada en  $R^\times$ . Estas son las propiedades que definen a un grupo.  $\square$

Un caso especial muy importante es:

**Definición 7.7.** Un anillo comunitativo en el que todos los elementos distintos de 0 son invertibles se llama *campo*.

Ya habíamos encontrado este concepto al discutir  $\mathbb{R}$  en el capítulo 5.

Para simplificar la notación usaremos  $x$  con  $0 \leq x \leq m - 1$  para denotar al conjunto  $[x]_m$ , y usaremos  $+ y \cdot$  (o simplemente omitiremos la multiplicación) en vez de  $\oplus$  y  $\odot$ . Para eliminar paréntesis, usaremos la convención común de “multiplicaciones antes de sumas”. El valor de  $m$  se debe indicar o quedar claro por el contexto.

Nótese que en  $\mathbb{Z}_m$  no hay orden ni idea de “positivo”. Como en  $\mathbb{Z}_m$  es

$$0, 1, \dots, m-1, 0, 1, \dots$$

(al llegar al final comienza nuevamente) a veces se le llama “aritmética de reloj”.

Algunas de las propiedades conocidas de  $\mathbb{Z}$  no siempre valen en  $\mathbb{Z}_m$ . Por ejemplo, en  $\mathbb{Z}$  si  $a \cdot c = b \cdot c$  con  $c \neq 0$  entonces  $a = b$ . Sin embargo, en  $\mathbb{Z}_{15}$  tenemos

$$4 \cdot 9 = 14 \cdot 9 = 6$$

e incluso

$$12 \cdot 10 = 0$$

También pueden haber elementos que tienen más de dos raíces cuadradas. Por ejemplo:

$$4 = 2 \cdot 2 = 7 \cdot 7 = 8 \cdot 8 = 13 \cdot 13$$

Nótese que módulo 15 tenemos  $13 \equiv -2$  y  $8 \equiv -7$ , con lo que las raíces cuadradas de 4 en  $\mathbb{Z}_{15}$  son  $\pm 2$  y  $\pm 7$ , mientras en  $\mathbb{Z}$  solo están  $\pm 2$ . Algunos elementos tienen inverso multiplicativo en  $\mathbb{Z}_{15}$ , como:

$$7 \cdot 13 = 8 \cdot 2 = 1$$

Otros no lo tienen, por ejemplo 6, como es fácil verificar revisando todos los productos  $6 \cdot k$  con  $0 \leq k < 15$  módulo 15. Hay elementos con una única raíz cuadrada, como  $15 = 15 \cdot 15$  en  $\mathbb{Z}_{30}$ , que incluso es su propia raíz cuadrada.

**Definición 7.8.** Si en un anillo hay elementos  $a, b$  tales que  $a \odot b = 0$  se les llama *divisor izquierdo de cero* a  $a$  y *divisor derecho de cero* a  $b$ . A ambos se les llama *divisores de cero*.

Nótese que 0 siempre es un divisor de cero.

Casos muy importantes de anillos son:

**Definición 7.9.** Un anillo comunitativo en el cual sólo 0 es divisor de cero se llama *dominio integral*.

El ejemplo clásico de dominio integral es  $\mathbb{Z}$ . En un dominio integral podemos cancelar en productos:

**Teorema 7.20.** *En un dominio integral, si  $ax = bx$  con  $x \neq 0$  entonces  $a = b$ .*

*Demostración.* Tenemos:

$$\begin{aligned} ax &= bx \\ ax - bx &= 0 \\ (a - b)x &= 0 \end{aligned}$$

Como  $x \neq 0$  es  $a - b = 0$ , o sea  $a = b$ . □

Veamos criterios para identificar subgrupos.

**Teorema 7.21.** *Sea  $G$  un grupo, y  $H \subset G$ . Si para todo  $a, b \in H$  es  $a \odot b^{-1} \in H$ ,  $H$  es un subgrupo de  $G$ .*

*Demostración.* Que  $H$  sea subgrupo de  $G$  significa simplemente que ese subconjunto es cerrado respecto de la operación e inversos (las demás propiedades se “heredan” del grupo), y que contiene al neutro  $e$ .

Si  $a \in H$ , por hipótesis está  $a \odot a^{-1} = e$ . Pero así también está  $e \odot a^{-1} = a^{-1}$ . Con esto, si  $a, b \in H$ , tenemos que  $a \odot (b^{-1})^{-1} = a \odot b \in H$ , completando la demostración. □

Por ejemplo, vemos que en el grupo  $D_8$  mostrado en el cuadro 7.2 los elementos  $\{e, r, r^2, r^3\}$  forman un subgrupo.

**Lema 7.22.** *Sean  $A$  y  $B$  subgrupos de  $G$ . Entonces  $A \cap B$  es un subgrupo de  $G$ .*

*Demostración.* Supongamos  $x, y \in A \cap B$ . Entonces  $y^{-1} \in A$  y también  $y^{-1} \in B$ , por ser grupos. Pero entonces  $y^{-1} \in A \cap B$ . De forma similar,  $x \cdot y^{-1} \in A \cap B$ , y por el teorema 7.21  $A \cap B$  es un subgrupo de  $G$ . □

También para anillos:

**Lema 7.23.** *Sean  $A$  y  $B$  subanillos de  $R$ . Entonces  $A \cap B$  es un subanillo de  $R$ .*

La demostración se omite, sigue la misma idea que la del lema 7.22.

Los axiomas de anillo tienen algunas consecuencias simples.

**Teorema 7.24.** *En un anillo, 0 y 1 son únicos, y para cada  $a$  hay un único  $-a$ .*

*Demostración.* Para la suma, el que 0 es único no es más que el teorema 7.14; la misma técnica de la demostración puede aplicarse a 1 y la multiplicación.

Que hay un único  $-a$  es el teorema 7.18 aplicado a la suma.  $\square$

Para evitar paréntesis, usaremos la convención tradicional que las operaciones son asociativas izquierdas, y que  $\odot$  tiene mayor precedencia que  $\oplus$ . A veces anotaremos  $a \odot b$  para  $a \oplus (-b)$ .

Otras consecuencias simples son:

**Teorema 7.25.** *En un anillo, para todo  $a$  tenemos  $0 \odot a = a \odot 0 = 0$*

*Demostración.* Es aplicar los axiomas de anillo. Para  $0 \odot a$ :

$$\begin{aligned} 0 \odot a &= (0 \oplus 0) \odot a \\ &= (0 \odot a) \oplus (0 \odot a) \end{aligned}$$

Sumando  $-(0 \odot a)$  a ambos lados obtenemos la conclusión buscada. Que  $a \odot 0 = 0$  se demuestra de forma similar.  $\square$

De acá, si  $a$  es una unidad del anillo, entonces no es un divisor de cero, ya que si:

$$\begin{aligned} a \odot b &= 0 \\ a^{-1} \odot (a \odot b) &= (a^{-1} \odot a) \odot b \\ &= 1 \odot b \\ &= b \end{aligned}$$

Por el otro lado:

$$a^{-1} \odot 0 = 0$$

O sea,  $b = 0$ , y  $a$  no es divisor de cero.

**Teorema 7.26.** *En un anillo, tenemos  $(-a) \odot b = a \odot (-b) = -(a \odot b)$ . Asimismo,  $(-a) \odot (-b) = a \odot b$ .*

*Demostración.* Primero demostramos  $(-1) \odot a = a \odot (-1) = -a$ .

$$\begin{aligned} (-1) \odot a \oplus a &= (-1) \odot a \oplus 1 \odot a \\ &= ((-1) \oplus 1) \odot a \\ &= 0 \odot a \\ &= 0 \end{aligned}$$

Esto corresponde precisamente a la definición de  $-a$  en un grupo, y sabemos por el teorema 7.18 que el inverso es único. En forma afín se demuestra que  $a \odot (-1) = -a$ .

Usando esto:

$$\begin{aligned} (-a) \odot b &= ((-1) \odot a) \odot b \\ &= (-1) \odot (a \odot b) \\ &= -(a \odot b) \end{aligned}$$

De la misma forma se demuestra que  $a \odot (-b) = -(a \odot b)$ .

Finalmente:

$$\begin{aligned} (-a) \odot (-b) &= -(a \odot (-b)) \\ &= -(-(a \odot b)) \\ &= a \odot b \end{aligned}$$

□

Tenemos también:

**Teorema 7.27.** *En un anillo finito  $R$ , los elementos son unidades o divisores de cero.*

*Demostración.* Tomemos  $a \neq 0$  del anillo, y consideremos el conjunto  $aR = \{a \odot x : x \in R\}$ . Supongamos que hay elementos repetidos en  $aR$ , digamos  $a \odot x_1 = a \odot x_2$  con  $x_1 \neq x_2$ . Entonces:

$$\begin{aligned} a \odot x_1 &= a \odot x_2 \\ a \odot x_1 \ominus a \odot x_2 &= 0 \\ a \odot (x_1 \ominus x_2) &= 0 \end{aligned}$$

Como  $x_1 \ominus x_2 \neq 0$ ,  $a$  es un divisor de cero.

Si no hay elementos repetidos en  $aR$ , como hay  $|R|$  elementos en ese conjunto tiene que estar 1, digamos  $a \odot b = 1$ . Entonces:

$$\begin{aligned} a \odot b &= 1 \\ (a \odot b) \odot a &= a \\ a \odot (b \odot a) &= 0 \\ a \odot ((b \odot a) \ominus 1) &= 0 \end{aligned}$$

Sabemos que  $a \odot 0 = 0$ , como en  $aR$  no hay elementos repetidos es:

$$\begin{aligned} b \odot a \ominus 1 &= 0 \\ b \odot a &= 1 \end{aligned}$$

y  $b$  es el inverso de  $a$ ,  $a$  es una unidad.

□

Una consecuencia inmediata del teorema 7.27 es:

**Corolario 7.28.** *Todo dominio integral finito es un campo.*

Ejemplos adicionales de anillo los ponen los enteros  $\mathbb{Z}$ , los complejos  $\mathbb{C}$  y matrices cuadradas sobre  $\mathbb{R}$ .

### 7.5.1. Curvas elípticas

Una *curva elíptica* está definida por una ecuación de la forma:

$$y^2 = x^3 + ax + b$$

que no tiene puntos aislados, no se intersecta a sí misma y no tiene cuernos. Algebraicamente, el discriminante  $\Delta = -16(4a^3 + 27b^2) \neq 0$ . El gráfico de la curva tiene dos componentes si  $\Delta > 0$  y uno

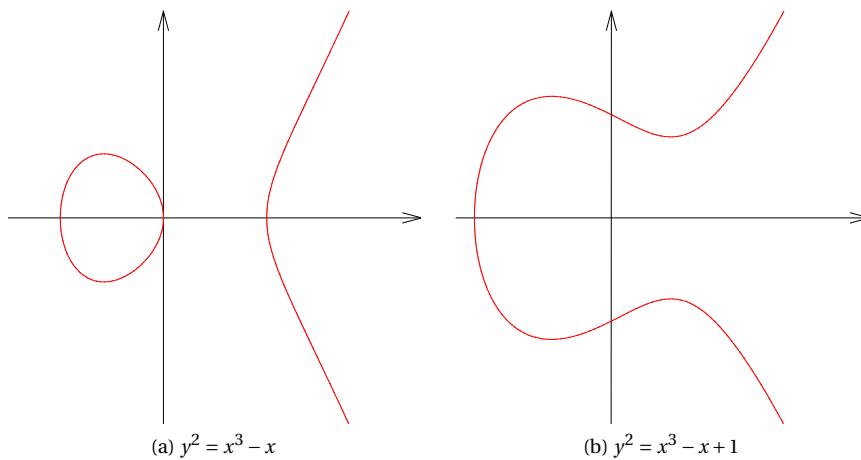


Figura 7.2 – Curvas elípticas

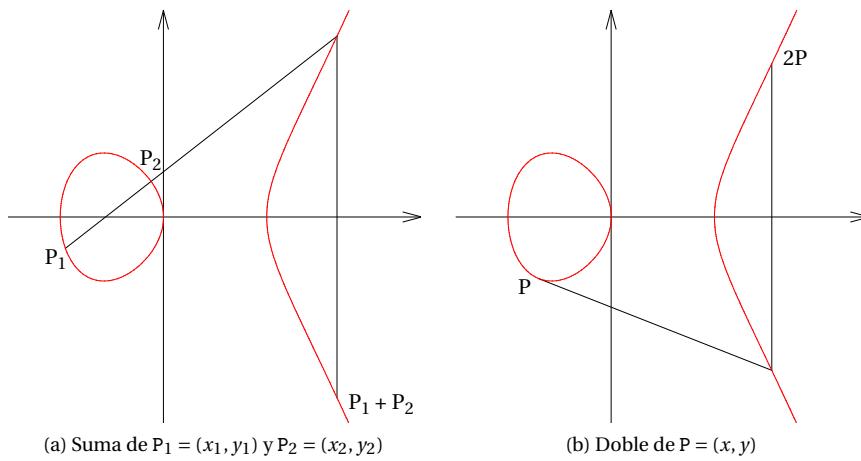


Figura 7.3 – Sumas en curvas elípticas

solo si  $\Delta < 0$ , ver la figura 7.2. El nombre no tiene relación con la forma de la curva, sino con el hecho que se requieren funciones elípticas para representarlas paramétricamente.

Dados dos puntos  $P_1 = (x_1, y_1)$  y  $P_2 = (x_2, y_2)$  sobre una curva elíptica podemos definir la suma como el punto donde la recta entre los puntos corta la curva reflejado en el eje  $x$ , véase 7.3a para un ejemplo. Esto hace que si  $P_1$ ,  $P_2$  y  $P_3$  son puntos sobre la curva, es  $P_1 + P_2 + P_3 = 0$ , donde 0 es el punto en el infinito. En caso que  $x_1 = x_2$  hay dos posibilidades: Si  $y_1 = -y_2$ , (incluyendo el caso en que los puntos coinciden), la suma se define como 0 (el punto en el infinito). Tenemos así para  $P = (x, y)$  que  $-P = (x, -y)$ . En caso contrario definimos  $P_1 + P_2 = P_3$  con  $P_3 = (x_3, y_3)$  mediante:

$$\begin{aligned} s &= \frac{y_2 - y_1}{x_2 - x_1} \\ x_3 &= s^2 - x_1 - x_2 \\ y_3 &= y_1 + s(x_3 - x_1) \end{aligned} \tag{7.19}$$

Para sumar el punto  $P = (x, y)$  consigo mismo corresponde usar la tangente a la curva, ver la figura 7.3b, lo que da  $P_2 = (x_2, y_2)$ :

$$\begin{aligned} s &= \frac{3x + a}{2y} \\ x_2 &= s^2 - 2x \\ y_2 &= y + s(x_2 - x) \end{aligned} \tag{7.20}$$

Es rutina verificar que esto define un grupo abeliano.

Lo interesante es que las relaciones que definen la suma en curvas elípticas valen en cualquier campo, por lo que podemos considerar el grupo definido por la curva elíptica sobre un campo cualquiera. Si la característica del campo  $F$  no es 2 ni 3 (vale decir, no es  $2x = 0$  ni  $3x = 0$  para todo  $x \in F$ ; la discusión formal deberá esperar al capítulo 10), toda curva elíptica puede escribirse en la forma:

$$y^2 = x^3 - px - q$$

tal que el lado derecho no tiene ceros repetidos. Interesan los puntos con coordenadas en  $F$ . El teorema de Hasse [165–167] da las cotas para el número  $N$  de elementos en curvas elípticas sobre el campo finito de  $q$  elementos:

$$|N - (q + 1)| \leq 2\sqrt{q}$$

Las curvas elípticas son importantes en teoría de números, y tienen bastantes aplicaciones prácticas, particularmente se están haciendo muy populares en criptografía. El sistema PARI/GP [278] incluye soporte para operar en los grupos respectivos. El paquete GAP [139] tiene extenso soporte para trabajar con grupos, incluyendo grupos de curvas elípticas.

### 7.5.2. Anillos cuadráticos

Un ejemplo menos conocido de anillo comutativo lo pone  $\mathbb{Z}[\sqrt{2}]$ , definido como el conjunto  $\{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ , con las operaciones tradicionales de los reales. Primeramente, las operaciones en  $\mathbb{Z}[\sqrt{2}]$  están bien definidas:

$$\begin{aligned} (a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) &= (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \\ (a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2}) &= (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \end{aligned}$$

Los coeficientes en estas expresiones son todos enteros, y al ser  $\sqrt{2}$  irracional no hay maneras alternativas de representar el mismo elemento. Como los elementos son simplemente números reales, las asociatividades y conmutatividades de las operaciones, y la distributividad, se “heredan” de  $\mathbb{R}$ . Podemos representar:

$$\begin{aligned} 0 &= 0 + 0 \cdot \sqrt{2} \\ 1 &= 1 + 0 \cdot \sqrt{2} \end{aligned}$$

Tenemos

$$(a + b\sqrt{2}) + ((-a) + (-b)\sqrt{2}) = 0$$

lo que provee de un inverso aditivo. Como este es un subanillo de los reales, no hay divisores de cero salvo 0, y es un dominio integral.

Busquemos el inverso de  $a + b\sqrt{2}$  en  $\mathbb{Z}[\sqrt{2}]$ :

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} \quad (7.21)$$

Para que (7.21) pertenezca a nuestro anillo, debe ser:

$$a^2 - 2b^2 = \pm 1 \quad (7.22)$$

Una solución es  $a = b = 1$ , con lo que  $1 + \sqrt{2}$  es una unidad.

A ecuaciones de la forma

$$x^2 - dy^2 = 1 \quad (7.23)$$

con  $d > 1$  se les llama *ecuaciones de Pell*,<sup>1</sup> discutimos el caso  $d = 2$  más arriba. La discusión siguiente sigue esencialmente a Djukić [96].

Vemos que si  $d$  es un cuadrado perfecto, solo es posible la *solución trivial*  $x = 1, y = 0$ . Enseguida, podemos suponer que  $x$  e  $y$  son no negativos, por los cuadrados sus signos no importan. Podemos factorizar el lado derecho de la ecuación (7.23)

$$x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d})$$

lo que nos lleva de vuelta al anillo  $\mathbb{Z}[\sqrt{d}]$ .

**Definición 7.10.** En el anillo  $\mathbb{Z}[\sqrt{d}]$  el *conjugado* de  $z = a + b\sqrt{d}$  es  $\bar{z} = a - b\sqrt{d}$ , y su *norma* es  $N(z) = z \cdot \bar{z} = a^2 - db^2$ . Llamamos *parte entera* a  $a$  y *parte irracional* a  $b$ .

En estos términos, son unidades de  $\mathbb{Z}[\sqrt{d}]$  exactamente los elementos de norma  $\pm 1$ . El inverso de la unidad  $z$  es  $\pm \bar{z}$ , dependiendo del signo de  $N(z)$ . Resulta:

**Teorema 7.29.** En  $\mathbb{Z}[\sqrt{d}]$  la norma y el conjugado son multiplicativos, o sea  $N(z_1 z_2) = N(z_1) \cdot N(z_2)$  y  $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$

*Demuestra*ción. Primeramente, con  $z_1 = a_1 + b_1\sqrt{d}$  y  $z_2 = a_2 + b_2\sqrt{d}$ , tenemos:

$$\begin{aligned} \overline{z_1} \cdot \overline{z_2} &= (a_1 - b_1\sqrt{d}) \cdot (a_2 - b_2\sqrt{d}) \\ &= (a_1 a_2 + db_1 b_2) - (a_1 b_2 + a_2 b_1)\sqrt{d} \\ &= \overline{z_1 z_2} \end{aligned} \quad (7.24)$$

Con esto:

$$\begin{aligned} N(z_1 z_2) &= (z_1 z_2) \cdot (\overline{z_1 z_2}) \\ &= (z_1 \overline{z_1}) \cdot (z_2 \overline{z_2}) \\ &= N(z_1) \cdot N(z_2) \end{aligned}$$

□

Pero también:

**Teorema 7.30.** Si  $z_0$  es el elemento mínimo de  $\mathbb{Z}[\sqrt{d}]$  con  $z_0 > 1$  y  $N(z_0) = 1$ , todos los elementos  $z \in \mathbb{Z}[\sqrt{d}]$  con  $N(z) = 1$  están dados por  $z = \pm z_0^n$  con  $n \in \mathbb{Z}$ .

<sup>1</sup> Euler erróneamente se la atribuyó a John Pell (1611–1685), probablemente confundiéndolo con William Brouncker (1620–1684) quien fue el primer europeo en estudiarla. Brahmagupta en la India en 628 ya describe cómo resolverla. Los números de Pell (soluciones para el caso  $d = 2$ ) se conocen desde Pitágoras.

*Demostración.* Suponga que  $N(z) = z \cdot \bar{z} = 1$  para  $z > 1$ , con lo que  $z^{-1} = \bar{z}$ . Hay un único  $k \in \mathbb{N}_0$  tal que  $z_0^k \leq z < z_0^{k+1}$ . Así  $z_1 = zz_0^{-k} = z(\bar{z_0})^k$  cumple  $1 \leq z_1 < z_0$ , y tenemos  $N(z_1) = N(z) \cdot N(z_0)^{-k} = 1$ . Por la minimalidad de  $z_0$ , es  $z_1 = 1$  y  $z = z_0^k$ .  $\square$

Al par  $(x_0, y_0)$  o a  $z_0 = x_0 + y_0\sqrt{d}$  se le llama *solución fundamental* de la ecuación de Pell. Todos los anillos  $\mathbb{Z}[\sqrt{d}]$  tienen infinitas unidades.

**Teorema 7.31** (Dirichlet). *Sea  $\alpha$  un número irracional y  $n$  un entero positivo. Entonces hay  $p \in \mathbb{Z}$  y  $q \in [1, n]$  tales que:*

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{(n+1)q} \quad (7.25)$$

*Demostración.* La desigualdad (7.25) es equivalente a  $|q\alpha - p| < 1/(n+1)$ . Entre los  $n+2$  números  $0, \{\alpha\}, \{2\alpha\}, \dots, \{n\alpha\}, 1$ , por el principio del palomar (teorema 1.3) en el segmento  $[0, 1]$  hay dos que difieren en menos de  $1/(n+1)$  (si  $\alpha$  es racional podrían diferir en exactamente  $1/(n+1)$ ). Si éstos son  $\{aa\}$  y  $\{ba\}$  basta hacer  $q = |a - b|$ ; si son  $\{aa\}$  y 0 o 1, basta hacer  $q = a$ . En cualquiera de los casos,  $p$  es el entero más cercano a  $aa$ .  $\square$

De acá, como  $n+1 > q$  es  $1/((n+1)q) < 1/q^2$ , sigue inmediatamente:

**Corolario 7.32.** *Si  $\alpha$  es un real arbitrario, hay infinitos pares de enteros positivos  $(p, q)$  tales que:*

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}$$

Así resulta:

**Teorema 7.33.** *La ecuación de Pell*

$$x^2 - dy^2 = 1$$

donde  $d$  no es un cuadrado tiene una solución no trivial en los enteros.

*Demostración.* Aplicando el corolario 7.32 a  $\alpha = \sqrt{d}$ , vemos que hay infinitos pares  $(a, b)$  tales que:

$$\left| a - b\sqrt{d} \right| < \frac{1}{b}$$

Notamos que por la desigualdad triangular, teorema 1.2:

$$\left| a + b\sqrt{d} \right| \leq \left| a - b\sqrt{d} \right| + \left| 2b\sqrt{d} \right| \leq \frac{1}{b} + 2b\sqrt{d}$$

Con esto:

$$|a^2 - b^2 d| = \left| a + b\sqrt{d} \right| \cdot \left| a - b\sqrt{d} \right| \leq \left( \frac{1}{b} + 2b\sqrt{d} \right) \cdot \frac{1}{b} \leq 2\sqrt{d} + 1$$

Pero al haber infinitos pares con normas  $|N(a + b\sqrt{d})| \leq 2\sqrt{d} + 1$ , y siendo enteras las normas por el principio del palomar hay infinitos pares con una misma norma  $N$ . Acá  $N \neq 0$ , ya que solo para  $z = 0$  es  $N(z) = 0$ . Si ahora consideramos todos los pares de norma  $N$ , nuevamente por el principio

del palomar hay infinitos pares  $z_1 = (a_1, b_1)$  y  $z_2 = (a_2, b_2)$  tales que  $a_1 \equiv a_2 \pmod{N}$  y  $b_1 \equiv b_2 \pmod{N}$ , por lo que debe haber  $z_1 \neq \pm z_2$  entre ellos. Consideremos:

$$z = a + b\sqrt{d} = \frac{z_1}{z_2} = \frac{z_1\bar{z}_2}{N(z_2)}$$

$$N(z) = \frac{N(z_1)}{N(z_2)} = 1$$

Como  $z_1 \neq \pm z_2$ , sabemos que  $z \neq \pm 1$ . Como  $N(z_2) = N$ , resultan:

$$a = \frac{a_1 a_2 - d b_1 b_2}{N}$$

$$b = \frac{a_1 b_2 - a_2 b_1}{N}$$

Observamos que, ya que  $a_1 \equiv a_2 \pmod{N}$  y  $b_1 \equiv b_2 \pmod{N}$ :

$$a_1 a_2 - d b_1 b_2 \equiv a_1 a_1 - d b_1 b_1 \equiv 0 \pmod{N}$$

$$a_1 b_2 - a_2 b_1 \equiv a_1 b_1 - a_1 b_1 \equiv 0 \pmod{N}$$

con lo que  $a, b \in \mathbb{Z}$ , o sea  $z \in \mathbb{Z}[\sqrt{d}]$  con  $N(z) = 1$ .  $\square$

También nos interesa saber si hay soluciones a  $x^2 - dy^2 = -1$ , ya que también son unidades de  $\mathbb{Z}[\sqrt{d}]$ .

**Teorema 7.34.** *La ecuación  $x^2 - dy^2 = -1$  tiene solución si y solo si existe  $z_1 \in \mathbb{Z}[\sqrt{d}]$  tal que  $z_1^2 = z_0$ .*

*Demostración.* Demostramos implicancias en ambas direcciones. Si hay tal  $z_1$  es menor que  $z_0$ , y como  $N(z_0) = N(z_1^2) = N(z_1)^2 = 1$ , debe ser  $N(z_1) = -1$ .

Si  $z$  es solución de  $N(z) = -1$ , entonces  $N(z^2) = 1$ . En particular, la mínima solución  $z_1 \in \mathbb{Z}[\sqrt{d}]$  de la ecuación  $N(z) = -1$  tal que  $z_1 > 1$  da lugar a la mínima solución  $z_0 = z_1^2$  de  $N(z) = 1$ .  $\square$

Hace falta determinar raíces cuadradas en  $\mathbb{Z}[\sqrt{d}]$ :

$$(x_1 + y_1\sqrt{d})^2 = (x_1^2 + dy_1^2) + 2x_1y_1\sqrt{d} = (2dy_1 - 1) + 2x_1y_1\sqrt{d} = x_0 + y_0\sqrt{d}$$

Acá usamos  $x_1^2 + dy_1^2 = 1$ . O sea:

$$y_1 = \frac{x_0 + 1}{2d}$$

$$x_1 = \frac{y_0}{2y_1} = \frac{dy_0}{x_0 + 1}$$

En  $\mathbb{Z}[\sqrt{2}]$  la solución fundamental es  $(3, 2)$ , como su raíz cuadrada resulta el par  $(1, 1) \in \mathbb{Z}[\sqrt{2}]$ , con  $N(1 + \sqrt{2}) = -1$ , con lo que todas las unidades son  $\pm(1 + \sqrt{2})^n$  para  $n \in \mathbb{Z}$ .

Lenstra [239] da algo de la historia de la ecuación de Pell y describe algoritmos para obtener la solución fundamental. Mayores detalles de la fascinante teoría relacionada con estos anillos da por ejemplo Djukić [95] y en mayor detalle Lemmermeyer [236].

### 7.5.3. Cuaterniones

Otro ejemplo interesante de anillo lo ponen los *cuaterniones* [160], una extensión de los números complejos inventada para manejar posiciones en el espacio como se pueden manejar puntos en el plano con números complejos. Hoy han sido reemplazados casi universalmente por vectores, más flexibles y generales. Considerados una curiosidad histórica por mucho tiempo, últimamente han encontrado utilidad en diversas áreas, como representación eficiente de movimientos y rotaciones en el espacio en computación gráfica, ver por ejemplo Dorst, Fontijne y Mann [101].

Con  $a, b, c, d \in \mathbb{R}$  el cuaternion  $z \in \mathbb{H}$  puede describirse

$$z = a + bi + cj + dk \quad (7.26)$$

donde

$$i^2 = j^2 = k^2 = ijk = -1 \quad (7.27)$$

Definimos las operaciones con estos objetos como para polinomios en  $i, j$  y  $k$ , aplicando (7.27) luego.

Resulta que el anillo de cuaterniones no es comutativo, la tabla de multiplicación de los elementos unitarios es el cuadro 7.3, pero todo elemento diferente de cero tiene inverso multiplicativo. En

$\cdot$	1	$i$	$j$	$k$
1	1	$i$	$j$	$k$
$i$	$i$	-1	$k$	$-j$
$j$	$j$	$-k$	-1	$i$
$k$	$k$	$j$	$-i$	-1

Cuadro 7.3 – Multiplicación de cuaterniones

detalle, si definimos el *conjugado* del cuaternion  $q = a + bi + cj + dk$  como  $\bar{q} = a - bi - cj - dk$ , resulta que  $q\bar{q} = a^2 + b^2 + c^2 + d^2$ ; y la *norma* de  $q$  se define como  $\|q\| = \sqrt{q\bar{q}}$ . Nótese que  $\overline{pq} = \bar{q}\bar{p}$ . Con esto, resulta que la norma es multiplicativa, ya que la multiplicación entre un cuaternion cualquiera y un real conmuta:

$$\begin{aligned} \|pq\|^2 &= (pq) \cdot (\overline{pq}) \\ &= p \cdot q \bar{q} \cdot \bar{p} \\ &= \|p\|^2 \cdot \|q\|^2 \end{aligned}$$

Así resulta el *recíproco*

$$q^{-1} = \frac{\bar{q}}{\|q\|}$$

que claramente cumple  $qq^{-1} = q^{-1}q = 1$ . La notación  $p/q$  no tiene sentido en cuaterniones, ya que  $pq^{-1} \neq q^{-1}p$  en general.

## 7.6. Los teoremas de Lagrange, Euler y Fermat

Un resultado importante que relaciona grupos y subgrupos es el siguiente:

**Teorema 7.35** (Lagrange). *Sea  $G$  un grupo finito, y  $H$  un subgrupo de  $G$ . Entonces  $|H|$  divide a  $|G|$ .*

*Demostración.* Sea  $a \in G$ . Al conjunto  $aH = \{a \odot h : h \in H\}$  se le llama *coset (izquierdo) de H* (de forma afín el *coset derecho Ha = {h \odot a : h \in H}*). Demostraremos que todos los cosets tienen el mismo número de elementos, y que partitionan  $G$ , de lo que el resultado es inmediato.

Primeramente, el coset  $aH = \{a \odot h : h \in H\}$  no tiene elementos repetidos, porque supongamos que hay  $h, g \in H$  tales que  $a \odot h = a \odot g$ , por la ley de cancelación es  $h = g$ . Resulta simplemente  $|aH| = |H|$ .

Definamos la relación  $R$  sobre  $G$  mediante  $x R y$  si y solo si hay  $h \in H$  tal que  $x = y \odot h$ . Entonces  $R$  es una relación de equivalencia:

**Reflexiva:** Necesariamente  $1 \in H$ , con lo que  $x R x$ .

**Simétrica:** Esto porque  $x R y$  corresponde a  $x = y \odot h$  para  $h \in H$ , pero entonces también  $y = x \odot h^{-1}$ , y como  $h^{-1} \in H$  tenemos  $y R x$ .

**Transitiva:** Si  $x R y$  y  $y R z$  entonces hay  $h_1, h_2 \in H$  tales que  $x = y \odot h_1$  y  $y = z \odot h_2$ . Combinando éstos,  $x = z \odot (h_2 \odot h_1)$ , y  $h_2 \odot h_1 \in H$ , con lo que  $x R z$ .

Las clases de equivalencia de  $R$  son precisamente los cosets de  $H$ :  $x \in [y]$  siempre que podemos escribir  $x = y \odot h$  con  $h \in H$ , o sea,  $x \in yH$ , con lo que  $[y] = yH$ . Pero  $|aH| = |H|$  como vimos antes, y tenemos nuestro resultado.  $\square$

En particular, consideremos el subgrupo generado por el elemento  $a \in G$ , vale decir, si el orden de  $a$  es  $n$  los elementos  $a^0, a^1, \dots, a^{n-1}$ . Este subgrupo tiene orden  $n$ , con lo que  $n$  divide a  $|G|$ .

Nos abocaremos a un estudio más detallado de  $\mathbb{Z}_m^\times$ , una vez adquiridas algunas herramientas algebraicas adicionales.

**Teorema 7.36.** *El elemento  $a \in \mathbb{Z}_m$  es invertible si y solo si  $a$  y  $m$  son coprimos. En particular, si  $p$  es primo todos los elementos de  $\mathbb{Z}_p$  (salvo 0) son invertibles, y  $\mathbb{Z}_p$  es un campo.*

*Demostración.* Demostramos implicancia en ambos sentidos. Supongamos  $a$  invertible. Entonces existen enteros  $b$  y  $k$  tales que  $ab - 1 = km$ , que es decir  $ab - km = 1$ . Pero si existen tales  $b$  y  $k$  entonces  $\gcd(a, m) = 1$ .

Al revés, supongamos  $\gcd(a, m) = 1$ . Entonces (por la identidad de Bézout) existen  $s, t$  tales que:

$$\begin{aligned} s \cdot a + t \cdot m &= 1 \\ s \cdot a &\equiv 1 \pmod{m} \end{aligned}$$

y  $s$  es el inverso de  $a$ .  $\square$

Resulta que el número de unidades de  $\mathbb{Z}_m$  es una cantidad muy importante. Por el teorema 7.36, no es más que la cantidad de números en  $1, 2, \dots, m$  que son relativamente primos a  $m$ , que se anota  $\phi(m)$  (función  $\phi$  de Euler).

Un ejemplo lo pone  $\mathbb{Z}_{12}$ , donde tenemos la tabla de multiplicación 7.4. Pueden apreciarse los elementos invertibles  $\mathbb{Z}_{12}^\times = \{1, 5, 7, 11\}$ , con lo que  $\phi(12) = 4$ . Se ve también que los demás son todos divisores de cero, como asegura el teorema 7.27.

Al considerar el subgrupo de  $\mathbb{Z}_m^\times$  generado por  $a$  tenemos del teorema de Lagrange que el orden de  $a$  divide al orden de  $\mathbb{Z}_m^\times$ , que es  $\phi(m)$ , y así:

**Teorema 7.37 (Euler).** *Si  $a$  y  $m$  son relativamente primos, entonces*

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

En el caso de que  $m$  sea primo, como  $\phi(p) = p - 1$  para  $p$  primo, el teorema de Euler se reduce a:

$\cdot$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

Cuadro 7.4 – La tabla de multiplicación en  $\mathbb{Z}_{12}$ 

**Teorema 7.38** (Pequeño teorema de Fermat). *Si  $p$  es primo, y  $p \nmid a$  entonces*

$$a^{p-1} \equiv 1 \pmod{p}$$

El hecho de que a este se le llame “pequeño” no tiene ninguna relación con su importancia, veremos una gran variedad de aplicaciones en lo que sigue. El “gran” (o “último”) teorema de Fermat es uno de los resultados más famosos de las matemáticas. Fermat anotó por 1637 en el margen de una copia de la Aritmética de Diofante que había descubierto una demostración verdaderamente maravillosa de que  $a^n + b^n = c^n$  no tiene soluciones para números naturales  $a, b, c$  si  $n > 2$ , pero que esta no cabía en el margen (tenía esta mala costumbre, la publicación del libro rayado después de su muerte dio trabajo a ejércitos de matemáticos durante bastante tiempo). Se le llamó el “último teorema” no por ser la última de sus innumerables conjeturas, sino por ser la última importante que quedaba sin resolver una vez que Euler terminó de trabajar en ellas. Recién en 1995 Andrew Wiles con la ayuda de su estudiante Richard Taylor [346, 362] demostró el último teorema de Fermat, aunque mediante métodos muy recientes (y no es precisamente una demostración “maravillosa”). Generalmente se piensa que Fermat se equivocó al creer que tenía una demostración.

## 8 Estructura de $\mathbb{Z}_m$ y $\mathbb{Z}_m^\times$

---

En nuestras aplicaciones los anillos de residuos son las estructuras algebraicas más importantes. Estudiaremos brevemente en sus características principales. Suele resultar fructífero descomponer estructuras complejas en piezas más simples para ayudar a su análisis. Incursionaremos un poco en el área de analizar la estructura de grupos abelianos, obteniendo algunos resultados de gran interés en áreas como la criptología.

### 8.1. Descomposiciones

Consideremos nuevamente el grupo  $D_8$ , que vimos en la sección 7.5, véase el cuadro 8.1. Si

$\circ$	$e$	$r$	$r^2$	$r^3$	$s$	$rs$	$r^2s$	$r^3s$
$e$	$e$	$r$	$r^2$	$r^3$	$s$	$rs$	$r^2s$	$r^3s$
$r$	$r$	$r^2$	$r^3$	$e$	$rs$	$r^2s$	$r^3s$	$s$
$r^2$	$r^2$	$r^3$	$e$	$r$	$r^2s$	$r^3s$	$s$	$rs$
$r^3$	$r^3$	$e$	$r$	$r^2$	$r^3s$	$s$	$rs$	$r^2s$
$s$	$s$	$r^3s$	$r^2s$	$rs$	$e$	$r^3$	$r^2$	$r$
$rs$	$rs$	$s$	$rs$	$r^2s$	$r$	$e$	$r^3$	$r^2$
$r^2s$	$r^2s$	$rs$	$s$	$r^3s$	$r^2$	$r$	$e$	$r$
$r^3s$	$r^3s$	$r^2s$	$rs$	$s$	$r^3$	$r^2$	$r$	$e$

Cuadro 8.1 – El grupo  $D_8$

analizamos las operaciones que lo componen, vemos que las operaciones  $\{e, r, r^2, r^3\}$  por sí solas también conforman un grupo (corresponden a solo girar el cuadrado en el plano, sin salir de él), o sea forman un subgrupo de  $D_8$ . Otros subgrupos están formados por  $e$  solo (el grupo trivial, nuevamente),  $\{e, r^2\}$ ,  $\{e, s\}$ .

Un ejemplo más simple (porque es un grupo abeliano) lo da  $\mathbb{Z}_{12}$  con la suma, véase el cuadro 7.4. En  $\mathbb{Z}_{12}$  son subgrupos  $\{0\}$ ,  $\{0, 6\}$ ,  $\{0, 4, 8\}$ ,  $\{0, 3, 6, 9\}$ ,  $\{0, 2, 4, 6, 8, 10\}$  y  $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ .

#### 8.1.1. Homomorfismos e isomorfismos

Consideremos los grupos  $\mathbb{Z}_8^\times$  y  $\mathbb{Z}_{12}^\times$ , que casualmente tienen el mismo número de elementos. Estas tablas (cuadros 8.2a y 8.2b) son diferentes, pero podemos ver que tienen la misma estructura, por ejemplo el mapa

$$\begin{aligned} 1 &\leftrightarrow 1 \\ 3 &\leftrightarrow 5 \\ 5 &\leftrightarrow 7 \\ 7 &\leftrightarrow 11 \end{aligned}$$

.	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

(a)  $\mathbb{Z}_8^\times$ 

.	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

(b)  $\mathbb{Z}_{12}^\times$ Cuadro 8.2 – Los grupos  $\mathbb{Z}_8^\times$  y  $\mathbb{Z}_{12}^\times$ 

traduce entre ellos. Sin embargo, hay grupos diferentes con cuatro elementos. Por ejemplo, tenemos  $\mathbb{Z}_5^\times$  (cuadro 8.3a) y  $\mathbb{Z}_4$  (cuadro 8.3b). Nótese que entre  $\mathbb{Z}_4$  y  $\mathbb{Z}_5^\times$  también podemos construir una

.	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(a)  $\mathbb{Z}_5^\times$ 

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(b)  $\mathbb{Z}_4$ Cuadro 8.3 – Los grupos  $\mathbb{Z}_5^\times$  y  $\mathbb{Z}_4$ 

correspondencia, a pesar que la operación involucrada es diferente:

$$\begin{array}{l} 0 \leftrightarrow 1 \\ 1 \leftrightarrow 2 \\ 2 \leftrightarrow 4 \\ 3 \leftrightarrow 3 \end{array}$$

No hay correspondencia posible entre  $\mathbb{Z}_5^\times$  y  $\mathbb{Z}_8^\times$ : En la diagonal de la tabla para  $\mathbb{Z}_5^\times$  (cuadro 8.3a) aparecen dos valores diferentes, mientras para  $\mathbb{Z}_8^\times$  (cuadro 8.2a) hay uno solo.

Esta idea de “misma estructura” es importante, y la capturamos con lo siguiente.

**Definición 8.1.** Sean dos grupos  $(G, 1_G, \odot)$  y  $(H, 1_H, \otimes)$ , un *homomorfismo* de  $G$  a  $H$  es una función  $h: G \rightarrow H$  tal que  $h(a \odot b) = h(a) \otimes h(b)$ . A un homomorfismo que es una biyección se le llama *isomorfismo*, y se dice en tal caso que los grupos son *isomorfos*, y se anota  $G \cong H$ . Un caso importante de isomorfismos son los isomorfismos de  $G$  a  $G$ , los *automorfismos*.

Las mismas ideas son aplicables a otras estructuras algebraicas, como anillos, si la función es homomorfismo (o isomorfismo) para ambas operaciones.

Un ejemplo conocido de homomorfismo es la clasificación de números en pares e impares, con las correspondientes reglas de sumas y productos. Un isomorfismo útil es el entre  $(\mathbb{R}^+, \cdot)$  y  $(\mathbb{R}, +)$  dado por los logaritmos.

Si  $h: G \rightarrow H$  es un homomorfismo, y  $1_G$  y  $1_H$  son los elementos neutros de  $G$  y  $H$ , respectivamente, claramente  $h(1_G) = 1_H$ , y  $h(a^{-1}) = (h(a))^{-1}$ .

Una manera simple de entender un isomorfismo es considerando que los dos grupos “son el mismo”, solo cambiando los nombres de los elementos y la operación. Es fácil demostrar que los grupos cíclicos finitos de orden  $n$  son isomorfos a  $\mathbb{Z}_n$ , y los infinitos isomorfos a  $\mathbb{Z}$ .

En  $\mathbb{Z}_p$  para  $p$  primo hay automorfismos que asocian 1 con cada elemento no cero. Esto no es más que otra forma de decir que módulo  $p$  todos los elementos tienen inverso.

El isomorfismo entre grupos es una relación de equivalencia: Es reflexiva, un grupo es isomorfo a sí mismo; es simétrica, ya si hay una biyección como la indicada, existe la función inversa que cumple las mismas condiciones; y es transitiva, siendo la composición de los isomorfismos el isomorfismo buscado. Es por ser una equivalencia que tiene sentido considerar “iguales” estructuras algebraicas isomorfas.

Una aplicación es la *prueba de los nueves*, popular cuando operaciones aritméticas se hacen manualmente. Consiste en verificar operaciones aritméticas (sumas, restas y multiplicaciones) vía calcular el residuo módulo nueve de los operandos, operar con los residuos, y comparar con el residuo módulo nueve del resultado. El punto es que (por el teorema 7.13) el reducir módulo  $m$  es un homomorfismo del anillo  $\mathbb{Z}$  a  $\mathbb{Z}_m$ , por lo que ambos residuos debieran coincidir. Calcular el residuo módulo nueve de un número escrito en decimal es simplemente sumar sus dígitos hasta llegar a un resultado de un único dígito: Como  $10 \equiv 1$  (mód 9), tenemos:

$$\sum_{0 \leq k \leq n} d_k \cdot 10^k \equiv \sum_{0 \leq k \leq n} d_k \pmod{9}$$

Demostramos un resultado similar en el lema 3.1.

### 8.1.2. Sumas directas

En lo que sigue discutiremos grupos abelianos, pero la operación que interesa puntualmente es la multiplicación entre enteros. Para evitar confusiones, usaremos notación de multiplicación y potencias, y no sumas como sería por convención general. Por lo demás, la notación como multiplicación es más compacta.

Siempre es útil tratar de descomponer estructuras complejas en piezas más simples. Consideremos el grupo de unidades  $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$  y dos de sus subgrupos,  $\{1, 3\}$  y  $\{1, 5\}$ . Todo elemento de  $\mathbb{Z}_8^\times$  puede escribirse como un producto de un elemento de cada uno de estos:

$$\begin{aligned} 1 &= 1 \cdot 1 & 5 &= 1 \cdot 5 \\ 3 &= 3 \cdot 1 & 7 &= 3 \cdot 5 \end{aligned}$$

Otro ejemplo provee  $\mathbb{Z}_{15}^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$ , con subgrupos  $\{1, 2, 4, 8\}$  y  $\{1, 11\}$ :

$$\begin{aligned} 1 &= 1 \cdot 1 & 8 &= 8 \cdot 1 \\ 2 &= 2 \cdot 1 & 11 &= 1 \cdot 11 \\ 4 &= 4 \cdot 1 & 13 &= 8 \cdot 11 \\ 7 &= 2 \cdot 11 & 14 &= 4 \cdot 11 \end{aligned}$$

Esto motiva la siguiente:

**Definición 8.2.** Sean  $A$  y  $B$  subgrupos del grupo abeliano  $G$  tales que todo  $g \in G$  puede escribirse de forma única como  $g = a \cdot b$ , con  $a \in A$  y  $b \in B$ . Entonces escribimos  $G = AB$  y decimos que  $G$  es la *suma directa* de  $A$  y  $B$ .

La utilidad de esta noción se debe en buena parte a que si sabemos qué son  $A$  y  $B$  conocemos  $AB$ :

**Teorema 8.1.** Si  $G = AB$ ,  $G' = A'B'$  y  $A \cong A'$ ,  $B \cong B'$ , entonces  $G \cong G'$ .

*Demuestra*ción. Supongamos que  $f: A \rightarrow A'$  y  $h: B \rightarrow B'$  son isomorfismos, construimos un isomorfismo  $k: G \rightarrow G'$  definiendo:

$$k(g) = f(a) \cdot h(b)$$

donde  $a \in A$ ,  $b \in B$  y  $g = a \cdot b$ . Primeramente, esta definición tiene sentido, ya que para  $g \in G$  los elementos  $a$  y  $b$  son únicos, con lo que  $k$  es una función. Es uno a uno, ya que si tomamos  $g_1 \neq g_2$ , al escribir  $g_1 = a_1 \cdot b_1$  y  $g_2 = a_2 \cdot b_2$ , necesariamente estos pares son diferentes, y como  $f$  y  $h$  son uno a uno, tendremos  $k(g_1) = f(a_1) \cdot h(b_1) \neq f(a_2) \cdot h(b_2) = k(g_2)$ . Es sobre ya que si tomamos  $g' \in G'$ , este puede escribirse de forma única como  $g' = a' \cdot b'$ , y usando las inversas de  $f$  y  $h$  esto lleva al elemento único  $g = f^{-1}(a') \cdot h^{-1}(b') \in G$  tal que  $k(g) = g'$ .  $\square$

Este enredo oculta algo muy simple: Si  $G = AB$ , se puede expresar  $g \in G$  mediante las “coordenadas”  $(a, b)$  con  $g = a \cdot b$ , y considerar  $AB$  como  $A \times B$  con operación  $(a, b) \cdot (a', b') = (a \cdot a', b \cdot b')$ . En estos términos, la operación en  $AB$  está completamente determinada por las operaciones en  $A$  y  $B$ ; si  $A'$  es una copia de  $A$  y  $B'$  es una copia de  $B$ , entonces  $G' = A'B'$  es simplemente una copia de  $G = AB$ .

Analicemos  $\mathbb{Z}_{15}^\times$  y  $\mathbb{Z}_{16}^\times$ . Ya vimos que  $\mathbb{Z}_{15}^\times = \{1, 2, 4, 8\}\{1, 11\}$ ; mientras  $\mathbb{Z}_{16}^\times = \{1, 3, 5, 7, 9, 11, 13, 15\}$ , con subgrupos  $\{1, 3, 9, 11\}$  y  $\{1, 7\}$ , y tenemos  $\mathbb{Z}_{16}^\times = \{1, 3, 9, 11\}\{1, 7\}$ . Pero  $\{1, 2, 4, 8\}$  y  $\{1, 3, 9, 11\}$  son grupos cíclicos de orden 4, y por tanto isomorfos a  $\mathbb{Z}_4$ ; y por el otro lado  $\{1, 11\}$  y  $\{1, 7\}$  son cíclicos de orden 2, isomorfos a  $\mathbb{Z}_2$ . Entonces  $\mathbb{Z}_{15}^\times \cong \mathbb{Z}_{16}^\times$ .

Para cálculos concretos el siguiente teorema es útil:

**Teorema 8.2.** *Si  $A$  y  $B$  son subgrupos del grupo abeliano  $G$  tales que  $A \cap B = \{1\}$  y  $|A| \cdot |B| = |G|$  entonces  $G = AB$ .*

*Demostración.* Consideremos los productos  $ab$  con  $a \in A$  y  $b \in B$ . Demostramos que son diferentes por contradicción. Supongamos pares distintos  $(a_1, b_1)$  y  $(a_2, b_2)$  tales que  $a_1 \odot b_1 = a_2 \odot b_2$ . Entonces  $a_1 \odot a_2^{-1} = b_1^{-1} \odot b_2$ . Pero  $a_1 \odot a_2^{-1} \in A$  y  $b_1^{-1} \odot b_2 \in B$ , con lo que esto tiene que estar en la intersección entre ambos, o sea  $a_1 \odot a_2^{-1} = b_1 \odot b_2^{-1} = 1$ , con lo que  $a_1 = a_2$  y  $b_1 = b_2$ .

Con esto hay exactamente  $|A| \cdot |B| = |G|$  productos  $a \odot b$  diferentes, que tienen que ser todos los elementos de  $G$ .  $\square$

El grupo  $\mathbb{Z}_{16}^\times$  tiene  $8 = 4 \cdot 2$  elementos, con lo que de los subgrupos  $\{1, 3, 9, 11\}$  y  $\{1, 7\}$  tenemos  $\mathbb{Z}_{16}^\times = \{1, 3, 9, 11\}\{1, 7\}$ , ya que  $\{1, 3, 9, 11\} \cap \{1, 7\} = \{1\}$ .

Esto puede extenderse a más de dos subgrupos. Por ejemplo,  $\mathbb{Z}_{30}$  tiene subgrupos  $\{0, 6, 12, 18, 24\}$  y  $\{0, 5, 10, 15, 20, 25\}$ , de órdenes 5 y 6, con intersección  $\{0\}$ . Por el teorema 8.2 tenemos la descomposición  $\mathbb{Z}_{30} = \{0, 6, 12, 18, 24\}\{0, 5, 10, 15, 20, 25\}$ . Por su lado,  $\{0, 5, 10, 15, 20, 25\}$  tiene subgrupos  $\{0, 10, 20\}$  y  $\{0, 15\}$ , de órdenes 3 y 2, y es  $\{0, 5, 10, 15, 20, 25\} = \{0, 10, 20\}\{0, 15\}$ . Esto sugiere extender la definición 8.2 y escribir  $\mathbb{Z}_{30} = \{0, 6, 12, 18, 24\}\{0, 10, 20\}\{0, 15\}$ .

**Definición 8.3.** Sea  $G$  un grupo abeliano, y sean  $A_1, A_2, \dots, A_n$  subgrupos de  $G$  tales que todo elemento de  $G$  puede escribirse de forma única como  $a_1 \cdot a_2 \cdots a_n$ , con  $a_i \in A_i$  para todo  $1 \leq i \leq n$ . Entonces  $G$  es la *suma directa* de los subgrupos  $A_1, A_2, \dots, A_n$ , y anotamos  $G = A_1 A_2 \cdots A_n$ .

Si  $G = A_1 A_2 \cdots A_n$  y  $g = a_1 a_2 \cdots a_n$  con  $a_i \in A_i$  decimos que  $a_i$  es el *componente* de  $g$  en  $A_i$ . Por la definición de suma directa el componente de  $g$  en  $A_i$  es único. Una relación útil entre el orden del elemento y los órdenes de sus componentes es la siguiente:

**Teorema 8.3.** *Si  $G = A_1 A_2 \cdots A_n$  y  $g \in G$ , entonces el orden de  $g$  es el mínimo común múltiplo de los órdenes de los componentes de  $g$*

*Demostración.* Sea  $g = a_1 \cdot a_2 \cdots a_n$  con  $a_i \in A_i$ . Para cualquier entero  $s$  tendremos  $g^s = a_1^s \cdot a_2^s \cdots a_n^s$ . Como  $a_i^s \in A_i$ , el componente en  $A_i$  de  $g^s$  es  $a_i^s$ . Por otro lado, el componente de 1 en  $A_i$  es 1, y  $g^s = 1$  solo si  $a_i^s = 1$  para todo  $1 \leq i \leq n$ , con lo que  $s$  es un múltiplo del orden de  $a_i$  para cada  $1 \leq i \leq n$ , y el orden de  $g$  es el menor de todos los posibles múltiplos.  $\square$

11	4	8	1
$11^2 = 16$	$4^2 = 16$	$8^2 = 1$	
$11^3 = 8$	$4^3 = 1$		
$11^4 = 4$			
$11^5 = 2$			
$11^6 = 1$			

Cuadro 8.4 – Potencias en  $\mathbb{Z}_{21}^\times$ 

Para ilustrar lo anterior, consideremos  $\mathbb{Z}_{21}^\times = \{1, 4, 16\} \{1, 8\} \{1, 13\}$ . Si tomamos  $11 \in \mathbb{Z}_{21}^\times$ , se descompone en  $11 = 4 \cdot 8 \cdot 1$ . Las potencias respectivas las da el cuadro 8.4, lo que confirma que el orden de 11 es  $6 = 3 \cdot 2 \cdot 1$ .

### 8.1.3. Sumas directas externas

Hasta acá hemos descompuesto un grupo en la suma directa de subgrupos. La pregunta inversa es si dados grupos  $A_1, A_2, \dots, A_n$ , podemos construir  $G$  con subgrupos  $H_1, H_2, \dots, H_n$  tales que  $G = H_1 H_2 \cdots H_n$  con  $A_i \cong H_i$  para todo  $1 \leq i \leq n$ . La respuesta es afirmativa, y la construcción es muy simple. Vimos que si  $G = H_1 H_2 \cdots H_n$ , entonces  $g \in G$  puede escribirse  $g = h_1 h_2 \cdots h_n$  en forma única, con  $h_i \in H_i$ . Especificar  $g$  es lo mismo que especificar la tupla de coordenadas  $h_i$ . De igual manera, dado  $k \in G$  podemos escribirlo  $k = k_1 k_2 \cdots k_n$  en forma única, con  $k_i \in H_i$ , y  $gk = h_1 h_2 \cdots h_n \cdot k_1 k_2 \cdots k_n = (h_1 k_1)(h_2 k_2) \cdots (h_n k_n)$ , donde  $h_i k_i \in H_i$  resulta ser la coordenada de  $gk$ . Esta situación motiva la definición siguiente:

**Definición 8.4.** Sean  $A_1, A_2, \dots, A_n$  grupos abelianos. La *suma directa (externa)* de  $A_1, A_2, \dots, A_n$  es el conjunto de tuplas  $(a_1, a_2, \dots, a_n)$  con  $a_i \in A_i$  y operación dada por:

$$(a_1, a_2, \dots, a_n) \cdot (b_1, b_2, \dots, b_n) = (a_1 \cdot b_1, a_2 \cdot b_2, \dots, a_n \cdot b_n)$$

Escribiremos  $G = A_1 \times A_2 \times \cdots \times A_n$  para la suma directa externa de los grupos  $A_1, \dots, A_n$ .

De acá resulta:

**Teorema 8.4.** La suma directa (externa) de los grupos abelianos  $A_1, A_2, \dots, A_n$  es un grupo abeliano,  $G = H_1 H_2 \cdots H_n$ , donde  $H_i$  es el conjunto de tuplas de la forma  $(1, \dots, 1, a_i, 1, \dots, 1)$  con  $a_i \in A_i$  (todas las componentes, salvo la  $i$ -ésima, son 1). Además,  $H_i \cong A_i$  para todo  $1 \leq i \leq n$ .

*Demostración.* Demostrar que  $G$  es un grupo abeliano es automático; hay que verificar que la operación es cerrada (inmediato de la definición), asociatividad (resulta directamente de la asociatividad en cada  $A_i$ ), existencia de neutro (resulta ser  $(1, \dots, 1)$ ), conmutatividad (directamente de cada  $A_i$ ) e inverso (el inverso de  $(a_1, a_2, \dots, a_n)$  es  $(a_1^{-1}, a_2^{-1}, \dots, a_n^{-1})$ ).

Podemos escribir un elemento  $g \in G$  como:

$$(a_1, a_2, \dots, a_n) = (a_1, 1, \dots, 1) \cdot (1, a_2, \dots, 1) \cdots (1, 1, \dots, a_n)$$

Acá  $(1, \dots, 1, a_i, 1, \dots, 1) \in H_i$ , lo que puede hacerse de una única forma, y los  $H_i$  son subgrupos de  $G$ . Resulta  $G = H_1 H_2 \cdots H_n$ , y  $f_i: H_i \rightarrow A_i$  que mapea  $(1, \dots, 1, a_i, 1, \dots, 1)$  a  $a_i$  es un isomorfismo.  $\square$

La noción de sumas directas externas da una notación conveniente para describir grupos abelianos. Por ejemplo, vimos  $\mathbb{Z}_{15}^\times = \{1, 2, 4, 8\} \{1, 11\}$ ; pero estos dos son grupos cíclicos de orden 4 y 2, respectivamente, con lo que  $\mathbb{Z}_{15}^\times \cong \mathbb{Z}_4 \times \mathbb{Z}_2$  dice todo lo que hay que saber sobre  $\mathbb{Z}_{15}^\times$ .

### 8.1.4. Comentarios finales

Temas relacionados con grupos, anillos y otras estructuras algebraicas profundizan bastante textos del área como Connell [76] y Judson [190].

Lo que nosotros llamamos  $\mathbb{Z}_m$  se conoce formalmente como  $\mathbb{Z}/m\mathbb{Z}$ . Para justificar esta notación, primeramente definimos:

**Definición 8.5.** Sea  $G$  un grupo. Un subgrupo  $N$  de  $G$  se dice *normal* (se anota  $N \triangleleft G$ ) si para todo  $n \in N$  y  $g \in G$  tenemos  $gng^{-1} \in N$ .

Los subgrupos de un grupo abeliano son siempre normales.

En ciertas situaciones los cosets de un subgrupo se pueden dotar con una operación heredada del grupo  $G$  para dar un nuevo grupo, el *grupo cociente* o *factor*

$$G/N = \{gN : g \in G\}$$

con operación

$$(gN) \bullet (hN) = (gh)N$$

Esto solo funciona si  $N \triangleleft G$ , en cuyo caso el mapa  $g \mapsto gN$  es un homomorfismo de  $G$  a  $G/N$ .

Ahora bien, el coset  $m\mathbb{Z}$  es un subgrupo de  $\mathbb{Z}$ , y es un subgrupo normal ya que todos los subgrupos de un grupo abeliano son normales. Vemos que  $a + m\mathbb{Z}$  es precisamente el conjunto  $r + m\mathbb{Z}$ , donde  $r = a \pmod{m}$ , y la suma en  $\mathbb{Z}/m\mathbb{Z}$  es exactamente como la describimos en 7.5.

Otra notación común es  $\mathbb{Z}/(m)$ , usando la misma idea anterior pero describiendo el conjunto de los múltiplos de  $m$  como el ideal generado por  $m$ , vale decir el conjunto  $\{rm : r \in \mathbb{Z}\}$ . Estudiaremos este importante concepto en la sección 9.2.

Nuestra primera tarea es descomponer  $\mathbb{Z}_m$  en forma más sistemática. Lo que hemos hecho hasta ahora es tomar elementos que se ven bien y considerar los subgrupos que generan, tratando de encontrar intersecciones y órdenes adecuados. Acá veremos un método general para descomponer el grupo  $\mathbb{Z}_m$ , y plantear el camino para entender mejor los grupos  $\mathbb{Z}_m^\times$ .

Por ejemplo,  $\mathbb{Z}_{30} = \{0, 6, 12, 18, 24\} \cup \{0, 5, 10, 15, 20, 25\}$  o sea  $\mathbb{Z}_{30}$  es la suma directa de un grupo cíclico de orden 5 y otro de orden 6, y por el teorema 8.1 esto es  $\mathbb{Z}_{30} \cong \mathbb{Z}_5 \times \mathbb{Z}_6$ . Por otro lado, hay una función obvia  $f: \mathbb{Z}_{30} \rightarrow \mathbb{Z}_5 \times \mathbb{Z}_6$ : Si conocemos un entero  $x$  módulo 30, sabemos sus residuos módulos 5 y 6. Por ejemplo, si  $x \equiv 13 \pmod{30}$ , entonces  $x \equiv 13 \equiv 3 \pmod{5}$  y  $x \equiv 13 \equiv 1 \pmod{6}$ . En este caso, tendríamos  $f(13) = (3, 1)$ . Una tabla completa para  $f$  es:

$$\begin{array}{llllll} f(0) = (0, 0) & f(6) = (1, 0) & f(12) = (2, 0) & f(18) = (3, 0) & f(24) = (4, 0) \\ f(1) = (1, 1) & f(7) = (2, 1) & f(13) = (3, 1) & f(19) = (4, 1) & f(25) = (0, 1) \\ f(2) = (2, 2) & f(8) = (3, 2) & f(14) = (4, 2) & f(20) = (0, 2) & f(26) = (1, 2) \\ f(3) = (3, 3) & f(9) = (4, 3) & f(15) = (0, 3) & f(21) = (1, 3) & f(27) = (2, 3) \\ f(4) = (4, 4) & f(10) = (0, 4) & f(16) = (1, 4) & f(22) = (2, 4) & f(28) = (3, 4) \\ f(5) = (0, 5) & f(11) = (1, 5) & f(17) = (2, 5) & f(23) = (3, 5) & f(29) = (4, 5) \end{array}$$

El que  $f$  es uno a uno se ve directamente de la tabla. Las restantes propiedades son obvias si consideramos que cada entrada como  $f([x]_{30}) = ([x]_5, [x]_6)$ . Tenemos el siguiente teorema general:

**Teorema 8.5.** Sea  $m = ab$  con  $a, b$  enteros positivos tales que  $\gcd(a, b) = 1$ . Entonces la función:

$$f([x]_m) = ([x]_a, [x]_b) \quad x \in \mathbb{Z}$$

es un isomorfismo entre los anillos  $\mathbb{Z}_m$  y  $\mathbb{Z}_a \times \mathbb{Z}_b$ .

*Demostración.* Primero debemos demostrar que  $f$  siquiera tiene sentido, hay muchas elecciones de  $x$  que dan la misma clase  $[x]_m$  en  $\mathbb{Z}_m$ . El teorema 7.12 asegura que  $f$  es una biyección, ya que  $\gcd(a, b) = 1$ .

Además tenemos del teorema 7.11 que:

$$\begin{aligned} f([x+y]_m) &= ([x+y]_a, [x+y]_b) \\ &= ([x]_a + [y]_a, [x]_b + [y]_b) \\ &= ([x]_a, [x]_b) + ([y]_a, [y]_b) \\ &= f(x) + f(y) \\ f([xy]_m) &= ([xy]_a, [xy]_b) \\ &= ([x]_a \cdot [y]_a, [x]_b \cdot [y]_b) \\ &= ([x]_a, [x]_b) \cdot ([y]_a, [y]_b) \\ &= f(x) \cdot f(y) \end{aligned}$$

y es isomorfismo de anillo.  $\square$

Hay que tener cuidado en esto, la condición de que  $\gcd(a, b) = 1$  es necesaria. Por ejemplo,  $\mathbb{Z}_8 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_4$ , ya que:

$$\begin{array}{ll} 2 \equiv 0 \pmod{2} & 2 \equiv 2 \pmod{4} \\ 6 \equiv 0 \pmod{2} & 6 \equiv 2 \pmod{4} \end{array}$$

Esta no es una biyección.

Aplicando el teorema 8.5 repetidas veces tenemos:

**Corolario 8.6.** Sean  $a_1, a_2, \dots, a_r$  naturales relativamente primos a pares (o sea,  $\gcd(a_i, a_j) = 1$  si  $i \neq j$ ), y  $m = a_1 a_2 \cdots a_r$ . Entonces la función:

$$f([x]_m) = ([x]_{a_1}, [x]_{a_2}, \dots, [x]_{a_r})$$

es un isomorfismo de anillo entre  $\mathbb{Z}_m$  y  $\mathbb{Z}_{a_1} \times \mathbb{Z}_{a_2} \times \cdots \times \mathbb{Z}_{a_r}$

Una consecuencia inmediata es el siguiente importante teorema:

**Teorema 8.7** (Teorema chino de los residuos). Sean  $a_1, a_2, \dots, a_r$  naturales relativamente primos a pares, y  $b_1, b_2, \dots, b_r$  enteros cualquiera. Entonces hay un entero  $x$  tal que:

$$x \equiv b_1 \pmod{a_1}$$

$$x \equiv b_2 \pmod{a_2}$$

$\vdots$

$$x \equiv b_r \pmod{a_r}$$

El entero  $x$  es único módulo  $n = a_1 a_2 \cdots a_r$ .

*Demostración.* Considere el elemento  $([b_1]_{a_1}, [b_2]_{a_2}, \dots, [b_r]_{a_r})$  en  $\mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_r}$ . Por el isomorfismo del corolario 8.6 hay un único  $[x]_m \in \mathbb{Z}_m$  tal que  $[x]_{a_1} = [b_1]_{a_1}$ ,  $[x]_{a_2} = [b_2]_{a_2}$ , ...,  $[x]_{a_r} = [b_r]_{a_r}$ , lo que no es más que otra forma de decir que hay un entero  $x$ , único módulo  $n$ , que cumple el sistema de ecuaciones indicado.  $\square$

Al teorema 8.5 (o también al corolario 8.6) se le debiera llamar el *padre del teorema chino de los residuos*, son estos resultados los que en realidad más se usan bajo ese nombre. En inglés se abrevia *CRT*, por *Chinese Remainder Theorem*.

Usando la notación del teorema chino de los residuos, para cálculo concreto esto se puede expresar mediante lo siguiente. Defina  $s_i$  como  $s_i \cdot (n/a_i) \equiv 1$  (mód  $a_i$ ), y defina  $m_i = s_i \cdot (n/a_i)$ , con lo que  $m_i \equiv [i = j]$  (mód  $a_j$ ). Considere:

$$x = \sum_{1 \leq i \leq r} m_i \cdot b_i$$

Entonces:

$$\begin{aligned} x &\equiv \sum_{1 \leq i \leq r} m_i \cdot b_i \pmod{a_k} \\ &\equiv m_k \cdot b_k \pmod{a_k} \\ &\equiv b_k \pmod{a_k} \end{aligned}$$

Con esto el isomorfismo del corolario 8.6 puede usarse en la práctica. La demostración del teorema 8.7 no da luces de cómo obtener el valor  $x$ , solo asegura que si probamos todas las opciones hallaremos exactamente una solución.

Para clarificar ideas, resolveremos un ejemplo. Buscamos  $x$  tal que:

$$\begin{aligned} x &\equiv 3 \pmod{5} \\ x &\equiv 5 \pmod{7} \\ x &\equiv 1 \pmod{9} \end{aligned}$$

Los módulos son primos entre sí, hay una solución única módulo  $n = 5 \cdot 7 \cdot 9 = 315$ . Necesitamos los siguientes inversos:

$$\begin{aligned} s_5 &= (315/5)^{-1} = 2 \text{ en } \mathbb{Z}_5 \\ s_7 &= (315/7)^{-1} = 5 \text{ en } \mathbb{Z}_7 \\ s_9 &= (315/9)^{-1} = 8 \text{ en } \mathbb{Z}_9 \end{aligned}$$

lo que da los coeficientes, ahora módulo 315:

$$\begin{aligned} m_5 &= 2 \cdot (315/5) = 126 \\ m_7 &= 5 \cdot (315/7) = 225 \\ m_9 &= 8 \cdot (315/9) = 280 \end{aligned}$$

Para resolver nuestro problema concreto:

$$\begin{aligned} x &= 126 \cdot 3 + 225 \cdot 5 + 280 \cdot 1 \\ &= 1783 \\ &\equiv 208 \pmod{315} \end{aligned}$$

Como ejercicio, dejamos el problema planteado por Sunzi en el siglo IV.

Hay cierto número de objetos cuyo número es desconocido.  
Dividido por 3, el resto es 2;  
por 5 el resto es 3;  
y por 7 el resto es 2.  
¿Cuántos serán los objetos?

Supongamos ahora que piden:

$$x \equiv 2 \pmod{6}$$

$$x \equiv 1 \pmod{7}$$

$$x \equiv 3 \pmod{9}$$

Los módulos no son relativamente primos, puede no haber solución. Tenemos para el par en conflicto:

$$x = 6s + 2 = 9t + 3$$

$$6s - 9t = 1$$

Esto último es imposible, ya que significaría que el máximo común divisor entre 6 y 9 divide a 1, pero  $\gcd(6, 9) = 3$ . No hay solución.

Antes de continuar, algunas propiedades adicionales del máximo común divisor y el mínimo común múltiplo.

**Lema 8.8.** *Se cumplen:*

$$\gcd(a, \gcd(b, c)) = \gcd(\gcd(a, b), c)$$

$$\text{lcm}(a, \text{lcm}(b, c)) = \text{lcm}(\text{lcm}(a, b), c)$$

Además:

$$\gcd(\text{lcm}(a_1, b), \text{lcm}(a_2, b), \dots, \text{lcm}(a_r, b)) = \text{lcm}(\gcd(a_1, a_2, \dots, a_r), b)$$

$$\text{lcm}(\gcd(a_1, b), \gcd(a_2, b), \dots, \gcd(a_r, b)) = \gcd(\text{lcm}(a_1, a_2, \dots, a_r), b)$$

Básicamente, las operaciones son asociativas y cumplen leyes distributivas.

*Demostración.* Por el teorema fundamental de la aritmética, todo entero puede representarse por el conjunto de los divisores que son potencias de números primos. En estos términos, el máximo común divisor es la intersección de sus argumentos, y el mínimo común múltiplo su unión. Las identidades indicadas son entonces reflejo de la asociatividad de la unión e intersección, y la distributividad de la unión sobre la intersección y viceversa.  $\square$

Podemos extender el teorema chino de los residuos:

**Teorema 8.9** (Teorema chino de los residuos generalizado). *Para  $a_1, b_1, \dots, a_r, b_r$  cualquiera sean:*

$$x \equiv a_1 \pmod{b_1}$$

$$x \equiv a_2 \pmod{b_2}$$

$\vdots$

$$x \equiv a_r \pmod{b_r}$$

*Estas congruencias tienen solución si y solo si  $a_i \equiv a_j \pmod{\gcd(b_i, b_j)}$  para todo  $i, j$ . Módulo  $\text{lcm}(b_1, b_2, \dots, b_r)$  la solución es única en tal caso.*

*Demostración.* Por inducción sobre  $r$ . Cuando  $r = 1$ , el resultado es obvio. Partiremos con el caso  $r = 2$  porque lo usaremos en el paso de inducción.

**Base:** Tenemos las congruencias:

$$\begin{aligned}x &\equiv a_1 \pmod{b_1} \\x &\equiv a_2 \pmod{b_2}\end{aligned}$$

Si  $d \mid b_1$ , claramente  $x \equiv a_1 \pmod{d}$ . En particular, para  $m_2 = \gcd(b_1, b_2)$  debe ser:

$$\begin{aligned}x &\equiv a_1 \pmod{m_2} \\x &\equiv a_2 \pmod{m_2}\end{aligned}$$

con lo que no hay solución a menos que  $a_1 \equiv a_2 \pmod{m_2}$ . Esta es la condición sobre los  $b_i$  para el caso  $r = 2$ .

Si  $a_1 \equiv a_2 \pmod{m_2}$ , por la identidad de Bézout sabemos que existen enteros  $u_2$  y  $v_2$  tales que:

$$u_2 b_1 + v_2 b_2 = \gcd(b_1, b_2) = m_2$$

Como  $a_1 \equiv a_2 \pmod{m_2}$ , hay  $c_2 \in \mathbb{Z}$  tal que  $a_1 - a_2 = c_2 \cdot m_2$ , y  $a_1 - a_2 = c_2 u_2 b_1 + c_2 v_2 b_2$ . Con esto:

$$s_2 = a_1 - c_2 u_2 b_1 = a_2 + c_2 v_2 b_2$$

cumple ambas congruencias.

Para demostrar que es única, consideremos soluciones  $s$  y  $s'$ . Vemos que  $s \equiv s' \pmod{b_1}$  y  $s \equiv s' \pmod{b_2}$ , y el teorema 7.12 asegura que  $s \equiv s' \pmod{\text{lcm}(b_1, b_2)}$ .

**Inducción:** Suponiendo que vale para  $r$  congruencias, demostramos que vale para  $r + 1$ :

$$\begin{aligned}x &\equiv a_1 \pmod{b_1} \\x &\equiv a_2 \pmod{b_2} \\&\vdots \\x &\equiv a_r \pmod{b_r} \\x &\equiv a_{r+1} \pmod{b_{r+1}}\end{aligned}$$

Sea  $s_r$  la solución a las primeras  $r$  congruencias, que por inducción existe y es única módulo  $\text{lcm}(b_1, b_2, \dots, b_r)$ . Consideremos las congruencias:

$$\begin{aligned}x &\equiv s_r \pmod{\text{lcm}(b_1, b_2, \dots, b_r)} \\x &\equiv a_{r+1} \pmod{b_{r+1}}\end{aligned}$$

Por el caso  $r = 2$  sabemos que hay solución únicamente si:

$$s_r \equiv a_{r+1} \pmod{\gcd(\text{lcm}(b_1, \dots, b_r), b_{r+1})}$$

Por el lema 8.8:

$$\gcd(\text{lcm}(b_1, \dots, b_r), b_{r+1}) = \text{lcm}(\gcd(b_1, b_{r+1}), \gcd(b_2, b_{r+1}), \dots, \gcd(b_r, b_{r+1}))$$

que es equivalente a:

$$a_{r+1} \equiv a_i \pmod{\gcd(b_i, b_{r+1})} \quad \text{para todo } 1 \leq i \leq r$$

Esto extiende la condición sobre los  $a_i$ .

De cumplirse la condición sobre los  $a_i$ , hay una solución  $s_{r+1}$  única módulo  $\text{lcm}(b_1, \dots, b_{r+1})$ , que podemos calcular como antes. Sean  $u_{r+1}$  y  $v_{r+1}$  tales que:

$$u_{r+1}s_r + v_{r+1}b_{r+1} = \gcd(s_r, b_{r+1})$$

Como  $s_r \equiv a_{r+1}$  (mód  $b_{r+1}$ ), existe  $c_{r+1} \in \mathbb{Z}$  en  $s_r - a_{r+1} = c_{r+1}\gcd(s_r, b_{r+1})$ , y  $s_{r+1}$  definido como sigue cumple las  $r+1$  congruencias:

$$s_{r+1} = s_r - c_{r+1}u_{r+1}\text{lcm}(b_1, \dots, b_r) = a_{r+1} + c_{r+1}v_{r+1}b_{r+1}$$

Por inducción lo indicado vale para  $r \in \mathbb{N}$ . □

La demostración da un algoritmo para obtener la solución. Por ejemplo, consideremos el sistema:

$$x \equiv 3 \pmod{4}$$

$$x \equiv 5 \pmod{6}$$

$$x \equiv 2 \pmod{9}$$

Para las primeras dos congruencias tenemos:

$$4u_2 + 6v_2 = \gcd(4, 6) = 2$$

Obtenemos  $u_2 = -1$ ,  $v_2 = 1$ , y tenemos  $a_1 - a_2 = 3 - 5 = -2$  que da  $c_2 = -1$ , por lo que:

$$s_2 = 3 - (-1)(-1)4 = -1$$

Como  $\text{lcm}(4, 6) = 12$ , para el segundo paso queda el sistema:

$$x \equiv -1 \pmod{12}$$

$$x \equiv 7 \pmod{9}$$

Tenemos:

$$12u_3 + 9v_3 = \gcd(12, 9) = 3$$

Esto resulta en  $u_3 = 1$  y  $v_3 = -1$ , para  $s_2 - a_3 = -1 - 2 = -3$  es  $c_3 = -1$ , y queda:

$$s_3 = -1 - (-1) \cdot 1 \cdot 12 = 11$$

La solución es única módulo  $\text{lcm}(4, 6, 9) = 36$ .

El algoritmo implícito en el teorema 8.9 es bastante engorroso. Una forma diferente de enfocar el tema es dividir las congruencias según los máximos comunes divisores. Veamos el ejemplo:

$$x \equiv 9 \pmod{12}$$

$$x \equiv 12 \pmod{21}$$

Tenemos  $\gcd(12, 21) = 3$ , con lo que  $12 = 3 \cdot 4$  y  $21 = 3 \cdot 7$ . La primera congruencia se descompone:

$$x \equiv 9 \equiv 0 \pmod{3}$$

$$x \equiv 9 \equiv 1 \pmod{4}$$

La segunda da:

$$\begin{aligned}x &\equiv 12 \equiv 0 \pmod{3} \\x &\equiv 12 \equiv 5 \pmod{7}\end{aligned}$$

Las congruencias comunes (módulo 3) son consistentes, hay solución módulo  $\text{lcm}(12, 21) = 84$ . El sistema se reduce a:

$$\begin{aligned}x &\equiv 0 \pmod{3} \\x &\equiv 1 \pmod{4} \\x &\equiv 5 \pmod{7}\end{aligned}$$

El teorema chino de los residuos da:

$$\begin{aligned}s_3 &= (4 \cdot 7)^{-1} = 1 & m_3 &= 1 \cdot 4 \cdot 7 = 28 \\s_4 &= (3 \cdot 7)^{-1} = 1 & m_4 &= 1 \cdot 3 \cdot 7 = 21 \\s_7 &= (3 \cdot 4)^{-1} = 3 & m_7 &= 3 \cdot 3 \cdot 4 = 36\end{aligned}$$

y la solución es:

$$\begin{aligned}x &= 0 \cdot 28 + 1 \cdot 21 + 5 \cdot 36 \\&\equiv 33 \pmod{84}\end{aligned}$$

Un problema en esta línea planteó Brahmagupta en el siglo VII.

Una anciana va al mercado, y un caballo pisa su canasto y le aplasta los huevos.

El jinete ofrece pagar el daño y le pregunta cuántos huevos traía.

Ella no recuerda el número exacto, pero al sacarlos de a dos sobraba un huevo. Lo mismo ocurría si los sacaba de a tres, cuatro, cinco y seis a la vez, pero al sacarlos de a siete no sobró ninguno.

¿Cuál es el mínimo número de huevos que podría haber tenido?

Una aplicación adicional es la *prueba del once*: Vimos antes (sección 8.1) que una manera de verificar operaciones aritméticas es la prueba de los nueves, que es simple de aplicar porque calcular el residuo módulo nueve de un número escrito en decimal es sumar sus dígitos, repitiendo el proceso hasta reducir a uno solo. Resulta que calcular el residuo módulo once es sumar y restar alternativamente los dígitos comenzando por el menos significativo: Como  $10 \equiv -1 \pmod{11}$ , tenemos:

$$\sum_{0 \leq k \leq n} d_k \cdot 10^k \equiv \sum_{0 \leq k \leq n} (-1)^k d_k \pmod{11}$$

Si aplicamos la prueba del nueve y la prueba del once, como  $\text{gcd}(9, 11) = 1$ , estamos verificando el resultado módulo  $9 \cdot 11 = 99$ .

El teorema 8.7 (más bien, el corolario 8.6) ofrece una importante estrategia adicional para demostrar teoremas en  $\mathbb{Z}$ :

1. Primeramente, demuestre el resultado para  $p$  primo.
2. Enseguida, demuestre que es válido para  $p^\alpha$ , potencias de primos.
3. Use el (padre del) teorema chino de los residuos para combinar los resultados anteriores y obtener el caso general.

Más adelante aparecerán muchas aplicaciones de esta idea.

## 8.2. Estructura de $\mathbb{Z}_m^\times$

El isomorfismo del teorema 8.5 permite demostrar:

**Teorema 8.10.** Si  $a$  y  $b$  son naturales relativamente primos, entonces:

$$\mathbb{Z}_{ab}^\times \cong \mathbb{Z}_a^\times \times \mathbb{Z}_b^\times$$

*Demostración.* Sabemos que  $\mathbb{Z}_{ab}$  y  $\mathbb{Z}_a \times \mathbb{Z}_b$  son anillos isomorfos, con lo que  $\mathbb{Z}_{ab}^\times$  es isomorfo al grupo de unidades de  $\mathbb{Z}_a \times \mathbb{Z}_b$ . Ahora bien, un elemento de  $\mathbb{Z}_a \times \mathbb{Z}_b$  es invertible si lo son sus componentes:

$$(x, y) \cdot (x', y') = (xx', yy') = (1, 1)$$

con  $x \in \mathbb{Z}_a^\times$  e  $y \in \mathbb{Z}_b^\times$ , con lo que el grupo de unidades de  $\mathbb{Z}_a \times \mathbb{Z}_b$  es exactamente  $\mathbb{Z}_a^\times \times \mathbb{Z}_b^\times$ .  $\square$

Como corolario, tenemos para la función  $\phi$  de Euler:

**Corolario 8.11.** Sea  $\phi$  la función de Euler. Si  $a$  y  $b$  son naturales relativamente primos, entonces  $\phi(ab) = \phi(a) \cdot \phi(b)$

*Demostración.* Del teorema 8.10 sabemos que:

$$\phi(ab) = |\mathbb{Z}_{ab}^\times| = |\mathbb{Z}_a^\times \times \mathbb{Z}_b^\times| = |\mathbb{Z}_a^\times| \cdot |\mathbb{Z}_b^\times| = \phi(a) \cdot \phi(b)$$

$\square$

Esta propiedad es importante:

**Definición 8.6.** Una función  $f: \mathbb{N} \rightarrow \mathbb{C}$  se llama *aritmética*. Anotaremos  $\mathcal{A}$  para el conjunto de funciones aritméticas. Una función aritmética  $f$  se llama *multiplicativa* si  $f(a \cdot b) = f(a) \cdot f(b)$  siempre que  $\gcd(a, b) = 1$ . A su conjunto lo llamamos  $\mathcal{M}$ .

Supongamos que  $f$  es multiplicativa, y que para algún  $n \in \mathbb{N}$  es  $f(n) \neq 0$ . Como  $\gcd(1, n) = 1$ :

$$f(n) = f(n \cdot 1) = f(n) \cdot f(1)$$

con lo que  $f(1) = 1$  o  $f(n) = 0$  para todo  $n \in \mathbb{N}$ .

Por el teorema fundamental de la aritmética todo entero se puede descomponer en un producto de potencias de primos distintos. Como potencias de primos diferentes son relativamente primas, una función multiplicativa queda determinada por su valor para potencias de primos.

Como acabamos de demostrar que  $\phi$  es multiplicativa, tenemos una manera de calcularla:

**Corolario 8.12.** Sea  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$  la factorización completa de  $n$  en primos distintos  $p_i$ . Entonces:

$$\begin{aligned} \phi(n) &= p_1^{\alpha_1-1}(p_1 - 1)p_2^{\alpha_2-1}(p_2 - 1) \cdots p_r^{\alpha_r-1}(p_r - 1) \\ &= n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) \end{aligned}$$

*Demostración.* Del corolario 8.11 sabemos que  $\phi(n) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdots \phi(p_r^{\alpha_r})$ . Necesitamos el valor de  $\phi(p^\alpha)$ , para  $p$  primo y  $\alpha$  natural. Hay  $p^k$  números entre 1 y  $p^k$ , no son relativamente primos a  $p^\alpha$  los  $p^{\alpha-1}$  múltiplos de  $p$  en este rango:

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p - 1) = p^{\alpha-1} \cdot \left(1 - \frac{1}{p}\right)$$

Multiplicando esto sobre las potencias de primos factores de  $n$  da lo anunciado.  $\square$

Algunas funciones aritméticas interesantes adicionales son:

**La identidad:**  $\iota(n) = n$

**Potencias de  $n$ :**  $\iota_a(n) = n^a$

**El número de divisores de  $n$ :**  $\tau(n) = |\{d \in \mathbb{N} : d \mid n\}|$

**La suma de los divisores de  $n$ :**  $\sigma(n) = \sum_{d \mid n} d$

**El producto de los divisores de  $n$ :**  $\pi(n) = \prod_{d \mid n} d$

Acá hemos usado nuestra convención general de indicar los índices de sumas o productos mediante condiciones, en este caso de divisibilidad.

Un resultado importante para funciones multiplicativas es:

**Teorema 8.13.** *Sea  $f$  una función aritmética y  $S$  definida por:*

$$S(n) = \sum_{d \mid n} f(d)$$

*Entonces  $f$  es multiplicativa si y solo si lo es  $S$ .*

*Demostración.* Demostramos implicancia en ambas direcciones. Sean  $x, y \in \mathbb{N}$  relativamente primos, y sea  $f$  multiplicativa. Sean además  $x_1, x_2, \dots, x_r$  e  $y_1, y_2, \dots, y_s$  todos los divisores de  $x$  e  $y$ , respectivamente. Entonces  $\gcd(x_i, y_j) = 1$ , y  $\{x_i y_j\}_{i,j}$  son todos los divisores de  $xy$ :

$$S(x) \cdot S(y) = \sum_i f(x_i) \sum_j f(y_j) = \sum_{i,j} f(x_i) f(y_j) = \sum_{i,j} f(x_i y_j) = S(xy)$$

y  $S$  es multiplicativa.

Para el recíproco, sea  $S$  multiplicativa. Demostramos por inducción fuerte sobre  $n$  que cuando  $n = xy$  con  $\gcd(x, y) = 1$  es  $f(n) = f(x)f(y)$ .

**Base:** El caso  $n = 1$  es trivial:  $f(1) = S(1)$ .

**Inducción:** Para nuestros  $x$  e  $y$  tenemos, usando la hipótesis de inducción:

$$S(xy) = \sum_{\substack{u|x \\ v|y \\ uv < n}} f(uv) = \sum_{\substack{u|x \\ v|y \\ uv < n}} f(u)f(v) + f(xy)$$

Por otro lado, sacando de las sumatorias los términos para  $u = x$  y  $v = y$  queda:

$$S(x)S(y) = \sum_{u|x} f(u) \sum_{v|y} f(v) = \sum_{\substack{u|x \\ v|y \\ uv < n}} f(u)f(v) + f(x)f(y)$$

Ambas expresiones son iguales ya que  $S$  es multiplicativa, y es  $f(xy) = f(x)f(y)$ .

Por inducción vale para todo  $n \in \mathbb{N}$ . □

**Corolario 8.14.** *Sea  $f$  una función multiplicativa, y sea  $S$  su función suma:*

$$S(n) = \sum_{d \mid n} f(d)$$

*Si  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$  es la descomposición de  $n$  en factores primos distintos  $p_i$ , entonces:*

$$S(n) = \prod_{1 \leq i \leq r} (1 + f(p_i) + f(p_i^2) + \cdots + f(p_i^{\alpha_i}))$$

*Demostración.* Si  $f$  es multiplicativa, lo es  $S$ . El valor indicado de  $S(n)$  corresponde para potencias de primos.  $\square$

Del teorema 8.13 vemos que son multiplicativas:

$$\tau(n) = S_1(n) = \sum_{d|n} 1$$

$$\sigma(n) = S_t(n) = \sum_{d|n} d$$

Por el corolario 8.14 en términos de la factorización completa  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$  tenemos:

$$\tau(n) = \prod_{1 \leq i \leq r} (\alpha_i + 1)$$

$$\sigma(n) = \prod_{1 \leq i \leq r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

La función  $\pi(n)$  no es multiplicativa.

Para los griegos la relación de un número con sus divisores propios tenía relevancia mística. Así reverenciaban especialmente a los *números perfectos*, que son la suma de sus divisores propios. Conocían los casos  $6 = 1 + 2 + 3$ ,  $28 = 1 + 2 + 4 + 7 + 14$ ,  $496$  y  $8128$ . En términos de las funciones definidas antes,  $n$  es perfecto cuando  $\sigma(n) = 2n$  (los factores propios de  $n$  suman a  $n$ , con  $n$  suman  $2n$ ). Tenemos también, si  $p$  es primo:

$$\sigma(p) = p + 1$$

$$\sigma(p^\alpha) = 1 + p + \cdots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}$$

Del resultado siguiente cada uno de los participantes demostró una implicancia.

**Teorema 8.15** (Euclides – Euler). *Un par  $n$  es perfecto si y solo si  $n = 2^{m-1}(2^m - 1)$  con  $2^m - 1$  primo.*

*Demostración.* Demostramos implicancia en ambas direcciones.

Si  $n = 2^{m-1}(2^m - 1)$  con  $2^m - 1$  primo, entonces como  $\sigma$  es multiplicativa:

$$\sigma(n) = \sigma(2^{m-1})\sigma(2^m - 1) = \frac{2^m - 1}{2 - 1} \cdot ((2^m - 1) + 1) = 2^m(2^m - 1) = 2n$$

y  $n$  es perfecto. Esta parte fue demostrada por Euclides.

Para el recíproco, sea  $n = 2^{m-1}u$  un número perfecto con  $m > 1$  y  $u$  impar. Entonces:

$$2^m u = \sigma(2^{m-1}u) = (2^m - 1)\sigma(u)$$

$$\sigma(u) = \frac{2^m u}{2^m - 1} = u + \frac{u}{2^m - 1}$$

Claramente el último término es un divisor de  $u$ . Como  $m > 1$ ,  $2^m - 1 > 1$ . O sea, estamos expresando  $\sigma(u)$  como la suma de dos divisores distintos de  $u$ , por lo que  $u$  es primo; tiene que ser  $u = 2^m - 1$ . Este es el aporte de Euler.  $\square$

Esto resuelve completamente el caso de números perfectos pares. Es fácil ver que si  $m$  es compuesto lo es  $2^m - 1$ , por lo que basta considerar  $2^p - 1$  con  $p$  primo. A tales primos se les llama *primos de Mersenne*, quien los estudió a principios del siglo XVII. Se conocen 48 primos de Mersenne a febrero de 2013, incluso el mayor primo conocido a la fecha es  $2^{57885161} - 1$ .

Es primo  $2^2 - 1 = 3$  y  $2^{2-1}(2^2 - 1) = 6$  es perfecto. Asimismo  $2^{3-1}(2^3 - 1) = 28$ ,  $2^{5-1}(2^5 - 1) = 496$  y  $2^{7-1}(2^7 - 1) = 8128$  son perfectos.

Por el otro lado, determinar si hay números perfectos impares es un problema abierto desde antes de Euclides.

**Definición 8.7.** Sean  $f$  y  $g$  funciones aritméticas. Su *convolución de Dirichlet* es:

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d) = \sum_{ab=n} f(a)g(b) \quad (8.1)$$

Es claro que la operación  $*$  es conmutativa, y es fácil demostrar que es asociativa. Con:

$$\epsilon(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases} \quad (8.2)$$

para la función aritmética  $f$  tenemos  $f * \epsilon = \epsilon * f = f$ , lo que da un neutro multiplicativo. En particular:

**Teorema 8.16.** El conjunto  $\mathcal{M}$  de funciones aritméticas multiplicativas es cerrado respecto de la convolución de Dirichlet.

*Demostración.* Sean  $f, g \in \mathcal{M}$ , sea  $h = f * g$ , y  $a, b \in \mathbb{N}$  con  $\gcd(a, b) = 1$ . Como  $\gcd(a, b) = 1$  los factores de  $ab$  resultan de todas las combinaciones de factores de  $a$  y  $b$  por separado:

$$\begin{aligned} h(a)h(b) &= (f * g)(a) \cdot (f * g)(b) \\ &= \sum_{u_1 v_1 = a} f(u_1)g(v_1) \sum_{u_2 v_2 = b} f(u_2)g(v_2) \\ &= \sum_{\substack{u_1 v_1 = a \\ u_2 v_2 = b}} f(u_1)g(v_1)f(u_2)g(v_2) \\ &= \sum_{u_1 u_2 v_1 v_2 = ab} f(u_1)f(u_2)g(v_1)g(v_2) \\ &= \sum_{uv = ab} f(u)g(v) \\ &= (f * g)(ab) \\ &= h(ab) \end{aligned}$$

□

Incluso podemos calcular inversos.

**Lema 8.17.** Toda función aritmética tal que  $f(1) \neq 0$  tiene inversa de Dirichlet dada por:

$$f^{-1}(n) = \begin{cases} \frac{1}{f(1)} & \text{si } n = 1 \\ -\frac{1}{f(1)} \sum_{\substack{ab=n \\ b < n}} f(a)f^{-1}(b) & \text{si } n > 1 \end{cases}$$

*Demostración.* Corresponde a plantear el sistema de ecuaciones, escrito usando la convención de Iverson:

$$\begin{aligned} \epsilon &= f * f^{-1} \\ [n = 1] &= \sum_{ab=n} f(a)f^{-1}(b) \end{aligned}$$

La expresión indicada para  $f^{-1}$  satisface este sistema. □

Una función importante es:

**Definición 8.8.** La *función de Möbius* se define mediante:

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \text{ es divisible por el cuadrado de un primo} \\ (-1)^k & \text{si } n \text{ es el producto de } k \text{ primos diferentes} \end{cases} \quad (8.3)$$

Un momento de reflexión muestra que  $\mu$  es multiplicativa.

**Lema 8.18.** Para  $n \in \mathbb{N}$ , la función de Möbius satisface:

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \geq 2 \end{cases}$$

*Demostración.* Como  $\mu$  es multiplicativa, por el teorema 8.13 lo es la suma indicada. Basta entonces hallar el valor de la suma en potencias de un primo  $p$ . Hay dos casos a considerar:

**$p^0 = 1$ :** En este caso la suma es simplemente  $\mu(1) = 1$ .

**$p^\alpha, \text{ con } \alpha \geq 1$ :** Acá, como  $\mu(p^k) = 0$  si  $k > 1$ :

$$\sum_{d|p^\alpha} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^\alpha) = 1 + (-1) + 0 + \cdots + 0 = 0$$

Multiplicando sobre los factores primos de  $n$  se obtiene lo prometido.  $\square$

La curiosa definición de  $\mu$  resulta ser simplemente el inverso de la función 1,  $1 * \mu = \epsilon$ , cosa que puede verificarse usando el lema 8.17. En detalle, llamando  $\mu = 1^{-1}$ , tenemos:

**$n = 1$ :** Es  $\mu(1) = 1/1(1) = 1$ .

**$n > 1$ :** En general es:

$$\mu(n) = -\frac{1}{1} \sum_{\substack{ab=n \\ b < n}} 1 \cdot \mu(b) = -\sum_{\substack{d|n \\ d < n}} \mu(d)$$

O sea, sucesivamente por el lema 8.17:

$$\mu(2) = -\sum_{\substack{d|2 \\ d < 2}} \mu(d) = -\mu(1) = -1$$

$$\mu(3) = -\sum_{\substack{d|3 \\ d < 3}} \mu(d) = -\mu(1) = -1$$

$$\mu(4) = -\sum_{\substack{d|4 \\ d < 4}} \mu(d) = -(\mu(1) + \mu(2)) = 0$$

$$\mu(5) = -\sum_{\substack{d|5 \\ d < 5}} \mu(d) = -\mu(1) = -1$$

$$\mu(6) = -\sum_{\substack{d|6 \\ d < 6}} \mu(d) = -(\mu(1) + \mu(2) + \mu(3)) = 1$$

Es claro que calcular la inversa por esta vía es bastante engorroso.

Esto hace útil la función de Möbius:

**Teorema 8.19** (Inversión de Möbius). *Sean dos funciones aritméticas (no necesariamente multiplicativas) tales que para todo  $n \in \mathbb{N}$  se cumple:*

$$g(n) = \sum_{d|n} f(d)$$

*entonces para todo  $n \in \mathbb{N}$ :*

$$f(n) = \sum_{d|n} \mu(d)g(n/d)$$

*Demostración.* Tenemos:

$$g = 1 * f$$

$$f = \mu * g$$

□

También:

**Lema 8.20.** *Si  $g$  es multiplicativa, y lo es  $f * g$ , entonces  $f$  es multiplicativa.*

*Demostración.* Si alguna de las funciones es cero, el resultado es obvio. En caso contrario, la demostración es por contradicción. Definamos  $h = f * g$  para comodidad. Suponemos que  $f$  no es multiplicativa, con lo que existen  $m, n$  mínimos con  $\gcd(m, n) = 1$  tales que  $f(mn) \neq f(m)f(n)$ . No puede ser  $mn = 1$ , ya que  $h(1) = f(1)g(1)$ , como  $h$  y  $g$  son multiplicativas,  $h(1) = g(1) = 1$ , con lo que  $f(1) = 1$  y  $f(1) = f(1)f(1)$ .

Sabemos entonces que  $mn \neq 1$ . Calcularemos  $h(mn) = h(m)h(n)$  de dos maneras, dejando fuera el término que involucra a  $mn$  con  $f$  en ambos casos. Comparando ambas llegaremos a una contradicción.

$$\begin{aligned} h(mn) &= \sum_{uv=mn} f(u)g(v) \\ &= \sum_{\substack{uv=mn \\ u < mn}} f(u)g(v) + f(mn)g(1) \\ &= \sum_{\substack{uv=mn \\ u < mn}} f(u)g(v) + f(mn) \\ h(m)h(n) &= \sum_{u_1v_1=m} f(u_1)g(v_1) \sum_{u_2v_2=n} f(u_2)g(v_2) \\ &= \sum_{\substack{u_1v_1=m \\ u_2v_2=n}} f(u_1)g(v_1)f(u_2)g(v_2) \\ &= \sum_{u_1u_2v_1v_2=mn} f(u_1)f(u_2)g(v_1)g(v_2) \\ &= \sum_{\substack{u_1u_2v_1v_2=mn \\ u_1 < m \\ u_2 < n}} f(u_1)f(u_2)g(v_1)g(v_2) + f(m)f(n)g(1)g(1) \end{aligned}$$

Pero  $f$  es multiplicativa hasta antes de  $mn$ , y  $g$  es multiplicativa:

$$\begin{aligned} &= \sum_{\substack{uv=mn \\ u < mn}} f(u)g(v) + f(m)f(n) \\ h(mn) - h(m)h(n) &= f(mn) - f(m)f(n) \\ &\neq 0 \end{aligned}$$

Tenemos una contradicción,  $f * g$  no es multiplicativa, contrario a la hipótesis. □

**Corolario 8.21.** *La inversa de una función multiplicativa es multiplicativa.*

*Demostración.* Si  $f$  es multiplicativa, entonces  $f * f^{-1} = \epsilon$  cumplen las hipótesis del lema 8.20.  $\square$

Uniendo las piezas:

**Teorema 8.22.** *El conjunto de funciones aritméticas  $\mathcal{A}$  es un anillo conmutativo con suma de funciones y convolución de Dirichlet como multiplicación. Su grupo de unidades es el conjunto de funciones multiplicativas que no son cero,  $\mathcal{M} \setminus \{0\}$ .*

Tenemos también:

**Teorema 8.23** (Identidad de Gauß). *Tenemos:*

$$\sum_{d|n} \phi(d) = n$$

*Demostración.* La suma es multiplicativa, basta evaluarla para las potencias de un primo  $p$ . Pero:

$$\begin{aligned} \sum_{d|p^\alpha} \phi(d) &= \phi(p^0) + \sum_{1 \leq k \leq \alpha} \phi(p^k) \\ &= 1 + \sum_{1 \leq k \leq \alpha} (p^k - p^{k-1}) \\ &= p^\alpha \end{aligned}$$

Resulta la fórmula prometida al multiplicar sobre los primos factores de  $n$ .  $\square$

Un resultado útil es el siguiente:

**Teorema 8.24.** *Sea  $f$  una función multiplicativa distinta de cero, y sea  $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$  con  $p_k$  primos distintos y  $e_k \geq 1$ . Entonces:*

$$\sum_{d|n} \mu(d)f(d) = \prod_k (1 - f(p_k)) \tag{8.4}$$

*Demostración.* La función  $\mu(n)f(n)$  es multiplicativa, con lo que lo es la suma a evaluar. Basta evaluar la suma para  $p^e$  con  $p$  primo y  $e \geq 1$  y luego combinar. Como  $f(1) = 1$ :

$$\begin{aligned} \sum_{d|p^e} \mu(d)f(d) &= \sum_{0 \leq k \leq e} \mu(p^k)f(p^k) \\ &= \mu(1)f(1) + \mu(p)f(p) \\ &= 1 - f(p) \end{aligned}$$

$\square$

Usando la convolución de Dirichlet resulta simple demostrar fórmulas que de otra forma serían casi imposibles. Considere:

$$\tau = 1 * 1$$

$$\sigma = \iota * 1$$

$$\phi = \mu * \iota$$

La última no es más que la identidad de Gauß, que así podemos reescribir:

$$\sum_{d|n} d\mu(d) = \phi(n)$$

Evaluemos ahora:

$$\sum_{d|n} \phi(d)\tau(n/d)$$

que es decir:

$$\phi * \tau = \mu * \iota * 1 * 1 = \mu * 1 * \iota * 1 = \epsilon * \sigma = \sigma$$

También podemos calcular:

$$\sum_{d|n} \mu(d)\tau(n/d)$$

que es:

$$\mu * \tau = \mu * 1 * 1 = 1$$

Pero también, si  $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$  con  $p_k$  primos distintos y  $e_k \geq 1$ , por el teorema 8.24 al ser  $\tau(p) = 2$ :

$$\begin{aligned} \sum_{d|n} \mu(d)\tau(d) &= \prod_k (1 - \tau(p)) \\ &= (-1)^r \end{aligned}$$

La suma resulta ser 1 si  $n$  es divisible por un número par de primos distintos y  $-1$  en caso contrario. Asimismo:

$$\begin{aligned} \sum_{d|n} \mu^2(d) &= \prod_k (1 - \mu(p_k)) \\ &= 2^r \end{aligned}$$

Partiendo de la identidad de Gauß:

$$\begin{aligned} \sum_{d|n} \phi(d) &= n \\ \phi(n) &= \sum_{d|n} \mu(d) \frac{n}{d} \\ &= n \sum_{d|n} \frac{\mu(d)}{d} \\ &= n \prod_k \left(1 - \frac{1}{p_k}\right) \end{aligned}$$

Otra derivación de la fórmula para  $\phi$ .

Consideremos palabras formadas con símbolos de algún alfabeto  $\Sigma$ , por ejemplo  $\Sigma = \{a, b, c\}$ . Una palabra puede ser la repetición de una palabra más corta, como baba. A la parte mínima que se repite para formar una palabra le llamaremos su *raíz*. Así, la raíz de ababab es ab, la raíz de acaba es acaba. Nos interesa el número de palabras que son sus propias raíces (no son repeticiones de palabras más cortas), a las que llamaremos *primitivas*.

Por ejemplo, para  $\Sigma = \{a, b\}$  el número total de palabras de largo 4 es  $2^4 = 16$ . Debemos descontar las que se forman repitiendo palabras primitivas. Palabras primitivas de largo 1 son a y b, que dan lugar a aaaa y bbbb; primitivas de largo 2 son ab y ba, que dan lugar a abab y baba. En total hay 4 palabras no primitivas, y por lo tanto son 12 las primitivas.

Llamemos  $p(n)$  al número de palabras primitivas de largo  $n$  (esto claramente depende del número  $s$  de símbolos en el alfabeto). Como toda palabra es la repetición de alguna palabra (cuyo largo divide a  $n$ ) podemos escribir:

$$s^n = \sum_{d|n} p(d)$$

Inversión de Möbius nos da:

$$p(n) = \sum_{d|n} \mu(n/d) s^d$$

Para el ejemplo el alfabeto es  $\{a, b\}$ , que da  $s = 2$ , y es  $n = 4$ . Resulta:

$$\begin{aligned} p(4) &= \sum_{d|4} \mu(4/d) \cdot 2^d \\ &= \mu(4) \cdot 2^1 + \mu(2) \cdot 2^2 + \mu(1) \cdot 2^4 \\ &= 0 \cdot 2 - 1 \cdot 4 + 1 \cdot 16 \\ &= 12 \end{aligned}$$

lo que confirma nuestro cálculo anterior.

Pero la fórmula permite calcular valores mucho mayores en forma simple:

$$\begin{aligned} p(12) &= \sum_{d|12} \mu(12/d) \cdot 2^d \\ &= \mu(12) \cdot 2^1 + \mu(6) \cdot 2^2 + \mu(4) \cdot 2^3 + \mu(2) \cdot 2^6 + \mu(1) \cdot 2^{12} \\ &= 0 \cdot 2 + 1 \cdot 4 + 0 \cdot 8 - 1 \cdot 64 + 1 \cdot 4096 \\ &= 4036 \end{aligned}$$

Puede profundizarse bastante partiendo de los conceptos anteriores, aún sin usar técnicas sofisticadas, como muestra magistralmente Moser [260].



## 9 Anillos de polinomios

---

Los polinomios se cuentan entre las funciones más importantes, dada su simplicidad. Estudiarlos desde un punto de vista algebraico, tanto para determinar propiedades de sus ceros y su factorización como desde el punto de vista más abstracto como ejemplo de anillo, es fructífero. En particular, el estudio de anillos de polinomios lleva naturalmente a anillos de series formales, que nos ocuparán intensamente más adelante.

### 9.1. Algunas herramientas

Un paquete de álgebra simbólica, como `maxima` [251], ayuda bastante con la operatoria. El paquete `PARI/GP` [278] incluye extenso soporte para trabajar con polinomios. La biblioteca `GiNaC` [29, 142] permite manipular expresiones simbólicas y numéricas directamente en C++ [182, 342].

**Definición 9.1.** Sea  $(R, +, \cdot)$  un anillo, y  $x$  un *símbolo* (también llamado *indeterminada* o *variable*). Definimos  $R[x]$ , los *polinomios sobre R*, como el conjunto de las expresiones:

$$f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_0$$

El *grado* de  $f$  es la máxima potencia de  $x$  que aparece multiplicada por un coeficiente no cero, se anota  $\deg(f)$ . Al polinomio con todos los coeficientes cero (el *polinomio cero*) se le asigna el grado  $-\infty$ . Si solo el término constante ( $a_0$ ) es diferente de cero, el grado del polinomio es cero, y se dice que es un *polinomio constante*. A polinomios de grado 1 se les llama *lineales*, a los de grado 2 *cuadráticos* y a los de grado 3 *cúbicos*. Se habla del *coeficiente principal* para referirse al coeficiente de la máxima potencia de  $x$  en el polinomio. Si el coeficiente principal es 1, el polinomio se llama *mónico*.

Nótese que algunos autores simplemente no le asignan grado al polinomio cero.

No asignamos significado a  $x$  ni a sus potencias. Podemos desarrollar toda la teoría hablando únicamente de tuplas de coeficientes. La notación es sugestiva, y más adelante sí consideraremos los polinomios como definiendo funciones.

**Definición 9.2.** Para polinomios  $f, g \in R[x]$ , definimos la suma y producto entre ellos (bajo el supuesto que es una secuencia infinita de coeficientes 0 a partir de un cierto punto para simplificar) como si tratáramos con expresiones en  $R$ , solo que  $x^k$  commuta con los elementos de  $R$  y se cumple  $x^i x^j = x^{i+j}$ :

$$f(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \cdots \tag{9.1}$$

$$g(x) = b_0 + b_1 \cdot x + b_2 \cdot x^2 + \cdots \tag{9.2}$$

$$\begin{aligned} f(x) + g(x) &= (a_0 + b_0) + (a_1 + b_1) \cdot x + \cdots + (a_k + b_k) \cdot x^k + \cdots \\ &= \sum_{k \geq 0} (a_k + b_k) x^k \end{aligned} \tag{9.3}$$

$$\begin{aligned} f(x) \cdot g(x) &= a_0 \cdot b_0 + (a_1 b_0 + a_0 b_1) \cdot x + (a_2 b_0 + a_1 b_1 + a_0 b_2) \cdot x^2 + \cdots \\ &= \sum_{\substack{0 \leq i \leq m \\ 0 \leq j \leq n}} a_i b_j x^{i+j} \\ &= \sum_{k \geq 0} \left( \sum_{0 \leq i \leq k} a_{k-i} b_i \right) \cdot x^k \end{aligned} \tag{9.4}$$

Resulta que  $R[x]$  con las operaciones definidas por (9.3) y (9.4) es un anillo. Es cómodo considerar  $\alpha \in R$  como el polinomio constante  $\alpha \in R[x]$ . Las unidades de  $R[x]$  son los polinomios constantes  $\alpha \in R^\times$ . Es fácil ver que:

$$\deg(f + g) \leq \max\{\deg(f), \deg(g)\} \tag{9.5}$$

$$\deg(f \cdot g) \leq \deg(f) + \deg(g) \tag{9.6}$$

Por esto resulta útil definir el grado del polinomio 0 como  $-\infty$ , evita requerir casos especiales.

En caso que no hayan divisores de cero diferentes de cero en  $R$ , en (9.6) es igualdad. Si  $R$  es un dominio integral (un anillo comunitativo sin divisores de cero distintos de cero),  $R[x]$  también es un dominio integral (el coeficiente del término de mayor grado del producto  $f(x) \cdot g(x)$  no es cero si ambos polinomios son diferentes de cero).

Definimos la *derivada formal* de un polinomio mediante:

$$\begin{aligned} f(x) &= \sum_{0 \leq k \leq n} a_k x^k \\ Df(x) &= \sum_{0 \leq k \leq n-1} (k+1) a_{k+1} x^k \end{aligned}$$

Anotaremos alternativamente:

$$f'(x) = Df(x)$$

Es fácil verificar que se cumplen las propiedades conocidas de las derivadas:

**Teorema 9.1.** *Sean  $f(x)$  y  $g(x)$  polinomios sobre el dominio integral  $R$ ,  $\alpha$  y  $\beta$  elementos de  $R$ . Entonces:*

$$\begin{aligned} D(\alpha f(x) + \beta g(x)) &= \alpha f'(x) + \beta g'(x) \\ D(f(x) \cdot g(x)) &= f'(x)g(x) + f(x)g'(x) \\ D(f(x)^m) &= mf(x)^{m-1} f'(x) \end{aligned}$$

*Demostración.* Definamos:

$$\begin{aligned} f(x) &= \sum_{0 \leq k \leq m} f_k x^k \\ g(x) &= \sum_{0 \leq k \leq n} g_k x^k \end{aligned}$$

Por comodidad, anotaremos sumas infinitas bajo el entendido que los términos son todos cero desde un índice en adelante.

Para la primera parte, tenemos que:

$$\begin{aligned}\alpha f(x) + \beta g(x) &= \sum_{k \geq 0} (\alpha f_k + \beta g_k) x^k \\ D(\alpha f(x) + \beta g(x)) &= \sum_{k \geq 0} (k+1)(\alpha f_{k+1} + \beta g_{k+1}) x^k \\ &= \alpha \sum_{k \geq 0} (k+1)f_{k+1} x^k + \beta \sum_{k \geq 0} (k+1)g_{k+1} x^k \\ &= \alpha f'(x) + \beta g'(x)\end{aligned}$$

Acá usamos el que para  $k \in \mathbb{N}$  y  $a, b \in R$ :

$$\begin{aligned}k(ab) &= ab + ab + \cdots + ab \\ &= a(b + b + \cdots + b) \\ &= a(kb)\end{aligned}$$

Para la segunda parte:

$$\begin{aligned}(Df(x))g(x) + f(x)(Dg'(x)) &= \sum_{k \geq 0} \left( \sum_{0 \leq j \leq k} (j+1)f_{j+1}g_{k-j} + \sum_{0 \leq j \leq k} (k+1-j)f_jg_{k+1-j} \right) x^k \\ &= \sum_{k \geq 0} \left( \sum_{0 \leq j \leq k+1} j f_j g_{k+1-j} + \sum_{0 \leq j \leq k+1} (k+1-j) f_j g_{k+1-j} \right) x^k \\ &= \sum_{k \geq 0} (k+1) \left( \sum_{0 \leq j \leq k+1} f_j g_{k+1-j} \right) x^k \\ &= D(f(x)g(x))\end{aligned}$$

Para la tercera parte, usamos inducción sobre  $m$ .

**Base:** Cuando  $m = 1$  lo aseverado ciertamente se cumple.

**Inducción:** Suponiendo que vale para  $m$ , demostramos que vale para  $m+1$ :

$$\begin{aligned}D(f(x)^{m+1}) &= D(f(x)^m f(x)) \\ &= m f(x)^{m-1} f'(x) f(x) + f(x)^m f'(x) \\ &= (m+1) f(x)^m f'(x)\end{aligned}$$

Acá usamos la commutatividad de  $R[x]$ .

Por inducción, vale para todo  $m \in \mathbb{N}$ . □

Los anillos de polinomios tienen varias propiedades interesantes, por ejemplo un algoritmo de división afín al de los enteros:

**Teorema 9.2.** *Sean  $a(x), b(x)$  polinomios sobre un campo  $F$ , con  $b(x) \neq 0$ . Entonces existen polinomios únicos  $q(x), r(x)$  tales que:*

$$a(x) = b(x) \cdot q(x) + r(x)$$

con  $\deg(r) < \deg(b)$

*Demostración.* Consideremos el conjunto:

$$\mathcal{R} = \{a(x) - c(x) \cdot b(x) : c(x) \in F[x]\}$$

Elijamos un elemento  $r$  de  $\mathcal{R}$  de grado mínimo. Entonces  $\deg(r) < \deg(b)$ , ya que en caso contrario podríamos restar un múltiplo de  $b(x)$  que anule el término de grado mayor en  $r(x)$  y así obtener uno de grado menor.

Demostramos que son únicos por contradicción. Supongamos que hay dos pares diferentes, o sea:

$$a = bq' + r' \quad a = bq'' + r''$$

Sin pérdida de generalidad podemos suponer que  $\deg(r') \leq \deg(r'')$ . Como  $F[x]$  es un anillo, con  $F$  un campo:

$$\begin{aligned} r'' - r' &= b(q' - q'') \\ \deg(r'' - r') &= \deg(b(q' - q'')) \\ &= \deg(b) + \deg(q' - q'') \end{aligned} \tag{9.7}$$

Pero:

$$\begin{aligned} \deg(r') &\leq \deg(r'') < \deg(b) \\ \deg(r'' - r') &\leq \deg(r'') < \deg(b) \end{aligned} \tag{9.8}$$

En vista de (9.8) la única posibilidad en (9.7) es  $\deg(r'' - r') = \deg(q' - q'') = -\infty$ , vale decir,  $q' = q''$  y  $r' = r''$ . Esto contradice nuestra elección de dos pares diferentes.  $\square$

Vale la pena comparar esta demostración con la del algoritmo de división entre enteros, teorema 7.1.

## 9.2. Dominios euclidianos

A un dominio integral  $D$  equipado con una *función eucliana* (a veces llamada *función grado* o simplemente *grado*)  $g: D \setminus \{0\} \rightarrow \mathbb{N}$  tal que si  $a, b \in D$ , con  $b \neq 0$ , hay  $q, r \in D$  tales que  $a = qb + r$  con  $r = 0$  o  $g(r) < g(b)$  se le llama *dominio eucliano*. Estas estructuras tienen mucho en común con  $\mathbb{Z}$  (en particular, toman su nombre porque es aplicable el algoritmo de Euclides para calcular máximo común divisor, y tenemos el equivalente de la identidad de Bézout). En el caso de los polinomios, el grado sirve como función eucliana.

Tenemos algunos resultados simples:

**Teorema 9.3.** *Sea  $D$  un dominio eucliano con función eucliana  $g$ . El valor  $g(a)$  es mínimo si  $a$  es una unidad.*

*Demostración.* Tomemos  $a \neq 0$  en  $D$  tal que  $g(a)$  es mínimo. Por el algoritmo de división, teorema 9.2, tenemos  $1 = qa + r$  con  $r = 0$  o  $g(r) < g(a)$ . Pero  $g(a)$  es mínimo, por lo que debe ser  $r = 0$  y  $a$  es una unidad.  $\square$

También tenemos las propiedades (ver Rogers [306] y Samuel [310]):

**Teorema 9.4.** *Sea  $D$  un dominio eucliano con función eucliana  $g$ . La función definida por:*

$$f(a) = \min_{x \in D \setminus \{0\}} g(ax)$$

*es una función eucliana, y cumple:*

- (a)  $f(a) \leq f(ab)$  si  $ab \neq 0$
- (b)  $f(a) \leq g(a)$  para todo  $a \in D \setminus \{0\}$
- (c)  $f(au) = f(a)$  si y solo si  $u \in D^\times$

*Demostración.* Por la definición de  $f$  los puntos (a) y (b) son obvios.

Para demostrar que  $f$  es eucliana, consideremos elementos  $a, b$  cualquiera en  $D \setminus \{0\}$ . Debemos demostrar que si  $b = qa + r$  entonces  $r = 0$  o  $f(r) < f(a)$ .

El caso  $r = 0$  es trivial. Supongamos entonces  $r \neq 0$ . Por definición es  $f(a) = g(ac)$  para algún  $c \in D \setminus \{0\}$ . De la definición de  $r$  tenemos que  $g(r) < g(a)$  por ser  $g$  eucliana. De  $bc = qac + rc$ , por ser  $g$  eucliana es  $g(rc) < g(ac) = f(a)$ ; y por la definición de  $f$  es también  $f(r) \leq g(rc)$ . Uniendo las anteriores queda  $f(r) < f(a)$ , y  $f$  es eucliana.

Para (c) demostramos implicancia en ambas direcciones. Primero, sea  $u \in D^\times$ . Por el punto (a) es  $f(a) \leq f(au) \leq f((au)u^{-1}) = f(a)$ . Por otro lado, si  $f(ac) = f(a)$ , escribimos  $a = qac + r$  con  $f(r) < f(ac) = f(a)$ ; siendo  $r = a(1 - cq)$ , por la parte (a) si  $r \neq 0$  es  $f(r) \geq f(a)$ , lo que es absurdo. Así  $r = 0$  y  $c$  es una unidad.  $\square$

Supondremos una función eucliana tal que  $f(a) \leq f(ab)$  para todo  $a, b \in D$  desde ahora, ya que simplifica mucha de la discusión que sigue. Nótese que en particular el grado de polinomios cumple esto. Como la función eucliana no es única, no la incluimos en la definición del dominio.

**Definición 9.3.** Sea  $R$  un dominio integral. Si podemos escribir  $m = bc$ , decimos que  $b$  divide a  $m$ , y anotamos  $b | m$ .

Esto también se expresa diciendo que  $b$  es un *factor* de  $m$ , o que  $m$  es un *múltiplo* de  $b$ .

**Definición 9.4.** Sea  $R$  un dominio integral. Dos elementos  $a, b \in R$  se dicen *asociados* si  $a = ub$ , donde  $u$  es una unidad. Se anota  $a \sim b$ .

Es fácil ver que  $\sim$  es una relación de equivalencia.

**Definición 9.5.** Sea  $R$  un dominio integral. Un elemento  $e \in R \setminus R^\times$  se llama *irreducible* si siempre que  $e = u \cdot v$ ,  $u$  o  $v$  es una unidad. En caso contrario, decimos que  $e$  es *reducible*.

**Definición 9.6.** Sea  $R$  un dominio integral,  $p \in R \setminus R^\times$ . Si  $p | ab$  implica que  $p | a$  o  $p | b$ , se dice que  $p$  es *primo*.

Vemos que si un elemento es primo, es irreducible:

**Lema 9.5.** *Sea  $R$  un dominio integral. Si  $p \in R$  es primo, entonces es irreducible.*

*Demostración.* Por contradicción. Supongamos  $p$  primo pero no irreducible. Así podemos escribir  $p = uv$ , donde  $u, v \notin R^\times$ . Pero entonces  $p | uv$ , y por la definición de primo es  $p | u$  o  $p | v$ . Sin pérdida de generalidad podemos suponer  $u = ap$ , con lo que:

$$\begin{aligned} p &= apv \\ 0 &= p(1 - av) \end{aligned}$$

Como no hay divisores de cero distintos de cero en  $R$ , debe ser  $av = 1$  y  $v$  es una unidad, lo que contradice su elección.  $\square$

El recíproco del lema 9.5 no siempre se cumple. Consideremos el dominio integral  $\mathbb{Z}[\sqrt{-5}]$  (ver la sección 7.5.2, solo que este es un subanillo de  $\mathbb{C}$ ). Si  $3 = u \cdot v$ , debe ser  $N(u) \cdot N(v) = N(3) = 9$ , con lo que las normas posibles para  $u$  y  $v$  son los divisores de 9. Si  $N(u) = 1$ ,  $u$  es una unidad. Si  $N(u) = 3$ , con  $u = u_1 + u_2\sqrt{-5}$  es  $u_1^2 + 5u_2^2 = 3$ . Esto claramente es imposible con  $u_1, u_2$  enteros. Así 3 es irreducible en  $\mathbb{Z}[\sqrt{-5}]$ . Por el otro lado:

$$(2 + \sqrt{-5}) \cdot (2 - \sqrt{-5}) = 9$$

con lo que

$$3 \mid (2 + \sqrt{-5}) \cdot (2 - \sqrt{-5})$$

Claramente  $3 \nmid 2 \pm \sqrt{-5}$ , o sea 3 no es primo en  $\mathbb{Z}[\sqrt{-5}]$ .

**Definición 9.7.** Sea  $R$  un dominio integral, y sea  $a \in R$  con  $a \neq 0$ . Entonces se dice que  $a$  tiene factorización única en irreducibles si hay una unidad  $u$  e irreducibles  $p_i$  tales que  $a = up_1p_2 \cdots p_r$ , y además, si  $a = vq_1q_2 \cdots q_s$  para una unidad  $v$  e irreducibles  $q_i$ , entonces  $r = s$  y  $p_i = u_i q_i$  para unidades  $u_i$  salvo reordenamiento.

**Definición 9.8.** Se dice que  $R$  es un *dominio de factorización única* (en inglés *Unique Factorization Domain*, abreviado *UFD*) si todo elemento de  $R$  tiene factorización única en irreducibles.

En vista del algoritmo de división en el dominio eucliano, tenemos:

**Teorema 9.6.** Sea  $D$  un dominio eucliano con función eucliana  $f$  y  $a, b \in D$ . Entonces el conjunto  $I = \{ua + vb : u, v \in D\}$  consta de todos los múltiplos de un elemento  $m$ .

La demostración es muy similar a la discusión sobre máximo común divisor en el capítulo 7.

*Demostración.* Si  $a = b = 0$ , claramente  $I = \{0\}$ , y lo aseverado se cumple. Supongamos entonces que al menos uno de  $a, b$  es diferente de 0, en cuyo caso  $I$  contiene elementos diferentes de 0. Elijamos uno de ellos con  $f$  mínimo, llamémosle  $m$ . Tomemos ahora  $n \in I$  cualquiera. Si  $n = 0$ , se cumple  $m \mid n$ , y estamos listos. Si  $n \neq 0$ , podemos aplicar el algoritmo de división y escribir:

$$n = qm + r$$

donde  $r = 0$  o  $f(r) < f(m)$ . Dado que hay  $u, v, u', v'$  tales que  $n = ua + vb$  y  $m = u'a + v'b$  resulta:

$$\begin{aligned} r &= n - qm \\ &= (u - qu')a + (v - qv')b \end{aligned}$$

con lo que  $r \in I$ . Pero no puede ser  $f(r) < f(m)$ , hemos elegido  $m$  precisamente por ser  $f(m)$  mínimo. En consecuencia,  $r = 0$  y  $m \mid n$ .  $\square$

Conjuntos como  $I$  que aparece en la demostración del teorema 9.6 son muy importantes. Podemos definir  $m$  (o uno de sus asociados, que también son parte de  $I$ ;  $m$  no necesariamente es único) como un máximo común divisor de  $a$  y  $b$  (“máximo” en el sentido de la función eucliana  $f$ ).

**Definición 9.9.** Sea  $R$  un anillo comutativo. Un *ideal* de  $R$  es un conjunto  $I \subseteq R$  tal que:

1.  $(I, +)$  es un subgrupo de  $(R, +)$
2. Para todo  $x \in I$  y para todo  $r \in R$  se cumple  $r \cdot x \in I$

Los ideales son casi subanillos de  $R$  (solo falta el elemento 1). Hay quienes definen anillos sin 1, para ellos los ideales son subanillos.

**Definición 9.10.** Sea  $R$  un anillo comunitativo, y  $\{x_1, x_2, \dots, x_n\} \subseteq R$ . Al ideal  $\{\sum_{1 \leq k \leq n} u_k x_k : u_k \in R\}$  se le llama el *ideal generado por  $\{x_1, x_2, \dots, x_n\}$* , que se suele anotar  $(x_1, x_2, \dots, x_n)$ . Por la convención que sumas vacías son cero,  $\{0\}$  es generado por  $\emptyset$ . A un ideal generado por un único elemento  $x_1$ , anotado  $(x_1)$ , se le llama *ideal principal*. Si en  $R$  todos los ideales son principales, se dice que  $R$  es un *dominio de ideal principal* (en inglés *Principal Ideal Domain*, abreviado *PID*).

En estos términos, el teorema 9.6 asevera que todo dominio euclíadiano es un dominio de ideal principal.

**Lema 9.7.** *Sea  $p$  irreducible en un dominio euclíadiano  $D$ , y  $a$  otro elemento de  $D$ . Si  $p$  no divide a  $a$ , entonces 1 es un máximo común divisor entre  $a$  y  $p$ .*

*Demostración.* Sea  $m$  un máximo común divisor de  $a$  y  $p$ . Por el teorema 9.6 existen  $x, y \in D$  tales que:

$$m = xa + yp$$

Como  $m$  divide a  $p$ , que es irreducible,  $m$  es una unidad o  $m \sim p$ . Si  $m$  es una unidad, 1 es un máximo común divisor de  $a$  y  $p$  y estamos listos. En el otro caso, por ser  $m$  divisor de  $a$  es  $a = cm$  para algún  $c \in D$  y como a su vez  $m = up$  para una unidad  $u$ , entonces  $a = cup$  y  $p \mid a$ .  $\square$

Esto nos permite demostrar el recíproco del lema 9.5 en dominios euclidianos, como ya lo hicimos en el corolario 7.5 para los enteros:

**Teorema 9.8.** *En un dominio euclíadiano, si  $p$  es irreducible entonces  $p$  es primo.*

*Demostración.* Supongamos que el irreducible  $p$  divide a  $ab$ . Debemos demostrar que  $p$  divide a  $a$  o a  $b$  (o a ambos). Si  $p \mid a$ , estamos listos. En caso contrario, como  $p \mid ab$ , hay un  $c \in D$  tal que  $ab = cp$ . Por el lema 9.7 tenemos que 1 es un máximo común divisor de  $a$  y  $p$ , y por el teorema 9.6 podemos escribir:

$$\begin{aligned} 1 &= up + va \\ b &= bup + vab \\ &= (bu + vc)p \end{aligned}$$

con lo que  $p \mid b$ .  $\square$

**Lema 9.9.** *Si el primo  $p$  divide al producto  $x_1 x_2 \cdots x_n$ , entonces  $p \mid x_i$  para algún  $i$ .*

*Demostración.* Por inducción sobre  $n$ . Si  $n = 1$ , no hay nada que demostrar.

**Base:** Para  $n = 2$ , por la definición de primo tenemos que si  $p \mid x_1 x_2$ , entonces  $p \mid x_1$  o  $p \mid x_2$ .

**Inducción:** Por la hipótesis de inducción, si  $p \mid x_1 x_2 \cdots x_n$  entonces  $p \mid x_i$  para  $1 \leq i \leq n$ . Si ahora  $p \mid x_1 x_2 \cdots x_n x_{n+1}$  por el caso  $n = 2$  significa que ya sea  $p \mid x_1 x_2 \cdots x_n$  (lo que implica  $p \mid x_i$  para  $1 \leq i \leq n$ ) o  $p \mid x_{n+1}$ . En conjunto,  $p \mid x_i$  para  $1 \leq i \leq n+1$ .

Por inducción, vale para todo  $n \in \mathbb{N}$ .  $\square$

Así tenemos:

**Teorema 9.10.** *Si  $D$  es un dominio de ideal principal, entonces es un dominio de factorización única.*

*Demostración.* Por contradicción. Consideremos un elemento  $a \in D \setminus D^\times$  (distinto de 0) con  $f(a)$  mínimo y que no tiene factorización en irreducibles. Entonces  $a$  no es irreducible (sería el producto de un irreducible), por lo que podemos escribir  $a = bc$ , con  $b, c \notin D^\times$ . Por el teorema 9.4 resulta  $f(b) < f(a)$  y  $f(c) < f(a)$ . Pero entonces  $b$  y  $c$  son producto de irreducibles, con lo que lo es  $a$ . Vale decir, tal  $a$  no existe.

Para demostrar factorización única usamos reducción al absurdo. Sea  $a$  un elemento de mínimo  $f$  que tiene dos factorizaciones esencialmente diferentes:

$$a = up_1 p_2 \cdots p_m = vq_1 q_2 \cdots q_n$$

donde los  $p_i$  son primos (no necesariamente diferentes), y similarmente los  $q_i$ , y  $u$  y  $v$  son unidades. Por el lema 9.9, esto significa que  $p_1$  divide a  $q_i$  para algún  $i$ , o sea  $q_i = u_i p_i$  para alguna unidad  $u_i$ , con lo que:

$$a/p_1 = up_2 \cdots p_m = vu_i q_1 \cdots q_{i-1} q_{i+1} \cdots q_n$$

tendría dos factorizaciones diferentes, pero  $f(a/p_1) < f(a)$ , lo que contradice la elección de  $a$  como uno de mínimo  $f$  con dos factorizaciones.  $\square$

Esto viene a ser el equivalente del teorema fundamental de la aritmética (teorema 7.8): En un dominio euclíadiano todo elemento  $a$  es el producto de un número finito de primos. Además, si tenemos factorizaciones en primos  $p_i$  y  $q_i$ :

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

entonces cada  $p$  es el asociado de uno de los  $q$ . En particular,  $m = n$ .

### 9.3. Factorización de polinomios

Vimos que el conjunto de polinomios  $F[x]$  sobre el campo  $F$  es un dominio euclíadiano, el grado del polinomio sirve de función euclíadiana. Podemos elegir el polinomio mónico como el representante de la clase de asociados, con lo que tenemos:

**Teorema 9.11** (Teorema fundamental de la aritmética). *Todo polinomio en  $F[x]$  es una unidad o el producto de una unidad y polinomios monicos irreducibles. Esta factorización es única (salvo el orden de los factores).*

Podemos caracterizar polinomios con ceros repetidos:

**Lema 9.12.** *Si  $\alpha$  es un cero repetido del polinomio  $f(x) \in F[x]$ , es cero común de  $f(x)$  y  $f'(x)$ .*

*Demostración.* Consideremos  $f(x) = (x - \alpha)^m g(x)$ , donde  $(x - \alpha) \nmid g(x)$  y  $m > 1$ . Tenemos:

$$f'(x) = m(x - \alpha)^{m-1} g(x) + (x - \alpha)^m g'(x) = (x - \alpha)^{m-1} (mg(x) + (x - \alpha)g(x))$$

Como  $m > 1$ , esto siempre es divisible por  $x - \alpha$ .  $\square$

Tenemos también:

**Teorema 9.13** (Euclides). *Hay infinitos polinomios irreducibles sobre el campo  $F$ .*

*Demostración.* Por contradicción. Supongamos que hay finitos irreducibles  $p_1(x)$  a  $p_n(x)$ . Entonces  $p_1(x) \cdots p_n(x) + 1$  no es divisible por ninguno  $p_i(x)$ .  $\square$

Sobre un campo infinito no da nada nuevo (los polinomios lineales son todos irreductibles), pero sobre un campo finito sí es interesante.

Consideremos ahora los polinomios como funciones, substituyendo elementos del campo por  $x$ .

**Corolario 9.14.** *Sea  $F$  un campo, y  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$  un polinomio de grado  $n$  sobre  $F$ , y  $\alpha \in F$ . Entonces  $f(\alpha) = 0$  si y solo si  $f(x) = (x - \alpha)g(x)$  para algún polinomio  $g \in F[x]$ .*

*Demostración.* Demostramos implicancia en ambas direcciones.

Primeramente, si  $f(x) = (x - \alpha)g(x)$ , claramente  $f(\alpha) = 0 \cdot g(\alpha) = 0$ .

Por el algoritmo de división podemos escribir  $f(x) = q(x) \cdot (x - \alpha) + r(x)$ , donde  $\deg(r) < 1$  con lo que  $r(x)$  es constante. Ahora bien,  $f(\alpha) = q(\alpha) \cdot (\alpha - \alpha) + r(\alpha) = 0$ , con lo que al ser constante  $r(x)$  es  $r(x) = r(\alpha) = 0$ . Así  $f(x) = q(x) \cdot (x - \alpha)$ , y llamando  $g(x) = q(x)$  completa la demostración.  $\square$

Con esta herramienta básica podemos demostrar el resultado siguiente:

**Corolario 9.15.** *Si  $f(x) \in F[x]$  es un polinomio de grado  $n \geq 0$ , entonces  $f(x)$  tiene a lo más  $n$  ceros en  $F$ .*

*Demostración.* Por inducción.

**Bases:** Para  $n = 0$ , no hay ceros.

Para  $n = 1$ , tenemos:

$$\begin{aligned} a_1 \cdot x + a_0 &= 0 \\ x &= -a_1^{-1} \cdot a_0 \end{aligned}$$

que claramente es única.

**Inducción:** Suponiendo ahora que todos los polinomios de grado  $n$  tienen a lo más  $n$  ceros, consideremos un polinomio  $f(x)$  de grado  $n + 1$ . Si no hay  $\alpha$  tal que  $f(\alpha) = 0$ ,  $f(x)$  tiene 0 ceros y estamos listos. Si tiene un cero  $\alpha$ , por el corolario 9.14 podemos escribir  $f(x) = (x - \alpha) \cdot g(x)$  con  $\deg(g) = n$ . Por inducción,  $g(x)$  tiene a lo más  $n$  ceros, y  $f(x)$  tiene a lo más  $n + 1$  ceros.

Por inducción vale lo enunciado.  $\square$

Suelen ser útiles los términos más fáciles de calcular del polinomio con ceros  $\alpha_1, \alpha_2, \dots, \alpha_m$ ; o sea, los coeficientes en el producto:

$$(x - \alpha_1) \cdots (x - \alpha_m) = x^m - (\alpha_1 + \alpha_2 + \cdots + \alpha_m)x^{m-1} + \cdots + (-1)^m \alpha_1 \cdot \alpha_2 \cdots \alpha_m \quad (9.9)$$

El coeficiente de  $x^{m-1}$  es el negativo de la suma de los ceros, y el término constante es su producto con signo que depende de si  $m$  es par o impar. Las expresiones (9.9) son casos particulares de las fórmulas de Vieta: Para el polinomio  $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ , los ceros  $\alpha_1, \alpha_2, \dots, \alpha_n$  cumplen:

$$\sum_{1 \leq i_1 \leq i_2 \leq \cdots \leq i_k \leq n} \alpha_{i_1} \alpha_{i_2} \cdots \alpha_{i_k} = (-1)^k \frac{a_{n-k}}{a_n} \quad (9.10)$$

La suma en (9.10) es simplemente sobre todos los conjuntos de  $k$  de las ceros. Por ejemplo:

$$ax^3 + bx^2 + cx + d = a(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

resulta en las siguientes tres expresiones:

$$\begin{aligned}\alpha_1 + \alpha_2 + \alpha_3 &= -\frac{b}{a} \\ \alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_2 \alpha_3 &= \frac{c}{a} \\ \alpha_1 \alpha_2 \alpha_3 &= -\frac{d}{a}\end{aligned}$$

**Teorema 9.16.** *Sea  $F$  un campo finito, y  $F^\times$  su grupo de unidades. Entonces  $F^\times$  es cíclico.*

*Demostración.* Sea  $e$  el exponente de  $F^\times$ , vale decir, el mínimo natural tal que  $a^e = 1$  para todo  $a \in F^\times$ . Esto es el mínimo común múltiplo de los órdenes de los elementos de  $F^\times$ . Por el teorema de Lagrange todos ellos son factores de  $|F^\times|$ , con lo que  $e$  es factor de  $|F^\times|$  y  $e \leq |F^\times|$ .

Por otro lado, todos los elementos de  $F^\times$  cumplen:

$$x^e - 1 = 0$$

En el campo  $F$  este polinomio puede tener a lo más  $e$  ceros, o sea  $e \geq |F^\times|$ , con lo que  $e = |F^\times|$ . Siendo  $e$  el mínimo común múltiplo de los órdenes en  $F^\times$ , debe haber un elemento de orden  $e$  y  $F^\times$  es cíclico.  $\square$

**Corolario 9.17.** *Si  $p$  es primo,  $\mathbb{Z}_p^\times$  es cíclico.*

*Demostración.*  $\mathbb{Z}_p$  es un campo finito, y  $\mathbb{Z}_p^\times$  es su grupo de unidades.  $\square$

Esto implica el curioso resultado:

**Teorema 9.18** (Wilson).  *$(n-1)! \equiv -1 \pmod{n}$  si y solo si  $n$  es primo.*

*Demostración.* Demostramos implicancia en ambas direcciones. Si  $n$  es primo,  $\mathbb{Z}_n$  es un campo, y por la demostración del teorema 9.16 sabemos que:

$$x^{n-1} - 1 = \prod_{1 \leq k \leq n-1} (x - k)$$

La fórmula de Vieta (9.10) da para el término constante:

$$(-1)^{n-1} (n-1)! \equiv -1 \pmod{n}$$

Si  $n = 2$ , es  $(-1)^{n-1} = -1$  y  $1 \equiv -1 \pmod{n}$ ; si  $n$  es un primo impar,  $(-1)^{n-1} = 1$ . De cualquier forma,  $(n-1)! \equiv -1 \pmod{n}$ .

Para el recíproco, demostramos el contrapositivo: Si  $n$  no es primo,  $(n-1)! \not\equiv -1 \pmod{n}$ . Hay varios casos: Si  $n = 4$  es  $3! = 6 \equiv 2 \not\equiv -1 \pmod{4}$ , y se cumple lo enunciado. Sea ahora  $n > 4$  compuesto. En tal caso podemos escribir  $n = a \cdot b$ , con  $2 \leq a, b < n-1$ . De ser  $a \neq b$ , ambos factores aparecen en  $(n-1)!$ , y por tanto  $n \mid (n-1)!$ . Si es  $n = a^2$ , será  $a > 2$ , y entre los factores de  $(n-1)!$  estarán  $a$  y  $2a$ , con lo que nuevamente  $n \mid (n-1)!$ . En estas dos situaciones tenemos  $(n-1)! \equiv 0 \pmod{n}$ , y obtenemos lo enunciado.  $\square$

Este resultado no es útil para computación, y de uso teórico bastante limitado.

Una demostración alternativa es considerar un primo impar  $p$ , y parear cada  $a \in \mathbb{Z}_p$  con su inverso. Los únicos elementos que no tienen pareja en esto son 1 y  $-1$  (son sus propios inversos, en el campo  $\mathbb{Z}_p$  la ecuación  $x^2 - 1 = 0$  puede tener a lo más dos raíces), por lo que el producto de todos ellos es  $-1$ .

## 9.4. Raíces primitivas

Cuando  $R^\times$  es cíclico, a un generador de  $R^\times$  se le llama *elemento primitivo* de  $R$ . En el caso de  $\mathbb{Z}_n^\times$  se le llama una *raíz primitiva* módulo  $n$  (porque todo elemento de  $\mathbb{Z}_n^\times$  puede escribirse como potencia del generador). Lo anterior demuestra que todo primo  $p$  tiene raíces primitivas. Una pregunta obvia es qué valores de  $n$  tienen raíces primitivas (o sea, cuándo es cíclico  $\mathbb{Z}_n^\times$ ).

Consideremos  $n = 8$ , con  $\phi(8) = 4$ . Por cálculo directo tenemos los órdenes de los elementos de  $\mathbb{Z}_8^\times$  dados en el cuadro 9.1. Se aprecia que no hay elementos de orden 4, y 8 no tiene raíces primitivas.

$k$	$\text{ord}_8(k)$
1	1
3	2
5	2
7	2

Cuadro 9.1 – Órdenes de los elementos en  $\mathbb{Z}_8^\times$

Por otro lado, para  $n = 2$  tenemos  $\phi(2) = 1$  y claramente 1 es raíz primitiva módulo 2. Para  $n = 4$  tenemos  $\phi(4) = 2$ , y 3 es raíz primitiva módulo 4.

Más generalmente, tenemos:

**Teorema 9.19.** *No hay raíces primitivas módulo  $2^m$  si  $m \geq 3$ .*

*Demostración.* Demostraremos esto por inducción.

**Base:** Cuando  $m = 3$ , vimos antes que  $2^m = 8$  no tiene raíces primitivas.

**Inducción:** Suponemos que la aseveración vale para  $m - 1$ . Como  $\phi(2^m) = 2^{m-1}$  y el único divisor de  $2^{m-1}$  es 2, basta demostrar que el orden de todo elemento en  $\mathbb{Z}_{2^m}^\times$  es divisor de  $2^{m-2}$ .

Consideremos  $a$  cualquiera relativamente primo a  $2^m$ . Por inducción sabemos que  $a$  no es raíz primitiva de  $2^{m-1}$ , que expresado en los términos anteriores es:

$$\begin{aligned} a^{2^{m-3}} &\equiv 1 \pmod{2^{m-1}} \\ a^{2^{m-3}} &= c \cdot 2^{m-1} + 1 \end{aligned}$$

Elevando al cuadrado:

$$\begin{aligned} a^{2^{m-2}} &= (a^{2^{m-3}})^2 \\ &= c^2 \cdot 2^m + 2 \cdot c \cdot 2^{m-1} + 1 \\ &= (c^2 + c) \cdot 2^m + 1 \\ &\equiv 1 \pmod{2^m} \end{aligned} \tag{9.11}$$

Por (9.11) el orden de  $a$  módulo  $2^m$  es a lo más  $2^{m-2} < 2^{m-1} = \phi(2^m)$ , y  $a$  no es raíz primitiva.  $\square$

Esto da un conjunto infinito de enteros sin raíces primitivas. Pero aún más:

**Teorema 9.20.** *No hay raíces primitivas módulo  $mn$  si  $m$  y  $n$  son enteros impares relativamente primos mayores que 2.*

*Demostración.* Como  $m$  y  $n$  son impares y mayores que 2, sabemos que 2 es un factor común entre  $\phi(m)$  y  $\phi(n)$  (un primo impar  $p$  aporta  $p^{k-1}(p-1)$  a  $\phi(\cdot)$ ). Para cualquier  $a$  tal que  $\gcd(a, mn) = 1$ , por el teorema de Euler:

$$a^{\phi(m)\phi(n)/2} \equiv (a^{\phi(m)})^{\phi(n)/2} \equiv 1^{\phi(n)/2} \equiv 1 \pmod{m} \quad (9.12)$$

$$a^{\phi(m)\phi(n)/2} \equiv (a^{\phi(n)})^{\phi(m)/2} \equiv 1^{\phi(m)/2} \equiv 1 \pmod{n} \quad (9.13)$$

Combinando (9.12) con (9.13) mediante el teorema 7.12 resulta:

$$a^{\phi(m)\phi(n)/2} \equiv 1 \pmod{mn} \quad (9.14)$$

Por (9.14) el orden de  $a$  divide a  $\phi(mn)/2$ , y  $a$  no es raíz primitiva de  $mn$ . Pero  $a$  es arbitrario, con lo que  $mn$  no tiene raíces primitivas.  $\square$

Lo anterior excluye  $2^k$  para  $k \geq 3$ , y los números compuestos impares con factores primos distintos. Analicemos los restantes.

**Teorema 9.21.** *Sea  $p$  un primo impar, entonces hay una raíz primitiva módulo  $p^2$*

*Demostración.* Sea  $r$  una raíz primitiva de  $p$ , o sea  $\text{ord}_p(r) = p - 1$ . Sabemos que si  $n = \text{ord}_{p^2}(r)$  entonces  $n \mid \phi(p^2)$ , vale decir  $n \mid p(p-1)$ . Sabemos que si  $r^n \equiv 1 \pmod{p^2}$  entonces  $r^n \equiv 1 \pmod{p}$ , de forma que  $\phi(p) \mid n$ . Pero si  $p-1 \mid n$  y  $n \mid p(p-1)$ , entonces  $n = p(p-1)$  o  $n = p-1$ . En el primer caso, tenemos que  $r$  es raíz primitiva de  $p^2$ , y estamos listos.

En el segundo caso, consideraremos el elemento  $r + p$ , que sigue siendo raíz primitiva módulo  $p$ , con lo que su orden es  $p-1$  o  $p(p-1)$  módulo  $p^2$ . Calculamos:

$$(r + p)^{p-1} = r^{p-1} + \binom{p-1}{1} pr^{p-2} + \sum_{2 \leq k \leq p-1} \binom{p-1}{k} p^k r^{p-1-k} \quad (9.15)$$

Todos los elementos de la sumatoria en (9.15) son divisibles por  $p^2$ . Como estamos suponiendo que el orden de  $r$  módulo  $p^2$  es  $p-1$ , y sabemos que:

$$(p-1)pr^{p-2} \equiv -pr^{p-2} \not\equiv 0 \pmod{p^2}$$

(ya que  $\gcd(r, p) = 1$  también es  $\gcd(r^{p-2}, p) = 1$ ), y queda:

$$(r + p)^{p-1} \equiv 1 - pr^{p-2} \not\equiv 1 \pmod{p^2}$$

y  $r + p$  es raíz primitiva módulo  $p^2$ .  $\square$

Esto parece ser solo un paso al ir de  $p$  a  $p^2$ , pero resulta ser todo lo que se requiere. Antes de seguir, un lema técnico.

**Lema 9.22.** *Sea  $p$  un primo impar,  $r$  una raíz primitiva módulo  $p^2$ . Entonces para  $m \geq 2$ :*

$$r^{p^{m-2}(p-1)} \not\equiv 1 \pmod{p^m} \quad (9.16)$$

*Demostración.* La demostración es por inducción desde  $m = 2$ . De partida, si  $r$  es raíz primitiva módulo  $p^2$ , lo es módulo  $p$  y  $\gcd(r, p) = 1$ .

**Base:** Para  $m = 2$  el orden de la raíz primitiva  $r$  de  $p^2$  es  $\phi(p^2) = p(p-1)$ , por lo que:

$$r^{p-1} \not\equiv 1 \pmod{p^2} \quad (9.17)$$

**Inducción:** Supongamos que el resultado vale para  $m - 1$ . Del teorema de Euler tenemos:

$$\begin{aligned} r^{\phi(p^{m-2})} &\equiv 1 \pmod{p^{m-2}} \\ r^{p^{m-3}(p-1)} &= 1 + c \cdot p^{m-2} \end{aligned} \tag{9.18}$$

Nótese que  $p \nmid c$ , ya que de lo contrario tendríamos:

$$r^{p^{m-3}(p-1)} \equiv 1 \pmod{p^{m-1}} \tag{9.19}$$

y esto contradice nuestra hipótesis de inducción (9.16). Elevando (9.19) a la potencia  $p$ , queda:

$$\begin{aligned} r^{p^{m-2}(p-1)} &= (1 + cp^{m-2})^p \\ &= 1 + cp^{m-1} + \sum_{2 \leq k \leq p} \binom{p}{k} c^k p^{k(m-2)} \end{aligned} \tag{9.20}$$

Interesa demostrar que cada término de la sumatoria (9.20) es divisible por  $p^m$ . En ellos aparece el factor  $p^{k(m-2)+1}$  (incluyendo  $p$  del coeficiente binomial). Interesa acotar el exponente  $k(m-2) + 1$ , con  $k \geq 2$  y  $m \geq 3$ . Es  $m - 2 \geq 1$ , el mínimo exponente se da para  $k = 2$  y tenemos  $k(m-2) + 1 \geq 2m - 3 \geq m$ . En consecuencia:

$$\begin{aligned} r^{p^{m-2}(p-1)} &\equiv 1 + cp^{m-1} \pmod{p^m} \\ &\not\equiv 1 \pmod{p^m} \end{aligned}$$

como queríamos probar.  $\square$

**Teorema 9.23.** *Toda raíz primitiva módulo  $p^2$  para un primo impar  $p$  es raíz primitiva módulo  $p^m$  con  $m \geq 2$*

*Demostración.* Sea  $r$  raíz primitiva módulo  $p^2$ , con lo que  $\text{ord}_{p^2}(r) = p(p-1)$  ya que  $\phi(p^2) = p(p-1)$ , y llamemos  $n = \text{ord}_{p^m}(r)$ . Como antes, por el teorema de Euler sabemos que:

$$r^{\phi(p^m)} \equiv r^{p^{m-1}(p-1)} \equiv 1 \pmod{p^m}$$

con lo que:

$$n \mid p^{m-1}(p-1)$$

Pero también:

$$r^n \equiv 1 \pmod{p^m}$$

implica:

$$r^n \equiv 1 \pmod{p^2}$$

con lo que  $p(p-1) \mid n$ , y  $n = p^k(p-1)$  para algún  $1 \leq k \leq m-1$ . Por el lema 9.22 sabemos que:

$$r^{p^{m-2}(p-1)} \not\equiv 1 \pmod{p^m}$$

con lo que  $k = m-1$ , y  $r$  es raíz primitiva módulo  $p^m$ .  $\square$

Resta el caso  $2p^m$ , donde por el corolario 8.6 resulta  $\mathbb{Z}_{2p^m} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{p^m}$ , y  $\mathbb{Z}_{2p^m}^\times \cong \mathbb{Z}_2^\times \oplus \mathbb{Z}_{p^m}^\times \cong \mathbb{Z}_{p^m}^\times$ , y hay una raíz primitiva. En resumen, obtenemos el curioso resultado:

**Teorema 9.24.** *Hay raíces primitivas módulo n si y solo si n = 2, 4, p<sup>m</sup>, 2p<sup>m</sup>, donde p es un primo impar y m ≥ 1.*

Igual resulta interesante hallar el máximo orden módulo n, al que llamaremos  $\lambda(n)$ . En algunos casos lo conocemos por el teorema 9.24, falta completarlo para los demás valores de n.

**Lema 9.25.** *El máximo orden en  $\mathbb{Z}_{2^e}$  con e ≥ 3 es  $\lambda(2^e) = 2^{e-2}$*

*Demostración.* Consideremos a impar. Entonces uno de  $a \pm 1$  es divisible por 4, y tenemos para algún f ≥ 2 y un c:

$$\begin{aligned} a &\equiv 2^f \pm 1 \pmod{2^{f+1}} \\ &= c \cdot 2^{f+1} + 2^f \pm 1 \\ a^2 &= c^2 \cdot 2^{2(f+1)} + 2^{2f} + 1 + 2 \cdot c \cdot 2^{2f+1} \pm 2 \cdot c \cdot 2^{f+1} \pm 2 \cdot 2^f \\ &\equiv 2^{f+1} + 1 \pmod{2^{f+2}} \end{aligned}$$

Continuando de la misma forma, concluimos que para r ≥ 1:

$$a^{2^r} \equiv 2^{f+r} + 1 \pmod{2^{f+r+1}} \quad (9.21)$$

Cuando f + r + 1 = e, la ecuación (9.21) lleva a:

$$\begin{aligned} a^{2^{e-f-1}} &\equiv 2^{e-1} + 1 \pmod{2^e} \\ &\not\equiv 1 \pmod{2^e} \\ a^{2^{e-f}} &\equiv 2^e + 1 \pmod{2^{e+1}} \\ &\equiv 1 \pmod{2^e} \end{aligned}$$

O sea,  $\text{ord}_{2^e}(a) = 2^{e-f}$ , donde f es el valor determinado anteriormente. El mínimo valor posible de f es 2, y siempre podemos elegir a = 4 - 1 = 3 que da f = 2, así  $\lambda(2^e) = 2^{e-2}$ .  $\square$

Incidentalmente, hemos hallado una manera simple de calcular  $\text{ord}_{2^e}(a)$ .

**Teorema 9.26.** *El máximo orden está dado por:*

$$\begin{aligned} \lambda(2) &= 1, & \lambda(4) &= 2, & \lambda(2^e) &= 2^{e-2} \text{ si } e \geq 3 \\ \lambda(p^e) &= p^{e-1}(p-1) \text{ si el primo } p > 2 \\ \lambda(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) &= \text{lcm}(\lambda(p_1^{e_1}), \lambda(p_2^{e_2}), \dots, \lambda(p_r^{e_r})) \text{ si } p_1, \dots, p_r \text{ son primos} \end{aligned}$$

*Demostración.* Los casos 2 y 4 son obvios. El caso  $2^e$  es el tema del lema 9.25, el caso  $p^e$  es inmediato del teorema 9.24 y  $\phi(p^e) = p^{e-1}(p-1)$ .

Ahora, para  $\text{gcd}(m, n) = 1$  sabemos del teorema chino de los residuos (en realidad, del corolario 8.6) que  $\mathbb{Z}_{mn}^\times \cong \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$ . El orden de un elemento  $a \in \mathbb{Z}_{mn}^\times$  que podemos descomponer en  $uv$  con  $u \in \mathbb{Z}_m^\times$  y  $v \in \mathbb{Z}_n^\times$ , es  $\text{lcm}(\text{ord}_m(u), \text{ord}_n(v))$ . Si elegimos elementos de orden máximo para u y v, a será de orden máximo, su orden es  $\lambda(mn) = \text{lcm}(\lambda(m), \lambda(n))$ , y el resultado sigue.  $\square$

Algunos algoritmos requieren usar raíces primitivas de un primo grande p, y los anteriores no dan muchas luces de cómo encontrar una. Por suerte son relativamente numerosas: Si tomamos una raíz primitiva r, todos los elementos  $r^k$  con  $\text{gcd}(k, p-1) = 1$  también tendrán orden  $p-1$  y son raíces primitivas. Vale decir, hay  $\phi(p-1)$  raíces primitivas del primo p.

# 10 Campos finitos

---

Gran parte de las matemáticas giran alrededor del álgebra abstracta, que hemos conocido en los grupos y anillos. Pero sin duda las estructuras algebraicas más importantes son los campos, que definimos en el capítulo 7 como anillos conmutativos en los que todos los elementos (salvo 0) tienen inverso multiplicativo. Implícitamente usamos el campo de los reales  $\mathbb{R}$ , ocasionalmente nos aventuramos a los números complejos  $\mathbb{C}$ . Pero en realidad nuestros cálculos casi siempre son con aproximaciones racionales en  $\mathbb{Q}$ . De particular interés son los campos finitos, con una bonita teoría y abundantes aplicaciones prácticas.

## 10.1. Propiedades básicas

El orden aditivo de 1 en el campo  $F$  determina en gran medida la estructura del campo, y se le llama la *característica del campo*. Se dice  $\text{chr}(F) = n$  si el orden es  $n$  y  $\text{chr}(F) = 0$  si es infinito.

Si  $F$  es un campo, y  $K$  es un subcampo de  $F$  (cosa que se anota  $K \leq F$ ) se dice que  $F$  es un *campo extensión* de  $K$ ; si  $K \neq F$  decimos que  $K$  es un *subcampo propio* de  $F$  (se anota  $K < F$  en este caso). Se le llama *subcampo primo* de  $F$  a la intersección entre todos los subcampos de  $F$ . El subcampo primo no tiene subcampos a su vez. Anotamos  $K \cong F$  si los campos  $K$  y  $F$  son isomorfos

**Teorema 10.1.** *Sea  $K$  el subcampo primo de  $F$ . Entonces:*

- (I) *Si  $F$  tiene característica 0, entonces  $K \cong \mathbb{Q}$*
- (II) *Si  $F$  tiene característica  $p$ , entonces  $p$  es primo y  $K \cong \mathbb{Z}_p$*

*Demostración.* Llamaremos  $0_K$  y  $1_K$  a los elementos neutros de  $K$ .

- (I) En este caso para  $a \in \mathbb{Z}$  tenemos que  $a \cdot 1_K \in K$ , y como  $K$  es un campo para  $b \in \mathbb{N}$  también  $(a \cdot 1_K)(b \cdot 1_K)^{-1} \in K$ , y esto es isomorfo al campo  $\mathbb{Q}$ . Como  $K$  no tiene subcampos,  $K \cong \mathbb{Q}$ .
- (II) Nuevamente para  $a \in \mathbb{Z}$  tenemos que  $a \cdot 1_K \in K$ , pero  $p \cdot 1_K = 0_K$ , con lo que hay un subcampo de  $K$  que es isomorfo a  $\mathbb{Z}_p$ , y como  $K$  es mínimo es  $K \cong \mathbb{Z}_p$ . Pero  $\mathbb{Z}_p$  es campo si y solo si  $p$  es primo.  $\square$

Si el campo finito  $F$  no es isomorfo a ningún  $\mathbb{Z}_p$ , habrá algún elemento que no pertenece a su subcampo primo  $K$ , llamémosle  $\alpha$ . Pero en tal caso, los elementos  $\{k\alpha : k \in K\}$  deben ser todos distintos entre sí, y salvo 0 ninguno pertenece a  $K$ . Así tenemos elementos  $\{k_0 + k_1\alpha : k_0, k_1 \in K\}$ . Debemos además incluir las potencias de  $\alpha$ . Si la primera potencia de  $\alpha$  que pertenece a  $K$  es  $\alpha^m$ , tendremos elementos  $k_0 + k_1\alpha + \dots + k_{m-1}\alpha^{m-1}$ , todos diferentes. Cualquier elemento  $\beta$  aún no considerado dará lugar a una construcción similar sobre los anteriores. Repitiendo este proceso, vemos que hay una colección de  $n$  elementos  $\alpha_i \in F \setminus K$  (elementos como  $\alpha$  y  $\beta$  mencionados

arriba, sus potencias, y productos de ellas) tales que eligiendo adecuadamente los  $k_i \in K$  podemos representar cualquier elemento  $f \in F$  mediante la expresión:

$$f = \sum_{1 \leq i \leq n} k_i \alpha_i$$

Por la construcción anterior, cada elección de los  $k_i$  da lugar a un elemento diferente de  $F$ , con lo que concluimos que si la característica del campo es  $p$ , y el campo es finito, su orden debe ser  $p^n$  para  $n \in \mathbb{N}$ . Para discutir este fenómeno se requieren conceptos adicionales, para mayores detalles véase por ejemplo el texto de Strang [340].

## 10.2. Espacios vectoriales

Una estructura algebraica común es el espacio vectorial. Es aplicable a una gran variedad de situaciones, algunas bastante inesperadas.

**Definición 10.1.** Sea  $F$  un campo (sus elementos los llamaremos *escalares*) y  $V$  un conjunto (los *vectores*, que por convención anotaremos en negrita). Hay operaciones *suma de vectores* (anotada  $+$ ) y *producto escalar* entre un escalar y un vector (anotada  $\cdot$ ). Se dice que  $V$  es un *espacio vectorial sobre  $F$*  si cumple con los siguientes axiomas, donde  $\alpha, \beta, \dots \in F$ , y  $\mathbf{v}_1, \mathbf{v}_2, \dots \in V$ .

**V1:**  $(\mathbf{v}_1 + \mathbf{v}_2) + \mathbf{v}_3 = \mathbf{v}_1 + (\mathbf{v}_2 + \mathbf{v}_3)$

**V2:** Hay un elemento  $\mathbf{0} \in V$  tal que para todo  $\mathbf{v} \in V$  se cumple  $\mathbf{v} + \mathbf{0} = \mathbf{v}$

**V3:** Para cada  $\mathbf{v} \in V$  hay  $-\mathbf{v} \in V$  tal que  $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$

**V4:**  $\mathbf{v}_1 + \mathbf{v}_2 = \mathbf{v}_2 + \mathbf{v}_1$

**V5:**  $\alpha \cdot (\mathbf{v}_1 + \mathbf{v}_2) = \alpha \cdot \mathbf{v}_1 + \alpha \cdot \mathbf{v}_2$

**V6:**  $(\alpha + \beta) \cdot \mathbf{v} = \alpha \cdot \mathbf{v} + \beta \cdot \mathbf{v}$

**V7:**  $\alpha \cdot (\beta \cdot \mathbf{v}) = (\alpha\beta) \cdot \mathbf{v}$

**V8:** Si 1 es el neutro multiplicativo de  $F$ ,  $1 \cdot \mathbf{v} = \mathbf{v}$

En resumen,  $(V, +)$  es un grupo abeliano (axiomas V1 a V4), junto con el campo  $F$  y multiplicación escalar que cumple los axiomas adicionales V5 a V8. Normalmente indicaremos la multiplicación escalar por simple yuxtaposición. Dejamos de ejercicio demostrar que  $0 \cdot \mathbf{v} = \mathbf{0}$  y que  $(-\alpha) \cdot \mathbf{v} = -(\alpha \cdot \mathbf{v})$ .

**Definición 10.2.** Sea  $V$  un espacio vectorial sobre el campo  $F$ . Si para el conjunto de vectores  $B$  es:

$$\sum_{\mathbf{b} \in B} \alpha_{\mathbf{b}} \mathbf{b} = \mathbf{0}$$

solo si  $\alpha_{\mathbf{b}} = 0$  para todo  $\mathbf{b} \in B$  se dice que esos vectores son *linealmente independientes*.

Si un conjunto de vectores no es linealmente independiente se dice que son *linealmente dependientes*. Nótese que  $\mathbf{0}$  nunca pertenece a un conjunto de vectores linealmente independientes, ya que al multiplicarlo por cualquier escalar obtenemos  $\mathbf{0}$ .

**Definición 10.3.** Sea  $V$  un espacio vectorial sobre  $F$ , y  $B \subseteq V$  un conjunto de vectores. El *espacio vectorial generado por  $B$*  es el conjunto:

$$\langle B \rangle = \left\{ \sum_{\mathbf{b} \in B} \alpha_{\mathbf{b}} \mathbf{b} : \alpha_{\mathbf{b}} \in F \right\}$$

Si  $V = \langle B \rangle$ , se dice que  $B$  *abarca*  $V$ .

En particular:

**Definición 10.4.** Una *base* del espacio vectorial  $V$  es un conjunto linealmente independiente de vectores  $B$  que abarca  $V$ .

La representación de  $\mathbf{v} \in V$  en términos de la base  $B$  es única, ya que si hubieran dos representaciones diferentes darían una dependencia lineal en  $B$ . Para el vector:

$$\mathbf{v} = \sum_{\mathbf{b} \in B} \alpha_{\mathbf{b}} \mathbf{b}$$

a los coeficientes  $\alpha_{\mathbf{b}}$  se les llama *componentes* de  $\mathbf{v}$  (en la base  $B$ ).

**Definición 10.5.** Al número de vectores en una base de  $V$  se le llama la *dimensión* de  $V$ , anotada  $\dim V$ . Un espacio vectorial abarcado por un conjunto finito de vectores se dice de *dimensión finita*, en caso contrario es de *dimensión infinita*. Al espacio vectorial  $\{\mathbf{0}\}$  se le asigna dimensión cero. Se anota  $[V : F]$  para la dimensión de  $V$  sobre el campo  $F$ .

En el caso de espacios vectoriales de dimensión finita es simple demostrar que todas las bases tienen la misma cardinalidad, con lo que nuestra definición de dimensión tiene sentido.

**Teorema 10.2.** Si  $V$  es un espacio vectorial con base  $B = \{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$ , y  $A = \{\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_r\}$  es un conjunto linealmente independiente de vectores en  $V$ , entonces  $r \leq n$ .

*Demostración.* Como  $B$  abarca  $V$ ,  $B \cup \{\mathbf{a}_1\}$  también abarca  $V$ . Como  $\mathbf{a}_1 \neq \mathbf{0}$  ( $A$  es linealmente independiente), podemos expresar  $\mathbf{a}_1$  como combinación lineal de los  $B$ , y en ella algún  $\mathbf{b}_t$  tendrá coeficiente diferente de 0. Ese  $\mathbf{b}_t$  puede expresarse en términos de  $B_1 = \{\mathbf{a}_1, \mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_{t-1}, \mathbf{b}_{t+1}, \dots, \mathbf{b}_n\}$ . Como todo  $\mathbf{v} \in V$  puede escribirse como combinación lineal de los  $B$ , también puede escribirse como combinación lineal de los  $B_1$  (sustituyendo la combinación de  $B_1$  que da  $\mathbf{b}_t$  en la combinación lineal para  $\mathbf{v}$  se obtiene una nueva combinación lineal). Este proceso puede repetirse intercambiando un  $A$  por uno de los  $B$ , manteniendo siempre  $B_k$  como base, finalmente llegando a  $B_r = \{\mathbf{a}_1, \dots, \mathbf{a}_r, \mathbf{b}_{m_1}, \mathbf{b}_{m_2}, \dots, \mathbf{b}_{m_s}\}$  (posiblemente no queden  $\mathbf{b}_{m_k}$  en  $B_r$ ). No pueden quedar  $A$  si se acaban los  $B$ , ya que si fuera así un  $\mathbf{a}_i$  sobrante no podría representarse como combinación lineal de los  $B$ , y  $B$  no sería una base. Tenemos  $A \subseteq B_r$ , y claramente  $|A| \leq |B_r| = |B|$ .  $\square$

Esto justifica la definición de la dimensión en el caso de espacios vectoriales de dimensión finita:

**Corolario 10.3** (Teorema de dimensión de espacios vectoriales). Si  $A$  y  $B$  son bases de un espacio vectorial de dimensión finita, entonces  $|A| = |B|$ .

*Demostración.* La base  $A$  es linealmente independiente, con lo que por el teorema 10.2 es  $|A| \leq |B|$ . Por el mismo argumento, intercambiando los roles de  $A$  y  $B$ ,  $|B| \leq |A|$ , con lo que  $|A| = |B|$ .  $\square$

Esto nos lleva a:

**Teorema 10.4.** Todos los espacios vectoriales de la misma dimensión finita sobre  $F$  son isomorfos.

*Demostración.* Sean  $U$  y  $V$  espacios vectoriales de la misma dimensión finita, con bases  $\{\mathbf{a}_k\}_{1 \leq k \leq n}$  y  $\{\mathbf{b}_k\}_{1 \leq k \leq n}$ , respectivamente. Podemos representar todos los vectores  $\mathbf{u} \in U$  y  $\mathbf{v} \in V$  mediante:

$$\mathbf{u} = \sum_{1 \leq k \leq n} a_k \mathbf{a}_k \quad \mathbf{v} = \sum_{1 \leq k \leq n} b_k \mathbf{b}_k$$

Definimos la biyección  $f: U \rightarrow V$  mediante:

$$f: \sum_{1 \leq k \leq n} a_k \mathbf{a}_k \mapsto \sum_{1 \leq k \leq n} a_k \mathbf{b}_k$$

Demostrar que la suma vectorial y el producto escalar se preservan es rutinario.  $\square$

En vista de la demostración del teorema 10.4, en un espacio vectorial de dimensión finita basta elegir una base, cada vector puede representarse mediante la secuencia de los coeficientes en  $F$ . La suma vectorial es sumar componente a componente, el producto escalar es multiplicar cada componente por el escalar. Es por esta representación que a secuencias de largo fijo les llaman vectores.

Lo anterior solo cubre una pequeña parte de la extensa teoría relacionada con operaciones lineales. Para profundizar en ella recomendamos el texto de Treil [352].

### 10.3. Estructura de los campos finitos

Profundizaremos nuestro estudio de los campos finitos, apoyados ahora en lo que sabemos de espacios vectoriales.

**Lema 10.5.** *Sea  $K$  el subcampo primo de  $F$ , y sea  $\alpha \in F$  el cero de un polinomio en  $K[x]$ . Entonces hay un polinomio mónico único de grado mínimo en  $K[x]$  con  $\alpha$  de cero.*

*Demostración.* Es simple demostrar que  $I = \{f \in K[x] : f(\alpha) = 0\}$  es un ideal de  $K[x]$ . Como  $K[x]$  es un dominio de ideal principal,  $I = (h)$  para algún  $h \in K[x]$ , donde  $h$  es mónico y de mínimo grado entre los elementos de  $I$ , y es único con estas características.  $\square$

Al polinomio  $h$  de la demostración del lema 10.5 se le llama el *polinomio mínimo de  $\alpha$  sobre  $K$* . Un elemento  $\alpha$  que es cero de un polinomio en  $K[x]$  se dice *algebraico sobre  $K$* .

**Teorema 10.6.** *Sea  $\alpha \in F$  el cero de un polinomio en  $K[x]$  y sea  $g$  el polinomio mínimo de  $\alpha$ . Entonces*

- (I)  $g$  es irreducible en  $K[x]$
- (II)  $f(\alpha) = 0$  si y solo si  $g \mid f$

*Demostración.* Por turno.

- (I) Como  $g$  tiene un cero en  $F$ ,  $\deg(g) \geq 1$ . Demostramos que  $g$  es irreducible por contradicción. Supongamos que podemos expresar  $g = h_1 h_2$  en  $K[x]$  con  $1 \leq \deg(h_i) < \deg(g)$  para  $i = 1, 2$ . Entonces  $g(\alpha) = h_1(\alpha)h_2(\alpha) = 0$ , por lo que  $h_1(\alpha) = 0$  o  $h_2(\alpha) = 0$ ; o sea uno de los polinomios está en el ideal  $I$  de la demostración del lema 10.5. Al ser  $K[x]$  un dominio de ideal principal, ese ideal es el conjunto de los múltiplos de  $g$ , con lo que  $g \mid h_1$  o  $g \mid h_2$ , lo que es imposible porque sus grados son menores al de  $g$ .

- (II) Esto sigue de la definición de  $g$  como generador del ideal  $I$  del mencionado lema.  $\square$

Antes de continuar, demostraremos que todos los campos finitos de orden  $q$  son isomorfos (ya sabemos que  $q = p^n$  para un primo  $p$ ). De partida:

**Teorema 10.7** (Polinomio universal). *Sea  $F$  un campo finito de orden  $q$ . Entonces todos los elementos  $a \in F$  cumplen la ecuación:*

$$x^q - x = 0$$

*Demostración.* Por el teorema de Lagrange, si  $a \neq 0$  el orden multiplicativo de  $a$  divide a  $q - 1$ ; en particular:

$$a^{q-1} - 1 = 0$$

Si multiplicamos esta ecuación por  $a$ , resulta que para todo  $a \in F$ :

$$a^q - a = 0$$

$\square$

Nótese que el teorema 10.7 dice que los elementos del campo finito  $F$  de orden  $q$  son todas las raíces del polinomio universal  $x^q - x$ . En particular, los polinomios mínimos de los elementos de  $F$  dividen a  $x^q - x$ .

**Teorema 10.8.** *Sean  $F$  y  $F'$  campos finitos de orden  $q$ . Entonces  $F \cong F'$ .*

*Demostración.* Sabemos que si  $|F| = |F'| = p^n$ , la característica de ambos campos es  $p$ , en particular, el campo primo de ambos es isomorfo a  $\mathbb{Z}_p$ .

Sabemos que  $F^\times$  es cíclico (teorema 9.16), elijamos un generador  $\pi$  de  $F^\times$ , y sea  $m(x)$  el polinomio mínimo de  $\pi$ , que por la observación anterior (teorema 10.6) con  $q = p^n$  en  $F$  cumple:

$$m(x) \mid x^{q-1} - 1$$

Consideremos el polinomio  $m(x)$  en  $F'$  ahora, donde también divide a  $x^q - x$  (los coeficientes y las operaciones al dividir son estrictamente en el subcampo primo, serán las mismas en  $F$  y  $F'$ ). Acá podemos escribir:

$$x^{q-1} - 1 = \prod_{a' \in F'^\times} (x - a')$$

por lo que  $m(x)$  se factoriza completamente en  $F'$ :

$$m(x) = (x - a'_1)(x - a'_2) \cdots (x - a'_d)$$

Elijamos un cero cualquiera de  $m(x)$  en  $F'$ , digamos  $\pi' = a'_1$ . Observamos primeramente que  $\pi'$  genera  $F'^\times$ , ya que si su orden fuera  $d < q - 1$ , cumpliría:

$$x^d - 1 = 0$$

Pero como  $m(x)$  es un polinomio irreducible, debe ser su polinomio mínimo, y en  $F'$ :

$$m(x) \mid x^d - 1$$

Volviendo a  $F$ , esto significa que  $\pi$  también satisface esta ecuación, y tiene orden  $d < q - 1$  (o sea, no sería generador de  $F^\times$ ).

Hay un isomorfismo de grupo obvio entre  $(F^\times, \cdot)$  y  $(F'^\times, \cdot)$ :

$$\Theta(\pi^k) = \pi'^k$$

Podemos extenderlo a una biyección entre  $F$  y  $F'$  definiendo:

$$\Theta(0) = 0$$

Resta demostrar que  $\Theta$  es un isomorfismo para la suma. Sean  $a, b \in F$ , debemos mostrar que:

$$\Theta(a + b) = \Theta(a) + \Theta(b)$$

Si  $a = 0$  o  $b = 0$ , el resultado es inmediato, así que en lo que sigue  $a \neq 0$  y  $b \neq 0$ . Debemos considerar los dos casos  $a + b = 0$  y  $a + b \neq 0$ . Veamos primero el segundo, más general. Sean:

$$a = \pi^i \quad b = \pi^j \quad a + b = \pi^k$$

Entonces en  $F$ :

$$\pi^i + \pi^j = \pi^k$$

Vale decir,  $\pi$  satisface la ecuación:

$$x^i + x^j - x^k = 0$$

Por el teorema 10.6 en  $F$ :

$$m(x) \mid x^i + x^j - x^k$$

Pero en tal caso esto también se cumple en  $F'$ :

$$\pi'^i + \pi'^j = \pi'^k$$

Esto es precisamente:

$$\Theta(a + b) = \Theta(a) + \Theta(b)$$

Resta el caso  $a + b = 0$ . Si la característica de los campos es 2, esto significa  $a = b$ , y en consecuencia como  $\Theta(a) = \Theta(b)$  es:

$$\Theta(a + b) = \Theta(0) = 0 = \Theta(a) + \Theta(b)$$

Si la característica de  $F$  es impar, notamos que  $-1$  es el único elemento de orden 2, ya que:

$$x^2 - 1 = (x - 1)(x + 1)$$

no puede tener más de dos ceros. En efecto, como  $F$  tiene  $q$  elementos (y así  $F^\times$  tiene  $q - 1$  elementos), debe ser:

$$-1 = \pi^{\frac{q-1}{2}}$$

dado que el elemento al lado derecho tiene el orden correcto. Escribamos  $a = \pi^i$  y  $b = \pi^j$ , donde podemos suponer sin pérdida de generalidad que  $i > j$ , con lo que:

$$\begin{aligned} \pi^i + \pi^j &= 0 \\ \pi^i &= -\pi^j \\ \pi^{i-j} &= -1 \\ i - j &= \frac{q-1}{2} \\ \pi'^{(i-j)} &= -1 \end{aligned}$$

De acá, aplicando lo anterior en reversa en  $F'$ :

$$\pi'^i + \pi'^j = 0$$

Vale decir:

$$\Theta(a + b) = \Theta(a) + \Theta(b)$$

En resumen, la biyección  $\Theta$  preserva suma y multiplicación, es un isomorfismo entre los campos.  $\square$

Al campo finito de orden  $q$  se le anota  $\mathbb{F}_q$  (en la literatura más antigua se suele encontrar la notación  $\text{GF}(q)$ , por la abreviatura de *campo de Galois* en honor a quien comenzó su estudio). Resulta curioso que todo polinomio irreductible de grado  $n$  da el mismo campo. Resta demostrar que tales campos existen para todo primo  $p$  y todo  $n$ .

Vimos (teorema 7.36) que  $\mathbb{Z}_m = \mathbb{Z}/(m)$  es un campo solo cuando  $m$  es primo. Hay notables similitudes entre el anillo  $\mathbb{Z}$  y los anillos de polinomios  $K[x]$  sobre un campo  $K$  – particularmente si  $K$  es finito. Ya vimos un ejemplo de esto: En los números enteros hay infinitos primos, y pueden expresarse en forma esencialmente única como producto de primos (y un signo, vale decir multiplicar por una unidad), el teorema fundamental de la aritmética. Para polinomios tenemos el teorema 9.11. Los primos en  $\mathbb{Z}$  corresponden a los polinomios mónicos irreductibles en  $K[x]$ . Igual que la relación de congruencia entre enteros, podemos definirla para polinomios  $f(x), g(x), m(x) \in K[x]$ :

$$f(x) \equiv g(x) \pmod{m(x)}$$

siempre que para algún  $q(x) \in K[x]$ :

$$g(x) - f(x) = m(x)q(x)$$

Es rutinario verificar que es equivalencia en  $K[x]$ , y que las clases de equivalencia forman un anillo  $K[x]/(m(x))$ , el *anillo de polinomios sobre  $K$  módulo  $m(x)$* . Este anillo contiene el campo  $K$  como los polinomios constantes.

**Teorema 10.9.** *El anillo cociente  $K[x]/(m(x))$  es un campo si y solo si  $m(x)$  es irreductible.*

*Demostración.* Demostramos implicancia en ambas direcciones. Para el directo, sea  $f(x) \in K[x]$  tal que  $m(x) \nmid f(x)$ . Sabemos (sección 9.2) que los polinomios sobre un campo son un dominio euclidiano, es aplicable la identidad de Bézout y tenemos un inverso de  $f$ .

Para el recíproco, usamos contradicción. Supongamos que  $m(x)$  no es irreductible, vale decir:

$$m(x) = a(x) \cdot b(x)$$

donde  $a(x)$  y  $b(x)$  no son constantes. Las clases de equivalencia correspondientes no son cero, pero:

$$[a(x)] \cdot [b(x)] = [a(x) \cdot b(x)] = [m(x)] = 0$$

Al haber divisores de cero, no es campo. □

Considerando  $K[x]/(m(x))$  como espacio vectorial, es una extensión de  $K$ :

**Definición 10.6.** A la dimensión de  $F$  como espacio vectorial sobre  $K$  la anotamos  $[F : K]$ , y la llamamos el *grado de la extensión*.

**Lema 10.10.** *Si  $m(x)$  es un polinomio irreductible de grado  $d$ , entonces las clases de equivalencia:*

$$[1], [x], \dots, [x^{d-1}]$$

*forman una base para  $K[x]/(m(x))$ . En particular:*

$$\dim_K K[x]/(m(x)) = \deg m(x)$$

*Demostración.* Demostramos por contradicción que las clases son linealmente independientes. Supongamos:

$$c_0[1] + c_1[x] + \dots + c_{d-1}[x^{d-1}] = 0$$

Esto significa:

$$m(x) \mid c_0 + c_1x + \cdots + c_{d-1}x^{d-1}$$

Esto solo es posible si todos los  $c_i = 0$ , ya que el grado de  $m$  es  $d$ .

Para demostrar que las clases de equivalencia abarcan  $K[x]/(m(x))$ , elegimos  $f(x) \in K[x]$  cualquiera. Podemos dividir:

$$f(x) = m(x) \cdot q(x) + r(x) \quad \deg r(x) < \deg m(x)$$

Así:

$$f(x) \equiv r(x) \pmod{m(x)}$$

O sea, si:

$$r(x) = r_0 + r_1x + \cdots + r_{d-1}x^{d-1}$$

entonces:

$$[f(x)] = [r(x)] = r_0[1] + r_1[x] + \cdots + r_{d-1}[x^{d-1}] \quad \square$$

**Corolario 10.11.** Si  $m(x) \in \mathbb{F}_q[x]$  es irreducible de grado  $n$ , entonces  $\mathbb{F}_q[x]/(m(x))$  es de orden  $q^n$ .

*Demostración.* Inmediato del teorema 10.9:  $\mathbb{F}_q[x]/(m(x))$  es un espacio vectorial de dimensión  $n$  sobre  $\mathbb{F}_q$ , con lo que contiene  $q^n$  elementos.  $\square$

En lo anterior construimos un campo  $K[x]/(m(x))$  partiendo de un campo  $K$  y un polinomio irreducible sobre él. Vimos también que todos los campos finitos del mismo orden son isomorfos. Ahora la construcción inversa, buscando la relación entre un campo  $F$  y sus subcampos.

**Definición 10.7.** Sean  $\alpha_1, \alpha_2, \dots, \alpha_n \in F$ , y sea  $K$  un subcampo de  $F$ . Al mínimo subcampo de  $F$  que contiene  $\alpha_1, \alpha_2, \dots, \alpha_n$  y  $K$  se anota  $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ . A tales campos se les llama *extensiones* de  $K$ . Si  $F = K(\alpha)$ , se dice que  $F$  es una *extensión simple* de  $K$ .

Nótese la similitud entre la definición 10.7 y la noción de anillos cuadráticos vistos en la sección 7.5.2. Allá usamos la notación  $\mathbb{Z}[\sqrt{2}]$  para el anillo, acá hablamos del campo  $\mathbb{Q}(\sqrt{2})$ .

Por la discusión anterior  $K(\alpha_1, \dots, \alpha_n)$  es un espacio vectorial sobre  $K$ .

**Teorema 10.12.** Sea  $F$  una extensión del campo  $K$ , y sea  $\alpha \in F$  el cero de un polinomio en  $K[x]$ , con polinomio mínimo  $g$ . Entonces:

- (I)  $K(\alpha)$  es isomorfo a  $K[x]/(g(x))$
- (II)  $[K(\alpha) : K] = \deg(g)$  y  $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$  es una base de  $K(\alpha)$  sobre  $K$
- (III) Si  $\beta \in K(\alpha)$  es el cero de un polinomio en  $K[x]$ , el grado del polinomio mínimo de  $\beta$  divide al grado de  $g$

*Demostración.* Para el punto (I), por el lema 10.10 la clase  $[x]$  de  $K[x]/(g(x))$  satisface la ecuación:

$$g(x) = 0$$

En consecuencia,  $K(\alpha) \cong K[x]/(g(x))$  ya que son campos finitos del mismo orden. El punto (II) es inmediato de lo anterior.

Para (III), que  $K(\alpha)$  es un espacio vectorial sobre  $K(\beta)$ , con lo que el grado del polinomio mínimo de  $\alpha$  sobre  $K(\beta)$  da la condición de divisibilidad prometida.  $\square$

De lo anterior tenemos directamente:

**Corolario 10.13.** *Sean  $F \leq G \leq H$  campos finitos. Entonces:*

$$[H : F] = [H : G] \cdot [G : F]$$

Lo anterior muestra un cero de cada polinomio irreducible, pero nos interesan todas los ceros. Al efecto, definimos:

**Definición 10.8.** Sea  $f \in K[x]$  un polinomio de grado positivo, y  $F$  una extensión de  $K$ . Decimos que  $f$  se divide en  $F$  si hay  $a \in K$  y  $\alpha_i \in F$  para  $1 \leq i \leq n$  tales que podemos escribir:

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

El campo  $F$  se llama *campo divisor* de  $f$  sobre  $K$  si  $f$  se divide en  $F$  y además es  $F = K(\alpha_1, \alpha_2, \dots, \alpha_n)$ .

El siguiente resultado es una pieza angular de la teoría de campos.

**Teorema 10.14 (Kronecker).** *Para todo polinomio irreducible  $f(x)$  sobre el campo  $F$  hay una extensión en la cual  $f(x)$  tiene un cero.*

*Demostración.* Sea  $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$  irreducible. Consideremos el elemento  $[x]$  en el campo  $F[x]/(f(x))$ . Entonces en  $F[x]/(f(x))$ :

$$\begin{aligned} f([x]) &= [a_0] + [a_1][x] + \cdots + [a_n][x^n] \\ &= [a_0 + a_1x + \cdots + a_nx^n] \\ &= 0 \end{aligned}$$

Así  $F[x]/(f(x))$  es campo divisor, y en el  $[x]$  es cero. □

Esto parece ser solo jugar con la notación, pero es más profundo: Hay que distinguir entre  $x$  (el símbolo usado para describir polinomios formales) y  $[x]$  (la clase de equivalencia del polinomio  $x$  módulo  $f(x)$  sobre  $F$ ). Además usamos las definiciones y propiedades de las operaciones entre clases de congruencia. También vemos que al aplicar repetidas veces el teorema de Kroneker obtenemos finalmente el campo divisor de cualquier polinomio.

**Teorema 10.15.** *Sea  $F$  un campo,  $f$  un polinomio irreducible sobre el campo  $K$  con ceros  $\alpha, \beta \in F$ . Entonces  $K(\alpha) \cong K(\beta)$ , con un isomorfismo que mantiene fijos los elementos de  $K$  e intercambia los ceros  $\alpha$  y  $\beta$ .*

*Demostración.* Por el teorema de Kronecker, ambos son isomorfos a  $K[x]/(f(x))$ , dado que el irreducible  $f$  es el polinomio mínimo de  $\alpha$  y  $\beta$ . El isomorfismo claramente mantiene fijos los elementos de  $K$ ,  $\beta$  se expresa como una combinación lineal en  $K(\alpha)$  y similarmente  $\alpha$  en  $K(\beta)$ . □

Lo siguiente básicamente recoge resultados previos.

**Teorema 10.16 (Existencia y unicidad del campo divisor).** *Todo polinomio tiene campo divisor único:*

- (I) *Si  $K$  es un campo y  $f$  un polinomio de grado positivo en  $K[x]$ , entonces existe un campo divisor de  $f$  sobre  $K$ .*
- (II) *Cualquier par de campos divisores de  $f$  sobre  $K$  son isomorfos bajo un isomorfismo que mantiene fijos los elementos de  $K$  y permuta ceros de  $f$ .*

Así podemos hablar de *el* campo divisor de  $f$  sobre  $K$ , que se obtiene adjuntando un número finito de elementos algebraicos a  $K$ , y es una extensión finita de  $K$ .

**Teorema 10.17** (Existencia y unicidad de campos finitos). *Para cada primo  $p$  y natural  $n$  hay un campo finito de orden  $p^n$ . Todo campo finito de orden  $q = p^n$  es isomorfo al campo divisor de  $x^q - x$  sobre  $\mathbb{Z}_p$ .*

*Demostración.* Sea  $F$  el campo divisor de  $f(x) = x^q - x$  en  $\mathbb{Z}_p[x]$ . Como  $f'(x) = qx^{q-1} - 1 = -1$  sobre  $\mathbb{Z}_p$ , por el lema 9.12  $f(x)$  no tiene factores repetidos, con lo que  $f(x)$  tiene  $q$  ceros en  $F$ , exactamente los  $q$  elementos de  $F$ .

Por el teorema 10.12, el campo divisor es único. □

El polinomio universal  $U_n(x) = x^{p^n} - x$  tiene como ceros todos los elementos de  $\mathbb{F}_{p^n}$ . Resulta que  $U_m(x) \mid U_n(x)$  si y solo si  $m \mid n$ , pero curiosamente es más fácil demostrar algo bastante más general:

**Teorema 10.18.** *Sobre  $\mathbb{F}_p$ :*

$$\gcd(U_m(x), U_n(x)) = U_{\gcd(m,n)}(x)$$

*Demostración.* Si  $m = n$  no hay nada que demostrar. Usamos inducción fuerte sobre  $n$  para  $m < n$ .

**Base:** Cuando  $n = 1$ , no hay nada que demostrar.

**Inducción:** Sea  $r = n - m$  y consideremos:

$$(U_m(x))^p = x^{p^{m+1}} - x^p$$

ya que al aplicar el teorema del binomio los términos intermedios se anulan por ser divisibles por  $p$ . Aplicando lo anterior  $r$  veces resulta:

$$\begin{aligned} (U_m(x))^{p^r} &= x^{p^{m+n-m}} - x^{p^r} \\ &= x^{p^n} - x^{p^r} \\ &= U_n(x) - U_r(x) \end{aligned}$$

de lo que obtenemos:

$$\gcd(U_m(x), U_n(x)) = \gcd(U_r(x), U_m(x))$$

Por inducción:

$$\begin{aligned} \gcd(U_r(x), U_m(x)) &= U_{\gcd(r,m)}(x) \\ &= U_{\gcd(m,n)}(x) \end{aligned}$$

ya que  $\gcd(r, m) = \gcd(n - m, m) = \gcd(m, n)$ .

Por inducción lo prometido vale para todo  $m, n \in \mathbb{N}$ . □

Así:

**Corolario 10.19.** *Sobre  $\mathbb{F}_p$  es  $U_m(x) \mid U_n(x)$  si y solo si  $m \mid n$ .*

*Demostración.* Recurrimos a una cadena de equivalencias. Es claro que  $U_m(x) \mid U_n(x)$  si y solo si  $\gcd(U_m(x), U_n(x)) = U_m(x)$ . Por el teorema 10.18 esto es si y solo si  $\gcd(m, n) = m$ , que es si y solo si  $m \mid n$ . □

**Teorema 10.20.** *Sea  $F_q$  un campo finito y  $F_r$  una extensión finita de  $F_q$ . Entonces*

(I)  *$F_r$  es una extensión simple de  $F_q$ , vale decir, hay  $\beta \in F_r$  tal que  $F_r = F_q(\beta)$*

(II) *Cualquier elemento primitivo de  $F_r$  sirve como elemento definidor  $\beta$*

*Demostración.* Para (I), sea  $\alpha$  un elemento primitivo de  $F_r$ , con lo que  $F_q(\alpha) \subseteq F_r$ . Por otro lado,  $F_q(\alpha)$  contiene a 0 y todas las potencias de  $\alpha$ , que son los elementos de  $F_r^\times$ ; con lo que  $F_r \subseteq F_q(\alpha)$ . En consecuencia  $F_r = F_q(\alpha)$ . El punto (II) es inmediato de lo anterior.  $\square$

Así tenemos

**Corolario 10.21.** *Para cada primo  $p$  hay polinomios irreductibles de todo grado  $n \geq 1$  sobre  $\mathbb{Z}_p$ .*

*Demostración.* Por el teorema 10.12 toda extensión de  $\mathbb{Z}_p$  es isomorfa a algún  $\mathbb{Z}_p(\alpha) \cong \mathbb{Z}_p[x]/(g(x))$  donde  $g(x)$  es el polinomio mínimo de  $\alpha$ , por el teorema 10.6 el polinomio mínimo es irreductible. Por el teorema 10.17 hay campos finitos de  $p^n$  elementos para todo primo  $p$  y natural  $n$ . En consecuencia, hay polinomios irreductibles de todos los grados sobre  $\mathbb{Z}_p$ .  $\square$

Podemos hacer más:

**Teorema 10.22.** *Sea  $N_n$  el número de polinomios irreductibles de grado  $n$  sobre  $\mathbb{F}_q$ . Entonces:*

$$N_n = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d \quad (10.1)$$

*Demostración.* En  $\mathbb{F}_{q^n}$  cada elemento es cero de su polinomio mínimo. Tal polinomio mínimo de grado  $d$  es irreductible sobre  $\mathbb{F}_q$  y tiene  $d$  ceros distintos en  $\mathbb{F}_{q^n}$ . Contabilizando los elementos de  $\mathbb{F}_{q^n}$  como los ceros de sus polinomios mínimos:

$$\sum_{d|n} d N_d = q^n$$

Aplicando inversión de Möbius (teorema 8.19) obtenemos lo anunciado.  $\square$

Esto da otra demostración de que hay polinomios irreductibles de grado  $n$  sobre  $\mathbb{Z}_q$  para todo  $n \in \mathbb{N}$ : Para  $n = 1$ , todos los polinomios son irreductibles. Si  $n \geq 2$ , en la suma (10.1) el término  $q^n$  es mayor que la suma de los demás, ya que como  $|\mu(x)| \leq 1$  podemos acotar:

$$\left| \sum_{\substack{d|n \\ d < n}} \mu(n/d) q^d \right| \leq \sum_{\substack{d|n \\ d < n}} q^d \leq \sum_{0 \leq d \leq n-1} q^d = \frac{q^n - 1}{q - 1} < q^n$$

Así la suma en (10.1) nunca se anula si  $n \geq 2$ . Uniendo este resultado con el caso  $n = 1$ ,  $N_n > 0$  para todo  $n \in \mathbb{N}$ . En vista del corolario 10.19, podemos obtener todos los polinomios irreductibles sobre  $\mathbb{F}_p$  de grado hasta  $n$  como factores de  $U_n(x)$ .

## 10.4. Códigos de detección y corrección de errores

Consideremos *mensajes* de  $m$  bits de largo que se transmiten por algún medio (podría ser simplemente que se almacenan y se recuperan luego). En este proceso pueden ocurrir errores, que interesa detectar o corregir. El tema fue estudiado inicialmente por Hamming [162]. Para ello usamos *palabras de código* de  $n$  bits de largo, donde obviamente  $n \geq m$ , usando los bits adicionales para detectar o corregir errores, usando solo  $2^m$  de las  $2^n$  palabras posibles. Si se recibe una palabra errada (que no corresponde al código), una estrategia obvia es suponer que el código correcto es el más cercano al recibido, vale decir, el que difiere en menos bits del recibido. Al número de bits en que difieren dos palabras se les llama la *distancia de Hamming* entre ellas. Por ejemplo, la distancia de Hamming entre 10111011 y 10010100 es 5. A la distancia de Hamming mínima entre dos palabras de un código se le conoce como *distancia de Hamming del código*. Lo que interesa entonces es hallar códigos de distancia de Hamming máxima en forma uniforme (nos interesa que a cada código correcto le corresponda un número similar de palabras erróneas) y por el otro lado hallar formas eficientes de determinar si la palabra es correcta (solo detectar errores) o la más cercana a la recibida (para corregirlos). Para detectar  $d$  errores se requiere que la distancia de Hamming del código sea mayor a  $d + 1$  (así la palabra errada nunca coincide con una correcta, está al menos a un bit de distancia), para corregir  $d$  errores la distancia debe ser  $2d + 1$  (la palabra errada estará a distancia a lo más  $d$  de la correcta, la siguiente más cercana estará a la distancia al menos  $d + 1$ ).

### 10.4.1. Códigos de Hamming

Hamming [162] halló una manera de construir códigos de detección y corrección de errores de distancia 3 (capaces de detectar 2 errores y corregir 1). Suponiendo  $n = 2^w$  y contando los bits de 1 a  $2^w$ , se usan los bits en las posiciones  $k = 1, 2, \dots, 2^{w-1}$  como bits de paridad y los demás como bits de datos. La idea es calcular el bit en la posición  $2^k$  de forma que los bits en las posiciones escritas en binario que tienen 1 en la posición  $k$  tengan un número par de unos, como muestra el cuadro 10.1. Para determinar el bit errado, lo que se hace es calcular los bits de paridad correspondientes a los

Paridad	Posiciones
$0 2^0 = 1$	1, 3, 5, 7, 9, 11, 13, 15
$1 2^1 = 2$	2, 3, 6, 7, 10, 11, 14, 15
$2 2^2 = 4$	4, 5, 6, 7, 12, 13, 14, 15
$3 2^3 = 8$	8, 9, 10, 11, 12, 13, 14, 15

Cuadro 10.1 – Paridades para el código de Hamming (15,4)

datos recibidos, si son iguales a lo calculado, no se detectan errores; en caso de haber diferencias considerar los bits de paridad como un número binario da el bit errado. Por ejemplo, si  $w = 15$ , el código tendrá 4 bits de paridad (posiciones 1, 2, 4 y 8) y 11 bits de mensaje (en las posiciones 3, 5 a 7 y 9 a 15). Se recibe 0x6A6A, en binario 0110101001101010, revisamos los bits respectivos, lo que da 3 para 0, 6 para 1, 6 para 2 y 4 para 3. Esto corresponde a 0001, que significa que hay un error en la posición 1. El código correcto es 0110101001101011 o 0x6A6B, y los bits de mensaje son 11010101100, o 0x6AC. El código de Hamming es óptimo, en el sentido que tiene la máxima distancia de Hamming para el número de bits dado.

### 10.4.2. Verificación de redundancia cíclica

Una manera de construir códigos de detección de errores simples de analizar matemáticamente fue descubierta por Peterson [281]. La técnica tiene además la ventaja de poder implementarse en

circuitos sencillos y rápidos, como veremos luego. Se les llama *verificación de redundancia cíclica* (en inglés, *Cyclic Redundancy Check*, o CRC) dado que se agregan bits de verificación (*check* en inglés) que son redundantes (no aportan información) según un código cíclico.

Consideremos un mensaje binario de  $m$  bits,  $M = M_{m-1}M_{m-2}\dots M_0$ . Podemos considerarlo como un polinomio sobre  $\mathbb{Z}_2$ :

$$M(x) = M_{m-1}x^{m-1} + M_{m-2}x^{m-2} + \dots + M_1x + M_0$$

Sea además un polinomio  $G(x)$  de grado  $n - 1$ . Si calculamos:

$$r(x) = M(x)x^n \bmod G(x)$$

$$T(x) = M(x)x^n - r(x)$$

Es claro que  $T(x)$  es divisible por  $G(x)$ . La estrategia es entonces tomar el mensaje, añadirle  $n - 1$  bits cero al final, calcular el resto de esto al dividir por  $G(x)$  (un polinomio de grado  $n - 1$ ) y substituir los ceros añadidos por el resto (en  $\mathbb{Z}_2[x]$  suma y resta son la misma operación). A estos bits agregados los llamaremos *bits de paridad*. El resultado es el polinomio  $T(x)$ , que se transmite. Al recibirlo, se calcula el resto de la división con  $G(x)$ ; si el resto es cero, el dato recibido es correcto. Al polinomio  $G(x)$  se le llama *generador* del código. Esto es similar a la prueba de los nueves que discutimos en el capítulo 8.

Si se transmite  $T$  y se recibe  $R$ , el error (las posiciones de bit erradas) es simplemente la diferencia entre los polinomios respectivos:

$$E(x) = T(x) - R(x)$$

Para que nuestra técnica detecte el error, debe ser que  $G(x)$  no divida a  $E(x)$ . Nos interesa entonces estudiar bajo qué condiciones  $G(x)$  divide a  $E(x)$  en  $\mathbb{Z}_2[x]$ , de manera de obtener criterios que den buenos polinomios generadores (capaces de detectar clases de errores de interés).

Claramente no todo  $G(x)$  sirve, usaremos la teoría desarrollada antes para poner algunas condiciones. De partida, el término constante de  $G(x)$  no debe ser cero, de otra forma se desperdician bits de paridad:

$$(x^n M(x)) \bmod (x^k p(x)) = x^{n-k} (M(x) \bmod p(x))$$

Si consideramos cómo se multiplican polinomios en  $\mathbb{Z}_2[x]$ , vemos que si  $G(x)$  tiene un número par de coeficientes uno lo mismo ocurrirá con el producto  $p(x)G(x)$ , con lo que si  $G(x)$  tiene un número par de coeficientes uno detectará todos los errores que cambian un número impar de bits.

Por otro lado, si  $G(x)$  es de grado  $n - 1$  no puede dividir a polinomios de grado menor. Vale decir, será capaz de detectar todos los errores que cambian bits en un rango contiguo de menos de  $n$  bits.

Una *ráfaga* es un bloque de bits cambiados, con lo que  $E = 00\dots 011\dots 110\dots 0$ . Si se cambian  $r$  bits, esto significa que para algún  $k$ :

$$\begin{aligned} E(x) &= (x^{r-1} + x^{r-2} + \dots + 1)x^k \\ &= \frac{(x^r - 1)x^k}{x - 1} \end{aligned}$$

Esto es divisible por  $G(x)$  si lo es  $x^r - 1$ . De la teoría precedente sobre campos finitos sabemos que si  $G(x)$  es el polinomio mínimo de un generador de  $\mathbb{F}_{2^n}$  (lo que llaman un *polinomio primitivo*) dividirá a  $x^r - 1$  solo si  $r \geq 2^n - 1$ . Lamentablemente en  $\mathbb{Z}_2[x]$  el polinomio  $x + 1$  es primitivo y divide a todos los polinomios con un número par de términos (porque  $x - 1$  siempre divide a  $x^k - 1$ ).

Analicemos ahora cómo armar circuitos que calculen el resto de la división de polinomios en  $\mathbb{Z}_2[x]$ . Requeriremos memorias de un bit, que al pulso de una línea de reloj (que no se muestra)

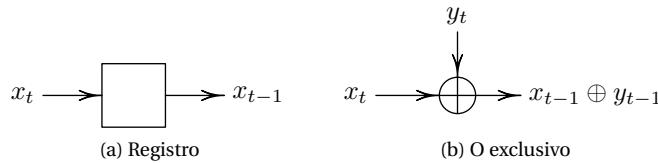


Figura 10.1 – Elementos de circuitos lógicos

aceptan un nuevo bit y entregan el anterior. La suma en  $\mathbb{Z}_2$  es la operación lógica *o exclusivo*, comúnmente anotada  $\oplus$ . Los elementos de circuito que emplearemos se ilustran en la figura 10.1. El amable lector verificará (por ejemplo dividiendo  $x^8 + x^5 + x^4 + x^2 + 1$  por  $x^4 + x + 1$ ) que el proceso para obtener el resto puede describirse de la siguiente forma: Si el primer bit del dividendo actual es 1, sume los términos de menor exponente a partir del segundo término del dividendo; en caso que el primer bit del dividendo sea 0, no haga nada. Luego descarte el primer bit del dividendo. Esto es lo mismo que sumar el primer bit del dividendo actual en ciertas posiciones, y luego correr todo en una posición. En términos de nuestros elementos, para el polinomio primitivo  $x^8 + x^4 + x^3 + x^2 + 1$  resulta el circuito de la figura 10.2. La operación es la siguiente: Inicialmente se cargan ceros en

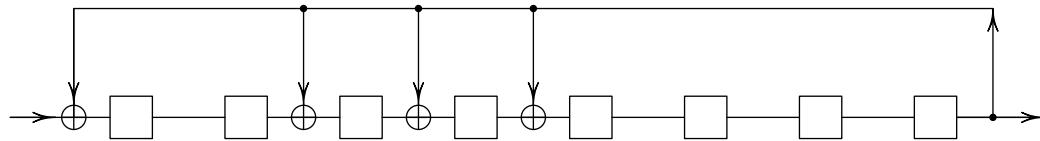


Figura 10.2 – Circuito para  $x^8 + x^4 + x^3 + x^2 + 1$

los registros, luego se van ingresando los bits del dividendo (partiendo por el más significativo) al circuito. El resto queda en los registros. Es claro que interesan polinomios primitivos con el mínimo número de términos (ya que esto minimiza la circuitería requerida).

Otro uso interesante resulta de inicializar los registros con un valor diferente de cero, y luego alimentar el circuito con una corriente de ceros (lo que puede lograrse simplemente obviando la primera operación a la izquierda en la figura) Como hay un número finito de posibilidades para los valores de los registros, en algún momento se repetirán. Si el valor inicial es  $p(x)$ , lo que estamos haciendo es calcular sucesivamente  $x^k p(x) \bmod G(x)$ . Si  $G(x)$  es primitivo, la repetición ocurrirá cuando  $k = 2^n$ , por lo que los valores en los registros habrán recorrido todas las combinaciones de  $n$  bits (salvo solo ceros). El resultado es un contador simple (si solo interesa obtener valores diferentes, no necesariamente en orden), y la salida del circuito (que en nuestra aplicación anterior descartamos) es una corriente de números aleatorios si se toman de a  $n$  bits. Si  $G(x)$  no es primitivo, la teoría precedente indica que habrá un  $k$  menor a  $n$  que hace que  $x^k p(x) \equiv p(x) \pmod{G(x)}$ , y nuevamente hay ciclos. El lector interesado determinará los posibles ciclos para algún polinomio no primitivo, como  $(x^4 + x + 1)(x + 1) = x^5 + x^4 + x^2 + 1$ .

# 11 Algoritmos aritméticos

---

Hay aplicaciones en las cuales se requieren cálculos con números de muchos miles de bits de largo. Tales algoritmos son particularmente relevantes en las técnicas criptográficas modernas, basadas en teoría de números y áreas afines. Algunos de los algoritmos que discutiremos son relevantes incluso para números pequeños. También ofrecen ejemplos de técnicas de análisis de algoritmos que tienen interés independiente.

## 11.1. Referencias detalladas

Esta es un área muy amplia, desarrollada explosivamente desde la aparición de criptografía basada en teoría de números. En este reducido espacio es imposible hacerle justicia. Una discusión exhaustiva de algoritmos aritméticos y afines, con análisis muy detallado de su rendimiento, es de Knuth [217]. Detalles sobre algoritmos numéricos adicionales, incluyendo resultados recientes en el área y con énfasis en algoritmos aplicables para criptología, dan Brent y Zimmermann [54]. Una discusión de algoritmos en C++ da Arndt [19]. Una implementación libre de algoritmos aritméticos de buen rendimiento es la biblioteca GMP [151]. Hay varias otras opciones, como NTL [324], que ofrece una interfaz más cómoda de usar, y CLN [157] para uso desde C++. Para cómputo en otras estructuras algebraicas (por ejemplo, grupos elípticos o campos finitos) se recomienda GAP [139].

## 11.2. Máximo común divisor

Para el máximo común divisor (que ya discutimos en la sección 7.3), notar que para  $q$  arbitrario debe ser:

$$\gcd(a, b) = \gcd(b, a - qb)$$

Esto porque cualquier divisor común de  $b$  y  $a - qb$  necesariamente divide a  $a$  también. Interesa disminuir lo más posible los valores en cada iteración, cosa que se logra si elegimos  $q = \lfloor a/b \rfloor$ . Como los valores son enteros no negativos y disminuyen en cada paso, el proceso no puede continuar indefinidamente. Esta observación lleva al algoritmo de Euclides, algoritmo 11.1, para calcular el máximo común divisor. Es interesante considerar el número de iteraciones del algoritmo. Sean  $r_i$  los restos en cada paso del algoritmo, con el entendido que  $r_0 = a$  y  $r_1 = b$ , y que  $a > b$  (en caso contrario, lo único que hace la primera iteración es intercambiarlos). Estamos calculando:

$$r_{i+2} = r_i \bmod r_{i+1}$$

O sea, para una secuencia de  $q_i$  tenemos las relaciones:

$$r_{i+2} = r_i - q_i r_{i+1}$$

---

Algoritmo 11.1: Algoritmo de Euclides para calcular  $\gcd(a, b)$

---

```

function gcd( $a, b$ )
  while  $b > 0$  do
     $(a, b) \leftarrow (b, a \text{ mód } b)$ 
  end
  return  $a$ 

```

---

donde  $r_k \neq 0$  y  $r_{k+1} = 0$  si hay  $k$  iteraciones. El peor caso se da cuando  $q_i = 1$  siempre, ya que en tal caso los  $r_i$  disminuyen lo más lentamente posible. Además, el caso en que  $\gcd(a, b) = 1$  es el en el cual más terreno se debe recorrer. Podemos dar vuelta esto, y preguntarnos qué tan lejos del final estamos, y calcular desde allí:

$$F_{k+2} = F_{k+1} + F_k \quad F_0 = 0, F_1 = 1 \quad (11.1)$$

Esto define la famosa secuencia de Fibonacci:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \dots$$

El resultado es entonces que si el algoritmo efectúa  $k$  iteraciones entonces  $b \geq F_k$ . Esto fue demostrado por Lamé en 1844 [231], lo que inauguró el área de análisis de algoritmos. Fue también el primer uso serio de los números de Fibonacci.

Para completar el análisis interesa saber cómo crece  $F_k$ . Más adelante (capítulo 19) veremos cómo tratar esta clase de situaciones, por ahora nos contentamos con una cota. Si calculamos las razones  $F_{k+1}/F_k$ , vemos que parecen converger a una constante cerca de 1,6. Llamemos:

$$\tau = \lim_{k \rightarrow \infty} \frac{F_{k+1}}{F_k}$$

Podemos expresar:

$$\begin{aligned} \frac{F_{k+2}}{F_k} &= \frac{F_{k+1}}{F_k} + 1 \\ \frac{F_{k+2}}{F_{k+1}} \cdot \frac{F_{k+1}}{F_k} &= \frac{F_{k+1}}{F_k} + 1 \end{aligned}$$

Si ahora hacemos  $k \rightarrow \infty$ , queda:

$$\tau^2 = \tau + 1 \quad (11.2)$$

La ecuación (11.2) tiene dos raíces, interesa la positiva (de mayor magnitud):

$$\tau = \frac{1 + \sqrt{5}}{2} \approx 1,618$$

Se cumplen las siguientes relaciones para  $k \geq 1$ :

$$\tau^{k-2} \leq F_k \leq \tau^{k-1} \quad (11.3)$$

Requerimos dos valores de partida, dado que a la recurrencia (11.1) entran dos valores. Estas se demuestran por inducción.

**Base:** Cuando  $k = 1$  y  $k = 2$  tenemos:

$$\begin{aligned}\tau^{-1} &\leq F_1 \leq 1 \\ 1 &\leq F_2 \leq \tau\end{aligned}$$

Ambas son ciertas.

**Inducción:** Suponiendo que la aseveración es cierta hasta  $k + 1$ , planteamos las cotas (11.3) para  $k$  y  $k + 1$ :

$$\begin{aligned}\tau^{k-2} &\leq F_k \leq \tau^{k-1} \\ \tau^{k-1} &\leq F_{k+1} \leq \tau^k\end{aligned}$$

Sumando las relaciones resultantes, y viendo de la ecuación (11.2) que  $\tau^2 = 1 + \tau$ :

$$\begin{aligned}\tau^{k-2} + \tau^{k-1} &\leq F_k + F_{k+1} \leq \tau^{k-1} + \tau^k \\ \tau^{k-2}(1 + \tau) &\leq F_{k+2} \leq \tau^{k-1}(1 + \tau) \\ \tau^k &\leq F_{k+2} \leq \tau^{k+1}\end{aligned}$$

que es el caso siguiente.

Con estas estimaciones de  $F_k$ , tenemos que si el algoritmo da a lo más  $k$  iteraciones:

$$\begin{aligned}b &\geq F_k \\ &\geq \tau^{k-2} \\ k &\leq \frac{\log b}{\log \tau} + 2\end{aligned}$$

O sea,  $k = O(\log b)$ .

Puede analizarse el comportamiento promedio del algoritmo, pero eso lleva a profundidades que escapan de este ramo. El detalle se encuentra en el texto de Knuth [217].

Un algoritmo alternativo (máximo común divisor binario) se obtiene de aplicar repetidas veces las siguientes observaciones:

1.  $\gcd(a, b) = \gcd(b, a)$  nos permite reordenar a gusto.
2.  $\gcd(a, 0) = a$  da el resultado final.
3.  $\gcd(a, b) = 2 \gcd(a/2, b/2)$  cuando  $a$  y  $b$  son pares.
4.  $\gcd(a, b) = \gcd(a/2, b)$  cuando  $a$  es par y  $b$  impar.
5.  $\gcd(a, b) = \gcd(b, (a - b)/2)$  cuando  $a$  y  $b$  son impares (en tal caso,  $a - b$  es par).

En máquinas en las cuales la división es lenta este algoritmo puede ser más eficiente si se programa con cuidado aprovechando operaciones con bits.

Nuestra versión (11.2) primero extrae la máxima potencia de 2 que tienen en común  $a$  y  $b$ , de allí en adelante trabaja solo con números impares, asegurándose de mantener siempre  $a \geq b$ . Un ejemplo del algoritmo binario sería el cálculo de  $\gcd(40902, 24140)$ . Como  $40902 = 2 \cdot 20451$  y  $24140 = 4 \cdot 6035$ , la máxima potencia de 2 que tienen en común  $a$  y  $b$  es  $u = 2$ , y el algoritmo propiamente tal se inicia con  $a = 20451$ ,  $b = 6035$ . La traza respectiva se reseña en el cuadro 11.1. El resultado final es  $\gcd(40902, 24140) = 2 \cdot 17 = 34$ .

El análisis completo del algoritmo parece ser intratable, Knuth [217] analiza en detalle un modelo aproximado y da algunos resultados exactos.

---

Algoritmo 11.2: Máximo común divisor binario

---

```

function gcd(a, b)
  u  $\leftarrow$  1
  while ( $2 \mid a$ )  $\wedge$  ( $2 \mid b$ ) do
    (u, a, b)  $\leftarrow$  ( $2u$ , a/2, b/2)
  end
  while  $2 \mid a$  do
    a  $\leftarrow$  a/2
  end
  while  $2 \mid b$  do
    b  $\leftarrow$  b/2
  end
  if a  $<$  b then
    (a, b)  $\leftarrow$  (b, a)
  end
  loop
    t  $\leftarrow$  a  $-$  b
    if t = 0 then
      return a  $\cdot$  u
    end
    repeat
      t  $\leftarrow$  t/2
    until  $2 \nmid t$ 
    (a, b)  $\leftarrow$  (b, t)
  end

```

---

<i>a</i>	<i>b</i>	<i>t</i>
20451	6035	$20451 - 6035 = 16 \cdot 901$
6035	901	$6035 - 901 = 2 \cdot 2567$
2567	901	$2567 - 901 = 2 \cdot 833$
901	833	$901 - 833 = 4 \cdot 17$
833	17	$833 - 17 = 16 \cdot 51$
51	17	$51 - 17 = 2 \cdot 17$
17	17	$17 - 17 = 0$

Cuadro 11.1 – Traza del algoritmo binario para máximo común divisor

### 11.3. Potencias

Otra operación importante es calcular potencias. Un algoritmo eficiente para calcular potencias es el 11.3. Es fácil ver que con este algoritmo el cálculo de  $a^n$  toma  $O(\log n)$  multiplicaciones. En

---

Algoritmo 11.3: Cálculo binario de potencias

---

```
function pow( $a, n$ )
     $r \leftarrow 1$ 
    while  $n \neq 0$  do
        if  $2 \nmid n$  then
             $r \leftarrow r \cdot a$ 
        end
         $a \leftarrow a^2$ 
         $n \leftarrow \lfloor n/2 \rfloor$ 
    end
    return  $r$ 
```

---

todo caso, el algoritmo 11.3 no es lo mejor que se puede hacer, un tratamiento detallado de este espinudo tema da Knuth [217].

<b><i>n</i></b>	<b><i>a</i></b>	<b><i>r</i></b>
10	3	1
5	9	9
9	81	9
1	6561	59049

Cuadro 11.2 – Cálculo de  $3^{10}$  por el método binario

Un ejemplo del método binario da el cálculo de  $3^{10}$  en el cuadro 11.2.

### 11.4. Factorizar

Una técnica básica para factorizar es la que hemos aprendido en el colegio: Para factorizar  $N$ , intentamos los primos entre 2 y  $\lfloor \sqrt{N} \rfloor$ . Si ninguno divide a  $N$ , entonces  $N$  es primo. Si  $N$  es grande, esto definitivamente no es viable, pero sirve muy bien para eliminar factores primos chicos de algún número.

Una alternativa que sirve bien cuando  $N$  tiene factores grandes es debida esencialmente a Fermat. Supongamos  $N = UV$ , donde podemos suponer que  $N$  es impar (y por tanto lo son  $U$  y  $V$ ). Entonces, definiendo  $X$  e  $Y$  como sigue:

$$X = (U + V)/2$$

$$Y = (U - V)/2$$

$$N = X^2 - Y^2$$

La idea entonces es buscar sistemáticamente valores de  $X$  e  $Y$  según lo anterior. Aprovechando que la suma de los primeros  $n$  números impares cumple:

$$\sum_{0 \leq k \leq n} (2k + 1) = n^2$$

obtenemos el algoritmo 11.4, donde usamos las variables  $x$ ,  $y$  y  $r$  para designar lo que en la exposición anterior llamamos  $2X+1$ ,  $2Y+1$  y  $X^2 - Y^2 - N$ , respectivamente. Durante la ejecución tenemos  $|r| < x$  e  $y < x$ . Lo más curioso es que no usa multiplicación ni división para factorizar. El lector podrá entretenérse aplicando a mano este algoritmo a 377.

El método de Fermat en realidad era diferente, el algoritmo 11.4 es muy eficiente en computadores pero no es muy adecuado para cálculo manual. Fermat no mantenía el valor de  $y$ , miraba  $x^2 - N$  y descartaba no cuadrados viendo sus últimos dígitos (en base 10, deben ser 00,  $p_1$ ,  $p_4$ , 25,  $i_6$  o  $p_9$ , donde  $p$  es un dígito par e  $i$  uno impar); en caso de sospechar que fuera un cuadrado perfecto extraía una raíz. Esta misma idea puede extenderse a otras bases, como muestra Knuth [217]. Tomemos por ejemplo  $N = 8616460799$ , y consideremos el cuadro 11.3. Si  $x^2 - N$  es un cuadrado perfecto  $y^2$ , entonces debe tener un residuo módulo  $m$  consistente con esto, para todo  $m$ . Por ejemplo, con  $N = 8616460799$  y  $x \bmod 3 \neq 0$ , entonces  $(x^2 - N) \bmod 3 = 2$ , y esto no puede ser un cuadrado perfecto, de forma que  $x$  debe ser un múltiplo de 3 para que  $N = x^2 - y^2$ . Nuestro cuadro dice que:

$$\begin{aligned} x \bmod 3 &= 0 \\ x \bmod 5 &= 0, 2 \text{ ó } 3 \\ x \bmod 7 &= 2, 3, 4 \text{ ó } 5 \\ x \bmod 8 &= 0 \text{ ó } 4 \text{ (o sea, } x \bmod 4 = 0) \\ x \bmod 11 &= 0, 2, 4, 7, 9 \text{ ó } 10 \end{aligned}$$

$m$	Si $x \bmod m$ es	$x^2 \bmod m$ es	$(x^2 - N) \bmod m$ es
3	0, 1, 2	0, 1, 1	1, 2, 2
5	0, 1, 2, 3, 4	0, 1, 4, 4, 1	1, 2, 0, 0, 2
7	0, 1, 2, 3, 4, 5, 6	0, 1, 4, 2, 2, 4, 1	5, 6, 2, 0, 0, 2, 6
8	0, 1, 2, 3, 4, 5, 6, 7	0, 1, 4, 1, 0, 1, 4, 1	1, 2, 5, 2, 1, 5, 2
11	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10	0, 1, 4, 9, 5, 3, 3, 5, 9, 4, 1	10, 0, 3, 8, 4, 2, 2, 4, 8, 3, 0

Cuadro 11.3 – Condiciones a  $x$  e  $y$  al factorizar 8616460799

Esto reduce la búsqueda en forma considerable. Por ejemplo, vemos que  $x$  debe ser múltiplo de 12. Debe ser  $x \geq \lceil \sqrt{N} \rceil = 92825$ , y el menor múltiplo de 12 que cumple es 92832. Pero este valor tiene residuos (2, 5, 3) módulos (5, 7, 11), y falla nuestra condición respecto del módulo 11. Incrementar  $x$  en 12 aumenta los residuos módulo 5 en 2, módulo 7 en 5 y módulo 11 en 1. El primer  $x$  que cumple todas las condiciones es 92880, y  $92880^2 - N = 10233601$ , que resulta ser el cuadrado de 3199. Hemos encontrado la solución  $x = 92880$  e  $y = 3199$ , que entrega la factorización:

$$8616460799 = (x - y)(x + y) = 89681 \cdot 96079$$

La importancia del número de marras es que el economista y lógico W. S. Jevons lo mencionó en un conocido libro en 1874 [185], diciendo que a pesar que es muy fácil multiplicar dos números, probablemente nunca nadie salvo él mismo conocería sus factores. Sin embargo, acabamos de demostrar que Fermat podría haberlo factorizado en unos minutos. El punto central de que factorizar es difícil es correcto, siempre que los factores no sean tan cercanos.

Un algoritmo curioso es rho de Pollard [287], que tiende a ser útil para factores más bien pequeños. La idea básica viene de lo que se conoce como *la paradoja del cumpleaños* (*birthday paradox* en inglés): En el año hay 365 días, si tomamos una persona la probabilidad que el cumpleaños de una segunda no coincida con la primera es  $1 - 1/365$ , para que el de una tercera no coincida con ninguno de los dos anteriores es  $1 - 2/365$ , y así sucesivamente. La probabilidad que en un grupo de  $n$  personas no hayan cumpleaños repetidos es:

$$P(n) = \prod_{1 \leq k \leq n-1} \left(1 - \frac{k}{365}\right)$$

Resulta que para  $n = 24$  la probabilidad de que hayan dos (o más) personas con el mismo cumpleaños ya es mayor a  $1/2$ , cuando intuitivamente uno pensaría que se requieren muchas más. Una manera alternativa de analizar aproximadamente el problema es considerar que hay  $n(n+1)/2$  pares de personas, basta que uno de los pares coincida, con lo que debiera ser suficiente que  $n(n+1)/2 \approx 365$  para que se produzca una coincidencia. Esto se traduce en  $n \approx \sqrt{2 \cdot 365} = 27$ . Acá lo que se busca es generar rápidamente una gran colección de pares módulo  $N$  y buscar coincidencias módulo un primo que divide a  $N$ . Un razonamiento como el anterior lleva a pensar que si  $p_1$  es el menor primo que divide a  $N$  con  $O(p_1^{1/\rho})$  pares hallaremos una coincidencia, que lleva a determinar  $p_1$ .

El nombre  $\rho$  viene de considerar una secuencia eventualmente periódica en la cual hay  $\mu$  elementos antes del primero que se repite (la cola de la letra  $\rho$ ), y luego un ciclo de largo  $\lambda$  (la cabeza de  $\rho$ ). Vale decir, sea  $f: \mathbb{N} \rightarrow \{0, 1, \dots, m-1\}$  una función, y consideremos la secuencia definida por  $x_{i+1} = f(x_i)$ . Entonces hay  $\mu$  y  $\lambda$  tales que  $x_0, x_1, \dots, x_\mu, \dots, x_{\mu+\lambda-1}$  son todos diferentes, pero  $x_\mu = x_{\mu+\lambda}$ . Estas relaciones definen  $\mu$  y  $\lambda$ . Tenemos  $0 \leq \mu < m$ ,  $0 < \lambda \leq m$  y  $\mu + \lambda \leq m$ . Así,  $x_j = x_k$  con  $j > k$  si y solo si  $j - k$  es múltiplo de  $\lambda$  y  $k \geq \mu$ ; con esto  $x_{2k} = x_k$  si y solo si  $k$  es múltiplo de  $\lambda$  y  $k \geq \mu$ . Vale decir, hay un  $k > 0$  con  $\mu \leq k \leq \mu + \lambda$  tal que  $x_k = x_{2k}$ , lo que lleva al algoritmo de Floyd [132] (ver 11.5) para detectar ciclos.

---

#### Algoritmo 11.5: Detectar ciclos (Floyd)

---

```

 $x \leftarrow x_0;$ 
 $y \leftarrow x_0;$ 
repeat
   $x \leftarrow f(x);$ 
   $y \leftarrow f(f(y));$ 
until  $x = y;$ 

```

---

Sea ahora  $f(x)$  un polinomio con coeficientes enteros,  $p$  un factor primo de  $N$ , y consideremos las secuencias definidas con un inicio  $A$  arbitrario:

$$\begin{aligned}x_0 &= y_0 = A \\x_{m+1} &= f(x_m) \text{ mód } N \\y_{m+1} &= f(y_m) \text{ mód } p\end{aligned}$$

Por el teorema chino de los residuos  $y_m \equiv x_m \pmod{p}$ . La secuencia  $y_m$  debe repetirse con un período a lo más  $p$ , digamos  $y_{k+\lambda} = y_k$ . Entonces  $x_{k+\lambda} \equiv x_k \pmod{p}$ , y  $\gcd(N, x_{k+\lambda} - x_k)$  da un factor de  $N$ . Funciones de la forma  $f(x) = (\alpha x + \beta) \pmod{N}$  no sirven, ya que con ellas  $x_{k+\lambda} \equiv x_k \pmod{p}$  exactamente cuando  $x_{k+\lambda} \equiv x_k \pmod{N}$ . Se usa lo siguiente más simple,  $f(x) = (x^2 + 1) \pmod{N}$ ; y si esto no tiene éxito, se intenta  $f(x) = (x^2 + c) \pmod{N}$  con  $c \neq 0$  y  $c \neq -2$  (porque estos caen en un ciclo de unos al toparse con  $x \equiv \pm 1 \pmod{N}$ ). Todo esto lleva al algoritmo 11.6. Brent [53] da una

---

Algoritmo 11.6:  $\rho$  de Pollard

---

```
function factor( $N$ )
    Elegir  $A$  al azar
     $x \leftarrow A$ 
     $y \leftarrow A$ 
    repeat
         $x \leftarrow f(x)$ 
         $y \leftarrow f(f(y))$ 
         $d \leftarrow \gcd(|x - y|, N)$ 
    until  $d \neq 1$ 
    if  $d = N$  then
        return Falló
    else
        return  $d | N$ 
    end
```

---

variante usando un algoritmo de detección de ciclos más rápido.

El método descrito, con  $f(x) = x^2 + 1$  y  $x_0 = 42$ , factoriza  $16843\,009 = 257 \cdot 65\,537$  como muestra el cuadro 11.4.

Otra técnica es el método  $p - 1$  de Pollard [286]. Recordemos el teorema de Fermat para  $p$  primo y  $p \nmid a$ :

$$a^{p-1} \equiv 1 \pmod{p}$$

Podemos elevar esta congruencia a una potencia cualquiera  $k$ :

$$a^{k(p-1)} \equiv 1 \pmod{p}$$

Vale decir,  $p \mid a^{k(p-1)} - 1$ . Consideremos ahora el entero  $N$  a factorizar y  $p$  un factor primo (desconocido) de  $N$  y un valor  $M$  a determinar. Si  $p - 1 \mid M$  tenemos:

$$p \mid (a^M \pmod{N} - 1)$$

y  $\gcd(a^M \pmod{N} - 1, N)$  dará un factor no trivial de  $N$ . La idea es elegir  $a$  pequeño y hacer  $M$  el producto de muchos primos (ojalá más bien chicos). Si los factores de  $p - 1$  están en este conjunto, tendremos éxito.

<b><i>i</i></b>	<b><i>x<sub>i</sub></i></b>	<b><i>x<sub>2i</sub></i></b>	<b>gcd</b>
0	42		
1	1765	3115226	1
2	3115226	4805758	1
3	11262448	4817235	1
4	4805758	9598062	1
5	7583675	11476471	1
6	4817235	2534841	1
7	11064323	443204	1
8	9598062	6015649	1
9	6959372	6454177	1
10	11476471	15725109	1
11	3760417	9439232	1
12	2534841	574959	247

Cuadro 11.4 – Ejemplo de Pollard  $\rho$ 

Otra colección de métodos, más apropiados para computación distribuida y números grandes, se deben a una idea de Maurice Kraitchik en los 1920s. Supongamos que podemos encontrar la congruencia:

$$a^2 \equiv b^2 \pmod{N} \quad a \not\equiv \pm b \pmod{N}$$

Entonces  $N \mid (a^2 - b^2)$ , pero  $a^2 - b^2 = (a+b)(a-b)$ , y ninguno de estos dos factores es divisible por  $N$ , por lo que si  $N = pq$ , entonces  $p$  divide a uno de los factores y  $q$  al otro, y  $\gcd(a+b, N)$  y  $\gcd(a-b, N)$  son factores no triviales de  $N$ . La manera de obtener esta ecuación es construir una *gran* colección de relaciones de la forma  $a^2 \equiv q \pmod{N}$  en las cuales  $q$  es pequeño, e intentar factorizar tales  $q$ , en particular en términos de primos chicos. Para la mayoría de los  $q$  esto no funcionará, pero bastan unos pocos que se puedan factorizar completamente. Si consideramos la expresión  $a^2 \equiv q \pmod{N}$ , el lado izquierdo ya es un cuadrado, y lo hemos factorizado. Buscamos otros  $q$  factorizados que completen las potencias de los primos factores de  $q$  a pares, o sea, tenemos:

$$\begin{aligned} a_1^2 &\equiv q_1 & (\text{mód } N) \\ a_2^2 &\equiv q_2 & (\text{mód } N) \\ &\vdots \\ a_n^2 &\equiv q_n & (\text{mód } N) \\ (a_1 a_2 \dots a_n)^2 &\equiv q_1 q_2 \dots q_n & (\text{mód } N) \end{aligned}$$

donde conocemos  $b^2 = q_1 q_2 \dots q_n$ , y esto entrega una factorización de  $N$  por lo anterior, claro que la factorización puede ser trivial. La búsqueda de los  $q$  y su factorización en términos de un conjunto de primos predefinidos puede distribuirse; para factorizar luego planteamos un sistema de ecuaciones lineales módulo 2 buscando una combinación de  $q$  que sea un cuadrado. Hay varias variantes de esta idea general, que difieren en la estrategia usada para buscar cuadrados pequeños (y ojalá fácilmente factorizables) para combinar. No entraremos en ese detalle acá, Pommerance [292] describe la historia con múltiples referencias.

### 11.5. Factorización con curvas elípticas

Un método reciente es la factorización por curvas elípticas de Lenstra [238], basado en grupos de curvas elípticas (ver la sección 7.5.1). Es un método cuyo tiempo de ejecución depende del factor primo más chico, por lo que se usa para eliminar factores pequeños para luego ir a un método general con los factores remanentes. Primero, si se cumple:

$$y^2 \equiv x^3 + ax + b \pmod{n} \quad (11.4)$$

por el (padre del) teorema chino de los residuos (corolario 8.6) también se cumple para los factores primos de  $n$ . En el fondo, estamos efectuando cálculos simultáneos en los grupos elípticos para los factores primos de  $n$ , y en alguno de ellos atinaremos al orden de  $P$  y obtenemos un factor de  $n$ . Por el teorema de Hasse [165–167] el orden del grupo sobre  $\mathbb{Z}_p$  está entre  $p+1-2\sqrt{p}$  y  $p+1+2\sqrt{p}$ , no depende directamente de  $p$ . En este sentido, este método es un refinamiento de método  $p-1$ , que busca detectar el orden de un elemento en  $\mathbb{Z}_p^\times$  (pero allí el orden del grupo es  $p-1$ , y el método solo funciona si  $p-1$  tiene factores chicos).

Calcularemos múltiplos  $kP$  para diversos valores de  $k$  para un punto  $P$  de la curva usando la suma del grupo de la curva elíptica, ecuaciones (7.19) y (7.20). Para valores grandes de  $k$  se puede usar un algoritmo afín al para calcular potencias, algoritmo 11.3, pero como en estos grupos calcular restas es tan rápido como sumar se pueden usar variantes que las incluyen (por ejemplo, calcular  $15P = 2(2(2P)) - P$  son 5 sumas/restas, calcular  $15P = P + 2P + 2(2P) + 2(2(2P))$  considera 6).

Las fórmulas de suma en el grupo involucran la “pendiente”  $s$ , que requiere un inverso multiplicativo módulo  $n$ . Si  $s = u/v$ , con  $v \equiv 0 \pmod{n}$ , el punto resultante es el punto en el infinito, el elemento neutro del grupo. Si es  $\gcd(v, n) \neq 1$  y  $\gcd(v, n) \neq n$ , no se obtiene un punto válido en la curva, pero sí un factor no trivial de  $n$ .

El algoritmo contempla los siguientes pasos:

1. Elija una curva elíptica sobre  $\mathbb{Z}_n$ , de la forma 11.4 y un punto al azar  $P$  sobre ella. Una posibilidad es elegir  $P = (x, y)$  con coordenadas al azar diferentes de cero módulo  $n$ , luego tomar un valor  $a \not\equiv 0 \pmod{n}$  y calcular:

$$b = (y^2 - x^3 - ax) \pmod{n}$$

2. Calcule  $mP$  para  $m$  un producto de muchos factores chicos, por ejemplo el producto de los primeros primos elevados a potencias chicas o  $B!$  para un  $B$  pequeño. Si en el proceso halla un factor de  $n$ , deténgase. Si no halla factores o llega al punto en el infinito, intente con otra curva.

Hay maneras de acelerar los cálculos usando curvas especiales o mediante descripciones alternativas de los puntos o las curvas, ver discusiones de implementación de Bernstein, Birkner, Lange y Peters [42]. Métodos relacionados usan grupos de curvas hiperelípticas, basadas en curvas de la forma  $y^2 = f(x)$  para polinomios  $f(x)$  de grado mayor a 4, ver Cosset [83].

### 11.6. Determinar primalidad

Para determinar si un número es primo, el teorema de Fermat es una herramienta poderosa. Por ejemplo, para  $2^{32} + 1 = 4294967297$  mediante 32 elevaciones al cuadrado módulo  $2^{32} + 1$  obtenemos que:

$$3^{2^{32}} \equiv 3029026160 \pmod{2^{32} + 1}$$

lo que dice que  $2^{32} + 1$  no es primo. Claro que no da ninguna luz sobre sus factores. En general, para  $N$  compuesto es posible hallar  $a$  con  $0 < a < N$  tal que  $a^{N-1} \not\equiv 1$  (mód  $N$ ), y la experiencia muestra que tales  $a$  se hallan rápidamente. Hay casos raros en los cuales frecuentemente se da  $a^{N-1} \equiv 1$  (mód  $N$ ), pero entonces  $N$  tiene un factor menor que  $\sqrt[3]{N}$ , como veremos más adelante. Para efectos prácticos basta considerar  $3^{N-1}$  mód  $N$ .

La forma clásica de demostrar que  $N$  es primo para  $N$  grande es hallar una raíz primitiva  $r$  de  $N$ . Por suerte, las raíces primitivas de números primos son bastante numerosas. De la discusión de grupos cíclicos de orden  $m$  sabemos que las potencias relativamente primas a  $m$  del generador del grupo también son generadores, con lo que hay  $\phi(p-1)$  raíces primitivas del primo  $p$ . Recientemente, Agrawal, Kayal y Saxena [3] describieron un algoritmo polinomial en el número de bits de  $n$  para determinar si es primo. La existencia de tal algoritmo se sospechaba hacía tiempo, pero el algoritmo en sí resultó sorprendente, su demostración requiere solo álgebra relativamente sencilla.

Consideremos  $p$  primo, con lo que hay una raíz primitiva módulo  $p$ , llamémosle  $r$ . Tomemos  $k$  tal que  $0 \leq k < p$ , sabemos que si  $\text{ord}_p(r^k) = n$  entonces  $kn$  es el mínimo común múltiplo de  $k$  y  $p-1$ , y será  $n = p-1$  exactamente cuando  $\gcd(k, p-1) = 1$ . Si  $x$  es raíz primitiva módulo  $N$ , para todo  $d$  que divide a  $N-1$  debe ser:

$$x^{(N-1)/d} \not\equiv 1 \pmod{N}$$

porque esto asegura que  $\text{ord}_N(x) = N-1$ . En todo caso, basta encontrar un  $x$  para cada primo  $p$  que divide a  $N-1$ , el producto de todos ellos será una raíz primitiva. Los cálculos involucrados (salvo posiblemente la factorización de  $N-1$ ) son simples de efectuar con los algoritmos discutidos antes. Esto lo discutiremos en conexión con el algoritmo Diffie-Hellman en la sección 12.3. El cuello de botella es factorizar  $N-1$ .

En la práctica, se usan métodos que no *garantizan* que el número es primo, pero que tienen alta probabilidad de detectar no-primos. El más usado actualmente es el test de Miller-Rabin [255, 295]. Monier [258] compara en detalle dos algoritmos similares, y concluye que el de Miller-Rabin es más eficiente en todos los casos.

El test de Miller-Rabin se basa en la observación que módulo un primo  $p$  solo 1 y  $-1$  pueden ser raíces cuadradas de 1 (el polinomio  $x^2 - 1$  puede tener a lo más dos ceros en el campo  $\mathbb{Z}_p$ , mientras por el teorema chino de los residuos en  $\mathbb{Z}_n$  con  $n$  compuesto hay un par diferente por cada factor primo de  $n$ ). Si  $p$  es un primo impar, podemos escribir  $p-1 = 2^s d$ , con  $d$  impar. Con esta notación, del teorema de Fermat para  $a \not\equiv 0$  (mód  $p$ ) tenemos que  $a^{2^s d} \equiv 1$  (mód  $p$ ). Por la observación anterior sobre raíces cuadradas en  $\mathbb{Z}_p$ , sacando raíz cuadrada sucesivamente partiendo de  $a^{p-1} = 1$  debemos llegar a que  $a^d = \pm 1$  o que alguno de los  $a^{2^r d} = -1$  para  $1 \leq r < s$ . El test de Miller-Rabin se basa en el contrapositivo de esto. Puede demostrarse que a lo más  $1/4$  de los valores  $a$  para un número compuesto “mienten”, con lo que repitiendo el proceso suficientes veces podemos tener gran confianza de que el número realmente es primo. El algoritmo 11.7 repite la prueba  $k$  veces.

## 11.7. Números de Carmichael

Queda la inquietud planteada antes sobre números para los cuales “falla” el teorema de Fermat, en el sentido que  $a^{n-1} \equiv 1$  (mód  $n$ ) se cumple con  $\gcd(a, n) = 1$ , pero  $n$  no es primo. A tal número se le llama *pseudoprimo* (de Fermat con base  $a$ ). El caso extremo lo dan los números de Carmichael [63], pseudoprimos de Fermat para todos los  $a$  relativamente primos a ellos.

**Teorema 11.1.** *Todo número de Carmichael  $n$  es libre de cuadrados, y para  $p$  primo, si  $p \mid n$  entonces  $p-1 \mid n-1$ .*

---

Algoritmo 11.7: Prueba de primalidad de Miller-Rabin

---

```

function is_prime( $N$ )
     $s \leftarrow 0$ 
     $d \leftarrow N - 1$ 
    while  $2 \mid d$  do
         $s \leftarrow s + 1$ 
         $d \leftarrow d/2$ 
    end
    for  $i \leftarrow 1$  to  $k$  do
        Elija  $a$  al azar en el rango  $[2, N - 2]$ 
         $x \leftarrow a^d \bmod N$ 
        if  $x = 1$  o  $x = N - 1$  then
            continue
        end
        for  $r \leftarrow 1$  to  $s - 1$  do
             $x \leftarrow x^2 \bmod N$ 
            if  $x = 1$  then
                return Compuesto
            else if  $x = N - 1$  then
                break
            end
        end
        if  $x \neq N - 1$  then
            return Compuesto
        end
    end
return Probablemente primo

```

---

*Demostración.* Consideremos un número de Carmichael  $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$  donde los  $p_i$  son primos distintos, y un  $a$  relativamente primo a  $n$ . Del padre del teorema chino de los residuos (corolario 8.6) sabemos que:

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_r^{k_r}}$$

con lo que  $a^{n-1} \equiv 1 \pmod{n}$  si y solo si  $a^{n-1} \equiv 1 \pmod{p_i^{k_i}}$  para todos los  $i$ . Esto a su vez para el primo  $p$  solo puede ser si  $\text{ord}_{p^k}(a) \mid n - 1$ . Sabemos por el teorema 9.24 que si  $p$  es un primo impar, hay raíces primitivas módulo  $p^k$  para todo  $k$ , vale decir, hay elementos de orden  $\phi(p) = p^{k-1}(p - 1)$ . (En realidad, basta con el teorema 9.21, ya que si un elemento es de orden  $p(p - 1)$  módulo  $p^2$ , tendrá que ser al menos de ese orden módulo  $p^k$ ; en particular,  $p$  divide a su orden.) Pero si  $p \mid n$ , entonces  $p$  no puede dividir a  $n - 1$ , y  $n$  no puede tener factores primos repetidos. Ahora, si  $n$  fuera par y  $p$  un primo impar que divide a  $n$ , tendríamos que  $p - 1 \mid n - 1$ , un número par dividiendo a uno impar, lo que es imposible.  $\square$

Esto fue demostrado por Korselt en 1899 [224], los números llevan el nombre de Carmichael por ser el primero de hallar uno.

Supongamos ahora que  $n = pq$ , con  $p$  y  $q$  primos tales que  $p < q$ . Entonces debe ser  $q - 1 \mid pq - 1$ , pero esto es  $q - 1 \mid p(q - 1) + (p - 1)$ , o sea  $q - 1 \mid p - 1$ , también imposible. En resumen, un número de Carmichael tiene al menos tres factores primos diferentes, todos impares.

Hay infinitos números de Carmichael, como demostraron Alford, Granville y Pollmerance [9], los primeros son:

$$561 = 3 \cdot 11 \cdot 17$$

$$1105 = 5 \cdot 13 \cdot 17$$

$$1729 = 7 \cdot 13 \cdot 19$$

El primero con cuatro factores primos es:

$$41041 = 7 \cdot 11 \cdot 13 \cdot 41$$



## 12 Criptología

---

Debe distinguirse entre *sistema criptográfico*, un conjunto de algoritmos diseñados para proteger secretos; la *criptografía*, el trabajo hecho para crear sistemas criptográficos; y finalmente *criptoanálisis*, trabajo hecho para burlar las protecciones de sistemas criptográficos. Se habla de *criptología* para referirse a la unión de criptografía y criptoanálisis. Es común que se confundan los términos *criptografía* y *criptología*, nos preocuparemos de usar los términos precisos.

La importancia práctica actual de la teoría de números está en sus aplicaciones a la criptografía, algunas de las cuales describiremos acá. Las técnicas mismas y los métodos que se han usado para romperlas hacen uso intensivo de conceptos de álgebra abstracta. Rutinariamente se hace necesario trabajar con enteros de cientos o miles de bits, o con elementos de grupos o campos finitos con números de elementos de similar envergadura.

### 12.1. Referencias adicionales

Esta es un área muy amplia, hay algunos detalles adicionales sobre la teoría (y mucho sobre las aplicaciones prácticas) en el clásico de Anderson [12]. Sinkov [325] describe métodos criptográficos elementales y cómo quebrarlos. Matt Curtin [85] discute signos de alerta sobre criptografía poco confiable. Bernstein, Lange y Schwabe [43] describen una biblioteca simple de usar para criptografía práctica, y discuten algunos de los ataques recientes basados en la operación de programas criptográficos.

Las aplicaciones de criptología suelen discutirse en términos de personajes *A* (también llamada Alice) y *B* (apodado Bob) que desean intercambiar mensajes. A veces aparecen otros actores, como *C* (alias Charlie) o *E* (Eve), quien desea interceptar el tráfico o intervenirlo de alguna forma (*eavesdrop*, en inglés), por ejemplo inyectando mensajes falsificados o modificando mensajes. Alice y Bob fueron presentados públicamente por Rivest, Shamir y Adleman [303], John Gordon [146] dio sus bibliografías definitivas. Schneier [314] presenta una larga lista de otros personajes que suelen aparecer.

No entraremos en más detalles en este amplio y complejo campo, nuestro interés es solo mostrar aplicaciones de la teoría de números vista hasta acá. Una referencia básica es el manual de Menezes y otros [253], el texto de Anderson [12] trata seguridad desde el punto de vista de ingeniería e incluye un capítulo accesible sobre el tema, mientras Schneier y coautores se concentran en aplicaciones prácticas [119, 314].

Debe tenerse cuidado, se suele confundir la criptografía con seguridad. La criptografía moderna es indispensable en muchas aplicaciones, pero es solo una entre la variedad de herramientas requeridas para la seguridad computacional.

## 12.2. Nomenclatura

Si solo el destinatario previsto puede extraer el significado del mensaje se habla de *confidencialidad*. La *integridad* del mensaje se refiere a que el receptor puede asegurarse que el mensaje no ha sido alterado, *autenticación* es que el receptor puede verificar la identidad de quien originó el mensaje, mientras *no repudiación* asegura que el origen no pueda negar que envió el mensaje.

Se habla de un mensaje en *texto claro* (en inglés *plaintext*) y su versión en *texto cifrado* (en inglés *ciphertext*). Para nuestros efectos, podemos considerar los textos como números grandes (por ejemplo, tomando el texto claro codificado en UTF-8), posiblemente dividido en *bloques* de tamaño cómodo. La transformación de texto claro a texto cifrado se lleva a cabo mediante una *función de cifrado*  $C$ , que toma el texto claro  $m$  y una *clave*  $k$  para producir el respectivo texto cifrado  $c$ :

$$c = C_k(m)$$

Para descifrar el texto se usa la *función de descifrado*  $D$  con clave  $k'$ :

$$m = D_{k'}(c)$$

En el caso que  $k = k'$ , se habla de un sistema *simétrico* o *de clave privada* (claramente, en esta situación debe mantenerse secreta la clave). En el caso que  $k \neq k'$ , obviamente habrá una relación entre las dos claves. Particularmente interesante es el caso en el que conociendo una de las dos es muy difícil obtener la otra. En tal caso, es perfectamente posible publicar  $k$ , manteniendo secreta  $k'$ . A estos sistemas se les llama *de clave pública*. Una aplicación interesante de sistemas de clave pública es *firmas digitales*: Dado un mensaje  $m$ , se calcula una función de hash  $h(m)$  del mensaje, y se envía  $m$  junto con  $f = D_{k'}(h(m))$ ; quien lo recibe puede aplicar  $C_k(f)$ , y comprobar que obtiene  $h(m)$ . Si la función de hash es tal que sea muy difícil construir un mensaje distinto que dé el mismo valor de la función, esto certifica que únicamente quien conoce  $k'$  puede originar la firma.

El gran problema con los sistemas simétricos es que las partes deben tener algún canal de comunicación seguro mediante el cual distribuir las claves. Los sistemas de clave pública no tienen esta dificultad, pero por otro lado son muchísimo más demandantes en computación que los sistemas simétricos tradicionales. Luego lo que se hace normalmente es generar una clave para un sistema simétrico tradicional al azar, y luego usar un sistema de clave pública para enviarle esta clave al receptor.

## 12.3. Protocolo Diffie-Hellman de intercambio de claves

En rigor, el protocolo no sirve para intercambiar claves sino para acordar una clave entre las partes, pero el nombre es el tradicional. El algoritmo que discutiremos es de amplio uso [64], forma la base de mucho de lo que es seguridad en Internet.

Supongamos que Alice y Bob desean acordar una clave  $K$ , usando un medio de comunicación que no es seguro. La idea básica es que Alice elige un primo  $p$  y una raíz primitiva  $g$  módulo  $p$ . Ambos valores puede incluso publicarlos, mantenerlos en secreto no es necesario para la seguridad del esquema y pueden perfectamente reutilizarse muchas veces. Para generar una clave, Alice elige un valor  $a$  (que mantiene en secreto), y envía  $A = g^a$  mód  $p$  a Bob. A su vez, Bob elige  $b$  (que también mantiene en secreto), y envía  $B = g^b$  mód  $p$  a Alice. Alice calcula  $K = B^a$  mód  $p = g^{ab}$  mód  $p$ , y Bob obtiene  $K = A^b$  mód  $p$ . Este valor puede usarse como clave por una sesión y descartarse después. El punto es que con los algoritmos conocidos actualmente si  $p$  es un primo de unos 300 dígitos, y  $a$  y  $b$  son números de 100 dígitos es imposible hallar  $a$  si solo se conocen  $p$ ,  $g$  y  $g^a$  mód  $p$ . Hay que tener cuidado con primos tales que  $p - 1$  tiene solo factores primos chicos, para ese caso hay algoritmos razonablemente eficientes que dan  $a$ . Por esta razón suele elegirse un primo de Sophie Germain, vale decir, uno de la forma  $2q + 1$  con  $q$  primo a su vez. Conviene trabajar en el subgrupo de orden

$q$ , dado que de otra forma el valor de  $g^a \pmod p$  revela el último bit de  $a$  (hay formas eficientes de determinar si un número es o no un cuadrado en  $\mathbb{Z}_p$ ). Está claro que exactamente lo mismo puede hacerse si  $g$  es un generador de algún otro grupo cíclico. La seguridad del esquema depende de la dificultad de calcular logaritmos discretos, vale decir, dados  $g$  y  $g^a$  calcular  $a$ .

Sabemos (ver sección 9.4) que hay  $\phi(p-1)$  raíces primitivas módulo  $p$ , con lo que son relativamente numerosas y es razonable buscar una raíz primitiva vía intentar valores al azar. Para un ejemplo numérico, tomemos  $p = 601$ , con lo que  $p-1 = 2^3 \cdot 3 \cdot 5^2$ , y hay  $\phi(p-1) = 160$  raíces primitivas. Una raíz primitiva  $g$  deberá cumplir:

$$g^{\frac{600}{2}} \not\equiv 1 \pmod{601} \quad g^{\frac{600}{3}} \not\equiv 1 \pmod{601} \quad g^{\frac{600}{5}} \not\equiv 1 \pmod{601}$$

Intentando con 31 tenemos:

$$31^{300} \equiv 600 \pmod{601} \quad 31^{200} \equiv 1 \pmod{601} \quad 31^{120} \equiv 432 \pmod{601}$$

La teoría anterior dice que aún requerimos algún valor  $u$  tal que  $u^{200} \not\equiv 1 \pmod{601}$  (ya tenemos cubiertas las potencias de 2 y 5, falta 3), algunos intentos dan:

$$357^{200} \equiv 576 \pmod{601}$$

con lo que  $g = 31 \cdot 357 \pmod{601} = 249$  es una raíz primitiva módulo  $p = 601$ .

Si ahora Alice elige  $a = 17$ , envía  $249^{17} \pmod{601} = 73$  a Bob, quien a su vez elige  $b = 58$  y envía  $249^{58} \pmod{601} = 149$  a Alice. Ambos están ahora en condiciones de calcular  $K$ : Alice calcula  $149^{17} \pmod{601} = 366$ , y Bob obtiene  $73^{58} \pmod{601} = 366$ .

Este ejemplo muestra que se requiere la factorización completa de  $p-1$  para obtener  $g$ , razón por la que es imprescindible poder reusar estos valores.

## 12.4. Sistema de clave pública de Rivest, Shamir y Adleman (RSA)

Es el sistema de clave pública más usado en la actualidad [302]. Se eligen dos números primos  $p$  y  $q$ , y se calcula el módulo  $n = pq$ . Se elige además un exponente  $e$ , y la clave pública es el par  $(n, e)$ . Para cifrar con RSA se usa:

$$c = m^e \pmod{n}$$

Conociendo  $p$  y  $q$  podemos generar la correspondiente clave privada  $(n, d)$  tal que:

$$c^d \pmod{n} = (m^e)^d \pmod{n} = m$$

Por el teorema de Euler, si  $\gcd(m, n) = 1$  es  $m^{\phi(n)} \equiv 1 \pmod{n}$ . Si  $de \equiv 1 \pmod{\phi(n)}$ , entonces  $c^d \equiv m^{de} \equiv m \pmod{n}$ . Más adelante discutiremos cómo elegir los parámetros del caso.

Podemos elegir el exponente  $e$  como un número relativamente pequeño (recuérdese que estamos interesados en módulos grandes; hoy se recomienda usar módulos de 4 096 bits, unos 1 300 dígitos decimales) de forma que sea cómodo elevar a esa potencia al cifrar, pero el exponente de descifrado resultará ser un número muy grande. Por el teorema chino de los residuos podemos calcular módulos  $p$  y  $q$ , o sea tenemos realmente:

$$c \equiv m^e \pmod{p}$$

$$c \equiv m^e \pmod{q}$$

Con esto requerimos que el exponente de descifrado  $d$  cumpla:

$$\begin{aligned} ed &\equiv 1 \pmod{(p-1)} \\ ed &\equiv 1 \pmod{(q-1)} \end{aligned}$$

Para cumplir con ambas, por el teorema 7.12 basta que:

$$ed \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$$

Hoy típicamente se usan claves (módulos) de 4 096 bits. Los primos  $p$  y  $q$  deben elegirse de forma de no ser demasiado cercanos, y ninguno de  $p-1, q-1, p+1$  y  $q+1$  debe tener muchos factores primos chicos, ya que de ser así  $n$  resulta relativamente fácil de factorizar. Puede demostrarse además (ver a Wiener [360]) que si  $d < n^{1/4}/3$  es muy fácil recuperar  $d$  conociendo solo  $n$  y  $e$ .

Para elegir  $e$ , una consideración importante es que sea relativamente pequeño y que su representación binaria tenga pocos unos, de forma que el cálculo de la potencia resulte simple (ver el algoritmo 11.3). Originalmente se recomendaba  $e = 3$ , pero exponentes chicos hacen posibles ciertos ataques que consideraremos luego. Hoy se recomienda  $e = 2^{16} + 1 = 65\,537$  (un primo de Fermat, de la forma  $2^{2^k} + 1$ ). Además de ser primo, este exponente tiene la virtud de tener solo dos unos en su expansión binaria; elevar a esta potencia involucra 5 multiplicaciones, 4 veces elevar al cuadrado y una multiplicación adicional por la base.

No hay similar control sobre  $d$ , el exponente para descifrar. Usar el mínimo común múltiplo  $\text{lcm}(p-1, q-1)$  en vez de  $\phi(n)$  disminuye el valor, pero no significativamente. Podemos acelerar el proceso usando el teorema chino de los residuos, teorema 8.7. Precalculamos valores  $d_1, d_2, q'$  (así, la clave privada es realmente  $(p, q, d_1, d_2, q')$ ), donde se cumplen las siguientes relaciones:

$$ed_1 \equiv 1 \pmod{(p-1)} \quad ed_2 \equiv 1 \pmod{(q-1)} \quad qq' \equiv 1 \pmod{p}$$

Dado el mensaje cifrado  $c$  se obtiene el mensaje  $m$  mediante:

$$\begin{aligned} m_1 &= c^{d_1} \pmod{p} \\ m_2 &= c^{d_2} \pmod{q} \\ h &= ((m_1 - m_2) \cdot q') \pmod{p} \\ m &= m_2 + qh \end{aligned}$$

Los cálculos de  $m_1$  y  $m_2$  se pueden efectuar en paralelo, e involucran exponentes y módulos mucho menores que en la formulación original, lo que hace más rápido el cálculo aún si es secuencial.

Está claro que exactamente la misma idea es aplicable a módulos que son productos de más de dos primos, aunque en la práctica se usan solo dos (mientras menos factores tenga el módulo, más difícil es factorizarlo).

La seguridad del sistema se basa en lo complejo que resulta factorizar números grandes, aunque hay algunas otras consideraciones [49, 108, 309]. El récord actual (a comienzos del 2012) de factorización de números generales es RSA-768 [208], un número de 768 bits (232 dígitos decimales) consumiendo el equivalente aproximado de 2000 años de procesamiento en un Opteron a 2,2 GHz.

Resulta que conocer  $d$  da una manera eficiente de factorizar  $n$ . Podemos calcular  $k = de - 1 = 2^s r$  con  $r$  impar y  $s > 0$ . Entonces  $a^k \equiv 1 \pmod{n}$  para todo  $a$ , y  $a^{k/2}$  es raíz cuadrada de 1 módulo  $n$ . Por el teorema chino de los residuos, 1 tiene cuatro raíces cuadradas módulo  $n = pq$ : son  $x = uv$  donde  $u \equiv \pm 1 \pmod{p}$  y  $v \equiv \mp 1 \pmod{q}$ . Como en la prueba de primalidad de Miller-Rabin, eligiendo  $a$  al azar e intentando  $a^r \pmod{n}, a^{2r} \pmod{n}, \dots, a^{k/2} \pmod{n}$  rápidamente hallaremos una raíz cuadrada  $x$  no trivial de 1, y obtenemos una factorización vía  $\gcd(x-1, n)$ .

Un uso típico de RSA es enviar el mismo mensaje  $m$  a un grupo de  $k$  personas, donde la persona  $i$  usa clave pública  $(n_i, e_i)$ . Por simplicidad, supongamos  $e_i = 3$ . Además, los  $n_i$  son relativamente

primos a pares (en caso contrario, factorizar algunos es trivial). Recolectando tres mensajes cifrados  $c_i = m^3 \pmod{n_i}$ , vía el teorema chino de los residuos podemos calcular  $c' \equiv m^3 \pmod{n_1 n_2 n_3}$ , y como  $m < n_i$  esto da  $c' = m^3$  en  $\mathbb{Z}$ , y basta calcular una raíz cúbica. Un ataque afín, debido a Franklin y Reiter [134], funciona si se tienen varios mensajes relacionados por una función lineal conocida (por ejemplo, si se “rellena” un mensaje corto agregando bits fijos o conocidos) cifrados con el mismo exponente. La complejidad del ataque es cuadrático en  $e$  y  $\log n$ . Otro ataque, debido a Coppersmith, Franklin, Patarin y Reiter [80], es aplicable cuando se conocen  $e$  mensajes cifrados con el mismo módulo relacionados por polinomios conocidos. Por esto se sugiere usar  $e = 2^{16} + 1 = 65537$  (un primo de Fermat).

#### 12.4.1. Firma digital usando RSA

Para firmar un mensaje usando RSA, se elige una función de *hash* criptográfica  $h$ . Se envía el mensaje  $m$  junto con  $h(m)^d \pmod{n}$ , cosa que solo puede hacer quien conozca el exponente secreto  $d$ . Quien recibe el mensaje puede verificar la firma elevando al exponente público  $e$  módulo  $n$  y confirmando que el resultado coincide con el valor de  $h(m)$ .

### 12.5. El estándar de firma digital (DSS)

El *Digital Signature Algorithm* (DSA) es un estándar del gobierno federal de Estados Unidos de Norteamérica para firmas digitales, a ser usado en el *Digital Signature Standard* (DSS), estándar FIPS 186 [122], adoptado en 1993. Es una modificación del esquema de ElGamal [112], Anderson y Vaudenay [11] discuten algo de su diseño y algunos ataques. Hubo una revisión menor en 1996 como FIPS 186-1 [123], fue expandido en 2000 (FIPS 186-2) y se rehizo completo en 2009, especificando algoritmos adicionales (FIPS 186-3 [124]). La versión actual data de 2013 (FIPS 186-4 [125]). El algoritmo DSA tiene dos fases, en la primera se eligen los parámetros del algoritmo, que pueden compartirse entre diferentes usuarios; mientras la segunda calcula claves públicas y privadas para un usuario individual. Con la clave privada se firma un documento, y con la correspondiente clave pública se verifica que la firma es genuina.

#### 12.5.1. Selección de parámetros

Se efectúan las siguientes operaciones:

- Se elige una función de *hash* criptográfica aprobada  $H$  (la versión original de DSA usaba SHA-1, actualmente también se especifica SHA-2 [121]). La salida de  $H$  puede truncarse al largo de la clave.
- Decida largo de clave, el par  $(L, N)$ , determinante para la seguridad del esquema. La versión actual [124] especifica pares  $(1024, 224)$ ,  $(2048, 224)$ ,  $(2048, 256)$  y  $(3072, 256)$ .
- Elija un primo  $q$  de  $N$  bits. Nótese que  $N$  debe ser menor o igual al largo de la salida de  $H$ .
- Elija un primo  $p$  de  $L$  bits tal que  $p - 1$  es múltiplo de  $q$ .
- Elija  $g$ , un número cuyo orden multiplicativo módulo  $p$  es  $q$ . Esto se obtiene fácilmente como  $h^{(p-1)/q}$  para  $1 < h < p - 1$  arbitrario, intentando nuevamente si el resultado es 1. La mayoría de los  $h$  producen lo buscado, suele simplemente usarse  $h = 2$ .

Los parámetros  $(p, q, g)$  pueden compartirse.

### 12.5.2. Generar claves para un usuario

Dado un conjunto de parámetros, se calculan las claves pública y privada para un usuario:

- Elija  $x$  al azar, donde  $0 < x < q$ .
- Calcule  $y = g^x$  mód  $p$ .

La clave pública es  $(p, q, g, y)$ , la clave privada es  $x$ .

### 12.5.3. Firmar y verificar firma

Sea  $m$  el mensaje. Para firmarlo, se procede como sigue:

- Genere un valor  $k$  al azar para este mensaje, donde  $0 < k < q$ .
- Calcule  $r = (g^k \text{ mód } p) \text{ mód } q$ , en el improbable caso que resulte  $r = 0$  elija un nuevo valor de  $k$ .
- Calcule  $s = (k^{-1} \cdot (H(m) + x \cdot r)) \text{ mód } q$ . En el improbable caso que  $s = 0$ , elija un nuevo valor de  $k$ .

La firma es  $(r, s)$ .

Para verificar la firma, se procede como sigue. Si no se cumplen  $0 < r < q$  y  $0 < s < q$ , la firma se rechaza. Enseguida:

- Calcule  $w = s^{-1} \text{ mód } q$
- Calcule  $u_1 = H(m) \cdot w \text{ mód } q$  y  $u_2 = r \cdot w \text{ mód } q$
- Calcule  $v = ((g^{u_1} \cdot y^{u_2}) \text{ mód } p) \text{ mód } q$

La firma es válida si  $v = r$ .

### 12.5.4. Correctitud del algoritmo

El algoritmo es correcto, en el sentido que quien verifica siempre acepta una firma válida.

Primeramente, por el teorema de Fermat  $g^q \equiv h^{p-1} \equiv 1 \pmod{p}$ ; como  $g > 1$  y  $q$  es primo, el orden de  $g$  es  $q$ . Al firmar se calcula:

$$s = k^{-1} \cdot (H(m) + xr) \pmod{q}$$

por lo que:

$$\begin{aligned} k &\equiv H(m) \cdot s^{-1} + xr s^{-1} \\ &\equiv H(m) \cdot w + xr w \pmod{q} \end{aligned}$$

Como  $g$  es de orden  $q$  módulo  $p$ , tenemos:

$$\begin{aligned} g^k &\equiv g^{H(m)w} y^{rw} \\ &\equiv g^{u_1} y^{u_2} \pmod{p} \end{aligned}$$

y finalmente:

$$r = (g^k \pmod{p}) \pmod{q} = (g^{u_1} y^{u_2} \pmod{p}) \pmod{q} = v$$

### 12.5.5. Ataques a DSS

Lawson [232] indica que si tenemos dos firmas efectuadas con el mismo  $k$ , en  $\mathbb{Z}_q$ :

$$r = g^k \text{ mód } p \quad (12.1)$$

$$S_a = k^{-1}(H(M_a) + x \cdot r) \quad (12.2)$$

$$S_b = k^{-1}(H(M_b) + x \cdot r) \quad (12.3)$$

De hallar dos firmas con el mismo  $r$ , sabemos que se repitió  $k$ ; con  $r$  de (12.2) y (12.3) podemos despejar  $k$  y en consecuencia calcular  $x$ . Un ataque similar es aplicable si se conocen algunos bits de  $k$ , usando más firmas.

El requerimiento de que  $k$  se elija al azar es crítico. Por ejemplo, el ampliamente publicitado problema de seguridad en Debian restringió el número de posibles  $k$  a 32767, lo que hace viable intentarlos todos para recuperar la clave. Nótese que esto no depende de lo seguro que haya sido el proceso de generarla, un único uso descuidado la revela.

## 12.6. Otras consideraciones

Los algoritmos criptográficos basados en teoría de números usan números primos como partes de sus claves. En el caso de Diffie-Hellman, el primo usado puede publicarse, en caso de RSA es clave que los factores del módulo permanezcan secretos (deben generarse al azar, haciendo que sea difícil adivinarlos). Sin embargo, estudios recientes [173, 237] han mostrado que una fracción no despreciable de las claves usadas en la práctica comparten factores, lo que las hace vulnerables.

Para determinar factores comunes entre las claves, estos trabajos usan un truco debido a Dan Bernstein [41], quien luego da una versión mejorada [40]. Supongamos el conjunto de módulos  $m_1, m_2, \dots, m_n$ . En el caso de [237] son 4,7 millones de módulos de 1024 bits, y calcular los máximos comunes divisores de todos los pares para detectar factores comunes está fuera de cuestión. Pero se puede proceder calculando primero  $M = m_1 \cdot m_2 \cdots m_n$ , y luego para cada  $m_i$  calcular  $\gcd(m_i, M \text{ mód } m_i^2)$ . Esto involucra un cálculo largo inicial para calcular  $M$ , luego una operación costosa al calcular  $M \text{ mód } m_i^2$  y determinar un máximo común divisor para cada módulo en el conjunto. Estas operaciones son razonablemente rápidas de efectuar en un computador común.

## 12.7. Criptografía de curvas elípticas

Recientemente se han introducido variantes de algunos métodos criptográficos que en vez de trabajar en el grupo  $\mathbb{Z}_p^\times$  usan el grupo de una curva elíptica [164]. La razón de usar curvas elípticas es que el problema de obtener  $k$  dados  $Q = kP$  y  $P$  en el grupo de una curva elíptica parece ser mucho más difícil de resolver que el problema equivalente en  $\mathbb{Z}_p^\times$ . Eso sí que la selección de la curva y los demás parámetros no son triviales, por lo que hay curvas sugeridas [265, 318, 319], mientras paranoicos terminales generarán sus propias curvas y parámetros. Para determinar el orden del grupo hay un algoritmo razonablemente eficiente ideado por Schoof [316], con mejoras de Elkies y Atkin que solo circulan como borradores, Dewaghe [90] describe la versión usada en la práctica. En [109] se describe el proceso para generar curvas en detalle (y se dan curvas alternativas para uso criptográfico). En 1997 Certicom publicó una colección de desafíos [67], discusión de algoritmos relevantes y estimaciones del trabajo para resolverlos se dan en [24], avances concretos respecto del menor problema aún sin resolver en 2012 se discuten en [25].

Los algoritmos que siguen suponen que se acuerdan parámetros de dominio: El campo  $F$ , los parámetros  $a$  y  $b$  de la curva, un generador  $g$  del grupo, el orden  $n$  de  $g$  (generalmente elegido como un primo), y el cofactor  $h$  (el orden del grupo de la curva dividido por el orden de  $g$ , conviene que sea pequeño, menor a 4 y ojalá 1).

### 12.7.1. Intercambio de claves

Es usar la idea de Diffie-Hellman (ver la sección 12.3) en una curva elíptica. En inglés le llaman *Elliptic Curve Diffie-Hellman*, abreviado *ECDH*. El funcionamiento es similar al algoritmo clásico. Para generar una clave compartida entre Alice y Bob proceden como sigue:

1. Alice y Bob tienen claves privadas  $d_A$  y  $d_B$  (enteros en el rango 1 a  $n - 1$ ), y calculan  $Q_A = d_A g$  y  $Q_B = d_B g$ .
2. Intercambian  $Q_A$  y  $Q_B$  a través del medio inseguro.
3. Alice calcula  $K = d_A Q_B$ , mientras Bob obtiene este valor como  $K = d_B Q_A$ . Dado  $K = (x_k, y_k)$ , la mayoría de los protocolos usan  $x_k$  para derivar la clave a ser usada.

Una variante resistente a ciertos ataques es FHMQV [311].

### 12.7.2. Firmas digitales

Esta es una variante del algoritmo DSA (sección 12.5). Alice tiene una clave privada  $d_A$  (un entero al azar en el rango 1 a  $n - 1$ ) y su clave pública  $Q_A = d_A g$ . Sea  $L_n$  el largo en bits del orden  $n$  del grupo. Si Alice quiere enviar un mensaje  $m$  firmado a Bob, procede como sigue:

1. Calcula  $e = h(m)$ , donde  $h$  es una función de *hash* criptográfica, y sea  $z$  los  $L_n$  bits más significativos de  $e$ .
2. Elige un entero  $k$  al azar entre 1 y  $n - 1$ .
3. Calcula  $r = x_1 \text{ mód } n$ , donde  $(x_1, y_1) = kg$ . Si  $r = 0$ , vuelve al punto 2.
4. Calcula  $s \equiv k^{-1}(z + rd_A) \pmod{n}$ . Si  $s = 0$ , vuelve al punto 2.

La firma es el par  $(r, s)$  resultante.

Para verificar la firma, Bob primero verifica la clave pública de Alice:

1. Verifica que  $Q_A \neq 0$  y que sus coordenadas son válidas.
2. Verifica que  $Q_A$  está en la curva.
3. Verifica que  $nQ_A = 0$ .

Enseguida, para verificar la firma del mensaje  $m$ , repite el cálculo que lleva a  $z$ , luego:

1. Verifica que  $r$  y  $s$  estén en el rango 1 a  $n - 1$ . En caso contrario, la firma no es válida.
2. Calcula  $w = s^{-1} \pmod{n}$ , luego  $u_1 = zw \pmod{n}$  y  $u_2 = rw \pmod{n}$ . Con esto determina  $(x_1, y_1) = u_1 g + u_2 Q_A$ .

La firma es válida si  $r \equiv x_1 \pmod{n}$ , en caso contrario no es válida.

# 13 Combinatoria elemental

---

Consideremos el problema de contar sistemáticamente los elementos de colecciones de objetos. Nuestro interés en el tema es que por ejemplo el comportamiento de un algoritmo de ordenamiento dependerá del número de disposiciones distintas en que pueden venir los datos, y ciertas características de dicho orden. Contar éstos, particularmente para conjuntos de datos de tamaño interesante, generalmente no es posible manualmente. Acá nos concentraremos en algunas técnicas simples, de aplicabilidad sorprendentemente amplia. Más adelante veremos herramientas adicionales.

## 13.1. Técnicas básicas

Las herramientas básicas son:

**Biyecciones (funciones 1–1):** Si hay una función 1 a 1 como  $f: \mathcal{X} \rightarrow \mathcal{Y}$ , entonces  $|\mathcal{X}| = |\mathcal{Y}|$  (esto incluso lo usamos para definir cardinalidades en el capítulo 6). Más en general para funciones  $k$  a 1: Si hay tal función  $g: \mathcal{X} \rightarrow \mathcal{Y}$ , entonces  $|\mathcal{X}| = k \cdot |\mathcal{Y}|$ .

**Regla de la suma:** Si  $\mathcal{A} \cap \mathcal{B} = \emptyset$ , entonces  $|\mathcal{A} \cup \mathcal{B}| = |\mathcal{A}| + |\mathcal{B}|$ . Esto se generaliza en forma obvia a un número mayor de conjuntos disjuntos a pares:

$$|\mathcal{A}_1 \cup \mathcal{A}_2 \cup \dots \cup \mathcal{A}_r| = |\mathcal{A}_1| + |\mathcal{A}_2| + \dots + |\mathcal{A}_r|$$

Si la intersección no es vacía, al sumar los tamaños estamos contando la intersección dos veces, o sea para dos conjuntos debemos hacer:

$$|\mathcal{A} \cup \mathcal{B}| = |\mathcal{A}| + |\mathcal{B}| - |\mathcal{A} \cap \mathcal{B}|$$

Más adelante (capítulo 15) veremos cómo se puede manejar esto en el caso general si hay más de dos conjuntos involucrados.

**Contar por filas y por columnas:** Si  $\mathcal{S} \subseteq \mathcal{X} \times \mathcal{Y}$ , y para  $x \in \mathcal{X}$  e  $y \in \mathcal{Y}$  definimos:

$$r_x(\mathcal{S}) = |\{(x, y) \in \mathcal{S} : y \in \mathcal{Y}\}|$$

$$c_y(\mathcal{S}) = |\{(x, y) \in \mathcal{S} : x \in \mathcal{X}\}|$$

Entonces:

$$|\mathcal{S}| = \sum_{x \in \mathcal{X}} r_x(\mathcal{S}) = \sum_{y \in \mathcal{Y}} c_y(\mathcal{S})$$

En forma más general, si hay dos (o más) maneras de contar algo, debieran coincidir los resultados.

**Regla del producto:** Si al contar por filas y columnas tomamos  $\mathcal{S} = \mathcal{X} \times \mathcal{Y}$ , resulta:

$$|\mathcal{S}| = |\mathcal{X}| \cdot |\mathcal{Y}|$$

dado que en ese caso  $r_x(\mathcal{S}) = |\mathcal{Y}|$  y  $c_y(\mathcal{S}) = |\mathcal{X}|$ .

Algunos ejemplos simples:

- ¿Cuántas patentes antiguas (2 letras, pero no Q ni W; y 4 dígitos) hay?

Podemos considerarlo como una tupla. Como hay 24 letras permitidas y 10 dígitos, por la regla del producto esto corresponde a:

$$24 \cdot 24 \cdot 10 \cdot 10 \cdot 10 = 5760000$$

posibilidades.

- Se estaban acabando los números con el esquema anterior, se agregó la letra W. ¿Cuántos números se agregan?

Nuevamente una tupla, pero ahora de 25 letras y 10 dígitos. La regla del producto da para el nuevo total:

$$25 \cdot 25 \cdot 10 \cdot 10 \cdot 10 = 6250000$$

Por la regla de la suma, las patentes actuales son las antiguas y las agregadas, con lo que las agregadas son:

$$6250000 - 5760000 = 490000$$

- ¿Cuántas patentes nuevas (4 consonantes y 2 dígitos) hay?

Otra vez una tupla. Son  $21 \cdot 21 \cdot 21 \cdot 21 \cdot 10 \cdot 10 = 19448100$ .

- ¿Cuántas patentes hay en total?

Son el conjunto de patentes antiguas y las nuevas, lo que da por la regla de la suma:

$$6250000 + 19448100 = 25698100$$

- En la Universidad de Miskatonic, el decano Halsey insiste en que todos los estudiantes deben tomar exactamente cuatro cursos por semestre. Pide a los profesores que le hagan llegar las listas de los alumnos en sus cursos, pero estos solo le informan los números de estudiantes, ver el cuadro 13.1. ¿Qué puede decir el decano Halsey con estos datos?

Si consideramos los pares (alumno, curso), la suma de cada fila es el número de cursos que el alumno toma. Por tanto, si cada alumno toma cuatro cursos, la suma total debe ser divisible por cuatro. La suma de cada columna es el número de alumnos en el curso. Pero en este caso la suma total de los alumnos por curso es 331, así que la condición del decano no se está cumpliendo.

Como un ejemplo más complejo, usando estas ideas podemos demostrar nuevamente para la función  $\phi$  de Euler:

**Teorema 13.1** (Identidad de Gauß). *Para todo entero  $n$ , tenemos:*

$$n = \sum_{d|n} \phi(d)$$

donde la suma se extiende sobre los enteros  $d$  que dividen a  $n$ .

Profesor	Materia	Nº
Ashley	Física	45
Dexter	Zoología	29
Dyer	Geología	33
Ellery	Química	2
Lake	Biología	12
Morgan	Arqueología	5
Pabodie	Ingeniería	103
Upham	Matemáticas	95
Wilmarth	Inglés	7

Cuadro 13.1 – Número de alumnos por curso

La idea de la siguiente demostración viene del conjunto de fracciones:

$$\left\{ \frac{1}{n}, \frac{2}{n}, \dots, \frac{n-1}{n} \right\} = \left\{ \frac{a_1}{b_1}, \frac{a_2}{b_2}, \dots, \frac{a_{n-1}}{b_{n-1}} \right\}$$

donde  $a_r/b_r$  está en mínimos términos, o sea con  $d_r = \gcd(r, n)$ :

$$\frac{a_r}{b_r} = \frac{r/d_r}{n/d_r}$$

Cada  $b_r$  aparece exactamente  $\phi(b_r)$  veces.

*Demostración.* Sean  $\mathcal{S}$  los pares  $(d, f)$  tales que  $d | n$ ,  $1 \leq f \leq d$  y  $\gcd(f, d) = 1$ . Sumando por filas tenemos:

$$|\mathcal{S}| = \sum_{d|n} \phi(d)$$

Para demostrar que  $n = |\mathcal{S}|$ , construimos una biyección  $\beta$  entre  $\mathcal{S}$  y los enteros entre 1 y  $n$ .

Sea  $\beta(d, f) = fn/d$ . Esto siempre es un entero positivo, ya que  $d | n$ ; y como  $1 \leq f \leq d$ , es a lo más  $n$ . Para demostrar que es una inyección, consideremos:

$$\begin{aligned} \beta(d, f) &= \beta(d', f') \\ fn/d &= f'n/d' \\ fd' &= f'd \end{aligned}$$

Esto último es  $d | fd'$ , y como  $f$  y  $d$  son relativamente primos, por el lema 7.2 significa que  $d | d'$ . De la misma forma  $d' | d$ , y resulta  $d = d'$ . Con esto también es  $f = f'$ .

Para demostrar que es sobre, supongamos dado  $1 \leq k \leq n$ , y sean:

$$\begin{aligned} g_k &= \gcd(k, n) \\ d_k &= n/g_k \\ f_k &= k/g_k \end{aligned}$$

Tanto  $d_k$  como  $f_k$  son enteros, y además  $\gcd(d_k, f_k) = 1$ . Resulta:

$$\begin{aligned} \beta(d_k, f_k) &= \frac{f_k n}{d_k} \\ &= \frac{kn/g_k}{n/g_k} \\ &= k \end{aligned}$$

□

### 13.2. Situaciones recurrentes

Según Albert [8] algunas circunstancias comunes se organizan bajo las siguientes ideas:

**Objetos distinguibles o no:** Al jugar cartas interesa fundamentalmente su pinta y valor, mientras al discutir un canasto de frutas no interesa la identidad de cada una de las manzanas.

**Repeticiones o no:** En un juego de cartas se considera de bastante mal gusto que una misma carta aparezca varias veces; si nos preguntamos de cuántas formas pueden entregarse \$100 usando monedas de \$1, \$5 y \$10, claramente se permite que una moneda se repita.

**Orden interesa:** Al jugar cartas, una mano queda determinada por el conjunto de cartas (el orden no importa), al discutir números escritos en decimal el orden de los dígitos es fundamental.

Esto da lugar a varias situaciones diferentes, ordenadas aproximadamente en orden de complejidad creciente del análisis:

**Secuencias:** Se dan siempre que el orden interesa. Pueden darse tanto situaciones donde se permiten repeticiones como cuando no se permiten.

**Conjuntos:** No hay repetición y no interesa el orden, solo si el elemento pertenece a la colección o no.

**Multiconjuntos:** Se permiten repeticiones y no interesa el orden. Un elemento dado puede pertenecer varias veces a la colección.

Veamos las distintas situaciones por turno, buscando expresiones simples para el número total de posibilidades suponiendo que estamos tomando  $k$  elementos de entre  $n$  opciones.

**Secuencias sin repeticiones:** Esta situación se conoce como *permutaciones*, suele anotarse  $P(n, k)$  para el número de permutaciones de  $k$  objetos tomados entre un total de  $n$ . El primer elemento puede elegirse de  $n$  formas, el segundo de  $n - 1$  maneras, y así hasta llegar al último, que se puede elegir de  $n - k + 1$  maneras. Aplicando la regla del producto, tenemos:

$$\begin{aligned} P(n, k) &= n \cdot (n - 1) \cdots (n - k + 1) \\ &= n^k \end{aligned} \tag{13.1}$$

En el caso particular en que  $k = n$  resulta:

$$\begin{aligned} P(n, n) &= n^n \\ &= n! \end{aligned} \tag{13.2}$$

**Secuencias con repeticiones:** Generalmente se llaman usando el término inglés *strings* (también *palabras*, o las podemos considerar como tuplas cuyos elementos se toman todos del mismo conjunto). No hay notación en uso común para este caso. Aplicando la regla de multiplicación, viendo que cada uno de los  $k$  elementos puede elegirse de  $n$  maneras independientemente, en este tenemos:

$$n^k$$

Un caso de interés es contar todas las secuencias hasta cierto largo  $k$ . Vimos que hay  $n^r$  secuencias de largo  $r$ , con lo que por el teorema 3.6 cuando  $n > 1$  el número buscado es:

$$\sum_{0 \leq r \leq k} n^r = \frac{n^{k+1} - 1}{n - 1}$$

Cuando  $n = 1$ , hay una sola secuencia de cada largo, lo que resulta en:

$$\sum_{0 \leq r \leq k} 1 = k + 1$$

**Conjuntos:** Para elegir  $k$  elementos de entre  $n$  sin interesar el orden (se llaman *combinaciones*, y suele anotarse  $C(n, k)$ ) podemos elegirlos en orden (hay  $P(n, k)$  maneras de hacer esto), y luego considerar que hay  $P(k, k) = k!$  maneras de ordenar los  $k$  elementos elegidos (un mapa  $k!$  a 1 entre las secuencias ordenadas y el conjunto de  $k$  elementos elegidos). Vale decir, el número buscado es:

$$C(n, k) = \frac{P(n, k)}{P(k, k)} \quad (13.3)$$

$$= \frac{n^k}{k!} \quad (13.4)$$

$$= \frac{n!}{k!(n - k)!} \quad (13.5)$$

$$= \binom{n}{k} \quad (13.6)$$

Debido a esto suele leerse  $\binom{n}{k}$  como “ $n$  elija  $k$ ” (en inglés  $n$  choose  $k$ ). La ecuación (13.6) es la notación tradicional para coeficientes binomiales. Nótese que:

$$\binom{n}{k} = \binom{n}{n - k}$$

lo que puede interpretarse diciendo que al elegir los  $k$  elementos incluidos en el subconjunto, lo que en realidad estamos haciendo es elegir los  $n - k$  elementos que estamos dejando fuera. A esta clase de razonamiento se le llama *demonstración combinatoria*.

**Multiconjuntos:** No hay una notación especial aceptada comúnmente para este caso. Algunos autores usan:

$$\binom{\binom{n}{k}}{k}$$

para el caso en que tenemos  $n$  tipos de elementos de los cuales tomamos en total  $k$ . Una manera de representar esta situación es mediante variables  $x_r$ , donde  $x_r$  representa el número de elementos de tipo  $r$  elegidos. Entonces el número de multiconjuntos de tamaño  $k$  tomando de entre  $n$  alternativas es el número de soluciones en números naturales a la ecuación:

$$x_1 + x_2 + \cdots + x_n = k$$

La solución  $x_1 = 2, x_2 = 0, x_3 = 3, x_4 = 1$  al caso  $n = 4$  y  $k = 6$  queda ilustrada en la figura 13.1. Esta distribución puede describirse con un total de  $k = 6$  asteriscos para la suma, separados por  $n - 1 = 3$  barras para marcar las separaciones (los extremos son fijos, y los omitimos):

\* \* | | \* \* \* | \*

Visto de esta forma, lo que estamos haciendo es distribuir  $k$  asteriscos en  $n + k - 1$  posiciones, un total de  $C(n + k - 1, k)$ . A este tipo de razonamiento se le conoce como *stars and bars* en inglés. Así, el número de soluciones se expresa:

$$\binom{\binom{n}{k}}{k} = \binom{n + k - 1}{k}$$

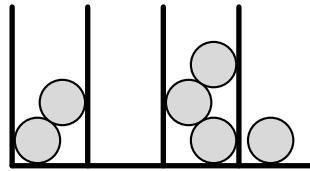


Figura 13.1 – Una distribución de 6 elementos en 4 grupos

Nótese que puede escribirse, de forma afín a los coeficientes binomiales:

$$\binom{n}{k} = \binom{n+k-1}{k} = \frac{n^{\bar{k}}}{k!}$$

Como  $n^{\bar{k}} = (-1)^k (-n)^k$  se cumple la curiosa identidad:

$$\binom{n}{k} = (-1)^k \binom{-n}{k} \quad (13.7)$$

Como ejemplo, determinemos el número de subconjuntos de  $k$  elementos de  $[n]$  que no contienen elementos consecutivos. Es claro que si  $k = 0$  hay un único subconjunto (el vacío), si  $k = 1$  hay  $n$ . Otros casos simples son:

- $n = 3, k = 2: 1 \quad \{1, 3\}$
- $n = 4, k = 2: 3 \quad \{1, 3\}, \{1, 4\}, \{2, 4\}$
- $n = 5, k = 2: 6 \quad \{1, 3\}, \{1, 4\}, \{1, 5\}, \{2, 4\}, \{2, 5\}, \{3, 5\}$
- $n = 5, k = 3: 1 \quad \{1, 3, 5\}$

Podemos nombrar un subconjunto de  $[n]$  como  $\{a_1, a_2, \dots, a_k\}$ , con  $1 \leq a_1 < a_2 < \dots < a_k \leq n$ . La restricción que no contenga elementos adyacentes se traduce en  $a_{r+1} \geq a_r + 2$  para  $1 \leq r < k$ . Definamos nuevas variables  $d_r$  para las diferencias entre elementos:

$$\begin{aligned} d_1 &= a_1 - 1 \\ d_{r+1} &= a_{r+1} - a_r - 2 \quad \text{para } 1 \leq r < k \\ d_{k+1} &= n - a_k \end{aligned}$$

Es claro que la restricción es que  $d_r \geq 0$ , y sus valores suman  $n - (k-1) \cdot 2 - 1 = n - 2k + 1$ . Por lo anterior, el número de soluciones para los  $d_r$  es:

$$\binom{k+1}{n-2k+1} = \binom{n-k+1}{k}$$

Esto coincide con los valores obtenidos antes.

Una aplicación simple de los resultados anteriores es la siguiente:

**Teorema 13.2.** *Sean  $\mathcal{X}$  e  $\mathcal{Y}$  conjuntos finitos. Entonces el número total de funciones  $f: \mathcal{X} \rightarrow \mathcal{Y}$  es:*

$$|\mathcal{Y}|^{|\mathcal{X}|}$$

*Demostración.* Supongamos que  $|\mathcal{X}| = m$ . Entonces podemos considerar esta situación como contar las tuplas  $(f(1), f(2), \dots, f(m))$ , en las cuales cada elemento toma un valor de entre  $|\mathcal{Y}| = n$ , con lo que por la regla del producto hay  $n^m$  funciones.  $\square$

Es por este resultado que una notación común para el conjunto de funciones de  $\mathcal{X}$  a  $\mathcal{Y}$  es  $\mathcal{Y}^{\mathcal{X}}$ .

Una manera de describir un subconjunto  $\mathcal{S}$  de un conjunto  $\mathcal{U}$  es mediante su *función característica*  $\chi_{\mathcal{S}}: \mathcal{U} \rightarrow \{0, 1\}$ , donde  $\chi_{\mathcal{S}}(u) = 0$  significa que  $u$  no pertenece al subconjunto, y  $\chi_{\mathcal{S}}(u) = 1$  que pertenece. Esta forma de ver las cosas lleva a:

**Corolario 13.3.** *Sea  $\mathcal{A}$  un conjunto finito. Entonces hay  $2^{|\mathcal{A}|}$  subconjuntos de  $\mathcal{A}$ .*

*Demostración.* Aplicar el teorema 13.2 al conjunto de funciones características.  $\square$

Es por esta razón que el conjunto de los subconjuntos de  $\mathcal{A}$  suele anotarse  $2^{\mathcal{A}}$ .

**Corolario 13.4.** *Sean  $\mathcal{A}$  y  $\mathcal{B}$  conjuntos finitos. Entonces hay  $2^{|\mathcal{A}||\mathcal{B}|}$  relaciones de  $\mathcal{A}$  a  $\mathcal{B}$ .*

*Demostración.* Una relación entre  $\mathcal{A}$  y  $\mathcal{B}$  no es más que un subconjunto de  $\mathcal{A} \times \mathcal{B}$ , aplicando la regla del producto y luego (13.3) obtenemos lo prometido.  $\square$

Otro caso importante es contabilizar el número de inyecciones.

**Teorema 13.5.** *Sean  $\mathcal{X}$  e  $\mathcal{Y}$  conjuntos finitos, de cardinalidades  $|\mathcal{X}| = m$  e  $|\mathcal{Y}| = n$ . Entonces el número total de funciones inyectivas  $i: \mathcal{X} \rightarrow \mathcal{Y}$  es  $n^m = n!/(n-m)!$*

*Demostración.* Si es una inyección, no se repiten valores de la función (y por tanto  $m \leq n$ ). Si consideramos que  $\mathcal{X}$  son índices (definen las posiciones), estamos frente a permutaciones de  $n$  elementos de los que se eligen  $m$ , vale decir es:

$$P(n, m) = n^m = \frac{n!}{(n-m)!}$$

Directamente resulta:

**Corolario 13.6.** *Sean  $\mathcal{X}$  e  $\mathcal{Y}$  conjuntos finitos tales que  $|\mathcal{X}| = |\mathcal{Y}| = n$ . Entonces el número de bijeciones  $b: \mathcal{X} \rightarrow \mathcal{Y}$  es  $n!$ .*

*Demostración.* Para el caso  $n = m$  el teorema 13.5 da  $n^n = n!$ .  $\square$

Otra forma de interpretar el corolario 13.6 es que hay  $n!$  maneras de ordenar  $n$  elementos diferentes.

Los números de combinaciones cumplen una colección inmensa de equivalencias curiosas.

**Teorema 13.7** (Identidad de Pascal). *Para  $n, k \in \mathbb{N}$  se cumplen:*

$$\begin{aligned} \binom{n}{0} &= \binom{n}{n} = 1 \\ \binom{n+1}{k+1} &= \binom{n}{k+1} + \binom{n}{k} \end{aligned}$$

*Demostración.* Primero:

$$\begin{aligned} \binom{n}{n} &= \binom{n}{n-n} = \binom{n}{0} \\ \binom{n}{0} &= \frac{n!}{n! 0!} = 1 \end{aligned}$$

Por el otro lado, podemos considerar que  $\binom{n+1}{k+1}$  corresponde a elegir  $k+1$  elementos de entre  $n+1$ , cosa que se puede hacer fijando uno de los elementos, y luego considerar aquellos conjuntos de  $k+1$  elementos que lo incluyen (corresponde a elegir los demás  $k$  de entre los  $n$  restantes, hay  $\binom{n}{k}$  casos de éstos), y los que no (corresponde a elegir  $k+1$  elementos de entre los  $n$  que son elegibles, hay  $\binom{n}{k+1}$  de estos casos). Como el conjunto de los subconjuntos que incluyen al elemento seleccionado y los que no son disjuntos, podemos aplicar la regla de la suma para obtener la recurrencia indicada.  $\square$

Una demostración alternativa es:

*Demostración.* Primeramente, siempre es:

$$\begin{aligned}\binom{n}{0} &= \frac{n^0}{0!} = 1 \\ \binom{n}{n} &= \frac{n^n}{n!} = \frac{n!}{n!} = 1\end{aligned}$$

Luego:

$$\begin{aligned}\binom{n}{k+1} + \binom{n}{k} &= \frac{n^{k+1}}{(k+1)!} + \frac{n^k}{k!} \\ &= \frac{n^k(n-k) + (k+1)n^k}{(k+1)!} \\ &= \frac{n^k(n+1)}{(k+1)!} \\ &= \frac{(n+1)^{k+1}}{(k+1)!} \\ &= \binom{n+1}{k+1}\end{aligned}$$

$\square$

Nótese que salvo en  $\binom{n}{n} = 1$  no presupone  $n \in \mathbb{N}_0$ .

Un resultado extremadamente importante es el que sigue:

**Teorema 13.8** (Binomio). *Para  $n \in \mathbb{N}$  tenemos:*

$$(a+b)^n = \sum_{0 \leq k \leq n} \binom{n}{k} a^k b^{n-k}$$

*Demostración.* Por inducción sobre  $n$ .

**Base:** Cuando  $n = 0$ , tenemos:

$$\sum_{0 \leq k \leq 0} \binom{0}{k} a^k b^{0-k} = \binom{0}{0} a^0 b^0 = 1$$

**Inducción:** Nótese que en las sumatorias siguientes el rango de las sumas es exactamente los índices para los cuales no se anulan los coeficientes binomiales respectivos, con lo que podemos obviar los límites de las sumas.

Usamos la identidad de Pascal, teorema 13.7, para simplificar la suma de coeficientes binomiales:

$$\begin{aligned}
 (a+b)^{n+1} &= (a+b)^n \cdot (a+b) \\
 &= \left( \sum_k \binom{n}{k} a^k b^{n-k} \right) \cdot (a+b) \\
 &= \sum_k \binom{n}{k} a^{k+1} b^{n-k} + \sum_k \binom{n}{k} a^k b^{n+1-k} \\
 &= \sum_k \binom{n}{k-1} a^k b^{n+1-k} + \sum_k \binom{n}{k} a^k b^{n+1-k} \\
 &= \sum_k \left( \binom{n}{k-1} + \binom{n}{k} \right) a^k b^{n+1-k} \\
 &= \sum_k \binom{n+1}{k} a^k b^{n+1-k} \\
 &= \sum_{0 \leq k \leq n+1} \binom{n+1}{k} a^k b^{n+1-k}
 \end{aligned}$$

Por inducción, vale para  $n \in \mathbb{N}_0$ . □

Por el teorema 13.8 es que los números  $\binom{n}{k}$  se llaman *coeficientes binomiales*.

Otro resultado importante es el siguiente.

**Teorema 13.9** (Multinomio). *Para  $n \in \mathbb{N}$  tenemos:*

$$(a_1 + a_2 + \cdots + a_r)^n = \sum_{k_1+k_2+\cdots+k_r=n} \binom{n}{k_1, k_2, \dots, k_r} a_1^{k_1} a_2^{k_2} \cdots a_r^{k_r}$$

donde:

$$\binom{n}{k_1, k_2, \dots, k_r} = \frac{n!}{k_1! k_2! \cdots k_r!}$$

Esta expresión está definida solo si  $n = k_1 + k_2 + \cdots + k_r$ .

*Demostración.* Si  $r = 0$ , ambas sumas son vacías, y lo aseverado se cumple. Para  $r = 1$  se reduce al trivial:

$$a_1^n = \frac{n!}{n!} a_1^n$$

Para  $r > 1$  la demostración es por inducción sobre  $r$ .

**Base:** Cuando  $r = 2$ , se reduce al teorema del binomio:

$$\sum_{k_1+k_2=n} \binom{n}{k_1, k_2} a_1^{k_1} a_2^{k_2} = \sum_{0 \leq k \leq n} \binom{n}{k, n-k} a_1^k a_2^{n-k} = \sum_{0 \leq k \leq n} \binom{n}{k} a_1^k a_2^{n-k}$$

**Inducción:** Tenemos:

$$\begin{aligned}
 & ((a_1 + \cdots + a_r) + a_{r+1})^n \\
 &= \sum_{0 \leq k_{r+1} \leq n} \binom{n}{k_{r+1}} (a_1 + \cdots + a_r)^{n-k_{r+1}} \cdot a_{r+1}^{k_{r+1}} \\
 &= \sum_{0 \leq k_{r+1} \leq n} \binom{n}{k_{r+1}} \left( \sum_{k_1+k_2+\cdots+k_r=n-k_{r+1}} \binom{n-k_{r+1}}{k_1, k_2, \dots, k_r} a_1^{k_1} a_2^{k_2} \cdots a_r^{k_r} \right) \cdot a_{r+1}^{k_{r+1}} \\
 &= \sum_{k_1+\cdots+k_{r+1}=n} \binom{n}{k_{r+1}} \binom{n-k_{r+1}}{k_1, k_2, \dots, k_r} a_1^{k_1} a_2^{k_2} \cdots a_{r+1}^{k_{r+1}} \\
 &= \sum_{k_1+\cdots+k_{r+1}=n} \binom{n}{k_1, k_2, \dots, k_{r+1}} a_1^{k_1} a_2^{k_2} \cdots a_{r+1}^{k_{r+1}}
 \end{aligned}$$

Acá usamos:

$$\begin{aligned}
 \binom{n}{k_{r+1}} \binom{n-k_{r+1}}{k_1, k_2, \dots, k_r} &= \frac{n!}{k_{r+1}!(n-k_{r+1})!} \cdot \frac{(n-k_{r+1})!}{k_1! k_2! \cdots k_r!} \\
 &= \frac{n!}{k_1! k_2! \cdots k_{r+1}!} \\
 &= \binom{n}{k_1, k_2, \dots, k_{r+1}}
 \end{aligned}$$

Por separado vimos que es válido para  $r = 0$  y  $r = 1$ , y por inducción es válido para  $r \geq 2$ , con lo que vale para  $r \in \mathbb{N}_0$ .  $\square$

Por razones obvias, a los  $\binom{n}{k_1, k_2, \dots, k_r}$  se les llama *coeficientes multinomiales*, y tenemos también:

$$\binom{n}{k, n-k} = \binom{n}{k}$$

### 13.3. Manos de poker

Nuestro siguiente tema de interés es contar subconjuntos que cumplen ciertas restricciones. Como conjuntos, siguiendo a Lehman, Leighton y Meyer [234], usaremos manos de poker.

En poker a cada jugador se le da una *mano* de cinco cartas, elegidas del mazo inglés, formado por cuatro *pintas*: Pica ( $\spadesuit$ ), corazón ( $\heartsuit$ ), trébol ( $\clubsuit$ ) y diamante ( $\diamondsuit$ ); en cada pinta hay trece *valores*: As, 2 a 10, Jack, Queen y King. El número total de manos posibles es:

$$\binom{52}{5} = 2598960$$

Como estrategia general, buscaremos secuencias que describan las manos que queremos contar (porque contar secuencias es fácil), y nos aseguraremos que hay una biyección (o que haya alguna otra relación clara, como un mapa 2 a 1) entre descripciones y manos. Proceder de esta manera es la manera más simple de asegurar que no se cometan errores, como contar varias veces u omitir parte de los objetos.

### 13.3.1. Royal Flush

Es la mano más alta en poker. Consta de As, King, Queen, Jack, 10 de la misma pinta, por ejemplo:

$\{A\spadesuit K\spadesuit Q\spadesuit J\spadesuit 10\spadesuit\}$

Está claro que hay una mano de éstas para cada pinta, con lo que hay exactamente 4.

### 13.3.2. Straight Flush

Consta de 5 cartas de la misma pinta en secuencia, donde As cuenta como 1 (no después de King, como en el Royal Flush). Ejemplos son:

$\{8\spadesuit 9\spadesuit 10\spadesuit J\spadesuit Q\spadesuit\}$   
 $\{A\heartsuit 2\heartsuit 3\heartsuit 4\heartsuit 5\heartsuit\}$   
 $\{3\clubsuit 4\clubsuit 5\clubsuit 6\clubsuit 7\clubsuit\}$

Estas manos podemos describirlas mediante una secuencia que indica:

- El valor de la primera carta en la secuencia. Este puede elegirse de 9 maneras (entre 1 y 9).
- La pinta, que puede elegirse de 4 maneras.

En nuestros ejemplos:

$(8, \spadesuit) \longleftrightarrow \{8\spadesuit 9\spadesuit 10\spadesuit J\spadesuit Q\spadesuit\}$   
 $(1, \heartsuit) \longleftrightarrow \{A\heartsuit 2\heartsuit 3\heartsuit 4\heartsuit 5\heartsuit\}$   
 $(3, \clubsuit) \longleftrightarrow \{3\clubsuit 4\clubsuit 5\clubsuit 6\clubsuit 7\clubsuit\}$

Por la regla del producto, el número total de estas manos es:

$$9 \cdot \binom{4}{1} = 36$$

Como esto no describe un Royal Flush, no hace falta ningún ajuste adicional.

### 13.3.3. Four of a Kind

Esta es una mano con cuatro cartas del mismo valor. Por ejemplo:

$\{8\spadesuit 8\heartsuit 8\clubsuit 8\diamondsuit 5\diamondsuit\}$   
 $\{2\spadesuit 2\heartsuit 2\clubsuit 2\diamondsuit 3\clubsuit\}$

Para calcular cuántas de estas hay, armamos un mapa de secuencias a manos de este tipo y contamos las secuencias. En este caso, una mano queda descrita por:

- El valor que se repite.
- El valor de la quinta carta.
- La pinta de la quinta carta.

Hay una biyección entre secuencias de estos tres elementos y manos. En nuestros ejemplos, las correspondencias son:

$(8, 5, \diamondsuit) \longleftrightarrow \{8\spadesuit 8\heartsuit 8\clubsuit 8\diamondsuit 5\diamondsuit\}$   
 $(2, 3, \clubsuit) \longleftrightarrow \{2\spadesuit 2\heartsuit 2\clubsuit 2\diamondsuit 3\clubsuit\}$

Para el valor tenemos 13 posibilidades, para el valor de la quinta carta quedan 12 posibilidades, y hay 4 opciones para la pinta de la quinta carta. En total, usando la regla del producto, son  $13 \cdot 12 \cdot 4 = 624$  posibilidades. Hay 1 en  $2598960/624 = 4165$  manos, no sorprende que se considere muy buena.

### 13.3.4. Full House

Es una mano con tres cartas de un valor y dos de otro. Ejemplos:

$$\begin{aligned} &\{2\heartsuit 2\clubsuit 2\diamondsuit Q\spadesuit Q\diamondsuit\} \\ &\{5\spadesuit 5\clubsuit 5\diamondsuit K\spadesuit K\heartsuit\} \end{aligned}$$

Nuevamente un mapa con secuencias:

- El valor del trío, que puede especificarse de 13 maneras.
- Las pintas del trío, que son elegir 3 de entre 4.
- El valor del par, que se puede tomar de 12 maneras.
- Las pintas del par, que se eligen 2 entre 4.

Las manos ejemplo corresponden con:

$$\begin{aligned} (2, \{\heartsuit, \clubsuit, \diamondsuit\}, Q, \{\spadesuit, \diamondsuit\}) &\longleftrightarrow \{2\heartsuit 2\clubsuit 2\diamondsuit Q\spadesuit Q\diamondsuit\} \\ (5, \{\spadesuit, \clubsuit, \diamondsuit\}, K, \{\spadesuit, \heartsuit\}) &\longleftrightarrow \{5\spadesuit 5\clubsuit 5\diamondsuit K\spadesuit K\heartsuit\} \end{aligned}$$

Por la regla del producto el número de Full Houses es entonces:

$$13 \cdot \binom{4}{3} \cdot 12 \cdot \binom{4}{2} = 3744$$

### 13.3.5. Flush

Mano con 5 cartas de la misma pinta, como por ejemplo:

$$\{A\heartsuit 3\heartsuit 4\heartsuit 8\heartsuit K\heartsuit\}$$

Esto se describe mediante la secuencia que da:

- Un conjunto de 5 valores, se eligen 5 de entre 13.
- Una pinta, se elige una entre 4.

En nuestro ejemplo:

$$(\{A, 3, 4, 8, K\}, \heartsuit) \longleftrightarrow \{A\heartsuit 3\heartsuit 4\heartsuit 8\heartsuit K\heartsuit\}$$

De estas manos hay entonces:

$$\binom{13}{5} \cdot \binom{4}{1} = 5148$$

Esto también describe al Royal Flush y al Straight Flush, debemos restar éstos (regla de la suma):

$$5148 - 4 - 36 = 5108$$

### 13.3.6. Manos con dos pares

Interesa calcular cuántas manos con dos pares hay, vale decir, dos cartas de un valor, dos cartas de otro valor, y una carta de un tercer valor. Ejemplos son:

$$\begin{aligned} &\{3\heartsuit 3\diamondsuit Q\spadesuit Q\clubsuit 5\diamondsuit\} \\ &\{9\heartsuit 9\clubsuit K\spadesuit K\diamondsuit 2\spadesuit\} \end{aligned}$$

Cada mano queda descrita por:

- El valor del primer par, puede elegirse de 13 maneras.
- Las pintas del primer par, se toman 2 de entre 4.
- El valor del segundo par, que se puede elegir de 12 maneras.
- Las pintas del segundo par, se eligen 2 entre 4.
- El valor de la carta extra, es uno de 11.
- La pinta de la carta extra, que es una de 4.

Se pensaría entonces que el número buscado es:

$$13 \cdot \binom{4}{2} \cdot 12 \cdot \binom{4}{2} \cdot 11 \cdot \binom{4}{1}$$

¡Esto es incorrecto! El mapa entre secuencias y manos no es una biyección, es 2 a 1 (hay dos maneras de describir la misma mano, podemos elegir cualquiera de los dos pares como primero). El valor correcto es:

$$\frac{13 \cdot \binom{4}{2} \cdot 12 \cdot \binom{4}{2} \cdot 11 \cdot \binom{4}{1}}{2} = 123\,552$$

No es una mano particularmente buena.

Pero además es perturbadora: Es fácil omitir el detalle de que no es una biyección. Hay dos salidas:

1. Cada vez que se usa un mapa  $f: \mathcal{A} \rightarrow \mathcal{B}$ , verifique que el mismo número de elementos de  $\mathcal{A}$  llevan a cada elemento de  $\mathcal{B}$ ; si este número es  $k$ , aplique la regla de división con  $k$ .
2. Intente otra forma de resolver el problema. Muchas veces hay varias formas de enfrentarlo – y debieran dar el mismo resultado. Claro que suele ocurrir que métodos distintos dan resultados que se *ven* diferentes, aunque resultan ser iguales.

Arriba usamos un método, veamos un segundo: Hay una biyección entre estas manos y secuencias que especifican:

- Los valores de los dos pares, se pueden elegir 2 entre 13.
- Las pintas del par de menor valor, se eligen 2 entre 4.
- Las pintas del par de mayor valor, se eligen 2 entre 4.
- El valor de la carta extra, es 1 entre 11.
- La pinta de la carta extra, es 1 entre 4.

Para nuestro ejemplo:

$$\begin{aligned} (\{3, Q\}, \{\diamondsuit, \heartsuit\}, \{\clubsuit, \spadesuit\}, 5, \diamondsuit) &\longleftrightarrow \{3\diamondsuit 3\heartsuit Q\spadesuit Q\clubsuit 5\diamondsuit\} \\ (\{9, K\}, \{\clubsuit, \heartsuit\}, \{\spadesuit, \diamondsuit\}, 2, \spadesuit) &\longleftrightarrow \{9\clubsuit 9\heartsuit K\spadesuit K\diamondsuit 2\spadesuit\} \end{aligned}$$

Esto lleva a:

$$\binom{13}{2} \cdot \binom{4}{2} \cdot \binom{4}{2} \cdot 11 \cdot \binom{4}{1}$$

Es el mismo resultado anterior, claro que escrito de forma ligeramente diferente.

### 13.3.7. Manos con todas las pintas

Buscamos el número de manos con cartas de todas las pintas. Por ejemplo:

$$\{7\heartsuit 8\diamondsuit K\clubsuit A\spadesuit 3\heartsuit\}$$

Esto podemos describirlo mediante:

- Los valores de las cartas de cada pinta, o sea  $13 \cdot 13 \cdot 13 \cdot 13$  posibilidades.
- El valor de la carta extra, con 12 selecciones posibles.
- La pinta de la carta extra, 4 opciones.

La mano del ejemplo se describe mediante:

$$(A, 7, 8, K, 3, \heartsuit) \longleftrightarrow \{7\heartsuit 8\diamondsuit K\clubsuit A\spadesuit 3\heartsuit\}$$

El problema es nuevamente que esto no es una biyección, en el ejemplo podemos considerar  $3\heartsuit$  o  $7\heartsuit$  como la carta extra, y el mapa es 2 a 1. El número buscado es:

$$\frac{13^4 \cdot 4 \cdot 12}{2} = 685\,464$$

Una forma alternativa es dar los valores del par de la misma pinta, y la pinta del par; y luego los valores de las tres cartas de las pintas restantes. Nuestro ejemplo se describe mediante:

$$(\{3, 7\}, \heartsuit, A, K, 8) \longleftrightarrow \{7\heartsuit 8\diamondsuit K\clubsuit A\spadesuit 3\heartsuit\}$$

Acá hemos supuesto el orden  $\spadesuit, \heartsuit, \clubsuit, \diamondsuit$  de las pintas. Esto da nuevamente:

$$\binom{13}{2} \cdot \binom{4}{1} \cdot 13 \cdot 13 \cdot 13 = 685\,464$$

### 13.3.8. Manos con valores diferentes

Nos interesa ahora contar el número de manos en las cuales todos los valores son diferentes. Una forma alternativa de describir estas manos es diciendo que no tienen pares. Veremos varias maneras de contarlas.

Una primera forma de enfrentar esto es considerar que la primera carta se puede elegir de entre 52, la segunda entre las 48 que no tienen el valor de la primera, y así sucesivamente. Pero el hablar de la primera, segunda y sucesivas cartas presupone orden, alerta del riesgo de contar demás. Como

son todas diferentes, basta dividir por el número de ordenamientos de 5 cartas, vale decir  $5! = 120$ . O sea:

$$\frac{52 \cdot 48 \cdot 44 \cdot 40 \cdot 36}{5!} = 1317888$$

Una solución alternativa consiste en seleccionar los valores de las 5 cartas, entre los 13 valores posibles, y luego a cada carta asignarle una pinta entre 4. Esto da:

$$\binom{13}{5} \cdot 4^5 = 1317888$$

### 13.4. El tao de BOOKKEEPER

Veremos maneras de contar secuencias que incluyen elementos repetidos. Para llegar a la iluminación siguiendo los pasos de Lehman, Leighton y Meyer [234], meditemos sobre la palabra BOOKKEEPER.

1. ¿De cuántas maneras se pueden ordenar las letras de POKE?
2. ¿De cuántas maneras se pueden ordenar las letras de B<sub>0</sub><sub>1</sub>O<sub>2</sub>K? (Note que los subíndices hacen que las dos O sean distintas).
3. Pequeño saltamontes, mapea los ordenamientos de B<sub>0</sub><sub>1</sub>O<sub>2</sub>K (las O son diferentes) a B<sub>0</sub>OK (las dos O son idénticas). ¿Qué clase de mapa es este?
4. ¡Muy bien, joven maestro! Dime ahora, ¿de cuántas maneras pueden ordenarse las letras de K<sub>E</sub><sub>1</sub>E<sub>2</sub>P<sub>E</sub><sub>3</sub>R?
5. Mapea cada ordenamiento de K<sub>E</sub><sub>1</sub>E<sub>2</sub>P<sub>E</sub><sub>3</sub>R a un ordenamiento de KEEPER tal que, borrando los subíndices, lista todos los que leen REPEEK. ¿Qué clase de mapa es este?
6. En vista de lo anterior, ¿cuántos ordenamientos de KEEPER hay?
7. ¡Ahora ya estás en posición de enfrentarte al terrible BOOKKEEPER! ¿Cuántos ordenamientos de B<sub>0</sub><sub>1</sub>O<sub>2</sub>K<sub>1</sub>K<sub>2</sub>E<sub>1</sub>E<sub>2</sub>P<sub>E</sub><sub>3</sub>R hay?
8. ¿Cuántos ordenamientos de BOOK<sub>1</sub>K<sub>2</sub>E<sub>1</sub>E<sub>2</sub>P<sub>E</sub><sub>3</sub>R hay?
9. ¿Cuántos ordenamientos de BOOKKEEPER hay?
10. ¿Cuántos ordenamientos de VOODOODOLL hay?
11. Esta es muy importante, pequeño saltamontes. ¿Cuántas secuencias de  $n$  bits tienen  $k$  ceros y  $n - k$  unos?

Prender subíndices, apagar subíndices. Ese es el tao de BOOKKEEPER.

### 13.5. Juegos completos de poker

Los señores George G. Akeley, Robert Blake, Randolph Carter y Edward P. Davis juegan poker. Interesa saber de cuántas maneras se pueden repartir las 52 cartas en 4 manos de 5 cartas, quedando 32 cartas en el mazo.

Podemos atacar el problema considerando que Akeley elige 5 cartas de las 52, que Blake elige 5 de las restantes, y así sucesivamente. El resultado es:

$$\binom{52}{5} \cdot \binom{52-5}{5} \cdot \binom{52-2 \cdot 5}{5} \cdot \binom{52-3 \cdot 5}{5} = \frac{52!}{5!5!5!32!}$$

$$= \binom{52}{5,5,5,5,32}$$

Si consideramos las cartas en un orden cualquiera, podemos representar la distribución asociando cada posición con quien la tiene. De esta forma, tenemos una biyección entre secuencias de 52 dueños de las cartas respectivas y las distribuciones de las cartas. Para simplificar notación, denotamos a los caballeros por las primeras letras de sus apellidos, y el mazo por M. Buscamos entonces el número de secuencias de 52 símbolos elegidos entre {A, B, C, D, M} formadas con 5 A, 5 B, 5 C, 5 D y 32 M. Esto nos lleva directamente al resultado anterior al aplicar el tao, sección 13.4.

### 13.6. Secuencias con restricciones

También interesa poder contar reordenamientos en los cuales hay ciertas restricciones, como elementos en posiciones fijas o elementos en posiciones fijas relativas entre sí.

Seguimos con nuestro ejemplo de BOOKKEEPER.

1. ¿De cuántas formas se puede escribir esta palabra si las dos O siempre están juntas?
2. ¿Cuántas formas hay de ordenar las letras si siempre están BPR juntas en ese orden?
3. ¿Si BPR están juntas, pero en cualquier orden?
4. ¿En cuántos aparecen BPR en ese orden, no necesariamente juntas?
5. ¿Cuántas maneras hay de ordenar las letras si las O están separadas por una letra?
6. ¿Cuántas maneras hay de ordenarlas si las E están separadas siempre por una letra?
7. ¿De cuántas maneras se pueden ordenar las letras si las 5 vocales están al principio y las 5 consonantes al final?
8. ¿Y si las vocales están en las posiciones impares?
9. ¿Qué pasa si las vocales ocupan las posiciones 2, 3, 6, 7, 9?
10. ¿Cuántos ordenamientos hay en los cuales las vocales están todas juntas?
11. ¿Cuántos ordenamientos con B en una posición impar hay?
12. ¿Y si solo pedimos una O en una posición par?
13. ¿Cuántos ordenamientos hay con las tres E en posiciones impares?
14. ¿Cuántos órdenes tienen la B separadas de la R por dos letras?
15. ¿Cuántos tienen la B separadas de la R por  $k$  letras?

Otra situación, que puede enfrentarse mediante nuestra estrategia general de construir el objeto de interés en fases independientes, se presenta si queremos determinar el número de maneras de ordenar las letras de MISSISSIPPI de forma que las vocales siempre estén separadas por consonantes. Vemos que hay 4 I, lo que deja 5 espacios en los cuales distribuir las consonantes. Si llamamos  $x_0$  al número de consonantes antes de la primera I,  $x_1$  a  $x_3$  al número de consonantes entre I y finalmente  $x_4$  al número de consonantes después de la última I, queda la ecuación:

$$x_0 + x_1 + x_2 + x_3 + x_4 = 7$$

Restricciones son que  $x_0 \geq 0$ ,  $x_k \geq 1$  para  $1 \leq k \leq 3$  y  $x_4 \geq 0$ . Si definimos nuevas variables  $y_0 = x_0$ ,  $y_k = x_k - 1$  para  $1 \leq k \leq 3$  e  $y_4 = x_4$ , queda:

$$y_0 + y_1 + y_2 + y_3 + y_4 = 4$$

lo que nos lleva a contar multiconjuntos: El número de soluciones es el número de multiconjuntos de 5 elementos de los que tomamos 4. Luego ordenamos el multiconjunto de consonantes {M, S<sup>4</sup>, P<sup>2</sup>}, distribuyendo las consonantes según los tramos definidos anteriormente. Como estas dos decisiones (número de consonantes en cada tramo y orden de las consonantes) son independientes, aplicamos la regla del producto:

$$\binom{5}{4} \cdot \binom{7}{1, 4, 2} = 7350$$

Más adelante (capítulo 14) veremos técnicas que permiten resolver problemas de palabras formadas con algunas de las letras y multisubconjuntos en forma general.



## 14 Funciones generatrices

---

Veremos cómo usar series de potencias (una herramienta del análisis, vale decir matemáticas de lo continuo) para resolver una variedad de problemas discretos. La idea de funciones generatrices permite resolver muchos problemas de forma simple y transparente, resultando de sorprendentemente amplia aplicabilidad. Mostraremos ejemplos de los principales usos. Incluso cuando no da soluciones puede iluminar, indicando relaciones entre problemas que a primera vista no son obvias.

La justificación rigurosa de nuestro uso despreocupado de series de potencias deberá quedar para el capítulo 17 sobre series formales. El aplicar herramientas analíticas (especialmente la teoría de funciones de variables complejas, tema del capítulo 28) permite deducir resultados que de otra forma serían muy difíciles de obtener.

Nos centramos en aplicaciones y en uso de las técnicas discutidas más que en exponer la teoría, nuestros ejemplos frecuentemente llevan a resultados de interés independiente.

### 14.1. No son funciones, y nada generan

La técnica de funciones generatrices fue introducida por Euler y de Moivre, pero desarrollada y usada sistemáticamente por Laplace, quien acuñó el nombre. Como muchos términos en uso común, la explicación original del nombre no es clara, y definitivamente no encaja en el uso actual del lenguaje ni con la interpretación como series formales de potencias (capítulo 17). Sin embargo, el término es tan popular que ya es imposible de cambiar.

Para detalles de la teoría y aplicaciones adicionales véanse por ejemplo a Flajolet y Segدewick [126] o Wilf [364], mientras Kauers [198] se centra en el uso de paquetes de álgebra simbólica alrededor de esto. Referencia obligatoria para todo lo que es combinatoria son los textos de Stanley [333, 334].

Acá nos interesa analizar las sumas resultantes al lanzar combinaciones de los dados no transitivos discutidos en la sección 2.1. Un dado puede representarse por una tupla que indica el número de caras con cada valor, agregando el valor cero para completar:

A (caras {1, 1, 3, 5, 5, 6}): (0, 2, 0, 1, 0, 2, 1)

B (caras {2, 3, 3, 4, 4, 5}): (0, 0, 1, 2, 2, 1, 0)

C (caras {1, 2, 2, 4, 6, 6}): (0, 1, 2, 0, 1, 0, 2)

Para lanzar la suma 7 con dos dados tenemos las opciones desde que uno aporte 1 y el otro 6 hasta aportes de 6 y 1. Debemos considerar además el número de caras del valor considerado en cada dado. Para los dados A y C esto se traduce en:

$$2 \cdot 2 + 0 \cdot 0 + 1 \cdot 1 + 0 \cdot 0 + 2 \cdot 2 + 1 \cdot 1 = 10$$

posibilidades. Esta es exactamente la manera en que se calcula el coeficiente de  $z^7$  al multiplicar polinomios con el coeficiente de  $z^n$  dando el número de caras con valor  $n$  para cada dado:

$$\begin{aligned} A(z) &= 2z + z^3 + 2z^5 + z^6 \\ B(z) &= z + 2z^3 + 2z^4 + z^5 \\ C(z) &= z + 2z^2 + z^4 + 2z^6 \end{aligned}$$

El coeficiente de  $z^7$  en el producto  $A(z) \cdot C(z)$  nos da el valor buscado:

$$A(z) \cdot C(z) = 2z^2 + 4z^3 + z^4 + 4z^5 + 2z^6 + 10z^7 + 2z^8 + 4z^9 + z^{10} + 4z^{11} + 2z^{12}$$

Una sencilla operación algebraica considera todas las combinaciones posibles. Nótese que los polinomios del caso nos interesan puramente por sus propiedades algebraicas, los valores de los polinomios para diversos valores de  $z$  no interesan en lo más mínimo.

Al lanzar dos dados tradicionales las sumas 2 y 12 se pueden obtener de una única manera, mientras para 4 hay tres ( $1+3=2+2=3+1$ ). Representamos un dado mediante el polinomio:

$$D(z) = z + z^2 + z^3 + z^4 + z^5 + z^6 \quad (14.1)$$

con lo cual para dos dados:

$$D^2(z) = z^2 + 2z^3 + 3z^4 + 4z^5 + 5z^6 + 6z^7 + 5z^8 + 4z^9 + 3z^{10} + 2z^{11} + z^{12} \quad (14.2)$$

Interesa hallar dados marcados en forma diferente que den la misma distribución de las sumas (“dados locos”). Para construirlos buscamos polinomios  $D_1(z)$  y  $D_2(z)$  que den el producto (14.2). Debemos además tener que ambas representen dados, o sea tengan 6 caras, y que cada cara debe tener al menos un punto. Que cada cara tenga al menos un punto se traduce en que la función generatriz sea divisible por  $z$ , el número de caras es simplemente el valor de la función en  $z=1$ . O sea:

$$D_1(1) = D_2(1) = 6 \quad (14.3)$$

Factorizamos (14.1):

$$D(z) = z(z+1)(z^2 - z + 1)(z^2 + z + 1) \quad (14.4)$$

Los factores  $z$  y  $z^2 - z + 1$  tienen valor 1 para  $z = 1$ ,  $z+1$  da 2 y  $z^2 + z + 1$  da 3. Tanto  $D_1(z)$  como  $D_2(z)$  deben tener los factores  $z$ ,  $z+1$  y  $z^2 + z + 1$ ; solo quedan por redistribuir los  $z^2 - z + 1$ :

$$\begin{aligned} D_1(z) &= z(z+1)(z^2 + z + 1) \\ &= z + 2z^2 + 2z^3 + z^4 \end{aligned} \quad (14.5)$$

$$\begin{aligned} D_2(z) &= z(z+1)(z^2 - z + 1)^2(z^2 + z + 1) \\ &= z + z^3 + z^4 + z^5 + z^6 + z^8 \end{aligned} \quad (14.6)$$

Los dados marcados con 1, 2, 2, 3, 3, 4 y 1, 3, 4, 5, 6, 8 se conocen como *dados de Sicherman* [140]. Broline [55] estudia el problema para dados de números distintos de caras y más de dos dados. Gallian y Rusin [138] tratan un problema más general.

Representar problemas combinatorios por funciones nos permite aplicar la sofisticada maquinaria del álgebra y el cálculo. Nuestro interés es obtener información sobre los coeficientes dada la función, el foco en el cálculo es deducir características de la función conociendo los coeficientes.

## 14.2. Funciones generatrices

Sea una secuencia  $\langle a_n \rangle_{n \geq 0} = \langle a_0, a_1, a_2, \dots, a_n, \dots \rangle$ . La *función generatriz* (ordinaria) de la secuencia es la serie de potencias:

$$A(z) = \sum_{n \geq 0} a_n z^n \quad (14.7)$$

El punto es que la serie (14.7) representa en forma compacta y manejable la secuencia infinita. Wilf [364] expresa que la función generatriz es una línea de ropa de la cual se cuelgan los coeficientes para exhibición. Entendemos el exponente de  $z$  como un contador, índice del coeficiente correspondiente. Como veremos, operaciones sobre la función generatriz corresponden a actuar sobre la secuencia, en muchos casos resulta más sencillo manipular la serie que trabajar con la secuencia. Para nuestros efectos, en general basta manipularlos como si fueran “polinomios infinitos”, cosa que justificaremos en el capítulo 17. Si tenemos la suerte que la serie converge para algún rango alrededor de  $z = 0$  (como en nuestros ejemplos), podremos aplicar las herramientas del cálculo.

Para otro ejemplo, la Competencia de Ensayos de la Universidad de Miskatonic (sección 3.10), llevó a la relación:

$$b_{2r+1} = b_{2r-1} + r + 1 \quad (r \geq 1) \quad b_1 = 1 \quad (14.8)$$

con lo que tenemos, como antes (arbitrariamente dando el valor cero a los que no quedan definidos por la recurrencia)  $\langle b_n \rangle_{n \geq 0} = \langle 0, 1, 0, 3, 0, 6, 0, 10, 0, 15, \dots \rangle$ . Contar con algunos valores sirve para verificar (y para “sentir” cómo se comportan).

Veamos cómo usar funciones generatrices para resolver (14.8). Definamos la serie (note que el subíndice en  $b_{2r+1}$  avanza de a dos):

$$B(z) = \sum_{r \geq 0} b_{2r+1} z^r \quad (14.9)$$

Multiplicando la recurrencia (14.8) por  $z^r$  y sumando para  $r \geq 1$  (índices positivos) queda:

$$\sum_{r \geq 1} b_{2r+1} z^r = \sum_{r \geq 1} b_{2r-1} z^r + \sum_{r \geq 1} (r+1) z^r \quad (14.10)$$

Expresando lo anterior en términos de  $B(z)$ , reconocemos:

$$\sum_{r \geq 1} b_{2r+1} z^r = \sum_{r \geq 0} b_{2r+1} z^r - b_1 = B(z) - 1 \quad (14.11)$$

$$\sum_{r \geq 1} b_{2r-1} z^r = \sum_{r \geq 0} b_{2r+1} z^{r+1} = z \sum_{r \geq 0} b_{2r+1} z^r = z B(z) \quad (14.12)$$

Usamos propiedades de las sumatorias, y debemos poner especial atención a los términos iniciales.

En (14.10) aparece  $(r+1)z^r$ , la derivada de  $z^{r+1}$ . De la sección 3.7.1 sabemos que para  $|z| < 1$  vale:

$$\frac{1}{1-z} = \sum_{r \geq 0} z^r \quad (14.13)$$

Nótese que como  $z$  nos interesa únicamente para marcar posiciones por sus potencias, basta que la serie converja para un rango alrededor de cero. Derivando la serie geométrica respecto de  $z$  término a término, lo que es válido dentro del radio de convergencia (no nos detendremos en este punto, para la teoría que lo justifica véanse por ejemplo a Chen [71], a Trench [353] o refiérase al capítulo 28), queda:

$$\begin{aligned} \frac{d}{dz} \left( \frac{1}{1-z} \right) &= \sum_{r \geq 0} \frac{d}{dz} z^r \\ \frac{1}{(1-z)^2} &= \sum_{r \geq 1} r z^{r-1} = \sum_{r \geq 0} (r+1) z^r \end{aligned} \quad (14.14)$$

También:

$$\sum_{r \geq 1} (r+1)z^r = \sum_{r \geq 0} (r+1)z^r - 1 = \frac{1}{(1-z)^2} - 1 \quad (14.15)$$

Reemplazando (14.11), (14.12) y (14.15) en (14.10) queda:

$$B(z) - 1 = zB(z) + \frac{1}{(1-z)^2} - 1$$

Despejando  $B(z)$ :

$$B(z) = \frac{1}{(1-z)^3} \quad (14.16)$$

Para algunas aplicaciones basta llegar hasta acá, puede extraerse bastante información sobre los coeficientes de la función. Mayores detalles deberán esperar al capítulo 29.

Interesa obtener una fórmula explícita (ojalá simple) para los coeficientes, de forma de poder determinar el tamaño requerido de las tarjetas. Derivando la serie geométrica por segunda vez:

$$\begin{aligned} \frac{d^2}{dz^2} \left( \frac{1}{1-z} \right) &= \sum_{r \geq 1} \frac{d}{dz} r z^{r-1} \\ \frac{2}{(1-z)^3} &= \sum_{r \geq 2} r(r-1)z^{r-2} = \sum_{r \geq 0} (r+2)(r+1)z^r \end{aligned} \quad (14.17)$$

Con (14.17) y (14.16) resulta:

$$B(z) = \sum_{r \geq 0} b_{2r+1} z^r = \frac{1}{2} \sum_{r \geq 0} (r+2)(r+1)z^r \quad (14.18)$$

Comparando coeficientes tenemos nuevamente la fórmula explícita (3.54):

$$b_{2r+1} = \frac{1}{2} (r+2)(r+1)$$

La ventaja frente al desarrollo de la sección 3.10 es que no tuvimos que “adivinar” esta solución y nos ahorraron la demostración por inducción. Nótese además que el valor de  $B(z)$  jamás fue del más mínimo interés en el desarrollo.

### Receta

Para resolver recurrencias se debe:

1. Plantear la recurrencia.
2. Recopilar valores iniciales.
3. Aclarar para qué valores del índice vale la recurrencia.
4. Definir la función generatriz de interés.
5. Multiplicar la recurrencia de (1) por  $z^n$  y sumar sobre todos los valores (3).
6. Expresar (5) en términos de la función generatriz (4).
7. Despejar la función generatriz de (5).
8. Extraer los coeficientes.

### 14.3. Algunas series útiles

Al trabajar con funciones generatrices es importante tener algunas expansiones en serie conocidas a la mano. Las que más aparecen son las siguientes.

#### 14.3.1. Serie geométrica

Es la serie más común en aplicaciones. Si  $|z| < 1$ , se cumple:

$$\sum_{n \geq 0} z^n = \frac{1}{1-z} \quad (14.19)$$

Una variante importante es la siguiente, expansión válida para  $|az| < 1$  (con la convención  $0^0 = 1$ ):

$$\sum_{n \geq 0} a^n z^n = \frac{1}{1-az} \quad (14.20)$$

#### 14.3.2. Teorema del binomio

Una de las series más importantes es la expansión de la potencia de un binomio (ver también el teorema 13.8, que cubre el caso de potencias naturales):

$$\sum_{n \geq 0} \binom{\alpha}{n} z^n = (1+z)^\alpha \quad (14.21)$$

Siempre que  $|z| < 1$  esto vale incluso para  $\alpha$  complejos, si definimos:

$$\binom{\alpha}{k} = \frac{\alpha \cdot \alpha - 1 \cdot \alpha - 2 \cdot \dots \cdot \alpha - k + 1}{1 \cdot 2 \cdot 3 \cdot \dots \cdot k} = \frac{\alpha^k}{k!} \quad (14.22)$$

y (consistente con la convención que productos vacíos son 1) siempre es:

$$\binom{\alpha}{0} = 1 \quad (14.23)$$

A los coeficientes (14.22) se les llama *coeficientes binomiales* por su conexión con la potencia de un binomio. La expansión (14.21) (también conocida como *fórmula de Newton* si  $\alpha$  no es un natural) es fácil de demostrar por el teorema de Maclaurin. Resulta que (14.19) es un caso particular de (14.21).

Si  $\alpha$  es un entero positivo, la serie (14.21) se reduce a un polinomio (el factor  $\alpha^n$  se anula si  $n > \alpha$ ) y la relación es válida para todo  $z$ . Además, en caso que  $n$  sea natural podemos escribir:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \quad (14.24)$$

Es claro que:

$$\binom{n}{k} = 0 \text{ si } k < 0 \text{ o } k > n \quad (14.25)$$

Esto con (14.24) sugiere la convención:

$$\frac{1}{k!} = 0 \quad \text{si } k < 0 \quad (14.26)$$

Nótese la simetría:

$$\binom{n}{k} = \binom{n}{n-k} \quad (14.27)$$

Casos especiales notables de coeficientes binomiales para  $\alpha \notin \mathbb{N}$  son los siguientes:

**Caso  $\alpha = 1/2$ :** Tenemos, como siempre:

$$\binom{1/2}{0} = 1 \quad (14.28)$$

Cuando  $k \geq 1$ :

$$\begin{aligned} \binom{1/2}{k} &= \frac{\frac{1}{2} \cdot (\frac{1}{2} - 1) \cdots (\frac{1}{2} - k + 1)}{k!} \\ &= \frac{1}{2^k} \cdot \frac{1 \cdot (1-2) \cdot (1-4) \cdots (1-2k+2)}{k!} \\ &= \frac{(-1)^{k-1}}{2^k k!} \cdot (1 \cdot 3 \cdots (2k-3)) \\ &= \frac{(-1)^{k-1}}{2^k k!} \cdot \frac{1 \cdot 2 \cdot 3 \cdot 4 \cdots (2k-3) \cdot (2k-2)}{2 \cdot 4 \cdot 6 \cdots (2k-2)} \\ &= \frac{(-1)^{k-1}}{2^k k!} \cdot \frac{(2k-2)!}{2^{k-1}(k-1)!} \\ &= \frac{(-1)^{k-1}}{2^{2k-1} \cdot k} \cdot \frac{(2k-2)!}{(k-1)!(k-1)!} \\ &= \frac{(-1)^{k-1}}{2^{2k-1} \cdot k} \cdot \binom{2k-2}{k-1} \end{aligned} \quad (14.29)$$

Hay que tener cuidado, la última fórmula no cubre el caso  $k = 0$ .

**Caso  $\alpha = -1/2$ :** Mucha de la derivación es similar a la del caso anterior. Tenemos, para  $k > 0$ :

$$\begin{aligned} \binom{-1/2}{k} &= \frac{(-1/2) \cdot (-1/2 - 1) \cdots (-1/2 - k + 1)}{k!} \\ &= (-1)^k \frac{1}{2^k} \cdot \frac{1 \cdot 3 \cdots (2k-1)}{k!} \\ &= (-1)^k \frac{1}{2^k} \cdot \frac{(2k)!}{k! 2^k k!} \\ &= (-1)^k \frac{1}{2^{2k}} \binom{2k}{k} \end{aligned} \quad (14.30)$$

Esta fórmula con  $k = 0$  da:

$$\binom{-1/2}{0} = 1$$

así no se necesita hacer un caso especial acá.

**Caso  $\alpha = -1$ :** Este es probablemente el caso más común en aplicaciones. La fórmula da:

$$\frac{(-1)^k}{k!} = \frac{(-1)(-2)\cdots(-k)}{k!} = (-1)^k \quad (14.31)$$

Como debiera ser, es la serie geométrica (14.13):

$$\frac{1}{1+z} = \sum_{k \geq 0} (-1)^k z^k$$

**Caso  $\alpha = -n$ :** Cuando  $\alpha$  es un entero negativo, podemos escribir:

$$\binom{-n}{k} = \frac{(-n)_k}{k!} = (-1)^k \frac{n^{\bar{k}}}{k!} = (-1)^k \frac{(n+k-1)_k}{k!} = (-1)^k \binom{k+n-1}{n-1} \quad (14.32)$$

Ya habíamos notado (13.7):

$$\binom{n}{k} = (-1)^k \binom{-n}{k}$$

Nótense los casos particulares (aparecieron en nuestra derivación de la solución para la Competencia de Ensayos de la Universidad de Miskatonic):

$$\begin{aligned} \binom{-2}{k} &= (-1)^k \binom{k+1}{1} = (-1)^k (k+1) \\ \binom{-3}{k} &= (-1)^k \binom{k+2}{2} = (-1)^k \frac{(k+1)(k+2)}{2} \end{aligned}$$

Estos coeficientes binomiales son polinomios de grado  $n-1$  en  $k$ . En general, resulta:

$$\frac{1}{(1-z)^{n+1}} = \sum_{k \geq 0} \binom{n+k}{n} z^k \quad (14.33)$$

Antes habíamos obtenido tales coeficientes derivando.

Un par de series útiles son las sumas dobles, que se obtienen usando (14.21) y (14.33) con (13.7):

$$\sum_{n,k} \binom{n}{k} x^k y^n = \sum_n (1+x)^n y^n = \frac{1}{1-(1+x)y} \quad (14.34)$$

$$\sum_{n,k} \binom{n}{k} x^k y^n = \sum_n \frac{y^n}{(1-x)^n} = \frac{1-x}{1-x-y} \quad (14.35)$$

Interesante resulta la serie al variar  $n$ , no  $k$ :

$$\sum_{n \geq 0} \binom{n}{k} z^n$$

Sabemos que  $\binom{n}{k} = 0$  si no es que  $0 \leq k \leq n$ , podremos ahorrarnos los límites de las sumas para simplificar:

$$\begin{aligned} \sum_n \binom{n}{k} z^n &= \sum_n \binom{n+k}{k} z^{n+k} \\ &= z^k \sum_n \binom{n+k}{n} z^n \\ &= \frac{z^k}{(1-z)^{k+1}} \end{aligned} \quad (14.36)$$

Al final usamos (14.33). Omitir los rangos de los índices ahorró interminables ajustes.

Para multiconjuntos, usando (14.35), y anotando extraer el coeficiente de  $z^k$  mediante  $[z^k]$ :

$$\begin{aligned} \sum_{n \geq 0} \binom{n}{k} z^n &= [z^k] \frac{1-z}{1-z-z} \\ &= \frac{1}{1-z} [z^k] \frac{1-z}{1-z/(1-z)} \\ &= \frac{1}{1-z} [z^k] (1-z) \sum_{n \geq 0} \frac{z^n}{(1-z)^n} \\ &= \frac{1}{1-z} \left( \frac{1}{(1-z)^k} - \frac{[k > 0]}{(1-z)^{k-1}} \right) \\ &= \frac{1 - [k > 0](1-z)}{(1-z)^{k+1}} \\ &= \frac{(1 - [k > 0]) + [k > 0]z}{(1-z)^{k+1}} \end{aligned}$$

Como el numerador es 1 si  $k = 0$  y  $z$  cuando  $k > 0$  podemos simplificar:

$$\sum_{n \geq 0} \binom{n}{k} z^n = \frac{z^{[k>0]}}{(1-z)^{k+1}} \quad (14.37)$$

### 14.3.3. Otras series

Una serie común es la exponencial:

$$e^z = \sum_{n \geq 0} \frac{z^n}{n!} \quad (14.38)$$

con sus variantes:

$$e^{az} = \sum_{n \geq 0} \frac{a^n z^n}{n!} \quad e^{-z} = \sum_{n \geq 0} \frac{(-1)^n z^n}{n!}$$

A veces aparecen funciones trigonométricas:

$$\sin z = \sum_{n \geq 0} (-1)^n \frac{z^{2n+1}}{(2n+1)!} \quad \cos z = \sum_{n \geq 0} (-1)^n \frac{z^{2n}}{(2n)!}$$

o hiperbólicas:

$$\sinh z = \sum_{n \geq 0} \frac{z^{2n+1}}{(2n+1)!} \quad \cosh z = \sum_{n \geq 0} \frac{z^{2n}}{(2n)!}$$

Una relación útil es la fórmula de Euler:

$$e^{u+i\nu} = e^u (\cos \nu + i \sin \nu) \quad (14.39)$$

Es frecuente la serie para el logaritmo:

$$\begin{aligned} \frac{d}{dz} \ln(1-z) &= -\frac{1}{1-z} = -\sum_{n \geq 0} z^n \\ \ln(1-z) &= -\sum_{n \geq 1} \frac{z^n}{n} \end{aligned} \quad (14.40)$$

Muchos ejemplos adicionales de series útiles se hallan en el texto de Wilf [364].

#### 14.4. Notación para coeficientes

Comúnmente extraeremos el coeficiente de un término de una serie. Generalmente no hay términos con potencias negativas de  $z$ , tales coeficientes serán cero. Para esto, dadas las series:

$$A(z) = \sum_{n \geq 0} a_n z^n \quad B(z) = \sum_{n \geq 0} b_n z^n$$

usaremos la notación:

$$[z^n] A(z) = a_n$$

Tenemos algunas propiedades simples:

$$\begin{aligned}[z^n] z^k A(z) &= [z^{n-k}] A(z) \\ [z^n] (\alpha A(z) + \beta B(z)) &= \alpha [z^n] A(z) + \beta [z^n] B(z)\end{aligned}$$

El teorema de Maclaurin puede expresarse (el superíndice  $(n)$  indica  $n$ -ésima derivada):

$$[z^n] A(z) = \frac{1}{n!} A^{(n)}(0)$$

La notación es de Goulden y Jackson [148]. Puede extenderse muchísimo, ver Knuth [215] y Merlini, Sprugnoli y Verri [254]. La idea se le atribuye a Egorychev [111], aunque con una notación mucho más engorrosa.

**Teorema 14.1** (Transformación de Euler). *Sea  $A(z) = \sum a_n z^n$ . Entonces:*

$$\sum_{0 \leq k \leq n} \binom{n}{k} a_k = [z^n] \frac{1}{1-z} A\left(\frac{z}{1-z}\right) \quad (14.41)$$

*Demuestra*ión. Como para  $k > n$  el coeficiente binomial se anula, podemos extender la suma a todo  $k \geq 0$ . Consideremos:

$$\begin{aligned}\sum_{n \geq 0} z^n \sum_{k \geq 0} \binom{n}{k} a_k &= \sum_{k \geq 0} a_k \sum_{n \geq 0} \binom{n}{k} z^n \\ &= \sum_{k \geq 0} a_k \frac{z^k}{(1-z)^{k+1}} \\ &= \frac{1}{1-z} \sum_{k \geq 0} a_k \left(\frac{z}{1-z}\right)^k \\ &= \frac{1}{1-z} A\left(\frac{z}{1-z}\right)\end{aligned}$$

Esto es equivalente a lo enunciado.  $\square$

Lo aplicaremos a la suma discutida por Greene y Knuth [152], originalmente de Jonassen y Knuth [186]:

$$S_m = \sum_{0 \leq k \leq m} \binom{m}{k} \left(-\frac{1}{2}\right)^k \binom{2k}{k}$$

Del teorema del binomio, con los coeficientes (14.30), sabemos que:

$$\frac{1}{\sqrt{1+2z}} = \sum_{n \geq 0} \binom{2n}{n} \left(-\frac{1}{2}\right)^n z^n$$

Por la transformación de Euler (14.41):

$$\sum_{0 \leq k \leq m} \binom{m}{k} \binom{2k}{k} \left(-\frac{1}{2}\right)^k = [z^m] \frac{1}{1-z} \left(1 + 2\frac{z}{1-z}\right)^{-1/2} = [z^m] \frac{1}{\sqrt{1-z^2}}$$

Resulta:

$$S_m = \begin{cases} \binom{2k}{k} 2^{-2k} & m = 2k \\ 0 & m = 2k+1 \end{cases}$$

Prodinger [294] usa esta suma para mostrar diversas técnicas para obtener una fórmula cerrada.

### 14.5. Decimar

Uno de los máximos castigos para una legión romana era la *decimación*, que consistía en ejecutar a uno de cada diez miembros. Nuestro objetivo acá es mucho más radical, aunque bastante menos sangriento.

Sea una secuencia  $\langle a_n \rangle_{n \geq 0}$ , con función generatriz ordinaria  $A(z)$ . Es fácil ver que:

$$\sum_{n \geq 0} a_{2n} z^{2n} = \frac{A(z) + A(-z)}{2} \quad (14.42)$$

$$\sum_{n \geq 0} a_{2n+1} z^{2n+1} = \frac{A(z) - A(-z)}{2} \quad (14.43)$$

Esto es útil si nos interesan términos alternos:

$$\begin{aligned} A_e(z) &= \sum_{n \geq 0} a_{2n} z^n \\ &= \frac{A(z^{1/2}) + A(-z^{1/2})}{2} \end{aligned} \quad (14.44)$$

$$\begin{aligned} A_o(z) &= \sum_{n \geq 0} a_{2n+1} z^n \\ &= \frac{A(z^{1/2}) - A(-z^{1/2})}{2z^{1/2}} \end{aligned} \quad (14.45)$$

Interesa extender esto a extraer uno cada  $m$  términos.

Sea  $\omega_m$  una raíz primitiva de 1, o sea por ejemplo el complejo:

$$\begin{aligned} \omega_m &= e^{\frac{2\pi i}{m}} \\ &= \cos \frac{2\pi}{m} + i \sin \frac{2\pi}{m} \end{aligned} \quad (14.46)$$

De ahora en adelante anotaremos simplemente  $\omega$  para simplificar,  $m$  quedará dado por el contexto. Los  $m$  ceros del polinomio  $x^m - 1$  son  $\omega^k$  para  $0 \leq k < m$ , ya que:

$$\begin{aligned} \omega^k &= e^{\frac{2k\pi i}{m}} \\ (\omega^k)^m &= e^{\frac{2mk\pi i}{m}} \\ &= e^{2k\pi i} \\ &= 1 \end{aligned}$$

Como  $\omega \neq 1$ , por lo discutido sobre polinomios (capítulo 9) de la factorización:

$$x^m - 1 = (x - 1)(x^{m-1} + x^{m-2} + \dots + 1)$$

vemos que:

$$\sum_{0 \leq k < m} \omega^k = 0$$

Resulta la curiosa (y útil) identidad:

$$\sum_{0 \leq k < m} \omega^{ks} = \begin{cases} 0 & \text{si } m \nmid s \\ m & \text{si } m \mid s \end{cases} \quad (14.47)$$

En vista de lo anterior, consideremos:

$$\begin{aligned} \sum_{0 \leq k < m} \omega^{-kr} A(\omega^k z) &= \sum_{0 \leq k < m} \omega^{-kr} \sum_{n \geq 0} a_n \omega^{kn} z^n \\ &= \sum_{n \geq 0} a_n z^n \sum_{0 \leq k < m} \omega^{k(n-r)} \end{aligned}$$

La suma interna es  $m$  si  $m \mid n - r$ , 0 en caso contrario. Con esto podemos construir:

$$\sum_{n \geq 0} a_{mn+r} z^{mn+r} = \frac{1}{m} \sum_{0 \leq k < m} \omega^{-kr} A(\omega^k z) \quad (14.48)$$

de donde es sencillo extraer la función generatriz de la secuencia  $\langle a_{mn+r} \rangle_{n \geq 0}$ .

## 14.6. Algunas aplicaciones combinatorias

Discutiremos algunos ejemplos, que muestran diferentes usos de funciones generatrices, algunos bastante complejos. Pueden omitirse sin pérdida de continuidad.

Se buscan las formas de llenar un canasto con  $n$  frutas si:

- El número de manzanas tiene que ser par.
- El número de plátanos debe ser un múltiplo de 5.
- Hay a lo más 4 naranjas.
- Hay a lo más 1 sandía.

La función generatriz para el número de canastos con  $n$  frutas es el producto de las funciones generatrices para cada tipo de fruta. Resultan ser series geométricas (ver el teorema 3.6). Si asumimos que  $|z| < 1$  (el valor de  $z$  no interesa), podemos usar la serie geométrica infinita. Las series son:

- Para manzanas:

$$1 + z^2 + z^4 + \dots = \frac{1}{1 - z^2}$$

- Los plátanos se representan por:

$$1 + z^5 + z^{10} + \dots = \frac{1}{1 - z^5}$$

- Para las naranjas:

$$1 + z + z^2 + z^3 + z^4 = \frac{1 - z^5}{1 - z}$$

- Las sandías aportan:

$$1 + z$$

Uniendo las anteriores, la función generatriz del número de formas de tener canastos con  $n$  frutas resulta ser:

$$C(z) = \frac{1}{1 - z^2} \cdot \frac{1}{1 - z^5} \cdot \frac{1 - z^5}{1 - z} \cdot (1 + z) = \frac{1}{(1 - z)^2}$$

Hay  $(-1)^n \binom{-2}{n} = \binom{n+1}{1} = n+1$  maneras de llenar el canasto con  $n$  frutas.

Un problema antiguo popularizado por Pólya [290] pide determinar de cuántas formas se puede dar un dólar, usando monedas de 1, 5, 10, 25 y 50 centavos. La figura 14.1 muestra una manera



Figura 14.1 – 52 centavos en monedas

de dar 52 centavos. Podemos representar una colección de monedas como el “producto” de las

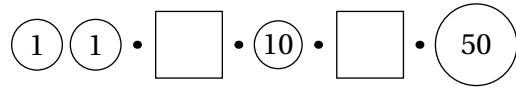


Figura 14.2 – Colección de monedas como producto

cantidades de cada denominación, véase la figura 14.2 para una manera de tener 62 centavos (el cuadrado representa una mesa vacía, ninguna moneda). Todas las cantidades posibles usando solo

$$\begin{aligned} & \square + (1) + (1)(1) + (1)(1)(1) + (1)(1)(1)(1) + \dots \\ & \square + (5) + (5)(5) + (5)(5)(5) + (5)(5)(5)(5) + \dots \end{aligned}$$

Figura 14.3 – Series para 1 o 5 centavos

monedas de 1 o 5 centavos se ilustran en la figura 14.3, donde el signo + separa las alternativas. Si “multiplicamos” las series, como muestra la figura 14.4 obviando las mesas vacías y los signos de

$$\square + (1) + (5) + (1)(1) + (1)(5) + (5)(5) + \dots$$

Figura 14.4 – Serie para combinaciones de 1 y 5 centavos

multiplicación, resultan todas las opciones para entregar una cantidad usando esas monedas. Nos

interesa el número de maneras de tener, digamos, 12 centavos, sin importar las monedas mismas. Esto lo logramos poniendo la denominación como exponente, o sea representando la moneda de 5 centavos como  $z^5$ . Al multiplicar se suman los exponentes, y al juntar los términos con el mismo exponente en su coeficiente estamos contando las maneras de tener esa suma. Las series de la figura 14.3 quedan como:

$$\begin{aligned} 1 + z + z^2 + z^3 + z^4 + \dots &= \frac{1}{1-z} \\ 1 + z^5 + z^{10} + z^{15} + z^{20} + \dots &= \frac{1}{1-z^5} \end{aligned}$$

El coeficiente de  $z^{12}$  en  $(1 + z + z^2 + \dots)(1 + z^5 + z^{10} + \dots)$  da el número de maneras de entregar 12 centavos usando solo monedas de 1 y 5 centavos:

$$\frac{1}{(1-z)(1-z^5)} = 1 + z + z^2 + z^3 + z^4 + 2z^5 + 2z^6 + 2z^7 + 2z^8 + 3z^{10} + 3z^{11} + 3z^{12} + 3z^{13} + \dots$$

Hay 3 maneras, a saber: Sólo monedas de 1 centavo, una moneda de 5 centavos y siete de 1 centavo, o dos de 5 y dos de 1.

Las cantidades que se pueden entregar con la moneda de denominación  $d$  se representan por:

$$1 + z^d + z^{2d} + z^{3d} + \dots = \frac{1}{1-z^d}$$

Como combinar denominaciones corresponde a multiplicar las series, para el conjunto completo de denominaciones tenemos la función generatriz:

$$P(z) = \frac{1}{(1-z)(1-z^5)(1-z^{10})(1-z^{25})(1-z^{50})} \quad (14.49)$$

El valor buscado es el coeficiente de  $z^{100}$  en (14.49).

No es viable expandir (14.49) hasta  $z^{100}$ , veremos un camino alternativo. La serie (14.49) es el producto de cinco factores, conocemos el primero (la serie geométrica) e iremos adicionando los demás uno a uno. Supongamos que ya tenemos el producto de los dos primeros factores:

$$\frac{1}{(1-z)(1-z^5)} = a_0 + a_1 z + a_2 z^2 + \dots$$

y queremos añadir el tercero:

$$\frac{1}{(1-z)(1-z^5)(1-z^{10})} = b_0 + b_1 z + b_2 z^2 + \dots$$

Multiplicando por  $1 - z^{10}$  vemos que:

$$(b_0 + b_1 z + b_2 z^2 + \dots)(1 - z^{10}) = a_0 + a_1 z + a_2 z^2 + \dots$$

Comparando coeficientes (es  $b_n = 0$  si  $n < 0$ ):

$$b_n = b_{n-10} + a_n$$

Esta relación permite calcular los  $b_n$  si ya conocemos los  $a_n$ , y obtenemos la serie completa en cuatro pasos similares al que discutimos recién. El cuadro 14.1 resume el cálculo hasta 50 centavos (solo se dan los valores necesarios para obtener  $p_{50} = 50$ ), el amable lector completará el cuadro y verificará que hay un total de 292 maneras de dar un dólar en monedas. En el clásico de Graham,

$n =$	0	5	10	15	20	25	30	35	40	45	50
$(1-z)^{-1}$	1	1	1	1	1	1	1	1	1	1	1
$(1-z^5)^{-1}$	1	2	3	4	5	6	7	8	9	10	11
$(1-z^{10})^{-1}$	1	2	4	6	9	12	16		25		36
$(1-z^{25})^{-1}$	1					13					49
$(1-z^{50})^{-1}$	1										50

Cuadro 14.1 – Tabla para calcular  $p_{50}$ 

Knuth y Patashnik [150] continúan este desarrollo. Aprovechan la forma especial de las recurrencias resultantes y obtienen una fórmula cerrada para  $p_n$ .

Un problema clásico propuesto por Sylvester en 1884 es el siguiente: Si solo se tienen estampillas de 5 y 17 centavos, ¿cuál es el máximo monto que *no* se puede franquear con ellas?

La solución de Bogomolny [48] muestra cómo representar conjuntos. En lo que sigue, usaremos congruencias y algunos resultados de teoría de números, capítulo 7. Para generalizar, digamos que los montos de las estampillas son  $p$  y  $q$ , ambos mayores a 1 y relativamente primos. Si no fueran relativamente primos, habrían infinitos valores imposibles de representar (solo es posible representar múltiplos de  $\gcd(p, q)$  mediante expresiones de la forma  $ap + bq$ , véase la sección 7.3).

Por la identidad de Bézout (ecuación (7.7)) sabemos que hay  $u, v$  tales que  $up - vq = 1$ , sin pérdida de generalidad podemos suponer que  $u, v > 0$ . Si tomamos  $xq$  para algún  $x$  por determinar, para  $1 \leq k < q$  podemos escribir:

$$xq + k = xq + k(up - vq) = kup + (x - kv)q$$

El primer término es siempre positivo, interesa acotar  $kv$  para asegurar que ambos sean no negativos y  $xq+k$  siempre sea representable. Como  $v$  es el inverso de  $q$  en  $\mathbb{Z}_p$  es  $1 \leq v < p$ , y por tanto al menos a partir de  $(q-1)(p-1)q$  todos son representables.

Formemos la familia de secuencias aritméticas  $f_a = \langle ap + bq \rangle_{b \geq 0}$ :

$$f_0 = \langle 0+0, 0+q, 0+2q, 0+3q, \dots \rangle$$

$$f_1 = \langle p+0, p+q, p+2q, p+3q, \dots \rangle$$

$$f_2 = \langle 2p+0, 2p+q, 2p+2q, 2p+3q, \dots \rangle$$

⋮

$$f_{q-1} = \langle (q-1)p+0, (q-1)p+q, (q-1)p+2q, (q-1)p+3q, \dots \rangle$$

La idea es que la secuencia  $f_k$  representa los franqueos posibles con  $k$  estampillas de  $p$  centavos y algún número de estampillas de  $q$  centavos. Como  $\gcd(p, q) = 1$ , estas secuencias son disjuntas, y cubren todas las posibilidades de  $ap + bq$  con  $a, b \geq 0$ . Los elementos de  $f_a$  son congruentes módulo  $q$ , siendo  $p$  y  $q$  relativamente primos el conjunto  $\{ap \bmod q : 0 \leq a < q\}$  es simplemente  $\{k : 0 \leq k < q\}$ . Si las secuencias hubiesen comenzado con los residuos respectivos, las secuencias cubrirían todo  $\mathbb{N}$ ; pero como  $f_a$  parte de  $ap$  la unión de las secuencias deja espacios al comienzo. Interesa hallar el máximo número que no aparece en la unión, que llamaremos  $g(p, q)$ .

Los elementos de la unión de las secuencias indicadas son los exponentes de la siguiente función generatriz (los coeficientes de la suma son todos uno, no hay intersección entre las secuencias):

$$f(z) = \frac{1}{1-z^q} (1+z^p+z^{2p}+\dots+z^{(q-1)p}) = \frac{1-z^{pq}}{(1-z^p)(1-z^q)}$$

Por el otro lado, el conjunto completo de los enteros no negativos se representa por:

$$h(z) = 1+z+z^2+z^3+\dots = \frac{1}{1-z}$$

La diferencia entre las dos es un polinomio, cuyos exponentes indican los números que no se pueden representar:

$$h(z) - f(z) = \frac{1}{1-z} - \frac{1-z^{pq}}{(1-z^p)(1-z^q)} = \frac{(1-z^p)(1-z^q) - (1-z)(1-z^{pq})}{(1-z)(1-z^p)(1-z^q)} \quad (14.50)$$

Restar el grado del denominador del grado del numerador da el grado del polinomio:

$$g(p, q) = (pq + 1) - (p + q + 1) = pq - p - q \quad (14.51)$$

En el caso específico indicado el máximo valor imposible de franquear franquearse es

$$g(5, 17) = 5 \cdot 17 - 5 - 17 = 63$$

Otra pregunta es cuántos son los valores que no pueden representarse, que no es más que la suma de los coeficientes del polinomio (14.50), o sea, el valor del mismo evaluado en  $z = 1$ . Aplicando l'Hôpital tres veces a (14.50) entrega:

$$\lim_{z \rightarrow 1} (h(z) - f(z)) = \frac{pq - p - q + 1}{2} = \frac{g(p, q) + 1}{2} \quad (14.52)$$

Los no representables resultan ser 32 en nuestro caso específico.

Este es el caso particular  $n = 2$  del problema de Frobenius, determinar para un conjunto de naturales relativamente primos  $\{a_1, a_2, \dots, a_n\}$  cuál es el máximo entero que no puede representarse como combinación lineal con coeficientes naturales. A este número se le llama el *número de Frobenius* del conjunto, y se anota  $g(a_1, \dots, a_n)$ . Para  $n > 2$  no se conocen fórmulas generales, solo soluciones en casos particulares. A pesar de parecer muy especializado, este problema y variantes aparecen en muchas aplicaciones. Un resumen reciente de la teoría y algoritmos presenta Ramírez Alfonsín [298].

## 14.7. Manipulación de series

Sea una secuencia  $\langle a_n \rangle_{n \geq 0} = \langle a_0, a_1, a_2, \dots, a_n, \dots \rangle$ . La *función generatriz* (ordinaria) de la secuencia es la serie de potencias:

$$A(z) = \sum_{0 \leq n} a_n z^n$$

Anotaremos  $A(z) \xrightarrow{\text{ogf}} \langle a_n \rangle_{n \geq 0}$  en este caso (*ogf* es por *Ordinary Generating Function*).

La *función generatriz exponencial* de la secuencia es la serie:

$$\hat{A}(z) = \sum_{0 \leq n} a_n \frac{z^n}{n!}$$

Anotaremos  $\hat{A}(z) \xrightarrow{\text{egf}} \langle a_n \rangle_{n \geq 0}$  en este caso (*egf* es por *Exponential Generating Function*).

Por comodidad, a veces escribiremos estas relaciones con la función generatriz al lado derecho.

### 14.7.1. Reglas OGF

Las propiedades siguientes de funciones generatrices ordinarias son directamente las definiciones del caso o son muy simples de demostrar, sus justificaciones detalladas quedarán de ejercicios.

**Linealidad:** Si  $A(z) \xrightarrow{\text{ogf}} \langle a_n \rangle_{n \geq 0}$  y  $B(z) \xrightarrow{\text{ogf}} \langle b_n \rangle_{n \geq 0}$ , y  $\alpha$  y  $\beta$  son constantes, entonces:

$$\alpha A(z) + \beta B(z) \xrightarrow{\text{ogf}} \langle \alpha a_n + \beta b_n \rangle_{n \geq 0}$$

**Secuencia desplazada a la izquierda:** Si  $A(z) \xrightarrow{\text{ogf}} \langle a_n \rangle_{n \geq 0}$ , entonces:

$$\frac{A(z) - a_0 - a_1 z - \cdots - a_{k-1} z^{k-1}}{z^k} \xrightarrow{\text{ogf}} \langle a_{n+k} \rangle_{n \geq 0}$$

**Multiplicar por  $n$ :** Consideremos:

$$\begin{aligned} A(z) &\xrightarrow{\text{ogf}} \langle a_n \rangle_{n \geq 0} \\ z \frac{d}{dz} A(z) &\xrightarrow{\text{ogf}} \langle n a_n \rangle_{n \geq 0} \end{aligned}$$

Esta operación se expresa en términos del operador  $zD$  (acá D es por derivada, para abreviar). Además:

$$(zD)^2 A(z) = zD(zDA(z)) \xrightarrow{\text{ogf}} \langle n^2 a_n \rangle_{n \geq 0}$$

Nótese que  $(zD)^2 = zD + z^2 D^2$  es diferente de  $z^2 D^2$ .

**Multiplicar por un polinomio en  $n$ :** Si  $p(n)$  es un polinomio, usando el operador  $zD$  varias veces para potencias de  $n$  y por linealidad:

$$p(zD) A(z) \xrightarrow{\text{ogf}} \langle p(n) a_n \rangle_{n \geq 0}$$

**Convolución:** Si  $A(z) \xrightarrow{\text{ogf}} \langle a_n \rangle_{n \geq 0}$  y  $B(z) \xrightarrow{\text{ogf}} \langle b_n \rangle_{n \geq 0}$  entonces:

$$A(z) \cdot B(z) \xrightarrow{\text{ogf}} \left\langle \sum_{0 \leq k \leq n} a_k b_{n-k} \right\rangle_{n \geq 0}$$

Sea  $k$  un entero positivo y  $A(z) \xrightarrow{\text{ogf}} \langle a_n \rangle_{n \geq 0}$ , entonces:

$$(A(z))^k \xrightarrow{\text{ogf}} \left\langle \sum_{n_1+n_2+\cdots+n_k=n} (a_{n_1} \cdot a_{n_2} \cdots a_{n_k}) \right\rangle_{n \geq 0}$$

Vale la pena tener presente el caso especial:

$$(A(z))^2 \xrightarrow{\text{ogf}} \left\langle \sum_{0 \leq i \leq n} a_i a_{n-i} \right\rangle_{n \geq 0}$$

**Sumas parciales:** Supongamos:

$$A(z) \xrightarrow{\text{ogf}} \langle a_n \rangle_{n \geq 0}$$

Podemos escribir:

$$\sum_{0 \leq k \leq n} a_k = \sum_{0 \leq k \leq n} 1 \cdot a_k$$

Esto no es más que la convolución de las secuencias  $\langle 1 \rangle_{n \geq 0}$  y  $\langle a_n \rangle_{n \geq 0}$ , y la función generatriz de la primera es nuestra vieja conocida, la serie geométrica, con lo que:

$$\frac{A(z)}{1-z} \xrightarrow{\text{ogf}} \left\langle \sum_{0 \leq k \leq n} a_k \right\rangle_{n \geq 0} \tag{14.53}$$

Un ejemplo importante da el contar las secuencias de paréntesis balanceados de largo  $2n$ . Anotaremos  $C_n$  para el número de *secuencias balanceadas* de  $2n$  paréntesis. Es claro que  $C_0 = 1$ , hay una única secuencia de largo cero. Vemos que en secuencias balanceadas el primer paréntesis (de haberlo) se cierra, luego de lo cual puede venir otra secuencia balanceada. Llamemos *perfecta* a una secuencia cuyo primer paréntesis se cierra con el último paréntesis de la secuencia. Anotemos  $P_n$  para el número de secuencias perfectas de largo  $2n$ . Claramente  $P_0 = 0$  (la secuencia vacía no tiene paréntesis inicial a cerrar), y  $P_1 = 1$ . La descomposición de secuencias balanceadas en una secuencia perfecta y una balanceada cuyos largos suman  $2n$  nos da la recurrencia:

$$C_n = \sum_{1 \leq k \leq n} P_k C_{n-k} \quad C_0 = 1 \quad (14.54)$$

Hay una biyección entre secuencias perfectas de largo  $2n+2$  y secuencias balanceadas de largo  $2n$ : Si a una secuencia perfecta le eliminamos el primer y último paréntesis, obtenemos una secuencia balanceada; si a una secuencia balanceada la rodeamos con paréntesis, el resultado es una secuencia perfecta. O sea:

$$P_{n+1} = C_n \quad (14.55)$$

Esto con la recurrencia (14.54) deducida antes da:

$$C_n = \sum_{1 \leq k \leq n} C_{k-1} C_{n-k} \quad C_0 = 1 \quad (14.56)$$

Escribamos la recurrencia (14.56) para que nos entregue  $C_{n+1}$ , y ajustemos los índices de la sumatoria, obteniendo una convolución:

$$C_{n+1} = \sum_{0 \leq k \leq n} C_k C_{n-k} \quad C_0 = 1 \quad (14.57)$$

Para resolver la recurrencia (14.57) definimos la función generatriz:

$$C(z) = \sum_{n \geq 0} C_n z^n \quad (14.58)$$

Aplicando las propiedades, como el lado izquierdo es un desplazamiento y el derecho la convolución de  $\langle C_n \rangle_{n \geq 0}$  consigo misma:

$$\frac{C(z) - C_0}{z} = C^2(z)$$

que con  $C_0 = 1$  se simplifica a la cuadrática:

$$zC^2(z) - C(z) + 1 = 0 \quad (14.59)$$

La solución a la cuadrática (14.59) es:

$$C(z) = \frac{1 \pm \sqrt{1 - 4z}}{2z} \quad (14.60)$$

Debemos determinar el signo correcto. La expresión (14.60) es indeterminada en  $z = 0$ . En todo caso, debiera ser  $C(0) = C_0 = 1$ , y vemos que:

$$\begin{aligned} \lim_{z \rightarrow 0} \frac{1 + \sqrt{1 - 4z}}{2z} &= \infty \\ \lim_{z \rightarrow 0} \frac{1 - \sqrt{1 - 4z}}{2z} &= 1 \end{aligned}$$

Vale decir:

$$C(z) = \frac{1 - \sqrt{1 - 4z}}{2z} \quad (14.61)$$

Para obtener los coeficientes de (14.61) expandimos la raíz en serie usando el teorema del binomio:

$$\begin{aligned} (1 - 4z)^{1/2} &= \sum_{n \geq 0} \binom{1/2}{n} (-4z)^n \\ &= 1 + \sum_{n \geq 1} \frac{(-1)^{n-1}}{2^{2n-1} \cdot n} \cdot \binom{2n-2}{n-1} \cdot (-1)^n 2^{2n} z^n \\ &= 1 - \sum_{n \geq 1} \frac{2}{n} \binom{2n-2}{n-1} z^n \\ 1 - (1 - 4z)^{1/2} &= \sum_{n \geq 1} \frac{2}{n} \binom{2n-2}{n-1} z^n \\ &= 2z \sum_{n \geq 0} \frac{1}{n+1} \binom{2n}{n} z^n \end{aligned}$$

con lo que finalmente:

$$C(z) = \sum_{n \geq 0} \frac{1}{n+1} \binom{2n}{n} z^n$$

y los coeficientes son:

$$C_n = \frac{1}{n+1} \binom{2n}{n} \quad (14.62)$$

Los coeficientes de (14.61) se conocen como *números de Catalan*. La serie (14.61) aparece con regularidad, al igual que los coeficientes (14.62).

Un ejemplo clásico (ver por ejemplo Knuth [218]) es el análisis de búsqueda binaria. Supongamos que contamos con un arreglo ordenado de  $n$  claves  $k_1 < k_2 < \dots < k_n$ , dada una clave  $K$  nos interesa identificar  $1 \leq j \leq n$  tal que  $K = k_j$  (búsqueda exitosa). Búsqueda binaria compara  $K$  con el elemento medio, en  $r = \lfloor (n+1)/2 \rfloor$ . Si  $K = k_r$ , estamos listos. En caso contrario, si  $K < k_r$  seguimos la búsqueda en  $k_1, \dots, k_{r-1}$ , mientras que si  $K > k_r$  seguimos la búsqueda en  $k_{r+1}, \dots, k_n$ . Interesa el número promedio  $b_n$  de comparaciones en búsquedas exitosas, si  $K$  se elige al azar. Hay un único elemento que puede encontrarse con una comparación, el elemento medio, y dos que pueden encontrarse con dos comparaciones. En general son  $2^{r-1}$  los elementos que se hallan con exactamente  $r$  comparaciones, hasta llegar a un máximo de  $1 + \lfloor \log_2 n \rfloor$  comparaciones. Si sumamos el número de comparaciones para cada una de las  $n$  claves obtenemos el número promedio de comparaciones:

$$b_n = \frac{1}{n} (1 + 2 + 2 + 3 + 3 + 3 + \dots + (1 + \lfloor \log_2 n \rfloor))$$

Para calcular la suma, consideraremos la secuencia infinita  $\langle 0, 1, 2, 2, 3, 3, 3, \dots \rangle$ , que se obtiene de sumar secuencias  $\langle 0, 1, 1, \dots \rangle$ ,  $\langle 0, 0, 1, 1, \dots \rangle$ , y así sucesivamente, donde la  $k$ -ésima secuencia comienza con  $2^k$  ceros. Podemos representar la secuencia como los coeficientes de la serie:

$$L(z) = \frac{z}{1-z} + \frac{z^2}{1-z} + \dots + \frac{z^{2^k}}{1-z} + \dots = \sum_{k \geq 0} \frac{z^{2^k}}{1-z}$$

Nos interesan sumas parciales, por lo que usamos (14.53):

$$\begin{aligned}
 nb_n &= [z^n] \frac{1}{1-z} \sum_{k \geq 0} \frac{z^{2^k}}{1-z} \\
 &= [z^n] \sum_{k \geq 0} \frac{z^{2^k}}{(1-z)^2} \\
 &= \sum_{k \geq 0} \left[ z^{n-2^k} \right] (1-z)^{-2} \\
 &= \sum_{k \geq 0} \binom{n-2^k+1}{n-2^k} \\
 &= \sum_{0 \leq k \leq \lfloor \log_2 n \rfloor} (n+1-2^k) \\
 &= (n+1)(\lfloor \log_2 n \rfloor + 1) - \sum_{0 \leq k \leq \lfloor \log_2 n \rfloor} 2^k \\
 &= (n+1)\lfloor \log_2 n \rfloor + n - 2^{\lfloor \log_2 n \rfloor + 1} + 2
 \end{aligned}$$

Manipulaciones formales dan directamente lo que buscamos.

### 14.7.2. Reglas EGF

Las siguientes resumen propiedades de las funciones generatrices exponenciales. Son simples de demostrar, y las justificaciones que no se dan acá quedarán de ejercicios.

**Linealidad:** Si  $\widehat{A}(z) \xrightarrow{\text{egf}} \langle a_n \rangle_{n \geq 0}$  y  $\widehat{B}(z) \xrightarrow{\text{egf}} \langle b_n \rangle_{n \geq 0}$ , y  $\alpha$  y  $\beta$  son constantes, entonces:

$$\alpha \widehat{A}(z) + \beta \widehat{B}(z) \xrightarrow{\text{egf}} \langle \alpha a_n + \beta b_n \rangle_{n \geq 0}$$

**Secuencia desplazada a la izquierda:** Si  $\widehat{A}(z) \xrightarrow{\text{egf}} \langle a_n \rangle_{n \geq 0}$ , entonces, usando nuevamente D para el operador derivada:

$$D^k \widehat{A}(z) \xrightarrow{\text{egf}} \langle a_{n+k} \rangle_{n \geq 0}$$

**Multiplicación por un polinomio en  $n$ :** Si es  $\widehat{A}(z) \xrightarrow{\text{egf}} \langle a_n \rangle_{n \geq 0}$ , y  $p$  es un polinomio, entonces:

$$p(zD) \widehat{A}(z) \xrightarrow{\text{egf}} \langle p(n) a_n \rangle_{n \geq 0}$$

Es la misma que en funciones generatrices ordinarias, ya que la operación  $zD$  no altera el exponente en  $z^n$ .

**Convolución binomial:** Si  $\widehat{A}(z) \xrightarrow{\text{egf}} \langle a_n \rangle_{n \geq 0}$  y  $\widehat{B}(z) \xrightarrow{\text{egf}} \langle b_n \rangle_{n \geq 0}$  entonces:

$$\begin{aligned}
 \widehat{A}(z) \cdot \widehat{B}(z) &= \sum_{n \geq 0} \left( \sum_{0 \leq k \leq n} \frac{a_k}{k!} \frac{b_{n-k}}{(n-k)!} \right) z^n \\
 &= \sum_{n \geq 0} \left( \sum_{0 \leq k \leq n} \binom{n}{k} a_k b_{n-k} \right) \frac{z^n}{n!}
 \end{aligned}$$

Vale decir:

$$\widehat{A}(z) \cdot \widehat{B}(z) \xrightarrow{\text{egf}} \left\langle \sum_{0 \leq k \leq n} \binom{n}{k} a_k b_{n-k} \right\rangle_{n \geq 0}$$

**Términos individuales:** Es fácil ver que si  $\widehat{A}(z) \xrightarrow{\text{egf}} \langle a_n \rangle_{n \geq 0}$  entonces:

$$a_n = \widehat{A}^{(n)}(0)$$

Esto en realidad no es más que el teorema de Maclaurin.

### 14.8. El truco $zD\log$

Los logaritmos ayudan a simplificar expresiones con exponentiales y potencias. Pero terminamos con el logaritmo de una suma si el argumento es una serie, que es algo bastante feo de contemplar. Eliminar el logaritmo se logra derivando:

$$\frac{d \ln(A)}{dz} = \frac{A'}{A}$$

Esto es mucho más decente. Multiplicamos por  $z$  para reponer la potencia “perdida” al derivar.

**Receta:**

1. Aplicar  $zD\ln$ .
2. Multiplicar para eliminar fracciones.
3. Igualar coeficientes.

### 14.9. Ejemplos de manipulación de series

Un ejemplo inicial de aplicación de las ideas planteadas es obtener la suma de los primeros  $N$  cuadrados. Por la suma de la serie geométrica, teorema 3.6:

$$\begin{aligned} 1 + z + z^2 + \dots + z^N &= \frac{1 - z^{N+1}}{1 - z} \\ (zD)^2 (1 + z + z^2 + \dots + z^N) &= (zD)^2 \frac{1 - z^{N+1}}{1 - z} \\ (0^2 + 1^2 z + 2^2 z^2 + \dots + N^2 z^N)|_{z=1} &= \lim_{z \rightarrow 1} (zD)^2 \frac{1 - z^{N+1}}{1 - z} \end{aligned}$$

Nótese que todas las expresiones involucradas son polinomios, con lo que cuestiones de convergencia y validez de las operaciones no son problema.

El resto es derivar, calcular límites y álgebra:

$$\sum_{1 \leq k \leq N} k^2 = \frac{N(N+1)(2N+1)}{6}$$

La misma idea sirve para otras potencias.

Otra alternativa es usar las propiedades de funciones generatrices ordinarias. Primero obtener la función generatriz de los cuadrados:

$$\begin{aligned} \sum_{N \geq 0} N^2 z^N &= (zD)^2 \frac{1}{1 - z} \\ &= \frac{z(1+z)}{(1-z)^3} \end{aligned}$$

La función generatriz de sumas parciales de lo anterior es así:

$$\begin{aligned} \sum_{N \geq 0} \left( \sum_{0 \leq k \leq N} k^2 \right) z^N &= \frac{z(1+z)}{(1-z)^4} \\ &= \frac{2}{(1-z)^4} - \frac{3}{(1-z)^3} + \frac{1}{(1-z)^2} \end{aligned}$$

con lo que los coeficientes son:

$$\begin{aligned} \sum_{0 \leq k \leq N} k^2 &= 2 \cdot (-1)^N \binom{-4}{N} - 3 \cdot (-1)^N \binom{-3}{N} + (-1)^N \binom{-2}{N} \\ &= 3 \binom{N+3}{3} - 2 \binom{N+2}{2} + \binom{N+1}{1} \\ &= \frac{N(N+1)(2N+1)}{6} \end{aligned}$$

La maquinaria de funciones generatrices permite obtener en forma rutinaria resultados que de otra forma serían complicados de sospechar, y luego deberían ser demostrados por inducción. La operatoria suele ser tediosa, es útil tener un programa de álgebra simbólica (como `maxima` [251]) a la mano.

Otra aplicación es obtener la serie para  $A(z)^\alpha$ , una potencia arbitraria ( $\alpha \in \mathbb{C}$ ) de una serie  $A(z)$  que ya conocemos. Sea entonces:

$$A(z) = \sum_{n \geq 0} a_n z^n$$

donde  $a_0 \neq 0$ . Definimos:

$$B(z) = A^\alpha(z) = \sum_{n \geq 0} b_n z^n$$

Aplicando la receta  $zD\log$  obtenemos:

$$\begin{aligned} \frac{zB'(z)}{B(z)} &= \alpha z \frac{A'(z)}{A(z)} \\ zB'(z) \cdot A(z) &= \alpha z A'(z) \cdot B(z) \\ \left( \sum_{n \geq 0} n b_n z^n \right) \cdot \left( \sum_{n \geq 0} a_n z^n \right) &= \alpha \left( \sum_{n \geq 0} n a_n z^n \right) \cdot \left( \sum_{n \geq 0} b_n z^n \right) \\ \sum_{n \geq 0} \left( \sum_{0 \leq k \leq n} k b_k a_{n-k} \right) z^n &= \sum_{n \geq 0} \left( \sum_{0 \leq k \leq n} \alpha k a_k b_{n-k} \right) z^n \end{aligned}$$

De acá sigue, igualando coeficientes:

$$\sum_{0 \leq k \leq n} a_k (n-k) b_{n-k} = \sum_{0 \leq k \leq n} \alpha k a_k b_{n-k}$$

Nuevamente, esto involucra solo finitas operaciones. Finalmente:

$$\sum_{0 \leq k \leq n} (a_k (n-k) b_{n-k} - \alpha k a_k b_{n-k}) = 0$$

$$\sum_{0 \leq k \leq n} (n-k-\alpha k) a_k b_{n-k} = 0$$

de donde resulta al separar el término con  $k = 0$ :

$$\begin{aligned} na_0 b_n &= - \left( \sum_{1 \leq k \leq n} (n - k - \alpha k) a_k b_{n-k} \right) \\ b_n &= - \frac{1}{na_0} \sum_{1 \leq k \leq n} (n - k - \alpha k) a_k b_{n-k} \end{aligned}$$

Para comenzar la recurrencia, usamos:

$$b_0 = a_0^\alpha$$

Compárese esta recurrencia con la expresión explícita para una potencia entera de una serie que derivamos al discutir convoluciones.

Nos interesa hallar las sumas de potencias:

$$S_m(n) = \sum_{1 \leq k \leq n-1} k^m \quad (14.63)$$

El desarrollo sigue a Aigner [5]. Definamos la función generatriz exponencial:

$$\widehat{S}_n(z) = \sum_{m \geq 0} S_m(n) \frac{z^m}{m!} \quad (14.64)$$

$$\begin{aligned} &= \sum_{1 \leq k \leq n-1} \sum_{m \geq 0} \frac{k^m z^m}{m!} \\ &= \sum_{1 \leq k \leq n-1} e^{kz} \\ &= \frac{e^{nz} - 1}{e^z - 1} \end{aligned} \quad (14.65)$$

Tenemos casi la función generatriz exponencial de las potencias de  $n$ :

$$\begin{aligned} \widehat{P}_n(z) &= \sum_{m \geq 0} n^m \frac{z^m}{m!} \\ &= e^{nz} \end{aligned} \quad (14.66)$$

Lamentablemente la serie  $e^z - 1$  no tiene recíproco, ya que su término constante se anula. Pero podemos escribir:

$$(\widehat{P}_n(z) - 1)\widehat{B}(z) = z\widehat{S}_n(z)$$

donde:

$$\widehat{B}(z) = \frac{z}{e^z - 1} \quad (14.67)$$

cuyos coeficientes son los *números de Bernoulli*:

$$\begin{aligned} \widehat{B}(z) &= \sum_{n \geq 0} B_n \frac{z^n}{n!} \\ &= 1 - \frac{1}{2}z + \frac{1}{6}\frac{z^2}{2!} - \frac{1}{30}\frac{z^4}{4!} + \frac{1}{42}\frac{z^6}{6!} - \frac{1}{30}\frac{z^8}{8!} + \frac{5}{66}\frac{z^{10}}{10!} - \frac{691}{2130}\frac{z^{12}}{12!} + \frac{7}{6}\frac{z^{14}}{14!} - \dots \end{aligned}$$

Podemos calcularlos usando:

$$\widehat{B}(z)(e^z - 1) = z$$

$$\sum_{0 \leq k \leq n} \binom{n}{k} B_k \frac{1}{(n-k+1)!} = [n=1]$$

de donde obtenemos la recurrencia:

$$B_m = [m=1] - \sum_{0 \leq k \leq m-1} \binom{m}{k} \frac{B_k}{m-k+1} \quad (14.68)$$

Volvamos a nuestro objetivo:

$$\sum_{m \geq 0} S_m(n) \frac{z^{m+1}}{m!} = \sum_{m \geq 0} z^m \sum_{0 \leq k \leq m} \binom{m}{k} \frac{(nz)^{m-k}}{(m-k)!} B_k$$

Comparando coeficientes de  $z^{m+1}$  y simplificando:

$$S_m(n) = \frac{1}{m+1} \sum_{0 \leq k \leq m} (-1)^k \binom{m+1}{k} B_k n^{m+1-k} \quad (14.69)$$

Los números de Bernoulli (14.67) son importantes, los veremos nuevamente en el capítulo 18.

## 14.10. Funciones generatrices en combinatoria

De nuevo la Competencia de Ensayos de la Universidad de Miskatonic. Para simplificar notación, sea  $a_r = b_{2r+1}$ , con condición inicial  $a_0 = b_1 = 1$ . Resulta:

$$a_r = a_{r-1} + r + 1 \quad (14.70)$$

Llamemos  $A(z)$  a la función generatriz ordinaria de la secuencia  $\langle a_r \rangle_{r \geq 0}$ :

$$A(z) = \sum_{r \geq 0} a_r z^r$$

La recurrencia (14.70) es incómoda de manejar como está escrita, primero ajustamos los índices para no hacer referencia a términos previos:

$$a_{r+1} - a_r = r + 2 \quad (14.71)$$

Las funciones generatrices de los términos al lado izquierdo de la recurrencia (14.71) son:

$$\langle a_{r+1} \rangle_{r \geq 0} \xrightarrow{\text{ogf}} \frac{A(z) - a_0}{z} = \frac{A(z) - 1}{z} \quad \langle a_r \rangle_{r \geq 0} \xrightarrow{\text{ogf}} A(z)$$

Necesitamos además la función generatriz de la secuencia  $r+2$  que aparece al lado derecho, que no es más que la secuencia  $\langle 1 \rangle_{r \geq 0}$  multiplicada por el polinomio  $r+2$ , con lo que:

$$\langle r+2 \rangle_{r \geq 0} \xrightarrow{\text{ogf}} (zD+2) \frac{1}{1-z} = \frac{z}{(1-z)^2} + \frac{2}{1-z}$$

Combinando las anteriores, tenemos:

$$\frac{A(z) - 1}{z} - A(z) = \frac{z}{(1-z)^2} + \frac{2}{1-z}$$

Despejando  $A(z)$  se tiene:

$$A(z) = \frac{1}{(1-z)^3}$$

y los coeficientes del caso son inmediatos:

$$a_r = (-1)^r \binom{-3}{r} = \binom{2+r}{2} = \frac{(r+2)(r+1)}{2}$$

Nuevamente resulta:

$$b_{2r+1} = \frac{(r+2)(r+1)}{2}$$

Esta derivación es aún más simple que la anterior. Siempre que sea posible se deben usar las propiedades de funciones generatrices, debe recurrirse a la receta general dada anteriormente solo cuando no es claro cómo aplicarlas.

Podemos igualmente intentar con la función generatriz exponencial:

$$\hat{A}(z) = \sum_{r \geq 0} a_r \frac{z^r}{r!}$$

Aplicando las propiedades respectivas a (14.71): (refiérase a la sección 14.7.2 y a la serie exponencial (14.38)):

$$\begin{aligned}\hat{A}'(z) - \hat{A}(z) &= \left( z \frac{d}{dz} + 2 \right) e^z \\ &= z e^z + 2 e^z\end{aligned}$$

Como condición inicial tenemos:

$$\hat{A}(0) = a_0 = 1$$

La solución de la ecuación diferencial es:

$$\hat{A}(z) = \frac{e^z}{2} (z^2 + 4z + 2)$$

Ahora tenemos dos caminos posibles: Expresar la solución mediante las propiedades, o calcular los términos mediante la expansión en serie. Para aplicar las propiedades, notamos:

$$\frac{1}{2} (z^2 + 4z + 2) e^z = \frac{1}{2} (z^2 D^2 + 4zD + 2) e^z$$

Además:

$$\begin{aligned}(zD)^2 &= z^2 D^2 + zD \\ z^2 D^2 + 4zD + 2 &= (zD)^2 + 3zD + 2\end{aligned}$$

O sea:

$$\hat{A}(z) = \frac{1}{2} ((zD)^2 + 3zD + 2) e^z$$

Esto corresponde a:

$$b_{2r+1} = a_r = \frac{1}{2}(r^2 + 3r + 2) = \frac{(r+2)(r+1)}{2}$$

El otro camino es:

$$\begin{aligned} e^z \frac{z^2 + 4z + 2}{2} &= \sum_{r \geq 0} \left( \frac{z^{r+2}}{2r!} + \frac{2z^{r+1}}{r!} + \frac{z^r}{r!} \right) \\ &= \frac{1}{2} \sum_{r \geq 2} \frac{z^r}{(r-2)!} + 2 \sum_{r \geq 1} \frac{z^r}{(r-1)!} + \sum_{r \geq 0} \frac{z^r}{r!} \\ &= \sum_{r \geq 0} \left( \frac{r(r-1)}{2} + 2r + 1 \right) \frac{z^r}{r!} \\ &= \sum_{r \geq 0} \frac{(r+2)(r+1)}{2} \frac{z^r}{r!} \end{aligned}$$

y nuevamente:

$$b_{2r+1} = a_r = \frac{(r+2)(r+1)}{2}$$

Si contamos el número de maneras de crear palabras de  $n$  letras usando únicamente A y B, es claro que esto corresponde a elegir  $k$  posiciones para las A (y dejar las  $n - k$  restantes a llenar por B). Si hay  $a_k$  maneras de tener  $k$  letras A y  $b_k$  maneras de tener  $k$  letras B, vemos que el total es:

$$\sum_{0 \leq k \leq n} \binom{n}{k} a_k b_{n-k}$$

Una convolución binomial. Deberemos multiplicar las funciones generatrices exponenciales de las secuencias  $\langle a_n \rangle_{n \geq 0}$  y  $\langle b_n \rangle_{n \geq 0}$  para obtener la función generatriz exponencial del número de palabras posibles. Por ejemplo, si la restricción es que el número de A es par y no hay restricciones para las B, las funciones generatrices respectivas son:

$$\widehat{A}(z) = 1 + \frac{z^2}{2!} + \frac{z^4}{4!} + \dots = \cosh z \quad \widehat{B}(z) = 1 + \frac{z}{1!} + \frac{z^2}{2!} + \dots = e^z$$

Resulta:

$$n! [z^n] e^z \cosh z = n! [z^n] \frac{e^{2z} + 1}{2} = \frac{n!}{2} \left( \frac{2^n}{n!} + 1 \right) = 2^{n-1} + \frac{n!}{2}$$

Consideremos nuevamente al fatídico BOOKKEEPER. Si nos preguntamos cuántos multisubconjuntos de  $n$  de sus letras pueden formarse, la respuesta viene de usar funciones generatrices ordinarias. Cada letra queda representada como sigue:

- B:  $1 + z$
- E:  $1 + z + z^2 + z^3$
- K:  $1 + z + z^2$
- O:  $1 + z + z^2$
- P:  $1 + z$
- R:  $1 + z$

El producto da el número de multisubconjuntos como coeficientes:

$$(1+z)^3(1+z+z^2)^2(1+z+z^2+z^3) = 1+6z+18z^2+36z^3+53z^4+60z^5+53z^6+36z^7+18z^8+6z^9+z^{10}$$

Si buscamos cuántas palabras de  $n$  letras se pueden formar, recurrimos a funciones generatrices exponenciales. La función generatriz exponencial de la secuencia buscada es la convolución binomial entre las siguientes:

$$\begin{aligned} B &: 1 + \frac{z}{1!} \\ E &: 1 + \frac{z}{1!} + \frac{z^2}{2!} + \frac{z^3}{3!} \\ K &: 1 + \frac{z}{1!} + \frac{z^2}{2!} \\ O &: 1 + \frac{z}{1!} + \frac{z^2}{2!} \\ P &: 1 + \frac{z}{1!} \\ R &: 1 + \frac{z}{1!} \end{aligned}$$

El producto da el número de palabras como coeficientes:

$$\begin{aligned} &\left(1 + \frac{z}{1!}\right)^3 \left(1 + \frac{z}{1!} + \frac{z^2}{2!}\right)^2 \left(1 + \frac{z}{1!} + \frac{z^2}{2!} + \frac{z^3}{3!}\right) \\ &= 1 + 6\frac{z}{1!} + 33\frac{z^2}{2!} + 166\frac{z^3}{3!} + 758\frac{z^4}{4!} + 3100\frac{z^5}{5!} + 11130\frac{z^6}{6!} \\ &\quad + 34020\frac{z^7}{7!} + 84000\frac{z^8}{8!} + 151200\frac{z^9}{9!} + 151200\frac{z^{10}}{10!} \end{aligned}$$

Un momento de reflexión muestra que el coeficiente principal (del término de máximo grado) en esta expansión es una explicación alternativa del Tao (sección 13.4).

Los objetos colgados para exhibición en la función generatriz no tienen porqué ser números. Un polinomio  $f(x_1, x_2, \dots, x_n)$  se llama *simétrico* si para cualquier permutación  $\sigma$  de  $[n]$ :

$$f(x_1, x_2, \dots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) \quad (14.72)$$

Vale decir, el polinomio se mantiene inalterado bajo cualquier reordenamiento de variables.

Considerando polinomios homogéneos de grado  $m$  en  $n$  variables, están las familias:

$$e_m(x_1, x_2, \dots, x_n) = \sum_{k_1 < k_2 < \dots < k_m} x_{k_1} x_{k_2} \cdots x_{k_m} \quad (14.73)$$

$$h_m(x_1, x_2, \dots, x_n) = \sum_{k_1 + k_2 + \dots + k_n = m} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} \quad (14.74)$$

$$p_m(x_1, x_2, \dots, x_n) = \sum_{1 \leq k \leq n} x_k^m \quad (14.75)$$

Los  $e_m$  son los llamados *elementales* (ya nos tropezamos con ellos en las fórmulas de Vieta (9.10)), los  $h_m$  se llaman *homogéneos completos* y los  $p_m$  simplemente *sumas de potencias*. Por ejemplo, para  $n = 3$ :

$$e_2(x_1, x_2, x_3) = x_1 x_2 + x_1 x_3 + x_2 x_3$$

$$h_3(x_1, x_2, x_3) = x_1^3 + x_1^2 x_2 + x_1^2 x_3 + x_1 x_2^2 + x_1 x_2 x_3 + x_1 x_3^2 + x_2^3 + x_2^2 x_3 + x_2 x_3^2 + x_3^3$$

$$p_3(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3$$

Tenemos los siguientes casos especiales:

$$e_0(x_1, x_2, \dots, x_n) = 1 \quad (14.76)$$

$$h_0(x_1, x_2, \dots, x_n) = 1 \quad (14.77)$$

$$p_0(x_1, x_2, \dots, x_n) = n \quad (14.78)$$

Definamos las funciones generatrices:

$$E(t) = \sum_{m \geq 0} e_m(x_1, x_2, \dots, x_n) t^m \quad (14.79)$$

$$= \prod_{1 \leq k \leq n} (1 + x_k t) \quad (14.80)$$

$$H(t) = \sum_{m \geq 0} h_m(x_1, x_2, \dots, x_n) t^m \quad (14.81)$$

$$= \prod_{1 \leq k \leq n} \frac{1}{1 - x_k t} \quad (14.82)$$

$$P(t) = \sum_{m \geq 0} p_{m+1}(x_1, x_2, \dots, x_n) t^m \quad (14.83)$$

$$= \sum_{1 \leq k \leq n} \frac{x_k}{1 - x_k t} \quad (14.84)$$

Las fórmulas dadas debieran estar claras: En  $E(t)$  contribuyen al coeficiente de  $t^m$  los factores para  $m$  variables diferentes; en  $H(t)$  vemos que al expandir las series geométricas de cada factor estas dan la variable elevada a cada posible potencia, y las combinaciones posibles que dan  $t^m$  son exactamente las indicadas en (14.74); mientras en  $P(t)$  el coeficiente de  $t^m$  proviene de la suma de todas las variables elevadas a  $m+1$ .

Hagamos uso de estas funciones generatrices ahora. De (14.80) y (14.82) está claro que:

$$E(t)H(-t) = 1$$

Comparando coeficientes (al lado derecho tenemos  $1 + 0z + 0z^2 + \dots$ ):

$$\sum_{0 \leq r \leq m} (-1)^{m-r} e_r(x_1, \dots, x_n) h_{m-r}(x_1, \dots, x_n) = [m = 1] \quad (14.85)$$

También vemos que:

$$\ln E(t) = \sum_{1 \leq k \leq n} \ln(1 + x_k t)$$

$$\begin{aligned} \frac{E'(t)}{E(t)} &= \sum_{1 \leq k \leq n} \frac{x_k}{1 + x_k t} \\ &= P(-t) \end{aligned}$$

$$E'(t) = E(t)P(-t)$$

De acá, comparando coeficientes:

$$\begin{aligned} (-1)^m m e_m(x_1, \dots, x_n) &= \sum_{0 \leq r \leq m-1} e_r(x_1, \dots, x_n) \cdot (-1)^{m-1-r} p_{m-r}(x_1, \dots, x_n) \\ m e_m(x_1, \dots, x_n) &= \sum_{0 \leq r \leq m-1} (-1)^{r-1} e_r(x_1, \dots, x_n) p_{m-r}(x_1, \dots, x_n) \end{aligned} \quad (14.86)$$

Similarmente:

$$\begin{aligned}\ln H(t) &= - \sum_{1 \leq k \leq n} \ln(1 - x_k t) \\ \frac{H'(t)}{H(t)} &= P(t) \\ H'(t) &= H(t)P(t)\end{aligned}$$

Igual que antes:

$$mh_m(x_1, \dots, x_n) = \sum_{0 \leq r \leq m-1} h_r(x_1, \dots, x_n) p_{m-r}(x_1, \dots, x_n) \quad (14.87)$$

Siquiera sospechar las relaciones (14.85), (14.86) y (14.87) de alguna otra forma sería sobrehumano.

Otro ejemplo lo ofrecen las *fuentes* (*fountain* en inglés), formadas por filas de monedas de forma que cada moneda esté en contacto con dos monedas de la fila inferior. Si la fuente es tal que las monedas en cada fila están contiguas, se les llama *fuentes de bloque* (en inglés *block fountain*). La

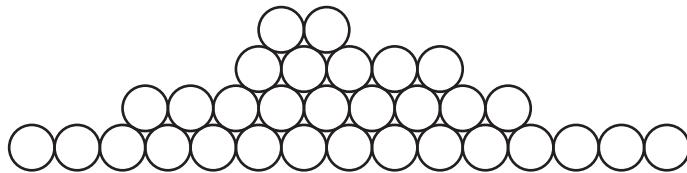


Figura 14.5 – Una fuente de bloque

figura 14.5 ilustra una fuente de bloque. Interesa saber el número de fuentes de bloque cuya primera fila (su base) tiene  $n$  monedas, llamémosle  $f_n$  a este número.

Un poco de experimentación lleva a  $f_0 = 1$  (hay una única forma de armar una fuente con base 0),  $f_1 = 1$ ,  $f_2 = 2$  y  $f_3 = 5$ . Es claro que si a una fuente con base  $n$  monedas le quitamos la base, queda una fuente con base a lo más  $n - 1$  monedas. Si no hay monedas en la segunda fila, hay una sola fuente; si es  $k \geq 1$  el largo de la segunda fila de monedas, tenemos una fuente de base  $k$  a partir de la segunda fila y esta fuente puede ubicarse sobre la base en  $(n - 1) - k + 1 = n - k$  posiciones. En consecuencia tenemos la recurrencia:

$$f_n = 1 + \sum_{1 \leq k \leq n} (n - k)f_k \quad (n \geq 1) \quad f_0 = 1 \quad (14.88)$$

Esto da los valores:

$$\langle 1, 1, 2, 5, 13, 34, 89, 233, 610, 1597, \dots \rangle \quad (14.89)$$

La sumatoria en (14.88) es la convolución de  $\langle n \rangle_{n \geq 1}$  con  $\langle f_n \rangle_{n \geq 1}$ . Definimos la función generatriz ordinaria:

$$f(z) = \sum_{n \geq 0} f_n z^n \quad (14.90)$$

Como:

$$\frac{1}{1-z} - 1 \xrightarrow{\text{ogf}} \langle 1 \rangle_{n \geq 1} \quad \frac{1}{(1-z)^2} - 1 \xrightarrow{\text{ogf}} \langle n \rangle_{n \geq 1} \quad f(z) - 1 \xrightarrow{\text{ogf}} \langle f_n \rangle_{n \geq 1}$$

aplicando las propiedades de las funciones generatrices ordinarias resulta:

$$f(z) - 1 = \frac{z}{1-z} + \frac{z}{(1-z)^2} \cdot (f(z) - 1) \quad (14.91)$$

Despejando  $f(z)$  obtenemos:

$$f(z) = \frac{1-2z}{1-3z+z^2} = \frac{5+\sqrt{5}}{10} \cdot \frac{1}{1-z\frac{3-\sqrt{5}}{2}} + \frac{5-\sqrt{5}}{10} \cdot \frac{1}{1-z\frac{3+\sqrt{5}}{2}} \quad (14.92)$$

Ciertamente bastante feo, pero da lugar a la expansión explícita:

$$f_n = \frac{5+\sqrt{5}}{10} \left( \frac{3-\sqrt{5}}{2} \right)^n + \frac{5-\sqrt{5}}{10} \left( \frac{3+\sqrt{5}}{2} \right)^n \quad (14.93)$$

La presente discusión se inspira en Bender [34]. Consideremos árboles binarios ordenados completos, definidos mediante:

- (I) Un vértice aislado es un árbol binario ordenado completo (esta es la raíz del árbol y su única hoja)
- (II) Si  $T_1$  y  $T_2$  son árboles binarios ordenados completos, lo es la estructura que agrega un nuevo nodo como raíz y pone la raíz de  $T_1$  como descendiente izquierdo de la raíz y la raíz de  $T_2$  como su descendiente derecho.

Nos interesa determinar el número de estas estructuras con  $n$  hojas, que llamaremos  $b_n$ . Claramente  $b_0 = 0$  y  $b_1 = 1$ . Para  $n > 1$ , tendremos dos subárboles; si el izquierdo aporta  $k$  hojas el derecho aporta  $n-k$ , y el número de árboles que podemos crear en esta situación, por la regla del producto es  $b_k b_{n-k}$ . Pero debemos considerar todos los posibles valores de  $k$ , la regla de la suma nos dice para  $n > 1$ :

$$b_n = \sum_{1 \leq k \leq n-1} b_k b_{n-k} \quad (14.94)$$

Fácilmente podemos calcular los primeros valores:

$$\langle 0, 1, 1, 2, 5, 14, 42, 132, \dots \rangle \quad (14.95)$$

Si definimos la función generatriz ordinaria  $B(z)$  de los  $b_n$ , aplicando nuestra receta queda para  $n > 1$ :

$$\begin{aligned} \sum_{n \geq 2} b_n z^n &= \sum_{n \geq 2} z^n \sum_{1 \leq k \leq n-1} b_k b_{n-k} \\ B(z) - b_0 - b_1 z &= \sum_{n \geq 2} \sum_{1 \leq k \leq n-1} b_k z^k \cdot b_{n-k} z^{n-1-k} \\ &= \left( \sum_{k \geq 1} b_k z^k \right) \cdot \left( \sum_{k \geq 1} b_k z^k \right) \\ &= (B(z) - b_0)^2 \\ B(z) - z &= B^2(z) \end{aligned} \quad (14.96)$$

De (14.96) resulta:

$$B(z) = \frac{1 \pm \sqrt{1-4z}}{2}$$

Como debe ser  $b_0 = 0$ , el signo correcto es el negativo:

$$B(z) = \frac{1 - \sqrt{1-4z}}{2} \quad (14.97)$$

Nuevamente números de Catalan, comparando con (14.61) es:

$$B(z) = zC(z)$$

con lo que tenemos:

$$b_n = \begin{cases} 0 & \text{si } n = 0 \\ C_{n-1} & \text{si } n \geq 1 \end{cases} \quad (14.98)$$

### 14.11. Múltiples índices

Una forma instructiva de obtener el número de subconjuntos de  $k$  elementos de un conjunto de  $n$  elementos (que sabemos son los coeficientes binomiales) es partir de la recurrencia (ver el teorema 13.7):

$$\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k} \quad \binom{0}{k} = [k=0] \quad \binom{n}{0} = 1 \quad (14.99)$$

Si definimos la función generatriz bivariada:

$$C(x, y) = \sum_{\substack{k \geq 0 \\ n \geq 0}} \binom{n}{k} x^k y^n \quad (14.100)$$

Por las propiedades de las funciones generatrices ordinarias resulta:

$$\frac{C(x, y) - C(0, y) - C(x, 0) + C(0, 0)}{xy} = C(x, y) + \frac{C(x, y) - C(0, y)}{x} \quad (14.101)$$

El lado izquierdo es partir de la suma (14.100), restar la fila con  $k = 0$  y la columna con  $n = 0$ ; pero al hacerlo hay que reponer el coeficiente con  $k = n = 0$  que se restó dos veces. Luego se divide por  $xy$  para ajustar los exponentes. Por las condiciones de contorno:

$$C(0, 0) = 1 \quad C(x, 0) = \sum_{k \geq 0} \binom{0}{k} x^k = 1 \quad C(0, y) = \sum_{n \geq 0} \binom{n}{0} y^n = \frac{1}{1-y} \quad (14.102)$$

Resulta nuevamente la función generatriz (14.34).

### 14.12. Aceite de serpiente

La manera tradicional de simplificar sumatorias (particularmente las que involucran coeficientes binomiales) es aplicar identidades u otras manipulaciones de los índices, como magistralmente exponen Knuth [216] y Graham, Knuth y Patashnik [150]. Acá mostramos un método alternativo, que no requiere saber y aplicar una enorme variedad de identidades. Wilf [364] le llama *Snake Oil Method*, por la cura milagrosa que se ve en las películas del viejo oeste. La técnica es bastante simple:

1. Identificar la variable libre, llamémosle  $n$ , de la que depende la suma. Sea  $f(n)$  nuestra suma.
2. Sea  $F(z)$  la función generatriz ordinaria de la secuencia  $\langle f(n) \rangle_{n \geq 0}$ .
3. Multiplique la suma por  $z^n$  y sume sobre  $n$ . Tenemos  $F(z)$  expresado como una doble suma, sobre  $n$  y la variable de la suma original.

4. Intercambie el orden de las sumas, y exprese la suma interna en forma simple y cerrada.

5. Encuentre los coeficientes, son los valores de  $f(n)$  buscados.

Sorprende la alta tasa de éxitos de la técnica. Tiene la ventaja de que no requiere mayor creatividad; resulta claro cuándo funciona y es obvio cuando falla.

Usaremos la convención que toda suma sin restricciones es sobre el rango  $-\infty$  a  $\infty$ . Como los coeficientes binomiales  $\binom{n}{k}$  que usaremos en los ejemplos se anulan cuando  $k$  no está en el rango  $[0, n]$ , esto evita interminables ajustes de índices. Por ejemplo, para  $n \geq 0$  tenemos:

$$\sum_k \binom{n}{r+k} z^k = z^{-r} \sum_k \binom{n}{r+k} z^{r+k} = z^{-r} \sum_s \binom{n}{s} z^s = z^{-r} (1+z)^n$$

Nuestro siguiente problema viene de Riordan [301], donde se resuelve mediante delicadas maniobras. Nuestro desarrollo sigue a Dobrushkin [98].

**Ejemplo 14.1.** Evaluar:

$$h_n = \sum_{0 \leq k \leq n} (-1)^{n-k} 4^k \binom{n+k+1}{2k+1}$$

Definimos  $H(z)$  como la función generatriz de los  $h_n$ ; multiplicamos por  $z^n$ , sumamos para  $n \geq 0$  e intercambiamos orden de suma:

$$\begin{aligned} H(z) &= \sum_{n \geq 0} z^n \sum_{0 \leq k \leq n} (-1)^{n-k} 4^k \binom{n+k+1}{2k+1} \\ &= \sum_{n \geq 0} \sum_{0 \leq k \leq n} (-4)^k (-z)^n \binom{n+k+1}{2k+1} \\ &= \sum_{k \geq 0} (-4)^k \sum_{n \geq k} \binom{n+k+1}{2k+1} (-z)^n \end{aligned}$$

Para completar el trabajo necesitamos la suma interna. Haciendo el cambio de variable  $r = n - k$ :

$$\sum_{n \geq k} \binom{n+k+1}{2k+1} (-z)^n = (-z)^k \sum_{r \geq 0} \binom{r+2k+1}{2k+1} (-z)^r = \frac{(-z)^k}{(1+z)^{2k+2}}$$

Substituyendo en lo anterior:

$$H(z) = \sum_{k \geq 0} \frac{(4z)^k}{(1+z)^{2k+2}} = \frac{1}{(1+z)^2} \cdot \frac{1}{1 - \frac{4z}{(1+z)^2}} = \frac{1}{(1-z)^2}$$

Resta extraer los coeficientes, lo que da:

$$h_n = (-1)^n \binom{-2}{n} = \binom{n+1}{1} = n+1$$

La siguiente es una sumatoria que le dio problemas a Knuth, como comenta en el prefacio del texto de Petkovsek, Wilf y Zeilberger [283].

**Ejemplo 14.2.** Considere la suma:

$$\sum_k \binom{2n-2k}{n-k} \binom{2k}{k}$$

Sabemos que la secuencia comienza  $\langle 1, 4, 16, 64, \dots \rangle$ , por lo que sospechamos que la suma vale  $4^n$ .

Aplicando la receta, con  $S(z)$  la respectiva función generatriz:

$$S(z) = \sum_{n \geq 0} \sum_{0 \leq k \leq n} \binom{2n-2k}{n-k} \binom{2k}{k} z^n = \left( \sum_{n \geq 0} \binom{2n}{n} z^n \right)^2$$

En este caso (como en todas las convoluciones) la sumatoria externa simplemente se disuelve sola. Por (14.30) la serie interna es:

$$S(z) = \left( \frac{1}{\sqrt{1-4z}} \right)^2 = \frac{1}{1-4z}$$

Una serie geométrica, y el resultado  $s(n) = 4^n$  es inmediato.

**Ejemplo 14.3.** Determine el valor de:

$$\sum_{0 \leq k \leq n} \binom{n}{k}^2$$

Esto es esencialmente una convolución:

$$\sum_{0 \leq k \leq n} \binom{n}{k} \binom{n}{n-k}$$

Acá producen problemas los distintos usos de  $n$ , delimita el rango de la suma y aparece en los índices superiores de los coeficientes binomiales. Una solución en tales casos es intentar demostrar algo más general. Dividiendo los distintos usos de  $n$  en variables separadas queda:

$$\sum_{0 \leq k \leq r} \binom{m}{k} \binom{n}{r-k}$$

Ahora hay varios índices libres, debemos elegir uno. Es una convolución, lo que hace sospechar que  $r$  es útil como variable libre. Así llamamos  $v(r)$  a nuestra suma, y su función generatriz  $V(z)$ .

$$\begin{aligned} V(z) &= \sum_{r \geq 0} z^r \sum_k \binom{m}{k} \binom{n}{r-k} \\ &= \left( \sum_{k \geq 0} \binom{m}{k} z^k \right) \cdot \left( \sum_{k \geq 0} \binom{n}{k} z^k \right) \\ &= (1+z)^m (1+z)^n \\ &= (1+z)^{m+n} \end{aligned}$$

En consecuencia, tenemos la *convolución de Vandermonde*<sup>1</sup>:

$$\sum_k \binom{m}{k} \binom{n}{r-k} = \binom{m+n}{r} \quad (14.103)$$

<sup>1</sup>Otro caso de injusticia histórica: Unos 400 años antes de Vandermonde la conocía Zhu Shijie en China [23, páginas 59–60].

que también puede escribirse en la forma simétrica:

$$\sum_k \binom{m}{r+k} \binom{n}{s-k} = \binom{m+n}{r+s} \quad (14.104)$$

Acá la suma es sobre todo  $k \in \mathbb{Z}$ , pero sólo para  $-r \leq k \leq s$  los términos no son cero. Indicarlo destruiría la simetría de la fórmula. Nótese además que nuestra demostración es aplicable también en caso que  $m$  o  $n$  no sean naturales.

Nuestra suma original es simplemente el caso especial  $m = n = r$  de (14.103):

$$\sum_k \binom{n}{k}^2 = \sum_k \binom{n}{k} \binom{n}{n-k} = \binom{2n}{n} \quad (14.105)$$

Nuevamente un caso de la paradoja del inventor.

Un ejemplo propuesto por Liu [240], que resuelve de forma afín a la nuestra:

**Ejemplo 14.4.** Calcular la suma:

$$S_r = \sum_{0 \leq k \leq r} \frac{r!}{(r-k+1)!(k+1)!} \quad (14.106)$$

Vemos que los términos son sospechosamente similares a coeficientes binomiales:

$$S_r = \sum_{0 \leq k \leq r} \binom{r}{k} \frac{1}{r-k+1} \frac{1}{k+1}$$

Esta es una convolución binomial, lo que sugiere la función generatriz exponencial:

$$\hat{S}(z) = \sum_{r \geq 0} S_r \frac{z^r}{r!} \quad (14.107)$$

Vemos que:

$$\begin{aligned} \hat{S}(z) &= \left( \sum_{r \geq 0} \frac{1}{r+1} \cdot \frac{z^r}{r!} \right)^2 \\ &= \left( \sum_{r \geq 0} \frac{z^r}{(r+1)!} \right)^2 \\ &= \left( \frac{e^z - 1}{z} \right)^2 \\ &= \frac{e^{2z} - 2e^z + 1}{z^2} \end{aligned}$$

Los coeficientes son inmediatos:

$$\begin{aligned} S_r &= r![z^r] \hat{S}(z) \\ &= r![z^r] \frac{e^{2z} - 2e^z + 1}{z^2} \\ &= r![z^{r+2}] (e^{2z} - 2e^z + 1) \\ &= r! \left( \frac{2^{r+2}}{(r+2)!} - \frac{2}{(r+2)!} \right) \\ &= \frac{2^{r+2} - 2}{(r+1)(r+2)} \end{aligned} \quad (14.108)$$

Finalmente, una identidad.

**Ejemplo 14.5.** Demostrar que para  $m, n \geq 0$

$$\sum_{k \geq 0} \binom{m}{k} \binom{n+k}{m} = \sum_{k \geq 0} \binom{m}{k} \binom{n}{k} 2^k \quad (14.109)$$

Multiplicamos (14.109) por  $z^n$  y sumamos, así queda demostrar  $L(z) = R(z)$ , donde:

$$L(z) = \sum_{n \geq 0} z^n \sum_{k \geq 0} \binom{m}{k} \binom{n+k}{m} \quad R(z) = \sum_{n \geq 0} z^n \sum_{k \geq 0} \binom{m}{k} \binom{n}{k} 2^k$$

Partimos por el lado izquierdo:

$$L(z) = \sum_{k \geq 0} \binom{m}{k} z^{-k} \sum_{n \geq 0} \binom{n+k}{m} z^{n+k}$$

Por la suma externa sabemos que  $0 \leq k \leq m$ , como en realidad la suma interna es para  $n+k \geq m$  podemos aplicar (14.36):

$$\begin{aligned} L(z) &= \sum_{k \geq 0} \binom{m}{k} z^{-k} \frac{z^m}{(1-z)^{m+1}} \\ &= \left(1 + \frac{1}{z}\right)^m \frac{z^m}{(1-z)^{m+1}} \\ &= \frac{(1+z)^m}{(1-z)^{m+1}} \end{aligned}$$

El lado derecho recibe un tratamiento similar:

$$\begin{aligned} R(z) &= \sum_{k \geq 0} \binom{m}{k} 2^k \sum_{n \geq 0} \binom{n}{k} z^n \\ &= \sum_{k \geq 0} \binom{m}{k} 2^k \frac{z^k}{(1-z)^{k+1}} \\ &= \frac{1}{1-z} \sum_{k \geq 0} \binom{m}{k} \left(\frac{2z}{1-z}\right)^k \\ &= \frac{1}{1-z} \left(1 + \frac{2z}{1-z}\right)^m \\ &= \frac{(1+z)^m}{(1-z)^{m+1}} \end{aligned}$$

Se verifica la identidad.

Hay métodos complementarios, capaces de resolver automáticamente grandes clases de sumatorias, o demostrar que no hay expresiones simples para ellas. Petkovšek, Wilf y Zeilberger [283] los describen en detalle, y hay implementaciones de los mismos para los principales paquetes de álgebra simbólica. Cipra [74] incluso se queja que estas demostraciones automatizadas quitan la entretenición a las matemáticas.

# 15 Principio de inclusión y exclusión

---

Es común querer contar el número de objetos de una colección que cumplen con ciertos conjuntos de características. Si las características de interés son muchas, o la colección de objetos subyacente es grande, necesitamos un esquema que organice y simplifique los cálculos. Veremos el planteo de Wilf [364], que además de ser mucho más simple que el tradicional aprovecha de buena forma lo que hemos aprendido de funciones generatrices. Con esto cerramos el estudio de las técnicas fundamentales de la combinatoria.

## 15.1. El problema general

Concluimos en el capítulo 13 que  $|\mathcal{A} \cup \mathcal{B}| = |\mathcal{A}| + |\mathcal{B}| - |\mathcal{A} \cap \mathcal{B}|$ . La figura 15.1 muestra tres conjuntos y sus posibles intersecciones. Calcular  $|\mathcal{A} \cup \mathcal{B} \cup \mathcal{C}|$  es contar los elementos que pertenecen

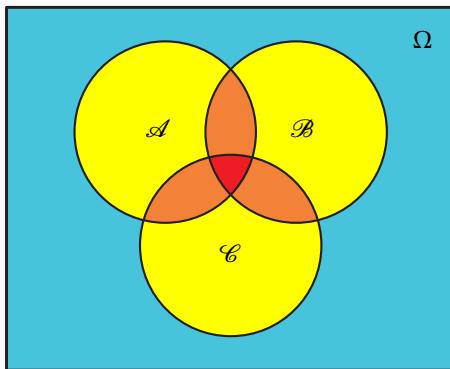


Figura 15.1 – Intersecciones entre tres conjuntos

al menos a uno de los conjuntos. Comenzamos con  $|\mathcal{A}| + |\mathcal{B}| + |\mathcal{C}|$ . Las intersecciones se cuentan dos veces, debemos restar  $|\mathcal{A} \cap \mathcal{B}| + |\mathcal{A} \cap \mathcal{C}| + |\mathcal{B} \cap \mathcal{C}|$ . Hemos restado  $|\mathcal{A} \cap \mathcal{B} \cap \mathcal{C}|$  demás, debemos restituirlo:

$$|\mathcal{A} \cup \mathcal{B} \cup \mathcal{C}| = (|\mathcal{A}| + |\mathcal{B}| + |\mathcal{C}|) - (|\mathcal{A} \cap \mathcal{B}| + |\mathcal{A} \cap \mathcal{C}| + |\mathcal{B} \cap \mathcal{C}|) + |\mathcal{A} \cap \mathcal{B} \cap \mathcal{C}|$$

El número de elementos que pertenecen exactamente a uno de los conjuntos es:

$$(|\mathcal{A}| + |\mathcal{B}| + |\mathcal{C}|) - 2 \cdot (|\mathcal{A} \cap \mathcal{B}| + |\mathcal{A} \cap \mathcal{C}| + |\mathcal{B} \cap \mathcal{C}|) + 3 \cdot |\mathcal{A} \cap \mathcal{B} \cap \mathcal{C}|$$

Al sumar los tamaños de los tres conjuntos incluimos dos veces las intersecciones en pares y tres veces la intersección entre los tres, debemos restarlas; al restar dos veces las tres intersecciones a pares estamos restando seis veces la intersección entre los tres conjuntos, debemos reponerla tres

veces. Al resultado general se le llama *principio de inclusión y exclusión*, porque incluimos demás, y luego corregimos excluyendo.

El tratamiento que sigue no es tradicional, seguimos a Wilf [364] Tomamos un conjunto universo, y los conjuntos que consideramos se representan mediante propiedades (un elemento pertenece a uno de los conjuntos si tiene la propiedad que representa a ese conjunto). Las diversas intersecciones quedan expresadas a través de los elementos que tienen todas las propiedades correspondientes a los conjuntos intersectados.

Sean:

$\Omega$ : El universo. Un conjunto de objetos.

$\mathcal{P}$ : Un conjunto de propiedades que los objetos pueden tener.

$\mathcal{S}$ : Un subconjunto de las propiedades,  $\mathcal{S} \subseteq \mathcal{P}$ .

$N(\supseteq \mathcal{S})$ : Número de objetos con las propiedades en  $\mathcal{S}$  (puedan tener otras).

Para todo posible número de propiedades  $r \geq 0$  definimos:

$$N_r = \sum_{|\mathcal{S}|=r} N(\supseteq \mathcal{S}) \quad (15.1)$$

Esto es la suma del tamaño de los conjuntos de objetos con al menos  $r$  de las propiedades. El conjunto de los objetos con al menos cero propiedades es el universo, o sea  $N_0 = |\Omega|$ . Si hay  $r$  propiedades en total,  $N_r$  es el número de objetos con todas las propiedades. Estas cantidades, que suelen ser mucho más fáciles de calcular que lo que buscamos, las relacionaremos con el número de objetos que tienen exactamente  $t$  de las propiedades.

Llámemos  $e_t$  al número de objetos con exactamente  $t$  propiedades. Un objeto con  $t$  propiedades se cuenta una vez en  $N_r$  por cada subconjunto de  $r$  de sus propiedades, vale decir, considerando todos los objetos:

$$N_r = \sum_{t \geq 0} \binom{t}{r} e_t \quad (15.2)$$

Del sistema lineal (15.2) se busca despejar los  $e_t$ . Para esta tarea definimos las funciones generatrices:

$$E(z) = \sum_{t \geq 0} e_t z^t \quad (15.3)$$

$$N(z) = \sum_{r \geq 0} N_r z^r \quad (15.4)$$

Substituyendo la expresión (15.2) para  $N_r$  en la definición (15.4) de  $N(z)$  y usando el teorema del binomio 13.8:

$$\begin{aligned} N(z) &= \sum_{r \geq 0} N_r z^r \\ &= \sum_{r \geq 0} \left( \sum_{t \geq 0} \binom{t}{r} e_t \right) z^r \\ &= \sum_{t \geq 0} e_t \left( \sum_{r \geq 0} \binom{t}{r} z^r \right) \\ &= \sum_{t \geq 0} e_t (1+z)^t \\ &= E(1+z) \end{aligned}$$

De acá se tiene la fórmula central:

$$E(z) = N(z - 1) \quad (15.5)$$

De la expresión (15.5) podemos extraer el  $e_t$  que se quiera. Tenemos:

$$\begin{aligned} e_t &= [z^t] E(t) \\ &= [z^t] N(z - 1) \\ &= [z^t] \sum_{r \geq 0} N_r (z - 1)^r \\ &= \sum_{r \geq 0} (-1)^{r-t} \binom{r}{t} N_r \end{aligned} \quad (15.6)$$

La fórmula (15.6) expresa el celebrado principio de inclusión y exclusión. Además de ser mucho más simple que la demostración tradicional, nuestro desarrollo no hace necesario recordar esta engorrosa fórmula, da las herramientas para deducirla sin mayor esfuerzo cada vez que la necesitemos, y en muchos casos obtener los resultados buscados directamente sin tener que recurrir a ella explícitamente, usando la función generatriz  $E(z)$ .

Esta técnica es sencilla de aplicar cuando se buscan los que no tienen ninguna de las propiedades, ya que  $e_0 = E(0) = N(-1)$  es inmediato. Conviene tratar de ajustar la definición de las propiedades de forma adecuada. También es crítico que el cálculo de los  $N(\exists S)$  y, en consecuencia, de los  $N_r$ , sea simple, cosa que nuevamente depende de la elección de las propiedades.

Volvamos al ejemplo de tres conjuntos, donde nos interesa saber cuántos elementos pertenecen exactamente a uno de ellos, o sea  $e_1$ , como en la figura 15.1. En tal caso:

$$\begin{aligned} N_0 &= |\Omega| & N_1 &= |\mathcal{A}| + |\mathcal{B}| + |\mathcal{C}| \\ N_2 &= |\mathcal{A} \cap \mathcal{B}| + |\mathcal{A} \cap \mathcal{C}| + |\mathcal{B} \cap \mathcal{C}| & N_3 &= |\mathcal{A} \cap \mathcal{B} \cap \mathcal{C}| \end{aligned}$$

Resultan ser:

$$\begin{aligned} N(z) &= N_0 + N_1 z + N_2 z^2 + N_3 z^3 \\ E(z) &= (N_0 - N_1 + N_2 - N_3) + (N_1 - 2N_2 + 3N_3)z + (N_2 - 3N_3)z^2 + N_3 z^3 \end{aligned}$$

Hay  $e_1 = N_1 - 2N_2 + 3N_3$  elementos que pertenecen a exactamente un conjunto, como dedujimos antes.

Típicamente interesa saber cuántos de los objetos no tienen ninguna de las propiedades, lo que en nuestro caso es  $(\mathcal{A} \cup \mathcal{B} \cup \mathcal{C})$ . O sea,  $e_0 = E(0) = N(-1) = N_0 - N_1 + N_2 - N_3$ .

La unión de todos los conjuntos, en este caso  $\mathcal{A} \cup \mathcal{B} \cup \mathcal{C}$ , la componen los que pertenecen al menos a uno de los conjuntos, vale decir, todos menos los que no pertenecen a ninguno:

$$|\mathcal{A} \cup \mathcal{B} \cup \mathcal{C}| = \sum_{t \geq 0} e_t - e_0 = E(1) - E(0) = N(0) - N(-1) = N_1 - N_2 + N_3$$

Nuevamente coincide con lo que obtuvimos antes.

Si solo interesa calcular el número promedio de propiedades por objeto, como  $t = \binom{r}{1}$  resulta:

$$\mathbb{E}[t] = \frac{\sum_{t \geq 0} t e_t}{\sum_{t \geq 0} e_t} = \frac{N_1}{N_0} \quad (15.7)$$

Para calcular la varianza del número de propiedades, partimos de:

$$\text{var}[t] = \mathbb{E}[t^2] - (\mathbb{E}[t])^2$$

Como  $\binom{t}{2} = (t^2 - t)/2$ :

$$\begin{aligned}\frac{N_2}{N_0} &= \frac{\sum_{t \geq 0} \binom{t}{2} e_t}{\sum_{t \geq 0} e_t} \\ &= \frac{\sum_{t \geq 0} (t^2 - t) e_t}{2 \sum_{t \geq 0} e_t} \\ &= \frac{1}{2} (\mathbb{E}[t^2] - \mathbb{E}[t])\end{aligned}$$

con lo cual:

$$\text{var}[t] = \frac{2N_2}{N_0} + \frac{N_1}{N_0} - \frac{N_1^2}{N_0^2} \quad (15.8)$$

### Receta

1. Definir  $\Omega$  y  $\mathcal{P}$ , expresar lo que se busca en términos de  $e_t$ .
2. Calcular los  $N(\supseteq \mathcal{S})$ .
3. Calcular los  $N_r$ , y en consecuencia obtener  $N(z)$ .
4.  $e_t = [z^t] N(z - 1)$ .

Hay que tener cuidado con esto, acá las series deben converger para que nuestras operaciones tengan sentido. Normalmente el número de propiedades y objetos de interés es finito, así que en realidad estamos manipulando polinomios y no hay problemas.

**Ejemplo 15.1.** Un curso rinde pruebas con los profesores Ellery, Upham y Atwood. Nos dicen que 10 aprobaron la prueba de física, 15 la de matemáticas y 12 pasaron la prueba de química; 6 pasaron física y matemáticas, 5 pasaron física y química, mientras 8 pasaron matemáticas y química. El total de estudiantes que pasaron al menos una prueba es 20. ¿Cuántos pasaron las tres pruebas?

Aplicamos nuestra receta:

1. El universo es el grupo de 20 estudiantes que aprobaron alguna de las pruebas, las propiedades son las pruebas aprobadas ( $F, M, Q$ ). Interesan los que aprobaron todas las pruebas, o sea  $e_3$ .
2. Los  $N(\supseteq \mathcal{S})$  están dados en el enunciado. Por ejemplo, dice que  $N(\supseteq \{F, Q\}) = 5$ .
3. Como se comentó antes, al haber 3 propiedades es  $N_3 = e_3$ . Tenemos:

$$N_0 = |\Omega| = 20$$

$$N_1 = N(\supseteq \{F\}) + N(\supseteq \{M\}) + N(\supseteq \{Q\}) = 10 + 15 + 12 = 37$$

$$N_2 = N(\supseteq \{F, M\}) + N(\supseteq \{F, Q\}) + N(\supseteq \{M, Q\}) = 6 + 5 + 8 = 19$$

$$N_3 = N(\supseteq \{F, M, Q\}) = e_3$$

Resulta:

$$N(z) = 20 + 37z + 19z^2 + e_3 z^3$$

4. Como todos los estudiantes del universo han aprobado al menos una de las pruebas:

$$e_0 = 0 = E(0) = N(-1) = 2 - e_3$$

Con esto resulta  $e_3 = 2$ .

Pero también tenemos:

$$\begin{aligned} E(z) &= N(z-1) \\ &= 5z + 13z^2 + 2z^3 \end{aligned}$$

lo que dice que 5 aprobaron una única prueba y que 13 aprobaron dos.

**Ejemplo 15.2.** ¿Cuántos números de largo  $n$  escritos en decimal tienen un número par de ceros?

Para tener valores con los cuales contrastar, analicemos algunos casos. Anotamos 9 para un dígito no cero, y 0 para un cero en el cuadro 15.1, y contamos cuántos de cada tipo hay.

<b><i>n</i></b>	<b>Descripción</b>	<b>Nº</b>
1	9	9
2	99	81
3	999 + 900	738
4	9999 + 9900 + 9090 + 9009	6804

Cuadro 15.1 – Posibilidades con un número par de ceros

El universo es el conjunto de todos los números con  $n$  dígitos. La propiedad  $i$  es que el dígito  $i$ -ésimo es cero. Lo que interesa entonces es:

$$e_0 + e_2 + \dots = \sum_{r \geq 0} e_{2r}$$

Podemos extraer los términos con potencia par mediante (ver sección 14.5):

$$\frac{E(z) + E(-z)}{2} = \sum_{r \geq 0} e_{2r} z^{2r}$$

y nuestra suma no es más que:

$$\frac{E(1) + E(-1)}{2}$$

Esto es válido, ya que estamos trabajando con polinomios.

Un número decimal de  $n$  dígitos comienza con un dígito no cero, los demás  $n-1$  dígitos pueden ser cualquiera. En este caso podemos calcular los  $e_r$  directamente, observando que hay  $r$  posiciones para los ceros, elegidas de entre  $n-1$  posiciones, los otros  $n-r$  dígitos (incluyendo el primero) pueden tomar uno de los 9 valores restantes:

$$\begin{aligned} e_r &= \binom{n-1}{r} \cdot 9^{n-r} \\ E(z) &= 9 \cdot \sum_{r \geq 0} \binom{n-1}{r} \cdot 9^{n-1-r} \cdot z^r = 9 \cdot (9+z)^{n-1} \end{aligned}$$

y el número buscado resulta ser:

$$\frac{1}{2} (E(1) + E(-1)) = \frac{1}{2} (9 \cdot (9+1)^{n-1} + 9 \cdot (9-1)^{n-1}) = \frac{9}{2} (10^{n-1} + 8^{n-1})$$

Esto coincide con los valores calculados antes, cuadro 15.1.

**Ejemplo 15.3.** Se lanzan 10 dados. ¿De cuántas maneras puede hacerse esto tal que aparezcan todas las caras?

Es más fácil calcular el número de lanzamientos en los que una cara dada *no* aparece, lo que a su vez lleva naturalmente a contar el número de maneras en que no falta ninguna cara. Aplicando la receta:

**Ω:** El conjunto de todos los lanzamientos posibles de 10 dados

**Propiedades:** Un lanzamiento tiene la propiedad  $k$  si la cara  $k$  no aparece

**Resultado:** Interesan los lanzamientos sin propiedades

Si en un lanzamiento las caras en  $\mathcal{S}$  no aparecen, quiere decir que es una secuencia de largo 10 de las restantes  $6 - |\mathcal{S}|$  caras:

$$N(\supseteq \mathcal{S}) = (6 - |\mathcal{S}|)^{10}$$

Como  $\mathcal{S}$  se elige entre 6 posibilidades, si hay  $r = |\mathcal{S}|$  caras excluidas:

$$N_r = \binom{6}{r} (6 - r)^{10}$$

Tenemos:

$$N(z) = \sum_{r \geq 0} \binom{6}{r} (6 - r)^{10} z^r$$

De la fórmula mágica:

$$\begin{aligned} e_0 &= E(0) \\ &= N(-1) \\ &= \sum_{r \geq 0} (-1)^r \binom{6}{r} (6 - r)^{10} \\ &= 16435440 \end{aligned}$$

## 15.2. Desarreglos

Un *punto fijo* de una permutación  $\pi$  ocurre cuando su elemento número  $k$  es  $k$  (vale decir,  $\pi(k) = k$ ). Un *desarreglo* (en inglés *derangement*) es una permutación sin puntos fijos. El primero en calcular el número de desarreglos fue Pierre R. de Montmort (1678–1719) [259]. Hathout [168, 169] presenta varias soluciones (incluyendo la presente, debida esencialmente a Nicolaus Bernoulli).

Siguiendo nuestra receta:

1. El universo son las  $n!$  permutaciones de  $n$  elementos. La permutación  $\pi$  tiene la propiedad  $i$  si  $i$  es un punto fijo en ella. Interesa obtener  $e_0$ .
2. Sea  $\mathcal{S} \subseteq \{1, \dots, n\}$ . Entonces  $N(\supseteq \mathcal{S})$  corresponde a las permutaciones para las cuales los elementos de  $\mathcal{S}$  son fijos, solo se pueden “mover” los  $n - |\mathcal{S}|$  restantes:

$$N(\supseteq \mathcal{S}) = (n - |\mathcal{S}|)!$$

3. Como  $r$  puntos fijos pueden elegirse de  $\binom{n}{r}$  maneras, se tiene que:

$$N_r = \sum_{|\mathcal{S}|=r} N(\mathcal{S}) = \sum_{|\mathcal{S}|=r} (n-r)! = \binom{n}{r} \cdot (n-r)! \quad (15.9)$$

Con esto:

$$N(z) = \sum_{0 \leq r \leq n} \binom{n}{r} (n-r)! z^r = \sum_{0 \leq r \leq n} \frac{n!}{r!(n-r)!} \cdot (n-r)! \cdot z^r = n! \sum_{0 \leq r \leq n} \frac{z^r}{r!} \quad (15.10)$$

En términos de la función exponencial truncada:

$$\exp|_n(z) = \sum_{0 \leq k \leq n} \frac{z^k}{k!} \quad (15.11)$$

la ecuación (15.10) es:

$$N(z) = n! \cdot \exp|_n(z)$$

4. En particular,  $e_0 = E(0) = N(-1)$  es el número de desarreglos de  $n$  elementos:

$$D_n = n! \exp|_n(-1) \quad (15.12)$$

$$\approx n! e^{-1} \quad (15.13)$$

Consideremos la serie de Maclaurin para  $e^x$  con el resto en la forma de Lagrange:

$$e^{-1} = \sum_{0 \leq k \leq n} \frac{(-1)^k}{k!} + \frac{(-1)^{n+1}}{(n+1)!} + \frac{e^{-\xi}}{(n+2)!} (-1)^{n+2} \quad (0 < \xi < 1)$$

Tenemos las cotas para el valor absoluto del error que comete la fórmula  $D_n \approx n!e^{-1}$ :

$$\begin{aligned} n! \left( \frac{1}{(n+1)!} - \frac{e^0}{(n+2)!} \right) &< \epsilon_n < n! \left( \frac{1}{(n+1)!} - \frac{e^{-1}}{(n+2)!} \right) \\ \frac{1}{n+2} &< \epsilon_n < \frac{n+2-e^{-1}}{(n+1)(n+2)} < \frac{1}{n+1} \end{aligned}$$

Para  $n \geq 1$  el error absoluto es menor a  $1/2$ , y  $D_n$  es el entero más cercano a  $n!e^{-1}$ . Algo como un 37% de las permutaciones no tienen puntos fijos. Es curioso que este resultado dependa tan poco de  $n$ .

Más en general, tenemos también:

$$\begin{aligned} e_t &= n! [z^t] \sum_{0 \leq r \leq n} \frac{(z-1)^r}{r!} = n! [z^t] \sum_{0 \leq r \leq n} \sum_{0 \leq k \leq r} \frac{1}{r!} \binom{r}{k} z^k (-1)^{r-k} \\ &= n! \sum_{0 \leq r \leq n} \frac{1}{r!} \binom{r}{t} (-1)^{r-t} = n! \sum_{t \leq r \leq n} \frac{(-1)^{r-t}}{t!(r-t)!} = \frac{n!}{t!} \sum_{0 \leq r \leq n-t} \frac{(-1)^r}{r!} \\ &= \frac{n!}{t!} \exp|_{n-t}(-1) \end{aligned} \quad (15.14)$$

Por 15.7 y 15.9 el número promedio de puntos fijos es:

$$\bar{t} = \frac{N_1}{N_0} = \frac{\binom{n}{1}(n-1)!}{n!} = 1$$

Curiosamente no depende de  $n$ .

### 15.3. El problema de ménages

Lucas [245] en 1891 planteó el problema de sentar  $n$  parejas en una mesa circular, alternando hombres y mujeres de forma que ninguna pareja se sentara junta. Este “problème des ménages” fue resuelto recién en 1934 por Touchard [351], pero sin dar una demostración. La primera demostración de la fórmula de Touchard fue dada por Kaplansky [194] en 1943, claro que al insistir en ubicar primero a las damas y luego ordenar a los caballeros lleva a un desarrollo innecesariamente complicado. Seguimos a Bogart y Doyle [47] en nuestra derivación.

Observamos primero que  $n$  parejas pueden ubicarse de  $2(n!)^2$  maneras alrededor de la mesa (hay dos maneras de elegir los asientos de las mujeres, luego ordenamos a damas y caballeros). Aplicamos el principio de inclusión y exclusión, numerando las parejas de 1 a  $n$ , y definiendo que una distribución tiene la propiedad  $i$  si la pareja  $i$  se sienta junta. Si  $W_k$  es el número de maneras de sentar las parejas de manera que  $k$  parejas dadas se sientan juntas, tenemos:

$$N_r = \binom{n}{r} W_r \quad (15.15)$$

de la fórmula mágica resulta:

$$M_n = \sum_{0 \leq r \leq n} (-1)^r \binom{n}{r} W_r \quad (15.16)$$

donde:

$$W_k = 2 \cdot d_k \cdot k! \cdot ((n - k)!)^2 \quad (15.17)$$

(debemos elegir asientos de las mujeres y hombres, dónde se ubican las parejas que se sientan juntas, y finalmente cómo se distribuyen las  $n - k$  damas y los  $n - k$  caballeros que no forman parte de las parejas). Acá  $d_k$  es el número de formas de ubicar  $k$  piezas de dominó sobre un ciclo de  $2n$  sin que se traslapen, ver la figura 15.2 para un ejemplo.

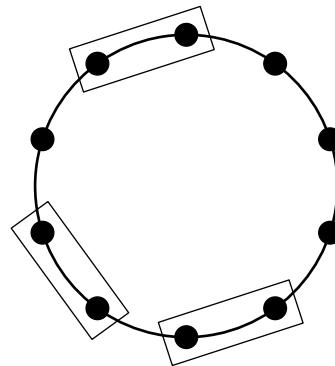


Figura 15.2 – Dominós no traslapados en ciclo

Analicemos  $d_k$ . Si cortamos el círculo, hay dos posibilidades: Una de las piezas de dominó se corta en dos, queda ubicar  $k - 1$  de ellas en línea sobre  $2n - 2$  asientos; o ninguna de las piezas se corta, debemos ubicar  $k$  piezas sobre una línea de  $2n$  asientos. Si llamamos  $f(m, k)$  al número de formas de ubicar  $k$  piezas en una línea de  $m$  asientos, esto resulta de  $k + 1$  bloques entre piezas de

dominó, entre los cuales se distribuyen las  $m - 2k$  posiciones no cubiertas:

$$\begin{aligned} f(m, k) &= \binom{k+1}{m-2k} \\ &= \binom{m-k}{k} \end{aligned} \tag{15.18}$$

Con (15.18), con  $m = 2n$  resulta:

$$\begin{aligned} d_k &= \binom{2n-k}{k} + \binom{2n-2-(k-1)}{k-1} \\ &= \frac{(2n-k)!}{k!(2n-2k)!} + \frac{(2n-k-1)!}{(k-1)!(2n-2k)!} \\ &= \frac{(2n-k-1)!}{(k-1)!(2n-2k)!} \left( \frac{2n-k}{k} + 1 \right) \\ &= \frac{2n}{2n-k} \binom{2n-k}{k} \end{aligned} \tag{15.19}$$

Uniendo las relaciones (15.16) a (15.18), como por simetría  $M_n$  debe ser divisible por  $2n!$ , al simplificar resulta la fórmula de Touchard:

$$\begin{aligned} M_n &= \sum_{0 \leq k \leq n} (-1)^k \binom{n}{k} \cdot 2 \cdot \frac{2n}{2n-k} \binom{2n-k}{k} \cdot k! \cdot ((n-k)!)^2 \\ &= 2n! \sum_{0 \leq k \leq n} (-1)^k \cdot \frac{2n}{2n-k} \cdot \binom{2n-k}{k} \cdot (n-k)! \end{aligned} \tag{15.20}$$

El principio de inclusión y exclusión completa las herramientas elementales de la combinatoria vistas en el capítulo 13.



# 16 Rudimentos de probabilidades discretas

---

Muchas aplicaciones involucran describir lo que ocurre cuando interviene el azar. Por ejemplo, cuál es la probabilidad con la que al lanzar dos dados la suma sea seis. Al analizar algoritmos suele ser de interés su rendimiento promedio, y poder cuantificar cuánto se espera pueda desviarse de él.

Las situaciones que se presentan en casos de nuestro interés se pueden describir en forma discreta. Nos restringiremos a esta situación. Para profundizar en el tema (incluyendo probabilidades continuas) se recomienda el texto de Grinstead y Snell [154], una visión más completa da Feller en sus textos clásicos [117, 118].

## 16.1. Probabilidades

Primero consideraremos experimentos al azar en los cuales hay un número finito de resultados  $\omega_1, \omega_2, \dots, \omega_n$ . El ejemplo tradicional es el lanzar un dado, con posibles resultados 1, 2, 3, 4, 5 y 6. Otro ejemplo es lanzar una moneda, con resultados cara o sello (generalmente anotados H por *head* y T por *tail* en inglés).

Comúnmente nos referiremos a resultados de experimentos, como lanzar un dado cuatro veces y preguntarnos por la suma de los cuatro valores. En tal circunstancia podemos denotar el valor de cada lanzamiento por  $X_i$ , con  $i = 1, 2, 3, 4$ . La suma de interés entonces es:

$$X_1 + X_2 + X_3 + X_4 \tag{16.1}$$

Los  $X_i$  son *variables aleatorias*, simplemente expresiones cuyo valor es el resultado de un experimento. La suma (16.1) también es una variable aleatoria.

Sea  $X$  la variable aleatoria que representa el resultado de un experimento. Asignaremos probabilidades a los posibles resultados de ese experimento. Esto lo hacemos a través de asignar un número no negativo  $f_X(\omega_j)$  a cada posible resultado  $\omega_j$  de manera que:

$$f_X(\omega_1) + f_X(\omega_2) + \cdots + f_X(\omega_n) = 1 \tag{16.2}$$

A la función  $f_X$  se le llama la *función de distribución* de la variable aleatoria  $X$ . Para el caso del lanzamiento de un dado asignaríamos iguales probabilidades de  $1/6$  a cada uno de los posibles resultados. Así podemos escribir para las probabilidades de que se cumplan las situaciones dadas:

$$\begin{aligned} \Pr(X = 1) &= \frac{1}{6} \\ \Pr(X \leq 4) &= \frac{2}{3} \\ \Pr(X \in \{1, 3, 4\}) &= \frac{1}{2} \end{aligned}$$

De la misma forma, al lanzar una moneda es natural asignar las probabilidades  $1/2$  a cara y a sello.

En los ejemplos precedentes las probabilidades asignadas a los distintos resultados son iguales, pero esto no siempre será así. Si se ha determinado que cierto tratamiento tiene un 70% de éxitos, asignaríamos la probabilidad 0,70 a que el siguiente tratamiento resulte exitoso. Esto, con los casos anteriores, ilustra el concepto intuitivo de *probabilidades como frecuencias*. Vale decir, si hay una probabilidad  $p$  que el resultado de un experimento sea  $A$ , si repetimos el experimento gran número de veces esperamos que una fracción  $p$  de los resultados sea  $A$ .

El lector alerta protestará que todo esto es circular: Estamos *aseverando* que las probabilidades corresponden a frecuencias relativas “en muchos experimentos” (pero también es posible que al lanzar una moneda mil veces resulte cara mil veces), para luego usar la idea que ciertos eventos son “igualmente probables” y extraer probabilidades de ello. Para una base realmente rigurosa véase por ejemplo Ash [21]. La teoría allí expuesta justifica nuestro tratamiento intuitivo, que sigue a Grinstead y Snell [154]. Para nuestros efectos generalmente bastará suponer que ciertos resultados son igualmente probables.

## 16.2. Distribuciones discretas

Analizaremos múltiples experimentos desde el punto de vista probabilístico en lo que sigue. La idea global de lo que haremos se puede describir como sigue: Cada experimento tiene asociada una variable aleatoria, que representa los posibles resultados del experimento. El conjunto de posibles resultados es el *espacio muestral*. Primero consideraremos el caso de espacios muestrales finitos, para luego extender la discusión a espacios muestrales infinitos numerables.

**Definición 16.1.** Suponga un experimento cuyo resultado depende del azar. El resultado del experimento se representa por una *variable aleatoria*. El *espacio muestral* del experimento es el conjunto de todos los posibles resultados. Si el espacio muestral es numerable, se dice que la variable aleatoria es *discreta*.

Completamos lo anterior con dos términos adicionales.

**Definición 16.2.** Los elementos del espacio muestral se llaman *resultados*. Un *evento* es un subconjunto del espacio muestral.

Usamos letras mayúsculas para representar el resultado del experimento, y generalmente anotaremos  $\Omega$  para el espacio muestral. Usaremos letras minúsculas para resultados y eventos por mayúsculas. Al lanzar un dado, si llamamos  $X$  al resultado del experimento (el número que muestra el dado), el espacio muestral es:

$$\Omega = \{1, 2, 3, 4, 5, 6\}$$

Un evento es que el resultado sea par, o sea  $E = \{2, 4, 6\}$ . Bajo la suposición que el dado no está cargado, es natural considerar que cada posible resultado tiene la misma probabilidad,  $f_X(i) = 1/6$  para  $1 \leq i \leq 6$ .

**Definición 16.3.** Considere un experimento cuyo resultado es la variable aleatoria  $X$ , con espacio muestral  $\Omega$ . Una *función de distribución* para  $X$  es una función  $f_X: \Omega \rightarrow \mathbb{R}$  tal que:

$$f_X(\omega) \geq 0 \tag{16.3}$$

$$\sum_{\omega \in \Omega} f_X(\omega) = 1 \tag{16.4}$$

Para cualquier subconjunto  $E \subseteq \Omega$  definimos la *probabilidad del evento E* como:

$$\Pr(E) = \sum_{\omega \in E} f_X(\omega)$$

Esto ya debiera alertar al lector que manipulaciones de conjuntos serán centrales en la discusión. La notación así introducida es consistente con la idea informal planteada antes.

Una consecuencia inmediata de la definición es que para todo  $\omega \in \Omega$ :

$$\Pr(\{\omega\}) = f_X(\omega)$$

Consideremos el experimento de lanzar una moneda dos veces. Podemos registrar el resultado de diversas maneras, dando el orden en que se dieron cara y cruz ( $\Omega = \{HH, HT, TH, TT\}$ ), el número de veces que salió cara ( $\Omega = \{0, 1, 2\}$ ) o como los pares sin importar el orden ( $\Omega = \{HH, HT, TT\}$ ). Sea  $X$  la variable aleatoria que corresponde a este experimento, con el primer espacio muestral descrito. Asumiremos que cada uno de los resultados es igualmente probable, o sea la función de distribución  $f_X$  dada por:

$$f_X(HH) = f_X(HT) = f_X(TH) = f_X(TT) = \frac{1}{4}$$

Para el evento  $E = \{HT, TH\}$  (una cara, una cruz) tenemos:

$$\Pr(E) = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

Tenemos algunas propiedades simples.

**Teorema 16.1.** *Sea  $f$  una función de distribución sobre el espacio muestral  $\Omega$ . Las probabilidades que  $f$  asigna a eventos  $E \subseteq \Omega$  cumplen:*

1.  $\Pr(E) \geq 0$  para todo  $E \subseteq \Omega$
2.  $\Pr(\Omega) = 1$
3. Si  $E \subseteq F \subseteq \Omega$  entonces  $\Pr(E) \leq \Pr(F)$ .
4. Si  $A$  y  $B$  son subconjuntos disjuntos de  $\Omega$ , entonces  $\Pr(A \cup B) = \Pr(A) + \Pr(B)$ . En este caso se dice que  $A$  y  $B$  son mutuamente excluyentes.
5.  $\Pr(\bar{A}) = 1 - \Pr(A)$

*Demostración.* Cada propiedad por turno.

1. Por definición:

$$\Pr(E) = \sum_{\omega \in E} f(\omega)$$

Como a su vez  $f(\omega) \geq 0$ , concluimos que  $\Pr(E) \geq 0$ .

2. Esto no es más que:

$$\Pr(\Omega) = \sum_{\omega \in \Omega} f(\omega) = 1$$

3. Supongamos  $E \subseteq F$ . Tenemos:

$$\Pr(E) = \sum_{\omega \in E} f(\omega) \leq \sum_{\omega \in F} f(\omega) = \Pr(F)$$

ya que cada término de la primera suma está en la segunda, y los términos de la segunda suma que no estén en la primera no son negativos.

4. Si  $A \cap B = \emptyset$ , entonces:

$$\Pr(A \cup B) = \sum_{\omega \in A \cup B} f(\omega) = \sum_{\omega \in A} f(\omega) + \sum_{\omega \in B} f(\omega) = \Pr(A) + \Pr(B)$$

5. Aplicando las propiedades 4 y 2 a  $A \cup \bar{A} = \Omega$  resulta:

$$\Pr(A) + \Pr(\bar{A}) = 1$$

que es equivalente a lo indicado.  $\square$

Es común que sea más fácil calcular la probabilidad de que un evento no ocurra, en tal caso es útil la propiedad 5.

La propiedad 4 del teorema 16.1 puede extenderse a uniones disjuntas finitas:

**Teorema 16.2.** Sean  $A_1, A_2, \dots, A_n$  subconjuntos de  $\Omega$ , disjuntos a pares. Entonces:

$$\Pr(A_1 \cup A_2 \cup \dots \cup A_n) = \sum_{1 \leq k \leq n} \Pr(A_k)$$

Usaremos la siguiente consecuencia con frecuencia:

**Corolario 16.3.** Sean  $A_1, A_2, \dots, A_n$  mutuamente excluyentes (vale decir, disjuntos a pares), tales que  $A_1 \cup A_2 \cup \dots \cup A_n = \Omega$ , y  $E$  un evento cualquiera. Entonces:

$$\Pr(E) = \sum_{1 \leq k \leq n} \Pr(E \cap A_k)$$

*Demostración.* Los conjuntos  $E \cap A_k$  son disjuntos a pares, y su unión es  $E$ .  $\square$

Una consecuencia útil es:

**Corolario 16.4.** Para cualquier par de eventos  $A$  y  $B$ :

$$\Pr(A) = \Pr(A \cap B) + \Pr(A \cap \bar{B})$$

Usando las anteriores con (1.7) obtenemos:

**Teorema 16.5.** Si  $A$  y  $B$  son subconjuntos de  $\Omega$ :

$$\Pr(A \cup B) = \Pr(A) + \Pr(B) - \Pr(A \cap B)$$

Extender este resultado a más conjuntos es precisamente el principio de inclusión y exclusión, tema del capítulo 15.

### 16.2.1. Función generatriz de probabilidad

Formalmente para la variable aleatoria  $X$  se define la *función generatriz de probabilidades* (abreviada *pgf*, del inglés *probability generating function*) como:

$$G(z) = \mathbb{E}[z^X] \tag{16.5}$$

En nuestro caso el espacio muestral es  $\Omega = \mathbb{N}_0$ , con la función de distribución  $f: \mathbb{N}_0 \rightarrow \mathbb{R}$ . La definición (16.5) se traduce en:

$$G(z) = \sum_{n \geq 0} f(n)z^n \tag{16.6}$$

Esto no es más que la función generatriz ordinaria de la secuencia  $\langle f(k) \rangle_{k \geq 0}$ . La condición (16.4) se traduce en:

$$G(1) = 1 \quad (16.7)$$

Un dato interesante es que si tenemos variables independientes  $X$  e  $Y$ , con distribuciones  $f_X$  y  $f_Y$ , respectivamente; y cuyas funciones generatrices de probabilidad son respectivamente  $G_X$  y  $G_Y$ , tenemos la función generatriz de probabilidad  $G_{X+Y}$  para la suma  $X + Y$ :

$$\begin{aligned} G_{X+Y}(z) &= \sum_{x,y} f_X(x)f_Y(y)z^{x+y} \\ &= \left(\sum_x f_X(x)z^x\right) \cdot \left(\sum_y f_Y(y)z^y\right) \\ &= G_X(z) \cdot G_Y(z) \end{aligned} \quad (16.8)$$

Planteado el modelo de un experimento al azar, queda el problema de determinar las probabilidades que mejor describen el experimento. Afortunadamente, en muchas situaciones simples cada evento elemental es igualmente probable.

**Teorema 16.6.** *Si  $\Omega$  es finito, y cada resultado es igualmente probable, la probabilidad del evento  $E$  es:*

$$\Pr(E) = \frac{|E|}{|\Omega|}$$

En tales situaciones el cálculo de probabilidades se reduce a contar los elementos de los eventos, lo que lleva a combinatoria como desarrollada en el capítulo 13, involucra aplicaciones del principio de inclusión y exclusión discutido en el capítulo 15 o técnicas más avanzadas como las expuestas en el capítulo 21 y siguientes.

### 16.2.2. Función generatriz de momentos

Formalmente, se define la *función generatriz de momentos* (abreviada *mgf*, del inglés *moment generating function*) para la variable aleatoria  $X$  mediante:

$$M(z) = E[e^{zX}] \quad (16.9)$$

Recordando (16.5) vemos que:

$$M(z) = G(e^z) \quad (16.10)$$

Podemos evaluar:

$$\begin{aligned} M(z) &= E[e^{zX}] \\ &= E\left[\sum_{r \geq 0} \frac{z^r X^r}{r!}\right] \\ &= \sum_{r \geq 0} E[X^r] \frac{z^r}{r!} \end{aligned} \quad (16.11)$$

Esta es la función generatriz exponencial de los momentos  $E[X^n]$  de la variable.

### 16.2.3. Problemas de urna

Muchas situaciones simples de probabilidades se pueden describir en el marco de una urna que contiene bolas, las cuales se extraen y se notan. Consideremos una urna que contiene  $n$  bolas, numeradas 1 a  $n$ , de las que se extraen  $k$ . Esto puede hacerse de diversas maneras. Primeramente, podemos extraer las bolas una a una (el orden en que se extraen importa) o sacarlas de una vez (el orden no importa). En el último caso resulta conveniente considerar igual que las bolas se sacan de a una, pero el orden no interesa. Enseguida, una vez que se extrae una bola podemos notarla y devolverla a la urna, o dejarla fuera (con y sin reemplazo). Parte del arte es reconocer estas cuatro situaciones aún si parecieran no ser aplicables. Para distinguir los casos anotamos elementos ordenados como tupla,  $(1, 3, 2)$ ; y elementos no ordenados como (multi)conjunto,  $\{1, 2, 3\}$ .

Podemos aplicar las técnicas del capítulo 13 para contar las posibilidades en los cuatro casos resultantes:

**Ordenadas, sin reemplazo:** Vemos que la primera bola se puede elegir de  $n$  maneras, la segunda entre las  $n - 1$  restantes, y así sucesivamente. Son permutaciones de  $k$  elementos tomados entre  $n$ :

$$G(n, k) = n^k$$

**Ordenadas, con reemplazo:** En este caso cada una de las  $k$  bolas se elige entre las  $n$ :

$$n^k$$

**Sin orden, sin reemplazo:** Es elegir un subconjunto de  $k$  los  $n$  elementos, lo que llamamos combinaciones:

$$C(n, k) = \binom{n}{k}$$

**Sin orden, con reemplazo:** En este caso lo relevante es cuántas veces aparece cada uno de los  $n$  elementos, es un multiconjunto de  $k$  elementos:

$$\binom{n}{k} = \binom{n+k-1}{k}$$

Ejemplos típicos son:

1. En una prueba de selección múltiple hay 20 preguntas, cada una con 5 alternativas. Considerando que se puede responder una de las opciones o dejar la pregunta en blanco, esto es elegir en orden  $k = 20$  bolas entre  $n = 6$  con reemplazo, el total de posibilidades es:

$$6^{20} = 3656158440062976$$

2. En el campeonato mundial de fútbol juegan 32 equipos. Ordenar los ganadores (primer a tercer lugar) corresponde a elegir  $k = 3$  entre  $n = 32$  en orden sin reemplazo:

$$32^3 = 32 \cdot 31 \cdot 30 = 29760$$

3. De un mazo de 52 cartas se saca una mano de poker. Esto es tomar  $k = 5$  elementos entre  $n = 52$  sin orden y sin reemplazo, un subconjunto:

$$\binom{52}{5} = 2598960$$

4. Si se lanzan tres dados, los resultados posibles corresponden a elegir  $k = 3$  valores de  $n = 6$  sin orden con reemplazo, un multiconjunto:

$$\binom{6}{3} = \binom{8}{3} = 56$$

El modelo de urna supone que todas las posibilidades así obtenidas son igualmente probables. Al menos en el caso del campeonato de fútbol deberemos acordar que esto no es realista (pocos apostarían que Chile resulte campeón el 2014).

#### 16.2.4. Distribuciones multivariadas

Podemos manejar de forma similar distribuciones conjuntas de varias variables. Para concretar la discusión, veremos el caso de la variable aleatoria  $(X, Y)$  compuesta por variables aleatorias  $X$  e  $Y$ . La extensión a más variables es simple, y no nos detendremos en ello.

Siendo consistentes con nuestra notación y definiciones previas, definimos la función de distribución  $f_{(X,Y)}$ , que cumple:

$$\begin{aligned} f_{(X,Y)}(x, y) &\geq 0 \\ \sum_{x,y} f_{(X,Y)}(x, y) &= 1 \end{aligned}$$

Como:

$$\Pr(X = x \wedge Y = y) = f_{(X,Y)}(x, y)$$

la probabilidad del evento  $X = x$  es simplemente:

$$\Pr(X = x) = \sum_y f_{(X,Y)}(x, y)$$

Esto define la función de distribución de  $X$  (y similarmente la de  $Y$ ) en esta situación:

$$f_X(x) = \sum_y f_{(X,Y)}(x, y) \tag{16.12}$$

$$f_Y(y) = \sum_x f_{(X,Y)}(x, y) \tag{16.13}$$

#### 16.2.5. Diagramas de árbol

Muchos experimentos pueden considerarse que se llevan a cabo en etapas. Por ejemplo, el lanzar tres monedas podemos describirlo como lanzando una moneda después de la otra, dando lugar a un diagrama como el de la figura 16.1 (su *diagrama de árbol*). Un *camino* a través del árbol representa un posible resultado del experimento. En el caso ilustrado de lanzar tres monedas hay ocho caminos, suponiendo cada uno de los resultados igualmente probables le asignaríamos probabilidad 1/8 a cada uno de ellos. Si  $E$  es el evento “hay al menos una cara”, el evento  $\bar{E}$  es “no hay ninguna cara”. Es claro que solo si el resultado es tres veces sello (o sea TTT, que corresponde a  $\omega_8$ ) se da  $\bar{E}$ , con lo que:

$$\Pr(\bar{E}) = \frac{1}{8}$$

Por lo tanto, usando el ítem 5 del teorema 16.1:

$$\Pr(E) = 1 - \Pr(\bar{E}) = \frac{7}{8}$$

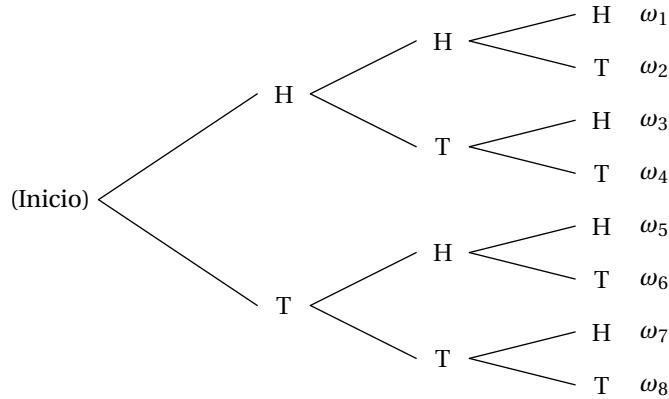


Figura 16.1 – Diagrama de árbol para lanzamiento de tres monedas

La utilidad del diagrama es que si en cada bifurcación anotamos la probabilidad de tomar los distintos caminos, la probabilidad de un evento es el producto de las probabilidades en el camino entre la raíz y ese evento. En nuestro caso, si asumimos que la probabilidad de cara y sello son ambas  $1/2$ , independiente de la posición en el árbol, obtenemos  $1/8$  para  $f(\omega_8)$ . Describir un experimento mediante un diagrama de árbol ayuda a organizar las ideas, y evita errores como omitir alguna de las posibilidades o asignación incoherente de probabilidades.

Un ejemplo más complejo provee el dilema de Monty Hall, discutido originalmente en la popular columna “Ask Marilyn” de Marilyn vos Savant en la revista Parade, recogido luego en su libro [312]. La controversia se inició con la pregunta:

Suppose you're on a game show, and you're given the choice of three doors. Behind one door is a car, behind the others, goats. You pick a door, say number 1, and the host, who knows what's behind the doors, opens another door, say number 3, which has a goat. He says to you, “Do you want to pick door number 2?” Is it to your advantage to switch your choice of doors? (Craig F. Whitaker, Columbia, MD)

El nombre viene de un popular presentador de televisión, en cuyo programa aparecía esta sección. El dilema dio lugar a encendidas discusiones, mientras aplicar las técnicas vistas lo resuelve sin ambigüedades.

Primeramente, necesitamos describir la situación en forma precisa. Supondremos que el auto está con la misma probabilidad tras cada puerta, que el participante elige la puerta con la misma probabilidad, independiente de la ubicación del auto, y finalmente que Monty elige la puerta a abrir con la misma probabilidad entre las no elegidas por el participante y que no ocultan el auto. Por simetría, podemos designar por  $A$  la puerta elegida por el participante, cosa que dará un tercio de los casos (y probabilidades) a considerar, y nuestro diagrama considera solo este caso. Enseguida, consideraremos las tres posibilidades para la ubicación del auto, y finalmente la elección de la puerta a abrir por Monty. Esto da el árbol de la figura 16.2, del que obtenemos la probabilidad de ganar el auto al cambiar de puerta o no. Resulta que la probabilidad de ganar al cambiar de puerta es de  $2/3$ , y de no cambiar de puerta solo  $1/3$ , cosa a primera vista contradictoria.

### 16.3. Probabilidad condicional

Es frecuente querer determinar la probabilidad de un evento  $A$  sabiendo que un evento  $B$  ocurrió. Expresando esta situación como conjuntos, nos interesa la intersección entre  $A$  y  $B$ ; como sabemos

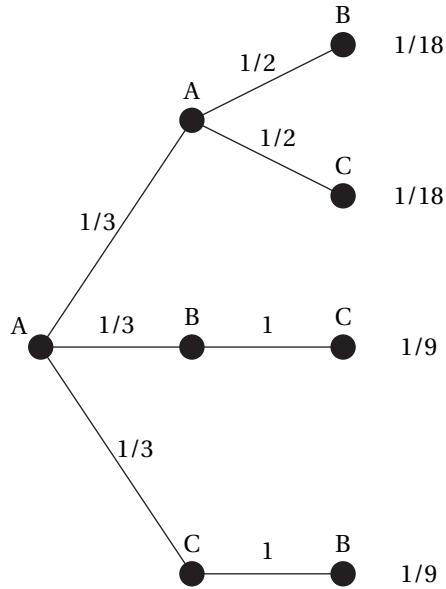


Figura 16.2 – Árbol para el dilema de Monty Hall

que ocurrió  $B$ , la probabilidad relativa es:

$$\frac{\Pr(A \cap B)}{\Pr(B)}$$

Adoptamos esto como definición:

**Definición 16.4.** La *probabilidad condicional* del evento  $A$  dado que ocurrió el evento  $B$  es:

$$\Pr(A|B) = \frac{\Pr(A \cap B)}{\Pr(B)} \quad (16.14)$$

Por ejemplo, si al lanzar dos dados la suma es diez, ¿cuál es la probabilidad de que haya un seis? En este caso, tenemos  $B$  como el evento que la suma es diez, vale decir:

$$B = \{(4, 6), (5, 5), (6, 4)\}$$

el evento  $A$  es que hay un único seis:

$$A = \{(1, 6), (2, 6), (3, 6), (4, 6), (5, 6), (6, 1), (6, 2), (6, 3), (6, 4), (6, 5)\}$$

Resulta  $A \cap B = \{(4, 6), (6, 4)\}$ , con la suposición que todos los eventos elementales son igualmente probables es:

$$\Pr(A|B) = \frac{2/36}{3/36} = \frac{2}{3}$$

Para el caso de una secuencia más larga de eventos,  $A_1 A_2 \dots A_n$ , resulta:

**Teorema 16.7.** Tenemos la regla del producto:

$$\Pr(A_1 A_2 \dots A_n) = \Pr(A_1) \cdot \Pr(A_2|A_1) \cdot \Pr(A_3|A_1 A_2) \cdots \Pr(A_n|A_1 A_2 \cdots A_{n-1}) \quad (16.15)$$

*Demostración.* La demostración formal es por inducción. Ilustraremos la idea con el caso  $n = 3$ :

$$\Pr(A) \Pr(B|A) \Pr(C|A \cap B) = \Pr(A) \frac{\Pr(A \cap B)}{\Pr(A)} \frac{\Pr(A \cap B \cap C)}{\Pr(A \cap B)} = \Pr(A \cap B \cap C)$$

Esto corresponde al lado derecho e izquierdo, respectivamente, de (16.15).  $\square$

#### 16.4. Regla de Bayes

Supongamos que  $B_1, B_2, \dots, B_n$  es una partición de  $\Omega$  (son eventos mutuamente excluyentes). Por el corolario 16.3 y la definición de probabilidad condicional obtenemos la *ley de probabilidad total*:

$$\begin{aligned} \Pr(A) &= \sum_{1 \leq k \leq n} \Pr(A \cap B_k) \\ &= \sum_{1 \leq k \leq n} \Pr(A|B_k) \Pr(B_k) \end{aligned} \quad (16.16)$$

Combinando la definición de probabilidad condicional con la ley de probabilidad total da la importante *ley de Bayes*:

$$\begin{aligned} \Pr(B_k|A) &= \frac{\Pr(A \cap B_k)}{\Pr(A)} \\ &= \frac{\Pr(A|B_k) \Pr(B_k)}{\sum_{1 \leq i \leq n} \Pr(A|B_i) \Pr(B_i)} \end{aligned} \quad (16.17)$$

Para ilustrar la regla de Bayes, consideremos una empresa que tiene tres fábricas que producen chips, la planta 1 produce un 20 % del total, la 2 un 35 % y la 3 el 45 % restante. Las tasas de fallas en los chips de las distintas plantas son 1 %, 5 % y 3 %, respectivamente. Se tiene un chip defectuoso. ¿Cuál es la probabilidad de que haya sido fabricado en la planta 1?

Sea  $A$  el evento que un chip es defectuoso, y sean los  $B_i$  los eventos que el chip haya sido fabricado en la planta  $i$ . Claramente los  $B_i$  partitionan  $\Omega$ . Las fracciones de la producción corresponden a los  $\Pr(B_i)$ , las tasas de fallas por planta son los  $\Pr(A|B_i)$ . Usando la regla de Bayes:

$$\Pr(B_1|A) = \frac{0,20 \cdot 0,01}{0,20 \cdot 0,01 + 0,35 \cdot 0,05 + 0,45 \cdot 0,03} = 0,0606$$

Es un poco más del 6 %.

#### 16.5. Independencia

Dos eventos se dicen *independientes* si saber que ocurrió uno de ellos no altera la probabilidad del otro. Vale decir,  $A$  y  $B$  son independientes si:

$$\Pr(A|B) = \Pr(A)$$

Alternativamente, incluyendo el caso  $B = \emptyset$ :

$$\Pr(A \cap B) = \Pr(A) \Pr(B) \quad (16.18)$$

Esto muestra que si  $A$  es independiente de  $B$  entonces  $B$  es independiente de  $A$ . Esto claramente se puede extender a más eventos independientes a pares.

De forma similar, si tenemos una variable aleatoria  $(X, Y)$ , se dice que las variables  $X$  e  $Y$  son independientes si la función de distribución conjunta cumple:

$$f_{(X,Y)}(x, y) = f_X(x) \cdot f_Y(y) \quad (16.19)$$

## 16.6. Las principales distribuciones discretas

Sabemos que cierta moneda da sello con probabilidad  $p$  y cara con probabilidad  $1 - p$  (no estamos suponiendo que ambos resultados son igualmente probables) al lanzarla. Al lanzarla una vez, considerando sello como “éxito” (o 1) y cara como “falla” (o 0) se habla de *ensayo de Bernoulli* (en inglés *Bernoulli trial*), la variable  $X$  que representa este experimento tiene probabilidad  $p$  de ser 1 y  $1 - p$  de ser 0. Se dice que  $X$  tiene *distribución de Bernoulli*, y se anota:

$$X \sim \mathbf{Ber}(p) \quad (16.20)$$

Su función generatriz de probabilidad es simplemente:

$$(1 - p) + zp = 1 + p(z - 1) \quad (16.21)$$

Considerando nuevamente la moneda anterior, pero ahora lanzándola  $n$  veces, podemos describir el espacio muestral como el conjunto de  $n$ -tuplas de 0 y 1, con 0 para cara y 1 para sello. ¿Cómo debiéramos definir las probabilidades para los eventos individuales? Es natural suponer que los lanzamientos son independientes, y que además la probabilidad de que resulte cara no cambia de un lanzamiento a otro. O sea, el número de caras es la suma de  $n$  ensayos de Bernoulli, independientes e idénticamente distribuidos. A esta situación común en que tenemos variables  $X_1, X_2, \dots, X_n$  independientes e idénticamente distribuidas se suele abreviar como *iid* (del inglés “*independent, identically distributed*”, que casualmente sirve de abreviación del castellano también). Por (16.8) y la función generatriz de probabilidad del ensayo de Bernoulli (16.21) esto significa que la función generatriz de probabilidad es:

$$(1 + p(z - 1))^n \quad (16.22)$$

De (16.22) la distribución es directamente:

$$\Pr(X = k) = \binom{n}{k} p^k (1 - p)^{n-k} \quad (16.23)$$

Esta es la *distribución binomial*. Si  $X$  representa el número de caras en este experimento, se anota:

$$X \sim \mathbf{Bin}(n, p) \quad (16.24)$$

Si llamamos  $C_k$  al evento que al primer sello ocurre en el lanzamiento  $k$ , sabemos que hay  $k - 1$  caras seguidas por un sello. Como discutido en la sección 16.2.5 esto resulta en:

$$\Pr(C_k) = (p - 1)^{k-1} p$$

Nótese que el espacio muestral es infinito en este caso. A esta distribución se le llama *geométrica*. Si  $X$  representa el número de lanzamientos, se anota:

$$X \sim \mathbf{G}(p) \quad (16.25)$$

La función generatriz de probabilidades es:

$$\sum_{k \geq 1} (1 - p)^{k-1} p z^k = \frac{zp}{1 - (1 - p)z} \quad (16.26)$$

Otra distribución importante resulta de considerar una urna conteniendo un total de  $N$  bolas,  $r$  de las cuales son rojas y las demás negras. Se extraen  $n$  bolas sin orden y sin reposición, y nos preguntamos cuántas de ellas son rojas. Esto sirve por ejemplo para modelar encuestas. Estamos

eliendo  $k$  de las  $r$  bolas rojas y  $n - k$  de las  $N - r$  bolas negras, al aplicar la regla del producto y luego calcular la proporción del total de posibles subconjuntos de  $n$  elementos tomados del total de  $N$  resulta la *distribución hipergeométrica*:

$$\Pr(X = k) = \frac{\binom{r}{k} \binom{N-r}{n-k}}{\binom{N}{n}} \quad (16.27)$$

En este caso escribimos:

$$X \sim \mathbf{Hyp}(n, r, N) \quad (16.28)$$

La función generatriz de probabilidades no es una función elemental.

Una distribución muy importante es la de Poisson. Resulta de considerar un intervalo de tiempo en el cual ocurren eventos al azar en promedio a una tasa de  $\lambda$ . Una manera de derivarla es considerar un intervalo de largo 1, en el cual ocurrirán en promedio  $\lambda$  eventos. Si dividimos el intervalo en  $n$  subintervalos del mismo largo, en cada subintervalo esperamos que ocurran  $\lambda/n$  eventos. Si  $n$  es grande, habrá a lo más un evento por subintervalo, y bajo el supuesto que los eventos ocurren al azar esto corresponde a una secuencia de  $n$  ensayos de Bernoulli con probabilidad  $\lambda/n$ , o sea el número de eventos sigue una distribución binomial:

$$\Pr(X = k) = \lim_{n \rightarrow \infty} \binom{n}{k} \left(\frac{\lambda}{n}\right)^k \left(1 - \frac{\lambda}{n}\right)^{n-k}$$

En términos de la notación asintótica de la sección 1.10 tenemos del límite clásico para  $n \rightarrow \infty$  y  $k$  fijo:

$$\left(1 - \frac{\lambda}{n}\right)^{n-k} \sim e^{-\lambda}$$

Por otro lado:

$$\frac{n!}{(n-k)!} = n(n-1)\cdots(n-k+1) \sim n^k$$

Uniendo las anteriores piezas queda en el límite:

$$\Pr(X = k) = \frac{\lambda^k}{k!} e^{-\lambda} \quad (16.29)$$

Escribimos:

$$X \sim \mathbf{Pois}(\lambda) \quad (16.30)$$

Para la función generatriz de probabilidad:

$$\sum_{k \geq 0} \frac{\lambda^k}{k!} e^{-\lambda} z^k = e^{\lambda(z-1)} \quad (16.31)$$

Otra distribución que se encuentra ocasionalmente es la *binomial negativa* (o de Pascal). Supongamos ensayos de Bernoulli independientes consecutivos, nos interesa el número de experimentos con resultado uno antes de acumular  $r$  ceros (se suele hablar de “éxitos” y “fallas”, interesa el número de éxitos para  $r$  fallas; pero las “fallas” no tienen porqué ser negativas, por ejemplo modela el número de penales antes de completar tres goles). Cuidado, hay una variedad de definiciones ligeramente

diferentes. Si son  $k$  éxitos, hay  $k+r$  ensayos en total, y sabemos que el último resultado es 0. Quedan por distribuir  $r-1$  fallas entre los primeros  $k+r-1$  experimentos:

$$\Pr(X = k) = \binom{k+r-1}{k} (1-p)^r p^k \quad (16.32)$$

Se le llama binomial negativa por (14.32):

$$\binom{k+r-1}{k} = (-1)^k \binom{-r}{k}$$

Si tomamos para  $r > 0$  cualquiera:

$$\Pr(X = k) = (-1)^k \binom{-r}{k} (1-p)^r p^k$$

Esta es una distribución de probabilidad, ya que:

$$\begin{aligned} \Pr(X = k) &\geq 0 \\ \sum_{k \geq 0} \Pr(X = k) &= \sum_{k \geq 0} (-1)^k \binom{-r}{k} (1-p)^r p^k \\ &= (1-p)^r \sum_{k \geq 0} \binom{-r}{k} (-p)^k \\ &= (1-p)^r (1-p)^{-r} \\ &= 1 \end{aligned}$$

Se anota:

$$X \sim \mathbf{NB}(r, p) \quad (16.33)$$

Por la discusión precedente  $r$  puede ser un real positivo, no solo un entero. Para la función generatriz de probabilidad tenemos:

$$\sum_{k \geq 0} (-1)^k \binom{-r}{k} (1-p)^r p^k z^k = (1-p)^r \sum_{k \geq 0} \binom{-r}{k} (-pz)^k = \left( \frac{1-p}{1-pz} \right)^r \quad (16.34)$$

Otra situación común es tener  $n$  posibilidades todas igualmente probables (1 a  $n$ , como en el caso de lanzar un dado). La distribución es simplemente:

$$\Pr(X = k) = \begin{cases} \frac{1}{n} & \text{si } 1 \leq k \leq n \\ 0 & \text{caso contrario} \end{cases} \quad (16.35)$$

La función generatriz de probabilidad es:

$$\sum_{1 \leq k \leq n} \frac{z^k}{n} = \frac{z(1-z^n)}{n(1-z)} \quad (16.36)$$

### 16.7. Valor esperado

Aunque la distribución de una variable aleatoria contiene toda la información sobre probabilidades, suele ser más útil contar con características numéricas simples. Formalmente:

**Definición 16.5.** Sea  $X$  una variable aleatoria discreta con valores reales y  $g: \mathbb{R} \rightarrow \mathbb{R}$  una función arbitraria. El *valor esperado* de  $g(X)$  se define como:

$$\mathbb{E}[g(X)] = \sum_{x \in \Omega} g(x) \Pr(X = x) \quad (16.37)$$

El caso más importante es el valor esperado de  $X$ , que amerita notación especial:

$$\mu = \mathbb{E}[X] \quad (16.38)$$

Por ejemplo, si  $X$  representa el número de puntos resultantes de lanzar un dado, suponiendo que todas las caras tienen la misma probabilidad:

$$\mathbb{E}[X] = \sum_{1 \leq k \leq 6} k \Pr(X = k) = \frac{1}{6} \sum_{1 \leq k \leq 6} k = \frac{7}{2}$$

Este ejemplo incidentalmente muestra que  $\mathbb{E}[X]$  no tiene porqué ser un posible resultado del experimento.

Una consecuencia extremadamente importante de la definición 16.5 es que el valor esperado es lineal:

**Teorema 16.8.** *Sea la variable aleatoria  $(X, Y)$  con distribución  $f_{(X,Y)}(x, y)$ . Sean  $\alpha$  y  $\beta$  números reales y  $g$  y  $h$  funciones arbitrarias de las variables aleatorias  $X$  e  $Y$ , respectivamente. Entonces:*

$$\mathbb{E}[\alpha g(X) + \beta h(Y)] = \alpha \mathbb{E}[g(X)] + \beta \mathbb{E}[h(Y)]$$

Nótese que no se hacen suposiciones sobre independencia de  $X$  e  $Y$ .

*Demostración.* Por definición:

$$\begin{aligned} \mathbb{E}[\alpha g(X) + \beta h(Y)] &= \sum_{(x,y)} (\alpha g(x) f_{(X,Y)}(x, y) + \beta h(y) f_{(X,Y)}(x, y)) \\ &= \alpha \sum_{x,y} g(x) f_{(X,Y)}(x, y) + \beta \sum_{x,y} h(y) f_{(X,Y)}(x, y) \\ &= \alpha \sum_x g(x) \sum_y f_{(X,Y)}(x, y) + \beta \sum_y h(y) \sum_x f_{(X,Y)}(x, y) \\ &= \alpha \sum_x g(x) f_X(x) + \beta \sum_y h(y) f_Y(y) \\ &= \alpha \mathbb{E}[g(X)] + \beta \mathbb{E}[h(Y)] \end{aligned} \quad \square$$

Nótese que esto vale incluso en caso que  $X = Y$ , el caso más extremo de dependencia entre las variables.

Resulta de interés acotar la dispersión de los posibles resultados.

**Teorema 16.9** (Desigualdad de Markov). *Sea  $X$  una variable aleatoria. Entonces para  $k > 0$ :*

$$\mathbb{P}(|X| \geq k) \leq \mathbb{E}[|X|]/k \quad (16.39)$$

*Demostración.* La desigualdad se cumple trivialmente a menos que  $k > \mathbb{E}[|X|]$ . Para tales  $k$ :

$$\begin{aligned} k\mathbb{P}(|X| \geq k) &= \sum_{r \geq k} k\mathbb{P}(|X| = r) \\ &\leq \sum_{r \geq k} r\mathbb{P}(|X| = r) \\ &\leq \sum_{r \geq 0} r\mathbb{P}(|X| = r) \\ &= \mathbb{E}[|X|] \end{aligned}$$

□

Una importante medida de la dispersión de los datos es la *varianza*, definida para una variable aleatoria  $X$  y una función  $g$  como:

$$\text{var}[g(X)] = \mathbb{E}[(g(X) - \mathbb{E}(g(X)))^2] \quad (16.40)$$

Podemos expresar:

$$\begin{aligned} \text{var}[g(X)] &= \mathbb{E}[(g(X) - \mathbb{E}(g(X)))^2] \\ &= \mathbb{E}[g^2(X)] - 2(\mathbb{E}[g(X)])^2 + (\mathbb{E}[g(X)])^2 \\ &= \mathbb{E}[g^2(X)] - (\mathbb{E}[g(X)])^2 \end{aligned} \quad (16.41)$$

Esto es más cómodo para cálculos.

Comúnmente se usa la *desviación estándar*, definida mediante:

$$\sigma_X = \sqrt{\text{var}[X]} \quad (16.42)$$

Nuevamente podemos obtener una cota elemental:

**Teorema 16.10** (Desigualdad de Chebychev). *Sea  $X$  una variable aleatoria, y sea  $k > 0$  un número real. Si el valor esperado de  $X$  es  $\mu = \mathbb{E}[X]$  y su desviación estándar es  $\sigma = \sqrt{\text{var}[X]}$  entonces:*

$$\mathbb{P}(|X - \mu| \leq k\sigma) \geq 1 - \frac{1}{k^2} \quad (16.43)$$

*Demostración.* Sea  $A = \{r : |x - \mu| > k\sigma\}$ . Entonces:

$$\begin{aligned} \text{var}[X] &= \mathbb{E}[(X - \mu)^2] \\ &= \sum_r (r - \mu)^2 \mathbb{P}(X = r) \\ &\geq \sum_{r \in A} (r - \mu)^2 \mathbb{P}(X = r) \\ &\geq k^2 \sigma^2 \sum_{r \in A} \mathbb{P}(X = r) \\ &= k^2 \sigma^2 \mathbb{P}(|X - \mu| > k\sigma) \end{aligned}$$

El resultado sigue de  $\text{var}[X] = \sigma^2$ .

□

Supongamos una variable aleatoria  $X$  con distribución  $f_X$  y función generatriz de probabilidad  $G$ . Es simple ver que:

$$\mathbb{E}[X] = \sum_x x f_X(x) = G'(1) \quad (16.44)$$

De forma similar:

$$G''(1) = \sum_x x(x-1)f_X(x) = E[X^2] - E[X]$$

Acá usamos el teorema 16.8;  $X^2$  y  $X$  definitivamente no son independientes, pero igual podemos sumar sus valores esperados. Combinando esto con (16.41) y recordando (16.44) resulta:

$$\text{var}[X] = G''(1) + G'(1) - (G'(1))^2 \quad (16.45)$$

Conociendo la función generatriz de probabilidad directamente tenemos los valores resumen más importantes de la variable. El lector curioso los tabulará para las distribuciones discutidas en la sección 16.2.

# 17 Series formales de potencias

---

Nuestro interés en las series de potencias no es en su capacidad de definir funciones, sino simplemente como una representación compacta de una secuencia infinita. El desarrollo de la teoría de series formales nació de la observación que ciertas manipulaciones de series “como si fueran polinomios” entregaban resultados correctos, incluso cuando una revisión más detallada demostraba que las operaciones no tenían validez. Quien primero buscó justificaciones formales de considerar series como “polinomios infinitos” fue Niven [267]. Resumiremos los resultados más importantes del área, que corroboran nuestras manipulaciones, a primera vista irresponsables y sin justificación, en los capítulos anteriores. Incluso veremos que las manipulaciones pueden justificarse si los coeficientes de la serie pertenecen a un anillo, no necesariamente son números reales o complejos. Esto es notable, estamos usando sumas infinitas en ámbitos en los cuales el concepto de límite necesario para justificar convergencia no es aplicable directamente.

## 17.1. Un primer ejemplo

Si dejamos de lado el requerimiento de que la serie converja (y defina una función), podemos darle sentido incluso a series como:

$$f(z) = \sum_{n \geq 0} n! z^n \tag{17.1}$$

que solo convergen para  $z = 0$ , y para las que el análisis no tiene ningún uso. Podemos considerar la serie (17.1) como la función generatriz ordinaria de los factoriales. Así:

$$\begin{aligned} zf(z) &= \sum_{n \geq 0} n! z^{n+1} \\ D(zf(z)) &= \sum_{n \geq 0} (n+1)! z^n = \frac{f(z)-1}{z} \end{aligned}$$

Por el otro lado, derivando el producto:

$$\begin{aligned} D(zf(z)) &= f(z) + zf'(z) \\ zf'(z) &= \frac{f(z)-1}{z} - f(z) \end{aligned}$$

El lado derecho es la función generatriz de  $(n+1)! - n!$ , e invita a sumar (dividir por  $1-z$  en funciones generatrices):

$$\begin{aligned} \frac{zf'(z)}{1-z} &= \frac{1}{1-z} \left( \frac{f(z)-1}{z} - (f(z)-1) - 1 \right) \\ &= \frac{1}{1-z} \left( (f(z)-1) \left( \frac{1}{z} - 1 \right) \right) - \frac{1}{1-z} \\ &= \frac{1}{1-z} \left( (f(z)-1) \frac{1-z}{z} \right) - \frac{1}{1-z} \\ &= \frac{f(z)-1}{z} - \frac{1}{1-z} \end{aligned}$$

Como:

$$\begin{aligned} zf'(z) &\xrightarrow{\text{ogf}} \langle n n! \rangle_{n \geq 0} \\ \frac{zf'(z)}{1-z} &\xrightarrow{\text{ogf}} \left\langle \sum_{0 \leq k \leq n} k \cdot k! \right\rangle_{n \geq 0} \end{aligned}$$

Aplicando nuevamente las propiedades, vemos que:

$$\sum_{0 \leq k \leq n} k \cdot k! = (n+1)! - 1 \quad (17.2)$$

A pesar de su espeluznante derivación (no falta un paso en que no hagamos operaciones al menos dudosas con series infinitas que solo para  $z = 0$  convergen) la relación (17.2) es correcta, cosa que el lector escéptico demostrará por inducción. Resulta que estas operaciones pueden justificarse rigurosamente, tema que nos ocupará en este capítulo.

Parte de lo que sigue viene de Shoup [323], las justificaciones siguen a Kauers [198]. Operaciones con series pueden efectuarse con paquetes de álgebra simbólica, como maxima [251], o aún mejor con sistemas especializados como PARI/GP [278]. La biblioteca GiNaC [29, 142] permite manipular expresiones simbólicas, incluyendo series formales, y numéricas directamente en C++.

## 17.2. Definición de serie formal

Sea la serie:

$$\sum_{n \geq 0} a_n z^n$$

donde los elementos  $a_n$  pertenecen a un anillo  $R$ .

Acá como en polinomios formales (capítulo 9)  $z$  es simplemente un *símbolo* (también llamado *indeterminada* o *variable*). La consideramos como una construcción puramente formal, sin darle sentido a  $z$  ni preocuparse por convergencia. La única restricción que impone esto es que toda vez que se calcula un coeficiente deben efectuarse un número finito de operaciones (en un anillo arbitrario no son aplicables las ideas de límite y convergencia, necesarias para darle sentido a un número infinito de operaciones). Trataremos el caso en que  $R$  es un campo, o al menos un dominio integral (un anillo comunitativo sin divisores de cero distintos de cero). Para evitar tener que mencionarlo infinitad de veces, usaremos la convención que  $R$  es un anillo general,  $D$  es un dominio integral y  $F$  es un campo.

Definimos la igualdad entre series formales sobre el anillo  $R$ :

$$\sum_{n \geq 0} a_n z^n = \sum_{n \geq 0} b_n z^n \quad \text{cuando } a_n = b_n \text{ para todo } n \geq 0$$

Definimos además las operaciones:

$$\begin{aligned}\alpha \sum_{n \geq 0} a_n z^n &= \sum_{n \geq 0} (\alpha a_n) z^n \quad \text{para } \alpha \in R \text{ o } \alpha \in \mathbb{Z} \\ \sum_{n \geq 0} a_n z^n + \sum_{n \geq 0} b_n z^n &= \sum_{n \geq 0} (a_n + b_n) z^n \\ \left( \sum_{r \geq 0} a_r z^r \right) \cdot \left( \sum_{s \geq 0} b_s z^s \right) &= \sum_{\substack{r \geq 0 \\ s \geq 0}} a_r b_s z^{r+s} \\ &= \sum_{\substack{n \geq 0 \\ 0 \leq k \leq n}} a_k b_{n-k} z^n \\ &= \sum_{n \geq 0} \left( \sum_{0 \leq k \leq n} a_k b_{n-k} \right) z^n\end{aligned}$$

Notar que en particular, para constantes  $\alpha$  y  $\beta$ :

$$\alpha \sum_{n \geq 0} a_n z^n + \beta \sum_{n \geq 0} b_n z^n = \sum_{n \geq 0} (\alpha a_n + \beta b_n) z^n$$

Las series formales como generalmente usadas hasta acá son un espacio vectorial de dimensión infinita sobre el campo  $\mathbb{R}$  (con base  $\{z^k\}_{k \geq 0}$ ), con la operación adicional de multiplicación.

Es rutina verificar que las series formales de potencias sobre el dominio integral  $D$  con variable  $z$  son un dominio integral, con:

$$\begin{aligned}0 &= \sum_{n \geq 0} 0 z^n \\ 1 &= \sum_{n \geq 0} [n = 0] z^n\end{aligned}$$

Al anillo de series formales sobre el anillo  $R$  lo llamaremos  $R[[z]]$  (recuérdese que llamamos  $R[z]$  al anillo de polinomios en  $z$  sobre  $R$ ). Para evitar distinciones inútiles consideramos  $R[z]$  subanillo de  $R[[z]]$  de la forma natural.

### 17.3. Unidades y recíprocos

Sea  $F$  un campo. En el anillo de series formales  $F[[z]]$  hay unidades que no son simplemente constantes (como ocurre en el correspondiente anillo de polinomios formales). Por ejemplo, en  $\mathbb{C}[[z]]$ :

$$(1 - z) \cdot (1 + z + z^2 + z^3 + \dots) = (1 + z + z^2 + \dots) - (z + z^2 + z^3 + \dots) = 1$$

Si  $a_0 = 0$  la serie no puede tener recíproco, ya que no hay forma de crear un término constante del producto en tal caso.

Por otro lado, supongamos que  $a_0 \neq 0$ :

$$\begin{aligned}\left( \sum_{n \geq 0} a_n z^n \right) \cdot \left( \sum_{n \geq 0} b_n z^n \right) &= 1 \\ \sum_{n \geq 0} \left( \sum_{0 \leq k \leq n} a_{n-k} b_k \right) z^n &= 1\end{aligned}$$

Para  $n = 0$  debe ser  $a_0 b_0 = 1$ , o sea,  $b_0 = 1/a_0$ ; luego para  $n > 0$  las sumas deben anularse:

$$b_n = -\frac{1}{a_0} \sum_{0 \leq k \leq n-1} a_{n-k} b_k$$

Con esto último se obtiene la secuencia de todos los  $b_n$ , que es la secuencia de coeficientes del recíproco de la serie  $A(z)$ .

### 17.4. Secuencias de series

Para justificar rigurosamente el operar con series formales debemos desarrollar el marco adecuado. En términos generales, las operaciones son válidas siempre que el cálculo de cada coeficiente involucre un número finito de operaciones. Por ejemplo, en la sección 17.3 vimos que el  $n$ -ésimo coeficiente del recíproco de una serie cuyo término constante no es cero es una combinación lineal de los coeficientes 0 al  $n - 1$  de la serie, una suma finita. En contraste, “evaluar” la serie  $A(z)$  en algún “punto” implica una suma infinita. Usaremos  $A(0)$  como una notación cómoda para  $[z^0] A(z)$ , eso sí.

Por otro lado, sí tiene sentido reemplazar  $z$  por  $z + z^2$  en la serie formal  $A(z)$  (note que en la serie que estamos reemplazando el coeficiente de  $z^0$  se anula). Observamos que:

$$(z + z^2)^n = z^n(z + 1)^n = z^n \sum_{0 \leq k \leq n} \binom{n}{k} z^k$$

Para:

$$A(z) = \sum_{n \geq 0} a_n z^n$$

resulta:

$$A(z + z^2) = \sum_{n \geq 0} a_n z^n \sum_{0 \leq k \leq n} \binom{n}{k} z^k = \sum_{n \geq 0} \left( \sum_{0 \leq k \leq n} \binom{n-k}{k} a_{n-k} \right) z^n$$

Como cada coeficiente de la nueva serie se calcula con un número finito de operaciones, tenemos una serie formal perfectamente definida.

Para generalizar esto, requerimos definir la noción de límite de secuencias en  $R[[z]]$ . Informalmente, consideramos dos series como “cercanas” si coinciden sus primeros términos.

**Definición 17.1.** El *orden* de una serie,  $\text{ord } A(z)$ , es el índice del primer coeficiente no cero.

**Definición 17.2.** La secuencia de series  $\langle A_k(z) \rangle_{k \geq 0}$  converge a la serie  $A(z)$  si

$$\lim_{k \rightarrow \infty} \text{ord}(A(z) - A_k(z)) = \infty$$

En tal caso escribimos  $\lim_{k \rightarrow \infty} A_k(z) = A(z)$ .

Si  $a_{nk} = [z^n] A_k(z)$ , hay un número finito de  $a_{nk}$  que difiere de  $[z^n] A(z)$ , y en un número finito de operaciones podemos calcular  $a_n$ .

Algunas consecuencias son las siguientes.

**Teorema 17.1.** Sean  $\langle A_n(z) \rangle_{n \geq 0}$  y  $\langle B_n(z) \rangle_{n \geq 0}$  secuencias de series que convergen a  $A(z)$  y  $B(z)$  en  $R[[z]]$ , respectivamente. Entonces:

1.  $\langle A_n(z) + B_n(z) \rangle_{n \geq 0}$  converge, y  $\lim_{n \rightarrow \infty} A_n(z) + B_n(z) = A(z) + B(z)$
2.  $\langle A_n(z) \cdot B_n(z) \rangle_{n \geq 0}$  converge, y  $\lim_{n \rightarrow \infty} A_n(z) \cdot B_n(z) = A(z) \cdot B(z)$

*Demostración.* La demostración es aplicar hechos simples como:

$$\begin{aligned} \text{ord}(A(z) + B(z)) &\geq \min\{\text{ord } A(z), \text{ord } B(z)\} \\ \text{ord}(A(z) \cdot B(z)) &\geq \text{ord } A(z) + \text{ord } B(z) \end{aligned}$$

Omitiremos los detalles. □

Para series en  $R[[z]]$ :

$$A(z) = \sum_{n \geq 0} a_n z^n \quad B(z) = \sum_{n \geq 0} b_n z^n$$

Si  $b_0 = 0$ ,  $\text{ord}(B(z))^k \geq k$ . Consideremos la secuencia:

$$C_0(z) = a_0$$

$$C_1(z) = a_0 + a_1 B(z)$$

$$C_2(z) = a_0 + a_1 B(z) + a_2 (B(z))^2$$

⋮

$$C_k(z) = a_0 + a_1 B(z) + a_2 (B(z))^2 + \cdots + a_k (B(z))^k$$

Los coeficientes de  $C_k(z)$  coinciden hasta el de orden  $k$  con todos los sucesores en la secuencia, luego esta converge a una serie  $C(z)$ .

**Definición 17.3.** Definimos la *composición* de las series  $A(z)$  y  $B(z)$ , donde  $b_0 = 0$ , como:

$$A(B(z)) = \sum_{n \geq 0} a_n (B(z))^n = \lim_{k \rightarrow \infty} C_k(z)$$

Un teorema importante es:

**Teorema 17.2.** Para todo  $U(z) \in R[[z]]$  con  $U(0) = 0$ , el mapa  $\Phi_U: R[[z]] \rightarrow R[[z]]$  definido mediante  $\Phi_U(A(z)) = A(U(z))$  es un homomorfismo de anillo.

*Demostración.* Sean:

$$A(z) = \sum_{n \geq 0} a_n z^n \quad B(z) = \sum_{n \geq 0} b_n z^n$$

Demostrar que  $\Phi_U(A(z) + B(z)) = \Phi_U(A(z)) + \Phi_U(B(z))$  es simple, y queda de ejercicio.

Para la multiplicación:

$$\begin{aligned} & \Phi_U(A(z) \cdot B(z)) - \Phi_U(A(z)) \cdot \Phi_U(B(z)) \\ &= \sum_{n \geq 0} \left( \sum_{0 \leq k \leq n} a_k b_{n-k} \right) U^n - \left( \sum_{n \geq 0} a_n U^n \right) \cdot \left( \sum_{n \geq 0} b_n U^n \right) \\ &= \lim_{N \rightarrow \infty} \sum_{0 \leq n \leq N} \left( \sum_{0 \leq k \leq n} a_k b_{n-k} \right) U^n \\ & \quad - \lim_{N \rightarrow \infty} \left( \sum_{0 \leq n \leq N} a_n U^n \right) \cdot \lim_{N \rightarrow \infty} \left( \sum_{0 \leq n \leq N} b_n U^n \right) \\ &= \lim_{N \rightarrow \infty} \left( \sum_{0 \leq n \leq N} \left( \sum_{0 \leq k \leq n} a_k b_{n-k} \right) U^n - \left( \sum_{0 \leq n \leq N} a_n U^n \right) \cdot \left( \sum_{0 \leq n \leq N} b_n U^n \right) \right) \\ &= - \lim_{N \rightarrow \infty} \sum_{N+1 \leq n \leq 2N} \left( \sum_{0 \leq k \leq n} a_k b_{n-k} \right) U(z)^n \end{aligned}$$

En esto hemos usado el teorema 17.1. Resta demostrar que el último límite es infinito:

$$\text{ord} \left( \sum_{N+1 \leq n \leq 2N} \left( \sum_{0 \leq k \leq n} a_k b_{n-k} \right) U(z)^n \right) \geq \text{ord } U(z)^{N+1}$$

Esto tiende a infinito cuando  $N \rightarrow \infty$ , y es  $\Phi_U(A(z) \cdot B(z)) = \Phi_U(A(z)) \cdot \Phi_U(B(z))$ .  $\square$

O sea, operar con las series  $A(z)$  y  $B(z)$  es lo mismo que operar con las series  $A(U(z))$  y  $B(U(z))$ . La importancia del teorema 17.2 radica en que expresiones como:

$$\frac{1}{1-z-z^2}$$

son ambiguas: ¿Es el recíproco de la serie  $1 - z - z^2$ , o es tal vez la composición de  $1/(1 - u)$  con  $u = z + z^2$ ? El teorema asegura que ambas son la misma serie.

Con las mismas herramientas se pueden justificar sumas y productos infinitos de series formales.

**Definición 17.4.** Sea la secuencia  $\langle A_k(z) \rangle_{k \geq 0}$  de series formales en  $R[[z]]$ . Decimos que la suma infinita

$$\sum_{k \geq 0} A_k(z)$$

converge si la secuencia

$$\sum_{0 \leq k \leq N} A_k(z)$$

converge en el sentido definido antes cuando  $N \rightarrow \infty$ . Igualmente, decimos que el producto infinito

$$\prod_{k \geq 0} A_k(z)$$

converge si la secuencia

$$\prod_{0 \leq k \leq N} A_k(z)$$

converge cuando  $N \rightarrow \infty$ .

Con esto:

**Teorema 17.3.** Sea  $\langle A_k(z) \rangle_{k \geq 0}$  una secuencia en  $R[[z]]$ . Entonces las siguientes son equivalentes:

1.  $\lim_{k \rightarrow \infty} \text{ord } A_k(z) = \infty$
2.  $\sum_{k \geq 0} A_k(z)$  converge
3.  $\prod_{k \geq 0} (1 + A_k(z))$  converge

*Demostración.* Demostraremos que (1) equivale a (2), la demostración que (1) equivale a (3) es similar y se omite.

Definamos:

$$C_n(z) = \sum_{0 \leq k \leq n} A_k(z)$$

Primero demostramos (1)  $\implies$  (2). Tenemos:

$$\forall n \exists k_0 \forall k \geq k_0: \text{ord } A_k(z) > n$$

Esto es equivalente a decir:

$$\forall n \exists k_0 \forall k \geq k_0: \text{ord}(C_{k+1}(z) - C_k(z)) > n$$

O sea, para cada  $n$  hay  $k_0$  tal que para todo  $k \geq k_0$  el valor de  $[z^n] C_k(z)$  es fijo, llamémosle  $c_n$ . Consideremos:

$$C(z) = \sum_{r \geq 0} c_r z^r$$

Por construcción:

$$\forall n \exists k_0 \forall k \geq k_0 : \text{ord}(C_k(z) - C(z)) > n$$

y la secuencia  $C_k(z)$  converge.

Ahora demostramos (2)  $\implies$  (1). Si  $C_k(z)$  converge a  $C(z)$ , entonces:

$$\forall n \exists k_0 \forall k \geq k_0 : \text{ord}(C_k(z) - C(z)) > n$$

Para tales  $n$  y  $k$  tenemos  $C_k(z) - C(z) > n$ , y:

$$[z^n] A_k(z) = [z] (C_{k+1}(z) - C_k(z)) = [z] C_{k+1}(z) - [z] C_k(z) = 0$$

lo que es equivalente a:

$$\forall n \exists k_0 \forall k \geq k_0 : \text{ord } A_k(z) > n$$

que es lo que había que demostrar.  $\square$

Nótese que en el ámbito de los reales  $a_n \rightarrow 0$  no asegura que  $\sum a_n$  ni  $\prod(1 + a_n)$  converjan.

## 17.5. El principio de transferencia

Cuando  $R = \mathbb{R}$  o  $R = \mathbb{C}$ , es obvio preguntarse sobre la relación entre la serie formal y la función definida por la serie de potencias. Es claro que no toda serie formal corresponde a una función analítica, por ejemplo la serie

$$\sum_{n \geq 0} n! z^n$$

converge únicamente para  $z = 0$ . Pero como  $0! = 1$ , tiene un recíproco como serie formal:

$$\left( \sum_{n \geq 0} n! z^n \right)^{-1} = 1 - z - z^2 - 3z^3 - 13z^4 - 71z^5 - 461z^6 - \dots$$

Razonamientos válidos para series formales no necesariamente tienen sentido para series de potencias.

Por el otro lado, si dos series de potencias son idénticas como funciones analíticas lo son como series formales:

**Teorema 17.4** (Principio de transferencia). *Sean:*

$$A(z) = \sum_{n \geq 0} a_n z^n \quad B(z) = \sum_{n \geq 0} b_n z^n$$

*funciones reales o complejas, analíticas en un vecindario  $\mathcal{U}$  no vacío de cero. Si  $A(z) = B(z)$  para todo  $z \in \mathcal{U}$ , entonces  $a_n = b_n$  para todo  $n \in \mathbb{N}_0$ .*

*Demostración.* Bajo las suposiciones,  $C(z) = A(z) - B(z)$  es analítica e idénticamente 0 en  $\mathcal{U}$ . Por el teorema de Taylor, esto significa que todos los coeficientes de  $C(z)$  son cero:

$$[z^n] C(z) = [z^n] (A(z) - B(z)) = [z^n] A(z) - [z^n] B(z) = a_n - b_n = 0 \quad \square$$

Esto permite demostrar algunas identidades en forma simple. Por ejemplo, tenemos las expansiones:

$$\begin{aligned} e^z &= \sum_{n \geq 0} \frac{z^n}{n!} && \text{para todo } z \in \mathbb{C} \\ \ln(1+z) &= \sum_{n \geq 1} \frac{z^n}{n} && \text{para } |z| < 1 \end{aligned}$$

Como para las funciones analíticas respectivas  $\exp(\ln(1+z)) = 1+z$ , esto vale para las series formales. Verificarlo en forma directa involucra largos y complicados cálculos.

### 17.6. Derivadas e integrales formales

Definimos:

$$\frac{d}{dz} \left( \sum_{n \geq 0} a_n z^n \right) = \sum_{n \geq 1} n a_n z^{n-1} = \sum_{n \geq 0} (n+1) a_{n+1} z^n$$

Esta es una definición puramente formal, no intervienen límites ni el significado de la serie como función. Definimos además para una serie formal  $f(z)$ :

$$\begin{aligned} f^{(0)}(z) &= f(z) \\ f^{(n+1)}(z) &= \frac{d}{dz} f^{(n)}(z) \end{aligned}$$

Una notación alternativa útil es:

$$Df(z) = \frac{d}{dz} f(z)$$

bajo el entendido  $D^n f(z) = f^{(n)}(z)$ . Para las primeras derivadas se suele usar:

$$f'(z) = \frac{df}{dx} \quad f''(z) = \frac{d^2 f}{dx^2} \quad f'''(z) = \frac{d^3 f}{dx^3}$$

Tenemos también:

**Teorema 17.5.** Sean  $f(z)$  y  $g(z)$  series formales. Entonces:

$$\begin{aligned} D^n (af(z) + bg(z)) &= af^{(n)}(z) + bg^{(n)}(z) \\ D^n (f(z) \cdot g(z)) &= \sum_{0 \leq k \leq n} \binom{n}{k} f^{(k)}(z) \cdot g^{(n-k)}(z) \end{aligned}$$

La fórmula para las derivadas de un producto se conoce bajo el nombre de Leibniz. Las demostraciones son rutinarias, y quedan de ejercicio.

Para la composición de series definida antes

**Teorema 17.6** (Regla de la cadena). Sean  $f(z)$  y  $g(z)$  series formales, con  $g(0) = 0$ . Entonces:

$$\frac{d}{dz} f(g(z)) = f'(g(z)) \cdot g'(z)$$

Para demostrarlo, primeramente se demuestra la derivada de una potencia de una serie, y usando esto se aplica término a término. Nuevamente es rutina, y nos ahorraremos los detalles.

De la misma manera que obtenemos derivadas término a término, podemos calcular integrales:

$$\int_0^z f(t) dt = \sum_{n \geq 1} \frac{a_{n-1}}{n} z^n$$

Es claro que se cumplen las relaciones fundamentales:

$$\frac{d}{dz} \int_0^z f(t) dt = \int_0^z \frac{d}{dt} f(t) dt = f(z)$$

Podemos anotar para la antiderivada:

$$D^{-1} f(z) = \int_0^z f(z) dz$$

## 17.7. Series en múltiples variables

Podemos también considerar series en más de una variable, si las variables son  $x$  e  $y$  anotaremos  $R[[x, y]]$ . Esto es, por ejemplo:

$$A(x, y) = \sum_{\substack{r \geq 0 \\ s \geq 0}} a_{r,s} x^r y^s$$

Es simple (aunque engorroso) demostrar que  $R[[x, y]]$  es isomorfo a  $R[[x]][[y]]$  y a  $R[[y]][[x]]$ , pero no nos detendremos en tales detalles.

Para desarrollar una teoría de secuencias en series multivariadas, definimos el *orden total* del término  $x_1^{n_1} x_2^{n_2} x_3^{n_3} \dots x_m^{n_m}$  como  $n_1 + n_2 + \dots + n_m$ . El orden (total) de la serie  $\text{ord } A(x_1, x_2, \dots, x_m)$  es el orden total del término de orden total mínimo en  $A(x_1, x_2, \dots, x_m)$ . Con esta definición si para una secuencia de series formales multivariadas  $A_k(x_1, x_2, \dots, x_n)$ :

$$\lim_{k \rightarrow \infty} \text{ord } A_k(x_1, x_2, \dots, x_n) = \infty$$

sabemos que solo en un número finito de los  $A_k(x_1, x_2, \dots, x_n)$  el coeficiente de  $x_1^{m_1} x_2^{m_2} \dots x_n^{m_n}$  difiere, y lo podemos calcular en un número finito de pasos. Omitimos los detalles de teoremas análogos a los para el caso univariado, solo notamos que esto permite justificar en  $R[[x, y]]$  series como:

$$\exp(x+y) = \sum_{n \geq 0} \frac{(x+y)^n}{n!}$$

Esto no resulta del caso univariado, en  $R[[x]][[y]]$  la serie  $x+y$  tiene término constante  $x$ , que no es cero. Podemos definir derivadas (parciales) e integrales de forma similar al caso univariado. Usaremos la notación  $D_x f$  para la derivada parcial respecto de  $x$  de la serie  $f$ , también  $f_{xy}$  para la derivada respecto de  $x$  e  $y$ .

**Teorema 17.7** (Funciones implícitas). *Sea  $A(x, y) \in F[[x, y]]$  tal que  $A(0, 0) = 0$  y  $D_y A(0, 0) \neq 0$ . Entonces existe una única serie formal  $f(x) \in F[[x]]$  con  $f(0) = 0$  tal que  $A(x, f(x)) = 0$ .*

*Demostración.* Escribamos

$$A(x, y) = \sum_{n \geq 0} a_n(x) y^n = \sum_{\substack{n \geq 0 \\ k \geq 0}} a_{nk} x^k y^n$$

donde  $a_n(x) \in F[[x]]$ . Las condiciones sobre  $A(x, y)$  resultan en  $a_0(x) = 0$  y  $a_1(x) \neq 0$ . Mostraremos cómo calcular sucesivamente los coeficientes  $f_n$  de

$$f(x) = \sum_{n \geq 0} f_n x^n$$

Como  $f(0) = 0$ , ya tenemos  $f_0 = 0$ . Enseguida:

$$[x] \sum_{n \geq 0} a_n(x) f(x)^n = 0$$

hace que baste considerar

$$[x] (a_0(x) + a_1(x)f(x)) = [x] (a_{00} + a_{01}x + a_{10}f_1 x + a_{11}f_0 x + \dots) = 0$$

de donde despejamos

$$f_1 = -\frac{a_{01}}{a_{11}}$$

Esto es válido, ya que  $a_{11} = D_y A(0, 0) \neq 0$ . Continuamos:

$$\left[ x^k \right] \sum_{n \geq 0} a_n(x) f(x)^n = 0$$

donde  $f(0) = 0$  permite truncar la suma, y se traduce en

$$\left[ x^k \right] \sum_{0 \leq n \leq k} a_n(x) f(x)^n$$

Observamos que el único término en esto que depende de  $f_k$  viene de  $a_1(0)f_k$ , todos los demás solo involucran  $f_0, \dots, f_{k-1}$ . Despejando, tenemos  $f_k$  en términos de los coeficientes anteriores, y  $f(x)$  queda determinada mediante un proceso convergente.  $\square$

Junto con el teorema 17.2, el teorema 17.7 nos dice que la sustitución  $z \rightsquigarrow U(z)$  es un isomorfismo de  $F[[z]]$  a sí mismo (un *automorfismo*) si  $\text{ord } U(z) = 1$ . Es claro que los coeficientes de tales funciones implícitas normalmente resultan bastante locos.

Por ejemplo, podemos definir:

$$W(z)e^{W(z)} = z$$

con  $W(0) = 0$ . Para esto tomamos  $A(x, y) = ye^y - x \in \mathbb{R}[[x, y]]$ , como  $A(0, 0) = 0$  y  $D_y A(0, 0) = 1 \neq 0$ , se cumplen las condiciones del teorema 17.7 y tal serie de potencias  $W(z)$  existe. La demostración da una receta para obtener los coeficientes.

Es relativamente sencillo el caso particular de ecuaciones de la forma

$$u = t\phi(u)$$

donde  $\phi$  es una función dada de  $u$ . Esta relación define  $u$  en función de  $t$ , y “estamos despejando  $u$  en términos de  $t$ ”. Fue demostrada por Lagrange y casi simultáneamente por Bürmann, la forma dada acá es la de Bürmann.

**Teorema 17.8** (Fórmula de inversión de Lagrange). *Sean  $f(u)$  y  $\phi(u)$  series formales de potencias en  $u$  sobre un campo  $F$ , con  $\phi(0) = 1$ . Entonces hay una única serie formal  $u = u(t)$  que cumple:*

$$u = t\phi(u)$$

*Además, el valor  $f(u(t))$  de  $f$  en el cero  $u = u(t)$ , expandido en serie alrededor de  $t = 0$ , cumple:*

$$[t^n] \{f(u(t))\} = \frac{1}{n} [u^{n-1}] \{f'(u)\phi(u)^n\}$$

Dadas  $f$  y  $\phi$ , esta fórmula da los coeficientes de  $f(u(t))$  en bandeja. No demostraremos este resultado, ya que nos llevaría demasiado fuera del rango de este ramo. La demostración del teorema puede encontrarse en el texto de Wilf [364].

La razón del nombre es que si  $t = A(u)$ , esta fórmula da  $u = u(t)$  mediante:

$$u = t \frac{u}{A(u)}$$

Una aplicación entretenida provee la función de Cayley, definida por:

$$C(z) = ze^{C(z)} \quad (17.3)$$

Con  $f(u) = u$  y  $\phi(u) = e^u$  tenemos directamente los coeficientes:

$$\begin{aligned} [z^n]C(z) &= \frac{1}{n}[u^{n-1}]e^{nu} \\ &= \frac{1}{n} \frac{n^{n-1}}{(n-1)!} \\ &= \frac{n^{n-1}}{n!} \end{aligned} \quad (17.4)$$

Por otro lado, con  $f(u) = e^{\gamma u}$  y  $\phi(u) = e^u$  resulta:

$$\begin{aligned} [z^n]e^{\gamma C(z)} &= \frac{1}{n}[u^{n-1}] \left( \frac{d}{du} e^{\gamma u} \cdot e^{nu} \right) \\ &= \frac{\gamma(\gamma+n)^{n-1}}{n!} \end{aligned}$$

Comparando coeficientes de:

$$e^{(\alpha+\beta)C(z)} = e^{\alpha C(z)} \cdot e^{\beta C(z)}$$

se obtiene la fórmula binomial de Abel [1]:

$$(\alpha + \beta)(\alpha + \beta + n)^{n-1} = \alpha\beta \sum_{0 \leq k \leq n} \binom{n}{k} (\alpha + k)^{k-1} (\beta + n - k)^{n-k-1} \quad (17.5)$$



# 18 La fórmula de Euler-Maclaurin

---

Es común que interese el valor de alguna suma, particularmente alguna suma infinita. En muchos casos de interés la suma converge muy lentamente, y resulta indispensable contar con alguna técnica que permita acelerarla. En otros casos una expresión simple para un valor aproximado de una suma finita resulta mucho más útil que el valor exacto. Una de las técnicas principales para aproximar sumas infinitas es la fórmula de Euler-Maclaurin. En su desarrollo toman lugar central los polinomios y números de Bernoulli, que a su vez aparecen inesperadamente en muchas situaciones combinatorias. Entre otras aplicaciones, la fórmula de Euler-Maclaurin permite obtener aproximaciones simples para factoriales y números harmónicos, valores que a su vez son ubicuos en la combinatoria (y por tanto el análisis de algoritmos).

## 18.1. Relación entre suma e integral

Conceptualmente la suma y la integral están íntimamente relacionadas, ambas podemos representarlas como áreas bajo curvas como en la figura 18.1. Pareciera ser que la integral (área bajo la

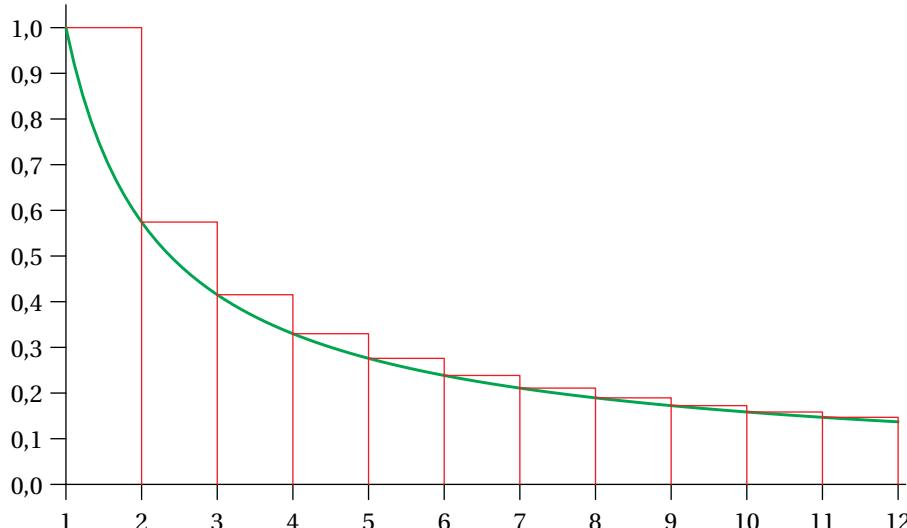


Figura 18.1 – Suma e integral como áreas

curva) y la suma (área bajo la escalera) tienden a tener una diferencia constante. Esto es exactamente lo que asegura nuestro siguiente teorema.

**Teorema 18.1** (Maclaurin-Cauchy). *Sea  $f(z)$  una función continua, positiva y que tiende monótonicamente a cero. Entonces existe la constante de Euler:*

$$\gamma_f = \lim_{n \rightarrow \infty} \left( \sum_{1 \leq k < n} f(k) - \int_1^n f(z) dz \right)$$

*Demostración.* Como  $f$  es continua, la integral existe para todo  $n \in \mathbb{N}$ . Por ser decreciente:

$$f(\lceil z \rceil) \leq f(z) \leq f(\lfloor z \rfloor)$$

Entonces:

$$\begin{aligned} \int_1^n f(\lceil z \rceil) dz &\leq \int_1^n f(z) dz \leq \int_1^n f(\lfloor z \rfloor) dz \\ \sum_{1 \leq k < n} f(k+1) &\leq \int_1^n f(z) dz \leq \sum_{1 \leq k < n} f(k) \\ \sum_{2 \leq k < n+1} f(k) &\leq \int_1^n f(z) dz \leq \sum_{1 \leq k < n} f(k) \end{aligned}$$

Así, la diferencia:

$$a_n = \sum_{1 \leq k < n} f(k) - \int_1^n f(z) dz$$

satisface  $0 \leq f(n) \leq a_n \leq f(1)$ . Además:

$$a_{n+1} - a_n = f(n+1) - \int_n^{n+1} f(z) dz \leq 0$$

O sea, la secuencia  $a_n$  es decreciente y acotada, y por tanto converge.  $\square$

Nótese que la demostración da cotas precisas:  $0 \leq \gamma_f \leq f(1)$ . Consideremos la situación geométrica: La diferencia entre la línea continua y la escalera de la figura 18.1 es una serie de “triángulos” de base 1 cuyas alturas suman  $f(1)$ , con lo que su área total es aproximadamente  $f(1)/2$ , y esto suele no ser tan mala aproximación de  $\gamma_f$ .

## 18.2. Desarrollo de la fórmula

Con la intención de tomar límites  $b \rightarrow \infty$  luego, para calcular la suma entre 1 y  $a$  escribimos:

$$\sum_{1 \leq k < b} f(k) - \int_1^b f(z) dz = \sum_{1 \leq k < a} f(k) - \int_1^a f(z) dz + \sum_{a \leq k < b} f(k) - \int_a^b f(z) dz$$

Nos falta aproximar los últimos términos.

Tomemos el tramo entre un entero y el siguiente, para simplificar el rango entre 0 y 1. Nuestro resultado final se obtendrá sumando sobre los diferentes tramos. Integrando por partes:

$$\begin{aligned} \int_0^1 f(z) dz &= zf(z) \Big|_0^1 - \int_0^1 zf'(z) dz \\ &= zf(z) \Big|_0^1 - \frac{1}{2} z^2 f'(z) \Big|_0^1 + \int_0^1 \frac{1}{2} z^2 f''(z) dz \\ &= zf(z) \Big|_0^1 - \frac{1}{2} z^2 f'(z) \Big|_0^1 + \frac{1}{2 \cdot 3} z^3 f''(z) \Big|_0^1 - \int_0^1 \frac{1}{2 \cdot 3} z^3 f'''(z) dz \end{aligned}$$

Están apareciendo las derivadas sucesivas de  $f$  multiplicadas por polinomios. Si queremos polinomios monómicos, aparecerán divididos por factoriales. Llamemos  $B_n(z)$  al polinomio monómico de grado  $n$ , partiendo con  $B_0(z) = 1$ . Integrando por partes tenemos la relación básica:

$$\int_0^1 B_n(z) f^{(n)}(z) dz = \frac{B_{n+1}(z)}{n+1} f^{(n)}(z) \Big|_0^1 - \int_0^1 \frac{B_{n+1}(z)}{n+1} f^{(n+1)}(z) dz$$

De acá:

$$B_0(z) = 1 \quad (18.1)$$

$$B'_{n+1}(z) = (n+1)B_n(z) \quad n \geq 0 \quad (18.2)$$

Queda por definir la constante de integración en (18.2). Tenemos primeramente:

$$\int_0^1 f(z) dz = \sum_{0 \leq k \leq n} \frac{(-1)^k B_{k+1}(z)}{(k+1)!} f^{(k)}(z) \Big|_0^1 - \int_0^1 (-1)^n \frac{B_{n+1}(z)}{(n+1)!} f^{(n+1)}(z) dz \quad (18.3)$$

Interesa sumar la expresión (18.3) para  $[a, a+1]$ ,  $[a+1, a+2]$ , ...,  $[b-1, b]$ , conviene que se cumpla:

$$B_n(0) = B_n(1) \quad (18.4)$$

de forma que los términos intermedios se cancelen. Como  $B_0(z) = 1$ ,  $B_1(z)$  es una función lineal que solo si fuera constante cumpliría  $B_1(0) = B_1(1)$ . La relación (18.4) es válida siempre que  $n \neq 1$ . Definimos en general:

$$B_n = B_n(1) \quad (18.5)$$

A los polinomios  $B_n(x)$  se les conoce como *polinomios de Bernoulli*, y las constantes  $B_n$  como *números de Bernoulli*, por razones que discutiremos en la sección 18.3. Los números y polinomios de Bernoulli aparecen en una amplia gama de situaciones. Debe tenerse cuidado, hay autores que definen la secuencia (bajo el mismo nombre e incluso con la misma notación) de forma que todos los elementos son cero o positivos.

En vista de la recurrencia (18.2), si  $n \geq 2$  la condición (18.4) puede expresarse también como:

$$\int_0^1 B_n(z) dz = 0 \quad (18.6)$$

Por el proceso que los produce, todos los coeficientes de los polinomios  $B_n(z)$  son racionales, por lo que también lo son las constantes  $B_n$ . Los primeros polinomios y constantes registra el cuadro 18.1. Se observa que salvo  $B_1$  los valores de  $B_n$  para  $n$  impar son cero, y que los  $B_{2n}$  alternan signo. Esto lo demostraremos en general más adelante.

Para simplificar la derivación que sigue, definimos una extensión periódica del polinomio  $B_n(z)$ :

$$\tilde{B}_n(z) = B_n(z - [z])$$

La función  $\tilde{B}_n(z)$  es continua dado que definimos  $B_n(0) = B_n(1) = B_n$  (salvo cuando  $n = 1$ ). Así tenemos:

$$\begin{aligned} \int_a^b f(z) dz &= \sum_{1 \leq k \leq n} \frac{(-1)^k \tilde{B}_k(z)}{k!} f^{(k-1)}(z) \Big|_a^b + (-1)^{n+1} \int_a^b \frac{\tilde{B}_{n+1}(z)}{(n+1)!} f^{(n+1)}(z) dz \\ &= \frac{1}{2} f(a) + \sum_{a < r < b} f(r) + \frac{1}{2} f(b) \\ &\quad + \sum_{2 \leq k \leq n} \frac{(-1)^k B_k}{k!} f^{(k-1)}(z) \Big|_a^b + (-1)^{n+1} \int_a^b \frac{\tilde{B}_{n+1}(z)}{(n+1)!} f^{(n+1)}(z) dz \\ &= \sum_{a \leq r < b} f(r) + \sum_{1 \leq k \leq n} \frac{(-1)^k B_k}{k!} f^{(k-1)}(z) \Big|_a^b + (-1)^{n+1} \int_a^b \frac{\tilde{B}_{n+1}(z)}{(n+1)!} f^{(n+1)}(z) dz \quad (18.7) \end{aligned}$$

$$\begin{aligned}
B_0(z) &= 1 & B_0 &= 1 \\
B_1(z) &= z - \frac{1}{2} & B_1 &= -\frac{1}{2} \\
B_2(z) &= z^2 - z + \frac{1}{6} & B_2 &= \frac{1}{6} \\
B_3(z) &= z^3 - \frac{3}{2}z^2 + \frac{1}{2}z & B_3 &= 0 \\
B_4(z) &= z^4 - 2z^3 + z^2 - \frac{1}{30} & B_4 &= -\frac{1}{30} \\
B_5(z) &= z^5 - \frac{5}{2}z^4 + \frac{5}{3}z^3 - \frac{1}{6}z & B_5 &= 0 \\
B_6(z) &= z^6 - 3z^5 + \frac{5}{2}z^4 - \frac{1}{2}z^2 + \frac{1}{42} & B_6 &= \frac{1}{42} \\
B_7(z) &= z^7 - \frac{7}{2}z^6 + \frac{7}{2}z^5 - \frac{7}{6}z^3 + \frac{1}{6}z & B_7 &= 0 \\
B_8(z) &= z^8 - 4z^7 + \frac{14}{3}z^6 - \frac{7}{3}z^4 + \frac{2}{3}z^2 - \frac{1}{30} & B_8 &= -\frac{1}{30} \\
B_9(z) &= z^9 - \frac{9}{2}z^8 + 6z^7 - \frac{21}{5}z^5 + 2z^3 - \frac{3}{10}z & B_9 &= 0 \\
B_{10}(z) &= z^{10} - 5z^9 + \frac{15}{2}z^8 - 7z^6 + 5z^4 - \frac{3}{2}z^2 + \frac{5}{66} & B_{10} &= \frac{5}{66}
\end{aligned}$$

Cuadro 18.1 – Polinomios y números de Bernoulli [274]

Acá aprovechamos que  $B_1 = -1/2$ , absorbimos el término  $f(a)$  en la primera sumatoria y reorganizamos.

Dividiendo el rango de la suma en (18.7)

$$\begin{aligned}
\sum_{1 \leq k < b} f(k) - \int_1^b f(z) dz &= \sum_{1 \leq k < a} f(k) - \int_1^a f(z) dz \\
&\quad - \sum_{1 \leq k \leq n} \frac{(-1)^k B_k}{k!} f^{(k-1)}(z) \Big|_a^b + (-1)^n \int_a^b \frac{\tilde{B}_{n+1}(z)}{(n+1)!} f^{(n+1)}(z) dz
\end{aligned} \tag{18.8}$$

Haciendo ahora  $b \rightarrow \infty$ , y reorganizando (18.8) bajo el entendido que:

$$\lim_{z \rightarrow \infty} f^{(n)}(z) = 0$$

Recordando que salvo  $B_1$  todos los  $B_{2k+1} = 0$ , obtenemos la fórmula de Euler-Maclaurin:

$$\sum_{1 \leq k < a} f(k) = \int_1^a f(z) dz + \gamma_f + B_1 f(a) + \sum_{1 \leq k \leq n} \frac{B_{2k}}{(2k)!} f^{(2k-1)}(a) + R_n(f; a) \tag{18.9}$$

En esto hemos escrito:

$$\gamma_f = \lim_{b \rightarrow \infty} \left( \sum_{1 \leq k \leq b} f(k) - \int_1^b f(z) dz \right) \tag{18.10}$$

$$R_n(f; a) = \int_a^\infty \frac{\tilde{B}_{2n+1}(z)}{(2n+1)!} f^{(2n+1)}(z) dz \tag{18.11}$$

Resta encontrar mejores maneras de determinar los polinomios  $B_n(z)$ , los coeficientes  $B_n = B_n(0)$ , y finalmente acotar el resto  $R_n(f; a)$ . Esto lo haremos en la sección 18.7. Lamentablemente, los  $B_n$  crecen muy rápidamente y (18.9) rara vez converge, por lo que la constante  $\gamma_f$  debe determinarse de alguna otra forma. Las cotas que daremos indican que el error cometido es a lo más el último término incluido, la fórmula igual es útil para obtener valores numéricos precisos.

### 18.3. Suma de potencias

Una aplicación obvia de la fórmula de Euler-Maclaurin es calcular las sumas:

$$S_m(n) = \sum_{1 \leq k \leq n-1} k^m$$

Ya resolvimos este problema (el desarrollo en el capítulo 14 para la suma (14.63)), daremos una perspectiva distinta. Acá tenemos:

$$\begin{aligned} f(z) &= z^m \\ f^{(k)}(z) &= m^k z^{m-k} \end{aligned}$$

La fórmula de Euler-Maclaurin sumando hasta el término  $m - 1$  (el resto es cero en este caso; en realidad estamos aplicando (18.7), no hay constante  $\gamma$  porque es parte del resto) y tomando la suma desde 0 para simplificar da:

$$\begin{aligned} S_m(n) &= \int_0^n z^m dz + \sum_{0 \leq k \leq m-1} \frac{B_{k+1}}{(k+1)!} m^k n^{m-k} \\ &= \frac{n^{m+1}}{(m+1)} + \sum_{0 \leq k \leq m-1} B_{k+1} \frac{m^k}{(k+1)!} n^{m-k} \\ &= \frac{1}{m+1} \left( n^{m+1} + \sum_{0 \leq k \leq m-1} \binom{m+1}{k+1} B_{k+1} n^{m-k} \right) \end{aligned}$$

Pero como  $B_0 = 1$ , podemos incorporar el primer término a la suma, y luego de ajustar índices queda:

$$S_m(n) = \frac{1}{m+1} \left( \sum_{0 \leq k \leq m} \binom{m+1}{k} B_k n^{m+1-k} \right) \quad (18.12)$$

Jakob Bernoulli había notado esta expansión, e incluso la usó para calcular  $S_{10}(1\,000)$ . Es en honor a su descubrimiento que llevan su nombre estos números.

La fórmula (18.12) a veces se atribuye erróneamente a Faulhaber, quien desarrolló fórmulas eficientes para expresar  $S_{2m+1}(n)$  en términos de  $n(n+1)$ . Una discusión detallada de sus resultados, reconstrucción de sus posibles métodos y una variedad de extensiones presenta Knuth [214].

### 18.4. Números harmónicos

Usemos ahora nuestro nuevo juguete para aproximar los números harmónicos. Tenemos prime-ramente:

$$D^k z^{-1} = (-1)^k z^{-k-1} = (-1)^k k! z^{-k-1}$$

Las derivadas tienden a cero cuando  $z \rightarrow \infty$ , así que vamos bien. La fórmula de Euler-Maclaurin da:

$$\begin{aligned} H_n &= \frac{1}{n} + \sum_{1 \leq r < n} \frac{1}{r} \\ &= \frac{1}{n} + \int_1^n \frac{dz}{z} + \gamma + B_1 \cdot (-1) 1! n^{-1} + \sum_{1 \leq k \leq s} \frac{B_{2k}}{(2k)!} \cdot (2k-1)! n^{-2k-2} + R_s(n) \\ &= \ln n + \frac{1}{n} + \gamma - \frac{1}{2n} + \sum_{1 \leq k \leq s} \frac{B_{2k}}{2k} \cdot n^{-2k-2} + R_s(n) \end{aligned} \quad (18.13)$$

$$= \ln n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \frac{1}{120n^4} - \frac{1}{252n^6} + O(n^{-8}) \quad (18.14)$$

Por el teorema de Maclaurin-Cauchy, existe la constante:

$$\begin{aligned} \gamma &= \lim_{n \rightarrow \infty} \left( \sum_{1 \leq k < n} \frac{1}{k} - \int_1^n \frac{dz}{z} \right) \\ &= \lim_{n \rightarrow \infty} (H_n - \ln n) \\ &\approx 0,57721\,56649\,01532\,65120 \end{aligned}$$

La aproximación simple obtenida luego del teorema de Maclaurin-Cauchy da  $\gamma \approx 1/2$ . Nada mal. Euler en 1736 obtuvo el valor de  $\gamma$  con 16 dígitos usando 8 términos de la expansión:

$$\gamma = H_{10} - \ln 10 - \frac{1}{20} + \frac{1}{1200} - \dots$$

Para calcular el número de términos requeridos para una precisión similar directamente podemos usar la aproximación que derivamos. Para la precisión que obtuvo Euler requeriríamos  $n$  tal que:

$$|\gamma - (H_n - \ln n)| \approx \frac{1}{2n} < 5 \cdot 10^{-17}$$

Resulta  $10^{16}$  términos.

Al número  $\gamma$  se le conoce como *constante de Euler* o también por *constante de Euler-Mascheroni*, por quien calculó su valor con 32 decimales, de los que solo 19 eran correctos. Gourdon y Sebah [149] incluso lo consideran el tercer número más importante de la matemática, después de  $\pi$  y  $e$ . Lagarias [227] describe la historia en bastante detalle y muestra algunos de los contextos en que aparece. Determinar si  $\gamma$  es racional, algebraico o trascendente es un problema abierto famoso.

## 18.5. Fórmula de Stirling

Veamos cómo podemos aproximar factoriales con esta herramienta. Primero tenemos:

$$\ln n! = \sum_{1 \leq k < n} \ln k + \ln n$$

El teorema de Maclaurin-Cauchy no sirve si (como acá) tenemos una función creciente. Pero en caso que la función  $f(z)$  sea monótona creciente es claro que:

$$\begin{aligned} \int_1^n \lfloor f(z) \rfloor dz &\leq \int_1^n f(z) dz \leq \int_1^n \lceil f(z) \rceil dz \\ \sum_{1 \leq k < n} f(k) &\leq \int_1^n f(z) dz \leq \sum_{1 \leq k < n} f(k+1) \\ &= \sum_{1 \leq k < n} f(k) + f(n) - f(1) \end{aligned}$$

Promediando ambas cotas (la diferencia entre la curva y las escaleras son casi triángulos) queda:

$$\sum_{1 \leq k < n} f(k) \approx \int_1^n f(z) dz - \frac{1}{2} (f(n) - f(1))$$

Hasta acá podemos decir que, burdamente:

$$\begin{aligned} \ln n! &= \sum_{1 \leq k < n} \ln n + \ln n \\ &\approx \int_1^n \ln z dz - \frac{1}{2} (\ln n - \ln 1) + \ln n \\ &= n \ln n - n + 1 + \frac{1}{2} \ln n \\ n! &\approx e \sqrt{n} \left(\frac{n}{e}\right)^n \end{aligned}$$

Esto nos hace albergar la esperanza de obtener algo útil.

Para una mejor aproximación usamos la fórmula de Euler-Maclaurin:

$$\begin{aligned} \int_1^n \ln z dz &= n \ln n - n + 1 \\ D^k \ln z &= (-1)^{k-1} (k-1)! z^{-k} \end{aligned}$$

Si suponemos que existe la constante  $\ln \sigma$  (*constante de Stirling*):

$$\ln n! = \ln n + \sum_{1 \leq k < n} \ln k \tag{18.15}$$

$$\begin{aligned} &= \ln n + \int_1^n \ln z dz + \ln \sigma + B_1 \ln n \\ &\quad + \sum_{1 \leq k \leq s} \frac{B_{2k}}{(2k)!} \cdot (-1)^{2k-2} (2k-2)! \cdot n^{-2k-1} + R_s(n) \\ &= \ln \sigma + (n+1) \ln n - n - \frac{1}{2} \ln n - \sum_{1 \leq k \leq s} \frac{B_{2k}}{(2k-1)2k} n^{-2k-1} + R_s(n) \\ &= \ln \sigma + n \ln n + \frac{1}{2} \ln n - n + \frac{1}{12n} - \frac{1}{360n^3} + \frac{1}{1260n^5} + R_3(n) \tag{18.16} \end{aligned}$$

La constante  $\ln \sigma$  en (18.16) queda determinada por el siguiente límite, si existe:

$$\begin{aligned} \ln \sigma &= \lim_{n \rightarrow \infty} \left( \sum_{1 \leq k \leq n} \ln k - \int_1^n \ln z dz \right) \\ &= \lim_{n \rightarrow \infty} (\ln n! - n \ln n - n) \end{aligned}$$

Veremos más adelante que  $\sigma = \sqrt{2\pi}$ , usando este valor en (18.16), y expandiendo la exponencial:

$$n! = \sqrt{2\pi n} \left(\frac{n}{e}\right)^n \cdot \left(1 + \frac{1}{12n} + \frac{1}{288n^2} - \frac{139}{51840n^3} - \frac{571}{2488320n^4} + O(n^{-5})\right) \tag{18.17}$$

Truncado en el primer término, queda:

$$n! \approx \sqrt{2\pi n} \left(\frac{n}{e}\right)^n \tag{18.18}$$

La ecuación (18.18) es la fórmula de Stirling para el factorial. La aproximación dada antes dice que ya para  $n \geq 8$  el error es de cerca de 1%, cosa que cálculo directo confirma.

Nótese que  $\sigma = \sqrt{2\pi} = 2,5066$ , nuestra burda aproximación  $\sigma \approx e$  no era tan mala. Falta el valor de  $\ln \sigma$ . Por el producto de Wallis (lo demostraremos más adelante):

$$\begin{aligned}\frac{\pi}{2} &= \prod_{k \geq 1} \frac{2k}{2k-1} \cdot \frac{2k}{2k+1} \\ &= \lim_{n \rightarrow \infty} \prod_{1 \leq k \leq n} \left( \frac{2k}{2k-1} \cdot \frac{2k}{2k} \right) \cdot \left( \frac{2k}{2k} \cdot \frac{2k}{2k+1} \right) \\ &= \lim_{n \rightarrow \infty} \frac{(2n!)^4}{(2n)!(2n+1)!} \\ &= \lim_{n \rightarrow \infty} \frac{1}{2n+1} \cdot \frac{2^{4n} n!^4}{(2n)!^2}\end{aligned}$$

Substituyendo la aproximación (18.16) para los factoriales:

$$\begin{aligned}\frac{\pi}{2} &= \lim_{n \rightarrow \infty} \frac{1}{2n+1} \cdot \frac{2^{4n} \sigma^4 n^2 (n/e)^{4n}}{\sigma^2 (2n) (2n/e)^{4n}} \\ \sigma^2 &= 2\pi\end{aligned}$$

Para completar, demostraremos el producto de Wallis, siguiendo a Lynn [246].

**Teorema 18.2** (Producto de Wallis). *Tenemos:*

$$\frac{\pi}{2} = \prod_{k \geq 1} \frac{2k}{2k-1} \cdot \frac{2k}{2k+1}$$

*Demostración.* Definamos:

$$a_n = \int_0^{\pi/2} \sin^n z dz$$

Como  $0 \leq \sin z \leq 1$  en el rango  $0 \leq z \leq \pi/2$ ,  $\langle a_n \rangle_{n \geq 0}$  es una secuencia positiva y monótona decreciente. Integrando por partes:

$$\begin{aligned}a_n &= -\sin^{n-1} z \cos z \Big|_0^{\pi/2} + \int_0^{\pi/2} (n-1) \sin^{n-2} z \cos^2 z dz \\ &= \int_0^{\pi/2} (n-1) \sin^{n-2} z (1 - \sin^2 z) dz\end{aligned}$$

O sea  $a_n = (n-1)a_{n-2} - (n-1)a_n$ , que resulta en:

$$a_n = \frac{n-1}{n} a_{n-2} \tag{18.19}$$

Por el otro lado, directamente tenemos  $a_0 = \pi/2$  y  $a_1 = 1$ . Con estos puntos de partida en (18.19):

$$a_{2n} = \frac{\pi}{2} \cdot \frac{1}{2} \cdot \dots \cdot \frac{2n-1}{2n} \tag{18.20}$$

$$a_{2n+1} = \frac{2}{3} \cdot \frac{4}{5} \cdot \dots \cdot \frac{2n}{2n+1} \tag{18.21}$$

Como la secuencia  $a_n$  es decreciente,  $a_{2n+1} \leq a_{2n} \leq a_{2n-1}$ , y de la recurrencia (18.19):

$$1 \leq \frac{a_{2n}}{a_{2n+1}} \leq \frac{a_{2n-1}}{a_{2n+1}} = 1 + \frac{1}{2n}$$

En consecuencia:

$$\lim_{n \rightarrow \infty} \frac{a_{2n}}{a_{2n+1}} = 1 \quad (18.22)$$

y por (18.22) con (18.20) y (18.21):

$$\lim_{n \rightarrow \infty} \frac{\pi}{2} \cdot \frac{1 \cdot 3 \cdots (2n-1)}{2 \cdot 4 \cdots (2n)} \cdot \frac{3 \cdot 5 \cdots (2n+1)}{2 \cdot 4 \cdots (2n)} = 1$$

que es equivalente a lo planteado.  $\square$

Una muy bonita demostración alternativa (originalmente de Euler, quien de forma similar obtuvo muchos otros resultados sorprendentes) es la siguiente. Tiene el problema de basarse en la fórmula de Euler para el seno, que es muy sugestiva pero no es sencilla de demostrar.

*Demostración.* La fórmula de Euler para el seno resulta de considerar esta función impar como un “polinomio infinito” con ceros 0 y  $\pm n\pi$ , como también:

$$\lim_{z \rightarrow 0} \frac{\sin z}{z} = 1$$

el coeficiente de  $z$  debe ser 1, por lo que puede expresarse:

$$\begin{aligned} \frac{\sin z}{z} &= \left(1 - \frac{z^2}{\pi^2}\right) \left(1 - \frac{z^2}{4\pi^2}\right) \left(1 - \frac{z^2}{9\pi^2}\right) \cdots \\ &= \prod_{k \geq 1} \left(1 - \frac{z^2}{k^2\pi^2}\right) \end{aligned}$$

Notamos que para  $z = \pi/2$ :

$$\begin{aligned} \frac{2}{\pi} &= \prod_{k \geq 1} \left(1 - \frac{1}{4k^2}\right) \\ \frac{\pi}{2} &= \prod_{k \geq 1} \left(\frac{4k^2}{4k^2 - 1}\right) \\ &= \prod_{k \geq 1} \frac{(2k)(2k)}{(2k-1)(2k+1)} \end{aligned}$$

$\square$

## 18.6. Propiedades de los polinomios y números de Bernoulli

Derivaremos algunas propiedades adicionales de los polinomios y números de Bernoulli. Algunas ya las usamos, otras las necesitaremos más adelante. En el proceso mostraremos algunas técnicas útiles para obtener información sobre los coeficientes de una serie.

De la recurrencia (18.2):

$$B'_n(z) = nB_{n-1}(z)$$

Con esto, à la Maclaurin en  $y$ :

$$\begin{aligned} B_n(z+y) &= B_n(z) + nB_{n-1}(z)y + \frac{n(n-1)}{2}B_{n-2}(z)y^2 + \cdots \\ &= \sum_{0 \leq k \leq n} \binom{n}{k} B_{n-k}(z)y^k \end{aligned} \quad (18.23)$$

Si ahora hacemos  $z = 0$  en (18.23), recordamos  $B_n(0) = B_n$  y cambiamos variables  $y \rightsquigarrow z$  en el resultado:

$$B_n(z) = \sum_{0 \leq k \leq n} \binom{n}{k} B_{n-k} z^k \quad (18.24)$$

Para  $z = 1$ , como  $B_n(1) = B_n$  salvo para  $n = 1$ , resulta:

$$B_n = \sum_{0 \leq k \leq n} \binom{n}{k} B_k \quad (18.25)$$

Si en (18.25) interpretamos  $\mathbf{B}^n$  como  $B_n$  tenemos la linda fórmula:

$$\mathbf{B}^n = (1 + \mathbf{B})^n \quad (18.26)$$

En la linda fórmula (18.26) para  $B_{n+1}$  se cancelan los  $B_{n+1}$ , y puede despejarse  $B_n$  dando la relación válida para  $n \geq 1$ :

$$B_n = -\frac{1}{n+1} \sum_{0 \leq k \leq n-1} \binom{n+1}{k} B_k$$

Por los factoriales definamos una función generatriz exponencial para los polinomios  $B_n(x)$  (estamos trabajando con series sobre el anillo  $\mathbb{Q}[x]$ ):

$$B(x, z) = \sum_{n \geq 0} B_n(x) \frac{z^n}{n!} \quad (18.27)$$

De la recurrencia (18.2) para los polinomios:

$$\begin{aligned} \frac{\partial B(x, z)}{\partial x} &= \sum_{n \geq 1} B'_n(x) \frac{z^n}{n!} \\ &= z \sum_{n \geq 1} B_{n-1}(x) \frac{z^{n-1}}{(n-1)!} \\ &= zB(x, z) \end{aligned} \quad (18.28)$$

La ecuación (18.28) indica que para alguna función  $c(z)$  que no depende de  $x$ :

$$B(x, z) = c(z) e^{xz} \quad (18.29)$$

Usamos ahora la otra condición sobre los polinomios. Debe cumplirse:

$$\begin{aligned} \int_0^1 B(x, z) dx &= \sum_{n \geq 0} \frac{z^n}{n!} \int_0^1 B_n(x) dx \\ &= 1 \end{aligned}$$

De nuestra expresión (18.29) para  $B(x, z)$ :

$$\begin{aligned} \int_0^1 B(x, z) dx &= c(z) \int_0^1 e^{xz} dx \\ &= c(z) \frac{1}{z} (e^z - 1) \end{aligned}$$

Comparando ambas expresiones para la integral obtenemos  $c(z)$ , y finalmente:

$$B(x, z) = \sum_{n \geq 0} B_n(x) \frac{z^n}{n!} = \frac{ze^{xz}}{e^z - 1} \quad (18.30)$$

Para justificar algunas de las manipulaciones que siguen, debemos asegurarnos que esta serie converge uniformemente para  $0 \leq z \leq 1$  (no hay problemas con  $x$ ). La función (18.30) en  $z = 0$  tiene una singularidad removible, y tiene polos en  $z = \pm 2n\pi i$  para  $n \geq 1$ , por lo que el radio de convergencia es  $2\pi > 1$ . Para detalles de estos conceptos véase el capítulo 28.

Con  $x = 0$  obtenemos la función generatriz de los coeficientes  $B_n = B_n(0)$ :

$$B(0, z) = \sum_{n \geq 0} B_n \frac{z^n}{n!} = \frac{z}{e^z - 1} \quad (18.31)$$

De los valores dados antes pareciera ser que los valores para índices impares son todos cero, salvo  $B_1 = -1/2$ . Consideremos la función:

$$\begin{aligned} \frac{z}{e^z - 1} + \frac{z}{2} &= \frac{z}{2} \cdot \frac{e^z + 1}{e^z - 1} \\ &= \frac{z}{2} \coth \frac{z}{2} \end{aligned}$$

Esta función es par, confirmando nuestra sospecha.

Anotamos el resultado siguiente en términos de la función  $\zeta$  de Riemann:

$$\zeta(z) = \sum_{n \geq 1} n^{-z} \quad (18.32)$$

Uno de los resultados más sensacionales de Euler fue la solución en 1734 del problema de Basilea, que venía siendo un tema recurrente desde 1650. Se buscaba el valor de la serie:

$$\zeta(2) = \sum_{n \geq 1} \frac{1}{n^2} \quad (18.33)$$

Hizo mucho más que esto, hallando los valores de  $\zeta(2k)$  para  $k$  hasta 13. Luego halló la fórmula general, para la que hay hermosas demostraciones (ver Aigner y Ziegler [6] o Kalman [193]). Podemos seguir uno de los razonamientos de Euler (Dunham [105] da otras de las demostraciones y algo del sabor del trabajo original) como sigue.

Por la fórmula de Euler para la exponencial de un complejo:

$$\begin{aligned} \cot z &= \frac{\cos z}{\sin z} \\ &= i \frac{e^{iz} + e^{-iz}}{e^{iz} - e^{-iz}} \\ &= i + \frac{2i}{e^{2iz} - 1} \\ \frac{z}{2} \cot \frac{z}{2} &= \frac{iz}{2} + \frac{iz}{e^{iz} - 1} \end{aligned}$$

Manejado los primeros dos términos en forma especial queda:

$$\frac{z}{2} \cot \frac{z}{2} = 1 + \sum_{k \geq 2} B_k \frac{(iz)^k}{k!} \quad (18.34)$$

Por el otro lado tenemos la fórmula de Euler para el seno:

$$\sin z = z \prod_{n \geq 1} \left(1 - \frac{z^2}{n^2 \pi^2}\right) \quad (18.35)$$

Aplicando  $zD\log$  a (18.35):

$$z \frac{d}{dz} \ln \sin z = z \frac{\cos z}{\sin z} = z \cot z$$

Con esto tenemos:

$$\begin{aligned} z \cot z &= 1 - \sum_{n \geq 1} \frac{2z^2}{1 - (z^2/n^2 \pi^2)} \\ &= 1 - 2 \sum_{n \geq 1} \sum_{k \geq 0} \frac{z^{2k+2}}{n^{2k} \pi^{2k}} \\ &= 1 - 2 \sum_{k \geq 0} \frac{z^{2k+2}}{\pi^{2k}} \cdot \sum_{n \geq 1} \frac{1}{n^{2k}} \\ &= 1 - 2 \sum_{k \geq 0} \frac{z^{2k+2} \zeta(2k)}{\pi^{2k}} \\ \frac{z}{2} \cot \frac{z}{2} &= 1 - 2 \sum_{k \geq 0} \frac{z^{2k+2} \zeta(2k)}{2^{2k+2} \pi^{2k}} \end{aligned} \quad (18.36)$$

Comparando coeficientes de  $z^{2k}$  entre (18.34) y (18.36) resulta:

$$\zeta(2k) = \frac{(-1)^{k+1} 4^k \pi^{2k} B_{2k}}{2(2k)!}$$

Incidentalmente, esto demuestra que los números  $B_{2k}$  alternan signo, ya que  $\zeta(2k)$  claramente es positivo. Como  $\zeta(2k) \sim 1$ , usando la fórmula de Stirling (18.18):

$$\begin{aligned} B_{2k} &\sim (-1)^{k+1} \frac{2(2k)!}{4^k \pi^{2k}} \\ &\sim (-1)^{k+1} 4\sqrt{k\pi} \left(\frac{k}{\pi e}\right)^{2k} \end{aligned} \quad (18.37)$$

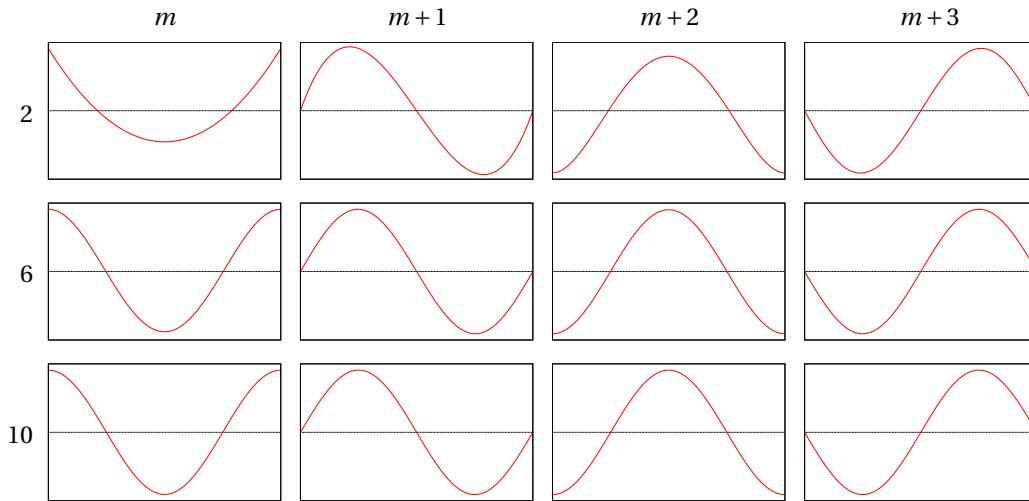
Con este crecimiento de  $B_{2k}$  las derivadas de  $f$  deben disminuir muy rápidamente para que la fórmula de Euler-Maclaurin converja.

La figura 18.2 grafica algunos polinomios de Bernoulli en el rango que nos interesa. Pareciera ser que  $B_{2k}(z)$  es simétrica alrededor de  $1/2$ , mientras  $B_{2k+1}(z)$  es antisimétrica. Para demostrar estos hechos consideramos:

$$\begin{aligned} B(1/2 + u, z) + B(1/2 - u, z) &= \frac{ze^{z(1/2+u)}}{e^z - 1} + \frac{ze^{z(1/2-u)}}{e^z - 1} \\ &= \frac{ze^{z/2}}{e^z - 1} \cdot (e^{zu} + e^{-zu}) \end{aligned}$$

Esta expresión es par en  $z$ :

$$\begin{aligned} \frac{-ze^{-z/2}}{e^{-z} - 1} \cdot \frac{e^z}{e^z} &= \frac{-ze^{z/2}}{1 - e^z} \\ &= \frac{ze^{z/2}}{e^z - 1} \end{aligned}$$

Figura 18.2 – Polinomios de Bernoulli en  $[0, 1]$  (escalados de mínimo a máximo)

Esto significa que los términos para  $z^{2k+1}$  se anulan:

$$B_{2k+1}(1/2 - u) = -B_{2k+1}(1/2 + u)$$

En particular,  $B_{2k+1}(1/2) = 0$ .

De forma similar:

$$\begin{aligned} B(1/2 + u, z) - B(1/2 - u, z) &= \frac{ze^{z(1/2+u)}}{e^z - 1} - \frac{ze^{z(1/2-u)}}{e^z - 1} \\ &= \frac{ze^{z/2}}{e^z - 1} \cdot (e^{zu} - e^{-zu}) \end{aligned}$$

Esta expresión es impar en  $z$ , lo que significa que ahora se anularon los términos pares:

$$B_{2k}(1/2 - u) = B_{2k}(1/2 + u)$$

De las gráficas 18.2 en el rango  $[0, 1]$  se ve que el polinomio  $B_{2k}(z)$  tiene dos ceros, mientras  $B_{2k+1}(z)$  tiene tres ( $0$  y  $\pm 1$ ). Esto vale en general.

**Teorema 18.3.** *Para  $k > 0$ , en el rango  $[0, 1]$  el polinomio  $B_{2k}(z)$  tiene exactamente dos ceros, mientras  $B_{2k+1}(z)$  tiene exactamente tres ( $0, 1/2$  y  $1$ ).*

*Demuestra*o. Demostramos por inducción que para  $k \geq 1$  en  $[0, 1/2]$  el polinomio  $B_{2k}(z)$  tiene exactamente un cero, y que  $B_{2k+1}(z)$  no cambia de signo y se anula únicamente en los extremos. De partida, ninguno de los polinomios es idénticamente cero.

**Base:** Para  $k = 1$  tenemos  $B_2(z) = z^2 - z + 1/6$  con ceros  $1/2 \pm \sqrt{3}/6$  (estos dos están en el rango  $[0, 1]$ , hay uno en  $[0, 1/2]$ ), y  $B_3(z) = z^3 - 3z^2/2 + z/2$  con ceros  $0, \pm 1$ .

**Inducción:** Supongamos que  $B_{2k}(z)$  tiene un único cero en  $[0, 1/2]$ , y que  $B_{2k+1}(z)$  se anula únicamente en  $0$  y  $1/2$ . Debemos demostrar que vale para  $B_{2k+2}(z)$  y  $B_{2k+3}(z)$  también.

Como  $B_{2k+1}(z)$  no cambia de signo en el rango,  $B_{2k+2}(z)$  es monótona y por tanto puede tener a lo más un cero. Pero pusimos como condición que la integral de  $B_{2k+2}(z)$  de  $0$  a  $1$  se anule;

como  $B_{2k+2}(z)$  es simétrica alrededor de  $z = 1/2$  se anula la integral de 0 a  $1/2$ , por lo que deben haber valores positivos y negativos en el rango, y hay exactamente un cero en él.

Por la recurrencia  $B'_n(z) = nB_{n-1}(z)$ , al tener un único cero  $B_{2k+2}(z)$ ,  $B_{2k+3}(z)$  tiene un único mínimo o máximo en el rango  $[0, 1/2]$ , y  $B_{2k+3}(z)$  puede tener a lo más dos ceros allí y conocemos dos (0 y  $1/2$ ).

Por inducción vale para todo  $k \geq 1$ . □

Como  $B'_{2k}(1/2) = 2kB_{2k-1}(1/2) = 0$ , sabemos que  $B_{2k}(z)$  tiene un mínimo o máximo en  $z = 1/2$ . Tenemos:

$$\begin{aligned} B(0, z/2) &= \frac{z}{2(e^{z/2} - 1)} \\ &= \frac{1}{2} \cdot \frac{z}{e^{z/2} - 1} \cdot \frac{e^{z/2} + 1}{e^{z/2} + 1} \\ &= \frac{1}{2} \cdot \frac{z(e^{z/2} + 1)}{e^z - 1} \\ &= \frac{1}{2} \left( \frac{ze^{z/2}}{e^z - 1} - \frac{z}{e^z - 1} \right) \\ &= \frac{1}{2} (B(1/2, z) - B(0, z)) \end{aligned}$$

Comparando coeficientes de  $z^k$ :

$$\begin{aligned} \frac{B_k}{2^k} &= \frac{1}{2} (B_k(1/2) - B_k) \\ B_k(1/2) &= -\left(1 - 2^{1-k}\right) B_k \end{aligned}$$

Como  $z = 1/2$  es el único máximo (mínimo) de  $B_{2k}(z)$  en el rango  $[0, 1]$  por ser monótona en  $[0, 1/2]$ , al ser simétrica alrededor de  $1/2$  los mínimos (máximos) se dan en los extremos, y en este rango:

$$|B_{2k}(z)| \leq |B_{2k}|$$

### 18.7. El resto

Nuestra fórmula maestra es:

$$\sum_{1 \leq k < a} f(k) = \int_1^a f(z) dz + \gamma_f + B_1 f(a) + \sum_{1 \leq k \leq n} \frac{B_{2k}}{(2k)!} f^{(2k-1)}(a) + \int_a^\infty \frac{\tilde{B}_{2n+1}(z)}{(2n+1)!} f^{(2n+1)}(z) dz$$

Interesa acotar la integral que determina el resto, la llamaremos  $R_n(f; a)$ . Podemos volver a integrar por partes:

$$R_n(f; a) = \int_a^\infty \frac{\tilde{B}_{2n+2}(z)}{(2n+2)!} f^{(2n+2)}(z) dz$$

Suponiendo que  $f^{(2n+2)}(z)$  y  $f^{(2n+1)}(z)$  tienden monótonamente a cero (con lo que en particular no cambian signo), la integral queda acotada por el valor extremo de  $\tilde{B}_{2n+2}(z)$  y la integral del segundo factor. Para el valor extremo de  $\tilde{B}_{2n+2}(z)$  tenemos la cota  $|B_{2n+2}|$ :

$$\begin{aligned} |R_n(f; a)| &\leq \frac{|B_{2n+2}|}{(2n+2)!} \cdot \left| \int_a^\infty f^{(2n+2)}(z) dz \right| \\ &= \frac{|B_{2n+2}|}{(2n+2)!} \cdot |f^{(2n+1)}(a)| \end{aligned}$$

Esto es del orden del primer término omitido, como se indicó.

# 19 Aplicaciones

---

Veremos varias aplicaciones concretas adicionales de la maquinaria de funciones generatrices, hallando funciones generatrices y también derivando (y demostrando) identidades. De particular interés para nosotros es la solución de recurrencias, que comúnmente aparecen en problemas combinatorios, en particular aplicaciones al análisis de algoritmos. En el camino estudiaremos algunas de las secuencias más comunes en la combinatoria.

## 19.1. Números harmónicos

Los números harmónicos se definen como:

$$H_n = \sum_{1 \leq k \leq n} \frac{1}{k} \quad (19.1)$$

Además definimos  $H_0 = 0$  (consistente con que sumas vacías son cero). Esta secuencia es importante en teoría de números, se requiere para calcular una variedad de funciones especiales, además que aparece con frecuencia al analizar algoritmos.

Los primeros valores son:

$$\left\langle 0, 1, \frac{3}{2}, \frac{11}{6}, \frac{25}{12}, \frac{137}{60}, \frac{49}{20}, \frac{363}{140}, \frac{761}{280}, \frac{7129}{2520}, \dots \right\rangle$$

Buscamos una expresión para:

$$H(z) = \sum_{n \geq 0} H_n z^n \quad (19.2)$$

Esto se reduce a:

$$\begin{aligned} H(z) &= \sum_{n \geq 1} \left( \sum_{1 \leq k \leq n} \frac{1}{k} \right) z^n \\ &= z \sum_{n \geq 1} \left( \sum_{0 \leq k \leq n-1} \frac{1}{k+1} \right) z^{n-1} \\ &= z \sum_{n \geq 0} \left( \sum_{0 \leq k \leq n} \frac{1}{k+1} \right) z^n \end{aligned}$$

Como tenemos una suma entre manos, usamos la regla de sumas parciales:

$$\begin{aligned} H(z) &= z \cdot \frac{1}{1-z} \cdot \sum_{k \geq 0} \frac{z^k}{k+1} \\ &= \frac{1}{1-z} \ln \frac{1}{1-z} \quad (19.3) \end{aligned}$$

Acá usamos la suma (14.40) para el logaritmo derivada en la sección 14.3.3.

Aprovechando que la serie (19.3) converge para  $|z| < 1$  (la expresión entra en problemas en  $z = 1$ , el radio de convergencia es  $|z| = 1$ ), podemos evaluar expresiones como:

$$\sum_{n \geq 0} H_n \cdot 2^{-n} = H(1/2) = 2 \ln 2$$

## 19.2. Funciones generatrices con logaritmos

Requeriremos coeficientes de varias series involucrando logaritmos, de la forma:

$$\frac{1}{(1-z)^{r+1}} \ln^s \frac{1}{1-z} \quad (19.4)$$

para  $r \in \mathbb{N}_0$  y  $s \in \mathbb{N}$  enteros. Los resultados se expresan en términos de *números harmónicos generalizados*:

$$H_n^{(m)} = \sum_{1 \leq k \leq n} \frac{1}{k^m} \quad (19.5)$$

Aprovechando la feliz coincidencia notada por Dobrushkin [98]:

$$\frac{d}{dx} (1-z)^x = (1-z)^x \ln(1-z) \quad (19.6)$$

y que la derivada y la extracción de coeficientes comutan, tenemos:

$$\begin{aligned} [z^n] \frac{1}{(1-z)^{r+1}} \ln \frac{1}{1-z} &= -[z^n] \frac{d}{dx} (1-z)^x \Big|_{x=-r-1} \\ &= -\frac{d}{dx} [z^n] (1-z)^x \Big|_{x=-r-1} \\ &= -\frac{d}{dx} (-1)^n \binom{x}{n} \Big|_{x=-r-1} \\ &= -\frac{d}{dx} (-1)^n \binom{x}{n} \Big|_{x=-r-1} \\ &= -\frac{(-1)^n}{n!} \frac{d}{dx} x^n \Big|_{x=-r-1} \end{aligned} \quad (19.7)$$

Para calcular la derivada, recurrimos a logaritmos:

$$\begin{aligned} \frac{d}{dx} x^n &= x^n \frac{d}{dx} \sum_{0 \leq k < n} \ln(x-k) \\ &= x^n \sum_{0 \leq k < n} \frac{1}{x-k} \end{aligned} \quad (19.8)$$

Específicamente para (19.7) nos interesa:

$$\begin{aligned} \frac{d}{dx} x^n \Big|_{x=-r-1} &= (-r-1)^n \sum_{0 \leq k < n} \frac{1}{-r-1-k} \\ &= -(-r-1)^n \sum_{0 \leq k < n} \frac{1}{r+1+k} \\ &= -(-r-1)^n \sum_{r+1 \leq k \leq n+r} \frac{1}{k} \\ &= -(-r-1)^n (H_{n+r} - H_r) \end{aligned} \quad (19.9)$$

Con (19.9) en nuestra expresión original (19.7):

$$\begin{aligned}
 [z^n] \frac{1}{(1-z)^{r+1}} \ln \frac{1}{1-z} &= \frac{(-1)^n (-r-1)^n}{n!} (H_{n+r} - H_r) \\
 &= (-1)^n \binom{-r-1}{n} (H_{n+r} - H_r) \\
 &= \binom{n+r}{r} (H_{n+r} - H_r)
 \end{aligned} \tag{19.10}$$

Podemos derivar (19.6) nuevamente:

$$\begin{aligned}
 [z^n] \frac{1}{(1-z)^{r+1}} \ln^2 \frac{1}{1-z} &= [z^n] \frac{d^2}{dx^2} (1-z)^x \Big|_{x=-r-1} \\
 &= \frac{d^2}{dx^2} [z^n] (1-z)^x \Big|_{x=-r-1} \\
 &= \frac{d^2}{dx^2} (-1)^n \binom{x}{n} \Big|_{x=-r-1} \\
 &= \frac{(-1)^n}{n!} \frac{d^2}{dx^2} x^n \Big|_{x=-r-1}
 \end{aligned} \tag{19.11}$$

De (19.8) conocemos la primera derivada de la potencia factorial. Derivando nuevamente:

$$\begin{aligned}
 \frac{d^2}{dx^2} x^n &= \frac{d}{dx} x^n \cdot \sum_{0 \leq k < n} \frac{1}{x-k} + x^n \cdot \frac{d}{dx} \sum_{0 \leq k < n} \frac{1}{x-k} \\
 &= x^n \left( \left( \sum_{0 \leq k < n} \frac{1}{x-k} \right)^2 - \sum_{0 \leq k < n} \frac{1}{(x-k)^2} \right)
 \end{aligned} \tag{19.12}$$

Necesitamos:

$$\begin{aligned}
 \frac{d^2}{dx^2} x^n \Big|_{x=-r-1} &= x^n \left( \left( \sum_{0 \leq k < n} \frac{1}{x-k} \right)^2 - \sum_{0 \leq k < n} \frac{1}{(x-k)^2} \right) \Big|_{x=-r-1} \\
 &= (-r-1)^n \left( \left( \sum_{r+1 \leq k \leq n} \frac{1}{k} \right)^2 - \sum_{r+1 \leq k \leq n} \frac{1}{k^2} \right) \\
 &= (-r-1)^n \left( H_{n+r}^2 - H_{n+r}^{(2)} - (H_r^2 - H_r^{(2)}) \right)
 \end{aligned} \tag{19.13}$$

reemplazando (19.13) en (19.11) y simplificando coeficientes binomiales resulta:

$$[z^n] \frac{1}{(1-z)^{r+1}} \ln^2 \frac{1}{1-z} = \binom{n+r}{r} \left( H_{n+r}^2 - H_{n+r}^{(2)} - (H_r^2 - H_r^{(2)}) \right) \tag{19.14}$$

Usando la fórmula de Leibnitz para calcular derivadas superiores de (19.8) se obtiene una recurrencia para las derivadas superiores de  $x^n$ , y en consecuencia se tienen los coeficientes de (19.4) para valores superiores de  $s$ . Zave [368] deriva las fórmulas completas. Para nuestros fines puntuales basta llegar hasta acá.

### 19.3. Potencias factoriales

Definamos:

$$G(z, u) = \sum_{n \geq 0} u^n \frac{z^n}{n!} \quad (19.15)$$

Como:

$$\frac{u^n}{n!} = \binom{u}{n}$$

tenemos:

$$G(z, u) = \sum_{n \geq 0} \binom{u}{n} z^n = (1 + z)^u$$

Esto implica:

$$G(z, u) \cdot G(z, v) = G(z, u + v)$$

Podemos evaluar entonces de dos formas:

$$G(z, u) \cdot G(z, v) = \sum_{n \geq 0} \left( \sum_{0 \leq k \leq n} \binom{n}{k} u^k v^{n-k} \right) \frac{z^n}{n!} \quad (19.16)$$

$$G(z, u + v) = \sum_{n \geq 0} (u + v)^n \frac{z^n}{n!} \quad (19.17)$$

Comparando los coeficientes de  $z^n$  en (19.16) y (19.17) resulta:

$$(u + v)^n = \sum_{0 \leq k \leq n} \binom{n}{k} u^k v^{n-k} \quad (19.18)$$

Curioso equivalente de la fórmula para la potencia de un binomio. Aprovechando la relación entre potencias factoriales en subida y en bajada se puede derivar una relación similar para las potencias factoriales en subida.

### 19.4. Números de Fibonacci

Consideremos la secuencia:

$$\langle 0, 1, 1, 2, 5, 8, 13, 21, 34, \dots \rangle \quad (19.19)$$

que se obtiene de la recurrencia válida para  $n \geq 0$ :

$$F_{n+2} = F_{n+1} + F_n \quad F_0 = 0, F_1 = 1 \quad (19.20)$$

Esta la encontramos al analizar el algoritmo de Euclides para el máximo común divisor en la sección 11.2. Aparece en una gran variedad de situaciones relacionadas con nuestra área, y muchos fenómenos naturales, como el crecimiento de los árboles y las espirales que se observan en los girasoles, siguen aproximadamente esta secuencia. Véanse por ejemplo el libro de Dunlap [106] para una variedad de situaciones donde aparecen, y la muy detallada discusión de Vajda [358].

### 19.4.1. Solución mediante funciones generatrices ordinarias

Definimos:

$$F(z) = \sum_{n \geq 0} F_n z^n$$

Aplicando las propiedades de funciones generatrices ordinarias a (19.20):

$$\frac{F(z) - F_0 - F_1 \cdot z}{z^2} = \frac{F(z) - F_0}{z} + F(z)$$

Substituyendo los valores de  $F_0$  y  $F_1$  y despejando resulta:

$$F(z) = \frac{z}{1 - z - z^2} \quad (19.21)$$

Necesitamos reducir (19.21) a fracciones con denominadores lineales, usando fracciones parciales. Buscamos factorizar de la siguiente manera:

$$1 - z - z^2 = (1 - r_+ z)(1 - r_- z)$$

Para obtener esta factorización realizamos el cambio de variable  $y = 1/z$  y tenemos:

$$y^2 - y - 1 = (y - r_+)(y - r_-)$$

$$r_{\pm} = \frac{1 \pm \sqrt{5}}{2}$$

y denotamos  $r_+ = \tau$  y  $r_- = \phi$ . El número  $\tau$  es la *sección áurea* (por la palabra griega para *corte*), que ya habíamos encontrado antes al analizar el algoritmo de Euclides para el máximo común divisor. Una notación común para la sección áurea (particularmente en matemáticas recreativas) es  $\phi$  o  $\varphi$ , en honor al escultor ateniense Fidias, quien se dice usó esta razón extensamente en su trabajo. Otros usan  $\phi = -r_-$  y  $\Phi = r_+$ , de forma de tener números positivos siempre.

Podemos expresar:

$$\begin{aligned} y^2 - y - 1 &= (y - \tau)(y - \phi) \\ &= y^2 - (\tau + \phi)y + \tau\phi \end{aligned}$$

Comparando coeficientes resulta  $\phi = 1 - \tau = -1/\tau$ . Las fracciones parciales resultan ser:

$$F(z) = \frac{1}{\tau - \phi} \cdot \left( \frac{1}{1 - \tau z} - \frac{1}{1 - \phi z} \right) \quad (19.22)$$

En (19.22) se reconocen dos series geométricas. Esto da la sorprendente relación, conocida como fórmula de Binet, que expresa los números de Fibonacci (enteros) en términos de números irracionales:

$$F_n = \frac{\tau^n - \phi^n}{\tau - \phi} \quad (19.23)$$

$$= \frac{(1 + \sqrt{5})^n - (1 - \sqrt{5})^n}{2^n \sqrt{5}} \quad (19.24)$$

Ahora bien:

$$\frac{1}{2\tau - 1} = \frac{1}{\sqrt{5}} = 0,4472\dots \quad \tau = 1,618\dots \quad \phi = -0,6180\dots$$

Resulta para todo  $n \geq 0$ :

$$\left| \frac{\phi^n}{2\tau - 1} \right| < 0,5$$

Por lo tanto,  $F_n = \tau^n / \sqrt{5}$ , redondeado al entero más cercano. De todas formas:

$$F_n \sim \frac{\tau^n}{\sqrt{5}} \quad (19.25)$$

Podemos obtener otras relaciones de la función generatriz (19.21):

$$F(z) = \frac{z}{1-z-z^2} = \frac{z}{1-z(1+z)} = \sum_{r \geq 0} z^{r+1}(1+z)^r = \sum_{r,s \geq 0} \binom{r}{s} z^{r+s+1}$$

De aquí, como con  $n = r + s$  tenemos  $r = n - s$ :

$$F_{n+1} = \sum_{0 \leq s \leq n} \binom{n-s}{s} \quad (19.26)$$

#### 19.4.2. Solución mediante funciones generatrices exponenciales

Definimos la función generatriz exponencial:

$$\hat{F}(z) = \sum_{n \geq 0} \frac{F_n z^n}{n!}$$

Aplicando las propiedades de funciones generatrices exponenciales a (19.20):

$$\hat{F}''(z) = \hat{F}'(z) + \hat{F}(z) \quad \hat{F}(0) = 0, \hat{F}'(0) = 1$$

Resolvemos esta ecuación diferencial ordinaria lineal de segundo orden, homogénea y de coeficientes constantes por el método de la ecuación característica:

$$r^2 = r + 1$$

Los ceros son  $\tau$  y  $\phi$ , con lo que tenemos:

$$\hat{F}(z) = \alpha e^{\tau z} + \beta e^{\phi z}$$

de donde:

$$\hat{F}(0) = \alpha + \beta = 0$$

$$\hat{F}'(0) = \alpha \tau + \beta \phi = 1$$

La solución de estas ecuaciones es:

$$\alpha = \frac{1}{\sqrt{5}} \quad \beta = -\frac{1}{\sqrt{5}}$$

y finalmente resulta la misma fórmula (19.24) anterior:

$$F_n = \frac{1}{\sqrt{5}} n! [z^n] (e^{\tau z} - e^{\phi z}) = \frac{\tau^n - \phi^n}{\sqrt{5}}$$

Si comparamos las derivaciones, obtener la ecuación y sus condiciones de borde es más simple al usar funciones generatrices exponenciales, luego debemos resolver una ecuación diferencial, pero obtener el resultado de la solución de la ecuación diferencial es inmediato. En la derivación usando funciones generatrices ordinarias obtener la ecuación era algo más trabajo, y tuvimos que usar fracciones parciales para poder obtener la secuencia; pero tratar la ecuación misma era más simple. De todas formas, siempre tendremos las dos opciones. Cuál resulta más conveniente dependerá de la situación específica.

### 19.4.3. Números de Fibonacci y fuentes

Si comparamos la secuencia (14.89) de números de fuentes de base  $n$  con los números de Fibonacci, parecieran ser los términos alternos:

$$\langle F_{2n+1} \rangle_{n \geq 0} = \langle 1, 2, 5, 13, 34, \dots \rangle$$

Una manera de verificar esto es extraer los términos impares de la función generatriz (19.21), o sea encontrar una función generatriz para  $\langle F_{2n+1} \rangle_{n \geq 0}$  y comparar con (14.92).

Aplicamos la técnica descrita en la sección 14.5 a la función generatriz (19.21). Para los números de Fibonacci impares resulta:

$$\frac{F(\sqrt{z}) - F(-\sqrt{z})}{2\sqrt{z}} = \frac{1-z}{1-3z+z^2}$$

En nuestro caso tenemos la secuencia desplazada en uno, de (14.90):

$$\frac{f(z) - f_0}{z} = \frac{1-z}{1-3z+z^2}$$

Coinciden, o sea:

$$f_n = \begin{cases} 1 & \text{si } n = 0 \\ F_{2n-1} & \text{si } n \geq 1 \end{cases} \quad (19.27)$$

### 19.4.4. Búsqueda de Fibonacci

La *búsqueda de Fibonacci* (ver por ejemplo a Kiefer [203]) es un método para encontrar el mínimo de una función en un rango dado. Resulta incluso que esta técnica es óptima en cuanto a número de veces que se evalúa la función siempre que nos restrinjamos a solo comparar valores.

**Definición 19.1.** Una función  $f : \mathbb{R} \rightarrow \mathbb{R}$  se dice *unimodal* sobre el rango  $[a, b]$  si hay un único  $\xi$  con  $a \leq \xi \leq b$  tal que  $f$  es decreciente en  $[a, \xi]$  y creciente en  $[\xi, b]$ .

Esto describe el caso en que la función tenga un único mínimo en el rango, de forma muy similar se define el caso que tiene un único máximo, y en ambas situaciones se llama unimodal la función.

Nos interesa acotar el mínimo en el rango  $[a, b]$  de una función unimodal  $f(z)$  recurriendo únicamente a evaluar la función. Por ejemplo, la función está dada por una computación compleja y no hay forma de calcular su derivada. Supongamos que tenemos los valores de la función en los puntos  $a$  y  $b$ . Elegimos dos puntos adicionales  $c < d$  dentro del rango  $[a, b]$ , y evaluamos la función en ellos, resultando la situación de la figura 19.1. Al ser unimodal  $f$  sabemos que  $f(c)$  y  $f(d)$  son ambos menores que  $\max\{f(a), f(b)\}$ . Si  $f(c) < f(d)$ , el mínimo está en el subintervalo  $[a, d]$ , descartamos el tramo  $(d, b]$  y trabajamos con el nuevo rango  $[a, d]$ . De la misma manera, si  $f(c) > f(d)$ , el mínimo está en el tramo  $[c, b]$ , descartamos el rango  $[a, c]$ .

Consideremos el ejemplo de la figura 19.1. Descartamos el rango  $[a, c]$  y elegimos un nuevo punto  $e$  entre  $d$  y  $b$ , y seguimos con nuevos puntos  $a'$ ,  $b'$ ,  $c'$  y  $d'$ . Para solo calcular una vez la función en la iteración se reutilizan los valores calculados en los puntos  $a$ ,  $c$  y  $d$  (de descartar  $(d, b]$ ) o en los puntos  $c$ ,  $d$  y  $b$  (de descartar  $[a, c]$ ). Queremos además que el método reduzca el tramo en la misma proporción en ambos casos. O sea, debe ser  $d - a = b - c$ . En el siguiente paso queremos que se vuelva a repetir esto, debe ser también  $b - d = e - c$ .

Definamos  $r$  mediante  $d - a = r(b - a)$ , con lo que  $c - a = (1 - r)(b - a)$ . Restando:

$$\begin{aligned} d - c &= (d - a) - (c - a) \\ &= r(b - a) - (1 - r)(b - a) \\ &= (2r - 1)(b - a) \end{aligned}$$

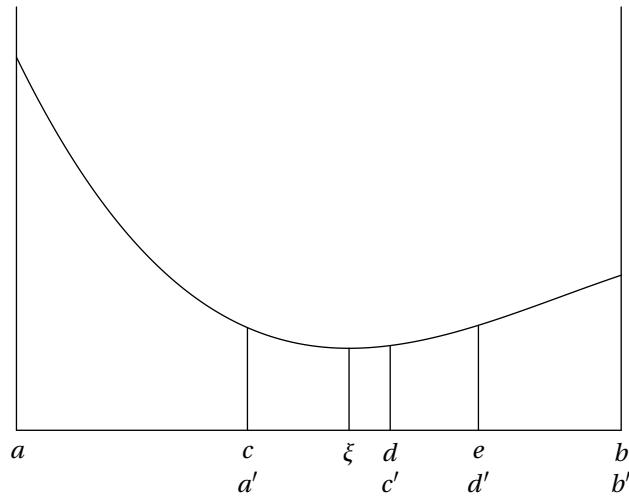


Figura 19.1 – Búsqueda de Fibonacci

Para el paso siguiente,  $a' = c$ ,  $c' = d$ ,  $d' = e$  y  $b' = b$ . Elegimos  $r'$  mediante  $d' - a' = r'(b' - a')$ , de donde resulta  $c' - a' = (1 - r')(b' - a')$ , que es decir  $d - c = (1 - r')(b' - a')$ . El intervalo  $[a, b]$  se redujo a  $[a', b']$ , con  $b' - a' = r(b - a)$ . Igualando los valores de  $d - c$ , y substituyendo el valor de  $b' - a'$  resulta:

$$\begin{aligned} (2r - 1)(b - a) &= (1 - r')(b' - a') \\ (2r - 1)(b - a) &= (1 - r')r(b - a) \\ 2r - 1 &= (1 - r')r \end{aligned}$$

Despejando  $r$ :

$$r = \frac{1}{r' + 1} \quad (19.28)$$

Partiendo del final, esto permite calcular las razones previas. En el caso extremo reducimos el intervalo en una razón de 1 (vale decir, se mantiene el tamaño). El paso final lo ilustra la figura 19.2. El algoritmo retorna el rango marcado  $a$  a  $b$  como resultado final, la mejor aproximación a  $\xi$  es  $c = d = (a + b)/2$ .

Esto sugiere la recurrencia:

$$r_{k+1} = \frac{1}{1 + r_k} \quad (k \geq 1) \quad r_0 = 1 \quad (19.29)$$

Intentando algunos valores obtenemos:

$$\left\langle 1, \frac{1}{2}, \frac{2}{3}, \frac{3}{5}, \frac{5}{8}, \dots \right\rangle$$

Da la impresión que:

$$r_k = \frac{F_{k+1}}{F_{k+2}} \quad (19.30)$$

Esto es fácil de demostrar por inducción, los detalles los proveerá el amable lector. Con esto estamos en condiciones de plantear la búsqueda de Fibonacci, algoritmo 19.1. Suponemos dados el intervalo

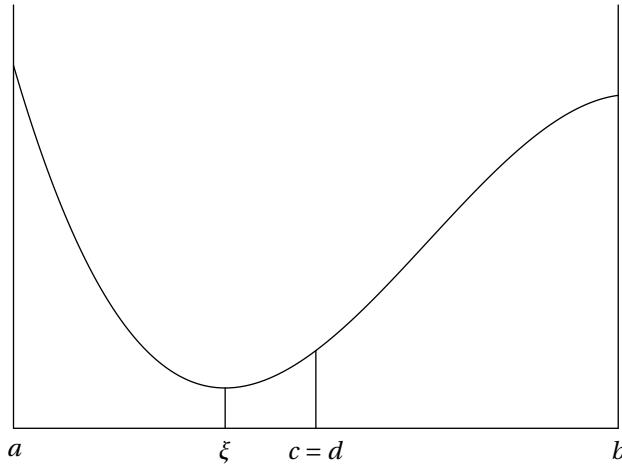


Figura 19.2 – Búsqueda de Fibonacci: Juego final

$[a, b]$  y la tolerancia  $\epsilon$  (el largo del último intervalo). Para reducir el largo del intervalo en un factor  $F_n$  se calcula la función  $n + 4$  veces. En vista de (19.25) para reducir el rango de largo  $L_0$  a  $L_f$  el número de llamadas de la función es:

$$\begin{aligned} n &\sim \frac{\ln(L_0/L_f)}{\ln \tau} + 4 + \frac{\ln 5}{2 \ln \tau} \\ &\sim 4,78497 \ln \frac{L_0}{L_f} + 5,67723 \end{aligned}$$

Un método relacionado es la búsqueda de sección áurea. La idea es similar, solo que en vez de ir modificando  $r$  se usa el valor límite:

$$\lim_{n \rightarrow \infty} \frac{F_{n+1}}{F_n} = \tau$$

El programa es un poco más sencillo, pero algo menos eficiente (requiere más evaluaciones de la función).

## 19.5. Coeficientes binomiales

Hagamos como que nada sabemos... ¿Cuántos subconjuntos de  $k$  elementos podemos obtener de un conjunto de  $n$  elementos? Obviamente, exactamente qué conjunto de  $n$  elementos tomemos da lo mismo, podemos usar el conjunto  $\{1, 2, \dots, n\}$  sin pérdida de generalidad. Podemos deducir algunas propiedades de estas:

- Tomar un número negativo de elementos del conjunto no tiene sentido, o sea,  $\binom{n}{k} = 0$  si  $k < 0$ .
- Tomar más de  $n$  elementos es imposible, así que  $\binom{n}{k} = 0$  si  $k > n$ .
- Hay una única forma de elegir cero elementos, y  $\binom{n}{0} = 1$ .
- De la misma forma, hay una única manera de elegirlos todos, y  $\binom{n}{n} = 1$ .
- Elegir  $k$  elementos a poner en el subconjunto es lo mismo que elegir los  $n - k$  que se dejan fuera, o sea  $\binom{n}{k} = \binom{n}{n-k}$ .

---

Algoritmo 19.1: Búsqueda de Fibonacci

---

```

function FibonacciSearch( $f, a, b, \epsilon$ )
     $L \leftarrow (b - a)/\epsilon$ 
     $(F_a, F_b) \leftarrow (1, 1)$ 
    while  $F_b < L$  do
         $(F_a, F_b) \leftarrow (F_b, F_a + F_b)$ 
    end
     $c \leftarrow b - (b - a) \cdot F_a/F_b$ 
     $d \leftarrow a + (b - a) \cdot F_a/F_b$ 
     $(f_a, f_b, f_c, f_d) \leftarrow (f(a), f(b), f(c), f(d))$ 
    while  $F_a \neq 1$  do
         $(F_a, F_b) \leftarrow (F_b - F_a, F_a)$ 
        if  $f_d < f_c$  then
             $e \leftarrow c + (b - c) \cdot F_a/F_b$ 
             $f_e \leftarrow f(e)$ 
             $(a, c, d, b) \leftarrow (c, d, e, b)$ 
             $(f_a, f_c, f_d, f_b) \leftarrow (f_c, f_d, f_e, f_b)$ 
        else
             $e \leftarrow d - (d - a) \cdot F_a/F_b$ 
             $f_e \leftarrow f(e)$ 
             $(a, c, d, b) \leftarrow (a, e, c, d)$ 
             $(f_a, f_c, f_d, f_b) \leftarrow (f_a, f_e, f_c, f_d)$ 
        end
    end
    if  $f_a < f_b$  then
        return  $[a, d]$ 
    else
        return  $[d, b]$ 
    end

```

---

Ahora buscamos encontrar una recurrencia para los  $\binom{n}{k}$ . Podemos descomponer los  $\binom{n}{k}$  subconjuntos en dos grupos:

**Aquellos conjuntos que no contienen a  $n$ :** Corresponden simplemente a tomar  $k$  elementos de los restantes  $n - 1$ , de estos hay  $\binom{n-1}{k}$ .

**Aquellos conjuntos que contienen a  $n$ :** Tomamos  $n$ , y  $k - 1$  elementos más de entre los restantes  $n - 1$ , de estos hay  $\binom{n-1}{k-1}$ .

Como estas dos posibilidades son excluyentes, y corresponden a todas las formas de armar subconjuntos de  $k$  elementos:

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Esto en principio es válido para  $1 \leq k \leq n - 1$ . Pero si substituimos  $k = n$  bajo los entendidos de arriba resulta  $\binom{n}{n} = 1$ , y con  $k > n$  se reduce a  $\binom{n}{k} = 0$ , y la recurrencia en realidad es válida para  $k \geq 1$ .

Partiremos de  $k+1$  y  $n+1$  para poder sumar desde  $k=0$  y  $n=0$ :

$$\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k} \quad (19.31)$$

Como condiciones de contorno bastan:

$$\binom{n}{0} = 1 \quad \binom{0}{k} = [k=0]$$

Ahora tenemos tres opciones de función generatriz ordinaria:

$$A_n(x) = \sum_{k \geq 0} \binom{n}{k} x^k \quad B_k(y) = \sum_{n \geq 0} \binom{n}{k} y^n \quad C(x, y) = \sum_{\substack{k \geq 0 \\ n \geq 0}} \binom{n}{k} x^k y^n$$

Las primeras dos opciones llevarán a recurrencias en la función generatriz, cosa que la tercera resuelve automáticamente. Nada indica particulares complicaciones (más allá del uso de dos variables y no una como ha sido común hasta acá), por lo que optaremos por esta. Aplicando las propiedades de funciones generatrices ordinarias a la recurrencia queda:

$$\frac{C(x, y) - C(x, 0) - C(0, y) + C(0, 0)}{xy} = \frac{C(x, y) - C(0, y)}{x} + C(x, y) \quad (19.32)$$

El numerador del lado izquierdo de (19.32) corresponde a:

$$\sum_{\substack{k \geq 0 \\ n \geq 0}} \binom{n+1}{k+1} x^{k+1} y^{n+1} = \sum_{\substack{k \geq 0 \\ n \geq 0}} \binom{n}{k} x^k y^n - \sum_{k \geq 0} \binom{0}{k} x^k y^0 - \sum_{n \geq 0} \binom{n}{0} x^0 y^n + \binom{0}{0}$$

que resulta de eliminar la primera fila y columna de la suma (de eso se hacen cargo los dos siguientes términos); al restarlas estamos restando dos veces  $C(0, 0)$ , y debemos reponerlo, lo que da lugar al último término. Esto es el principio de inclusión y exclusión, capítulo 15, haciendo su trabajo. De nuestras condiciones de contorno:

$$C(0, 0) = \binom{0}{0} = 1 \quad C(x, 0) = \sum_{k \geq 0} \binom{0}{k} x^k = 1 \quad C(0, y) = \sum_{n \geq 0} \binom{n}{0} y^n = \frac{1}{1-y}$$

Despejando obtenemos:

$$C(x, y) = \frac{1}{1 - (1+x)y}$$

Expandiendo la serie geométrica:

$$\binom{n}{k} = [x^k y^n] C(x, y) = [x^k y^n] \sum_{r \geq 0} (1+x)^r y^r = [x^k] (1+x)^n$$

Tenemos nuevamente la relación entre los coeficientes binomiales y el número de combinaciones de  $k$  elementos tomados entre  $n$ .

La recurrencia (19.31) mostrada de la siguiente manera:

$$\begin{array}{ccc} \binom{n}{k} & & \binom{n}{k+1} \\ \searrow & & \swarrow \\ \binom{n+1}{k+1} & & \end{array}$$

y recordando  $\binom{n}{0} = \binom{n}{n} = 1$  da el famoso triángulo de Pascal, ver cuadro 19.1 (comparar también con la sección 13.2, en particular el teorema 13.7).

$n = 0:$	1
$n = 1:$	1 1
$n = 2:$	1 2 1
$n = 3:$	1 3 3 1
$n = 4:$	1 4 6 4 1
$n = 5:$	1 5 10 10 5 1
$n = 6:$	1 6 15 20 15 6 1

Cuadro 19.1 – Triángulo de Pascal

## 19.6. Otras recurrencias de dos índices

Consideremos el problema de calcular cuántos subconjuntos de  $k$  elementos de  $\{1, 2, \dots, n\}$  hay tal que no contienen números consecutivos. Llaremos  $s(n, k)$  a este valor. Para construir una recurrencia para ellos, aplicamos el método general de ver qué pasa al incluir o excluir  $n$ .

**No incluye  $n$ :** Esto es simplemente elegir  $k$  de entre los primeros  $n - 1$ , o sea  $s(n - 1, k)$ .

**Incluye  $n$ :** Quedan por agregar  $k - 1$  elementos, que no pueden incluir a  $n - 1$ , o sea corresponde a  $s(n - 2, k - 1)$ .

Esto nos da la recurrencia:

$$s(n, k) = s(n - 1, k) + s(n - 2, k - 1)$$

Ajustando índices:

$$s(n + 2, k + 1) = s(n + 1, k + 1) + s(n, k) \quad (19.33)$$

Es claro que para  $n \geq 1$ :

$$s(n, 1) = n \quad (19.34)$$

Requeriremos los valores  $s(0, 0)$ ,  $s(n, 0)$ ,  $s(0, k)$ ,  $s(1, k)$ . De la recurrencia, con  $n \geq 0$ :

$$\begin{aligned} s(n + 2, 1) &= s(n + 1, 1) + s(n, 0) \\ n + 2 &= n + 1 + s(n, 0) \end{aligned}$$

Por tanto, definimos  $s(n, 0) = 1$ . Similarmente:

$$s(2, k + 1) = s(1, k + 1) + s(0, k)$$

Para  $k \geq 1$  resulta  $s(0, k) = 0$ , con lo que  $s(0, k) = [k = 0]$ . Además, uniendo los casos  $s(1, 0) = s(1, 1) = 1$  con  $s(1, k) = 0$  para  $k > 1$ :

$$s(1, k) = [0 \leq k \leq 1]$$

Definamos la función generatriz:

$$S(x, y) = \sum_{n,k \geq 0} s(n, k) x^n y^k \quad (19.35)$$

Para aplicar nuestra técnicas de solución de recurrencias, necesitaremos las sumas:

$$\begin{aligned} x^2 y \sum_{n,k \geq 0} s(n+2, k+1) x^n y^k &= S(x, y) - \sum_{k \geq 0} s(0, k) y^k - \sum_{k \geq 0} s(1, k) x y^k - \sum_{n \geq 0} s(n, 0) x^n \\ &\quad + s(0, 0) + s(1, 0) x \\ &= S(x, y) - 1 - x(1+y) - \frac{1}{1-x} + 1 + x \\ &= S(x, y) - xy - \frac{1}{1-x} \\ xy \sum_{n,k \geq 0} s(n+1, k+1) x^n y^k &= S(x, y) - \sum_{k \geq 0} s(0, k) y^k - \sum_{n \geq 0} s(n, 0) x^n + s(0, 0) \\ &= S(x, y) - 1 - \frac{1}{1-x} + 1 \\ &= S(x, y) - \frac{1}{1-x} \end{aligned}$$

Los términos que se suman se han restado dos veces, y deben reponerse. Esto con la recurrencia da:

$$\frac{S(x, y) - x(1+y) - \frac{1}{1-x}}{x^2 y} = \frac{S(x, y) - \frac{1}{1-x}}{xy} + S(x, y)$$

Despejando:

$$S(x, y) = \frac{1 + xy}{1 - x - x^2 y} \quad (19.36)$$

Podemos escribir (19.36) como:

$$\begin{aligned} S(x, y) &= \frac{1 + xy}{1 - x(1 + xy)} \\ &= \sum_{r \geq 0} x^r (1 + xy)^{r+1} \\ &= \sum_{r \geq 0} x^r \sum_{s \geq 0} \binom{r+1}{s} x^s y^s \\ &= \sum_{r,s \geq 0} \binom{r+1}{s} x^{r+s} y^s \end{aligned}$$

De aquí:

$$s(n, k) = [x^n y^k] S(x, y) = \binom{n-k+1}{k} \quad (19.37)$$

Para  $y = 1$  la función generatriz (19.36) da:

$$S(x, 1) = \frac{1+x}{1-x-x^2} = \frac{F(x)-x}{x^2}$$

Acá  $F(x)$  es la función generatriz de los números de Fibonacci (19.21). Esto concuerda con sumar la recurrencia (19.33) sobre todo  $k$ , como  $s(0, 0) = 1 = F_2$  y  $s(1, 0) + s(1, 1) = 2 = F_3$ .

Otro caso de interés son los números de Delannoy [89] (ver también la discusión de Banderier y Schwer [26]). Se define  $D(m, n)$  como el número de caminos entre  $(0, 0)$  y  $(m, n)$  en una cuadrícula, si se permiten únicamente pasos hacia el norte, el nordeste o este. De la definición es clara la recurrencia:

$$D(m, n) = D(m - 1, n) + D(m, n - 1) + D(m - 1, n - 1) \quad D(0, 0) = 1 \quad (19.38)$$

Para aplicar nuestra técnica requeriremos:

$$D(m, 0) = D(0, n) = 1 \quad (19.39)$$

Definiendo la función generatriz ordinaria:

$$d(x, y) = \sum_{m,n \geq 0} D(m, n)x^m y^n \quad (19.40)$$

obtenemos la ecuación funcional:

$$\frac{d(x, y) - d(0, y) - d(y, 0) + d(0, 0)}{xy} = \frac{d(x, y) - d(0, y)}{x} + \frac{d(x, y) - d(x, 0)}{y} + d(x, y) \quad (19.41)$$

Las condiciones de contorno dan:

$$d(0, y) = \frac{1}{1-y} \quad d(x, 0) = \frac{1}{1-x} \quad (19.42)$$

Substituyendo (19.42) en (19.41) y despejando  $d(x, y)$  resulta:

$$d(x, y) = \frac{1}{1-x-y-xy} \quad (19.43)$$

El lector interesado verificará que expandir como serie geométrica y extraer los coeficientes respectivos resulta en:

$$D(m, n) = \sum_t \binom{m+n-t}{n} \binom{n}{t} \quad (19.44)$$

La asimetría de (19.44) ofende las sensibilidades del autor. Puede escribirse en forma simétrica en términos de coeficientes trinomiales, eso sí.

La siguiente idea da una expansión más simétrica:

$$\begin{aligned} d(x, y) &= \frac{1}{(1-x)(1-y)-2xy} \\ &= \frac{(1-x)(1-y)}{1-\frac{2xy}{(1-x)(1-y)}} \\ &= (1-x)(1-y) \sum_{r \geq 0} \left( \frac{2xy}{(1-x)(1-y)} \right)^r \\ &= \sum_{r \geq 0} \frac{2^r x^r y^r}{(1-x)^{r-1} (1-y)^{r-1}} \\ &= \sum_{r \geq 0} 2^r \sum_{s \geq 0} \binom{r+s}{s} x^{r+s} \sum_{t \geq 0} \binom{r+t}{t} y^{r+t} \end{aligned}$$

Al extraer el coeficiente de  $x^m y^n$  solo sobreviven los términos con  $r+s = m$  y  $r+t = n$ , aprovechando la simetría de los coeficientes binomiales:

$$D(m, n) = \sum_{r \geq 0} 2^r \binom{m}{r} \binom{n}{r} \quad (19.45)$$

En todo caso, ya habíamos demostrado esta identidad como (14.109) usando aceite de serpiente.

## 19.7. Dividir y conquistar

Una de las estrategias más fructíferas para diseñar algoritmos es la que se llama *dividir y conquistar* (ver por ejemplo Cormen, Leiserson, Rivest y Stein [82]). La idea es resolver un problema “grande” por la vía de expresarlo en términos de varios problemas menores del mismo tipo, resolver estos (recursivamente) y luego combinar los resultados. Ejemplos típicos son el ordenamiento por intercalación y búsqueda binaria.

Un ejemplo menos conocido es el algoritmo de Karatsuba para multiplicación de números enteros [196]. Se desean multiplicar números de  $2n$  dígitos, llamémosles  $A$  y  $B$ , los dividimos en mitades más y menos significativas. Si la base es 10, escribimos:

$$A = a \cdot 10^n + b \quad B = c \cdot 10^n + d$$

donde  $0 \leq a, b, c, d < 10^n$ , y tenemos:

$$A \cdot B = ac \cdot 10^{2n} + (ad + bc) \cdot 10^n + bd$$

Esta fórmula permite calcular un producto de dos números de  $2n$  dígitos mediante cuatro multiplicaciones de números de  $n$  dígitos (y algunas operaciones adicionales, como sumas de números de a lo más  $2n$  dígitos). Si definimos:

$$u = a + b \quad v = c + d \quad uv = ac + ad + bc + bd$$

podemos expresar:

$$A \cdot B = ac \cdot 10^{2n} + (uv - ac - bd) \cdot 10^n + bd$$

Esta fórmula significa usar tres (no cuatro) multiplicaciones, a costa de más operaciones de suma. Si comenzamos con números con  $2^n$  dígitos, podemos aplicar esta estrategia recursivamente, y los ahorros se suman.

Un ejemplo lo da el producto  $23316384 \cdot 20936118$ . Tenemos:

$$n = 8$$

$$A = 23316384$$

$$B = 20936118$$

$$a = 2331 \quad b = 6384 \quad c = 2093 \quad d = 6118$$

$$u = 8715 \quad v = 8211$$

Debemos ahora calcular:

$$\begin{aligned} ac &= 2331 \cdot 2093 \\ &= (23 \cdot 20) \cdot 10^4 + ((23 + 31) \cdot (20 + 93) - 23 \cdot 20 - 31 \cdot 93) \cdot 10^2 + 31 \cdot 93 \\ &= 460 \cdot 10^4 + 2759 \cdot 10^2 + 2883 \\ &= 4878783 \end{aligned}$$

En esto hemos calculado, por ejemplo:

$$23 \cdot 20 = 2 \cdot 2 \cdot 10^2 + ((2 + 3) \cdot (2 + 0) - 2 \cdot 2 - 3 \cdot 0) \cdot 10 + 3 \cdot 0 = 4 \cdot 10^2 + 6 \cdot 10 + 0 = 460$$

Los otros valores intermedios a calcular son:

$$bd = 39057312 \quad uv = 71558865 \quad uv - ac - bd = 27622770$$

Combinando los anteriores queda finalmente:

$$\begin{aligned} 23316384 \cdot 20936118 &= 4878783 \cdot 10^8 + 27622770 \cdot 10^4 + 39057312 \\ &= 488154566757312 \end{aligned}$$

Otro ejemplo de esta estrategia es el algoritmo de Strassen [341] para multiplicar matrices. Consideraremos primeramente el producto de dos matrices de  $2 \times 2$ :

$$\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

Sabemos que:

$$\begin{aligned} c_{11} &= a_{11}b_{11} + a_{12}b_{21} & c_{12} &= a_{11}b_{12} + a_{12}b_{22} \\ c_{21} &= a_{21}b_{11} + a_{22}b_{21} & c_{22} &= a_{21}b_{12} + a_{22}b_{22} \end{aligned}$$

Esto corresponde a 8 multiplicaciones. Definamos los siguientes productos:

$$\begin{aligned} m_1 &= (a_{11} + a_{22})(b_{11} + b_{22}) & m_2 &= (a_{21} + a_{22})b_{11} \\ m_3 &= a_{11}(b_{12} - b_{22}) & m_4 &= a_{22}(b_{21} - b_{11}) \\ m_5 &= (a_{11} + a_{12})b_{22} & m_6 &= (a_{21} - a_{11})(b_{11} + b_{12}) \\ m_7 &= (a_{12} - a_{22})(b_{21} + b_{22}) \end{aligned}$$

Entonces podemos expresar:

$$\begin{aligned} c_{11} &= m_1 + m_4 - m_5 + m_7 & c_{12} &= m_3 + m_5 \\ c_{21} &= m_2 + m_4 & c_{22} &= m_1 - m_2 + m_3 + m_6 \end{aligned}$$

Con estas fórmulas se usan 7 multiplicaciones para evaluar el producto de dos matrices. Cabe hacer notar que estas fórmulas no hacen uso de commutatividad, por lo que son aplicables también para multiplicar matrices de  $2 \times 2$  cuyos elementos son a su vez matrices. Podemos usar esta fórmula recursivamente para multiplicar matrices de  $2^n \times 2^n$ .

Tal vez el algoritmo más importante basado en dividir y conquistar es el que se conoce como *transformada rápida de Fourier*, generalmente abreviado *FFT* (de *Fast Fourier Transform* en inglés); se acredita a Cooley y Tukey [79] (aunque para variar un poco, más de dos siglos antes Gauß ya lo empleaba, como relatan Heideman, Johnson y Burrus [172]). Elegido como uno de los 10 algoritmos más importantes del siglo XX [100], es la base de mucho de lo que es procesamiento de señales hoy día, es el corazón del algoritmo de Schönhage y Strassen, el mejor algoritmo conocido para multiplicar que resulta práctico para números muy grandes [315], y es central en el algoritmo de Fürer [137], el mejor que se conoce (aunque este último solo sería ventajoso para números fuera del rango útil).

Otro ejemplo clásico es el algoritmo Quicksort (ver la sección 19.7.2), claro que en este la división no es equitativa (como en los otros que se mencionan). También fue considerado uno de los 10 algoritmos más importantes del siglo XX [100].

### 19.7.1. Análisis de división fija

Consideraremos primero el caso en que el problema original se traduce en varios problemas de una fracción fija del tamaño del original. Si el tiempo de ejecución de un algoritmo de este tipo para una entrada de tamaño  $n$  lo denotamos por  $t(n)$ , el problema se reduce a  $a$  problemas de tamaño  $n/b$ , y el costo de reducir el problema y luego combinar las soluciones es  $f(n)$ , al sumar el tiempo para resolver los subproblemas y las otras operaciones obtendremos recurrencias de la forma:

$$t(n) = a t(n/b) + f(n) \quad t(1) = t_1$$

El restringir el análisis a potencias de  $b$  es válido ya que interesa el comportamiento asintótico de la solución a la recurrencia. Intuitivamente es claro que los algoritmos considerados se ejecutan en un tiempo intermedio para tamaños intermedios, y en cualquier caso podemos “rellenar” los datos hasta completar la potencia respectiva. Hacer esto no cambia nuestras conclusiones más abajo.

En el caso de ordenamiento por intercalación, dividimos en dos partes iguales que se procesan recursivamente. El proceso de dividir puede implementarse vía tomar elementos alternativos y ubicarlos en grupos separados, el combinar las partes ordenadas toma tiempo proporcional a su tamaño. Por lo tanto, el crear los subproblemas y combinar sus soluciones toma un tiempo proporcional al número de elementos a ordenar. Así tenemos que  $a = b = 2$ ,  $f(n) = cn$  para alguna constante  $c$ . Para búsqueda binaria, se divide en dos partes iguales de las cuales se procesa recursivamente solo una, y el proceso de división es simplemente ubicar el elemento medio y comparar con él, y no hay combinación de subproblemas; todo esto toma un tiempo constante. En este caso es  $a = 1$ ,  $b = 2$ ,  $f(n) = c$  para alguna constante. En el algoritmo de Karatsuba se transforma la multiplicación de dos números de largo  $2n$  en 3 multiplicaciones de números de  $n$  dígitos, las tareas adicionales son dividir los números en mitades y efectuar varias sumas y restas de números de  $2n$  dígitos, y finalmente juntar las piezas. El costo de estas operaciones es simplemente proporcional a  $n$ . Resulta  $a = 3$ ,  $b = 2$  y  $f(n) = cn$ . En la multiplicación de matrices de Strassen el multiplicar matrices de  $2n \times 2n$  se traduce en 7 multiplicaciones de matrices de  $n \times n$  y algunas sumas de matrices. Tenemos entonces  $a = 7$ ,  $b = 2$ , y las operaciones adicionales son básicamente sumas de matrices, lo que da  $f(n) = cn^2$ . Para cubrir el patio de  $2^n \times 2^n$  de la Universidad de Miskatonic con losas en L que vimos al discutir inducción fuerte (sección 3.7.6), la demostración que dimos reduce el problema de  $2^n \times 2^n$  a 4 problemas de  $2^{n-1} \times 2^{n-1}$  haciendo una cantidad fija de trabajo, lo que hace  $a = 4$ ,  $b = 2$ ,  $d = 0$ . Si aprovechamos simetrías con el cuadradito a cubrir siempre en una esquina, es un solo trabajo menor, con lo que  $a = 1$ ,  $b = 2$ ,  $d = 0$ . En caso que la posición de August es arbitraria, hay 2 tipos de subproblemas (uno con el espacio libre en la esquina, el otro con el espacio para August en una posición arbitraria), y  $a = 2$ ,  $b = 2$ ,  $d = 0$ .

Estos ejemplos son bastante representativos. El análisis es simple si  $f(n) = cn^d$ . Para búsqueda binaria tenemos  $d = 0$ , para ordenamiento por intercalación y en Karatsuba  $d = 1$ , Strassen da  $d = 2$ . El cuadro 19.2 resume los parámetros para los algoritmos dados.

Consideraremos entonces la recurrencia, válida para  $n$  una potencia de  $b$ :

$$t(bn) = at(n) + cn^d \quad t(1) = t_1$$

Efectuamos el cambio de variables:

$$\begin{aligned} n &= b^k & k &= \log_b n \\ t(n) &= T(k) & t(bn) &= T(k+1) \end{aligned}$$

En estos términos, dadas las condiciones del problema para constantes  $c > 0$  (el costo de dividir y combinar no es nulo) y  $t_1 > 0$  (el resolver un problema de tamaño mínimo tiene algún costo) tenemos para  $k \geq 0$ :

$$T(k+1) = aT(k) + c(b^d)^k \quad T(0) = t_1$$

Para resolver la recurrencia definimos la función generatriz:

$$g(z) = \sum_{k \geq 0} T(k)z^k$$

y aplicamos nuestra técnica a la recurrencia lineal resultante:

$$\begin{aligned} \frac{g(z) - t_1}{z} &= g(z) + c \frac{1}{1 - b^d z} \\ g(z) &= \frac{t_1 - (b^d t_1 - c)z}{(1 - b^d z)(1 - az)} \end{aligned}$$

Si  $a \neq b^d$ :

$$g(z) = \frac{c}{b^d - a} \cdot \frac{1}{1 - b^d z} + \frac{(b^d - a)t_1 - c}{b^d - a} \cdot \frac{1}{1 - az} \quad (19.46)$$

Cuando  $a = b^d$ :

$$g(z) = \frac{c}{a} \cdot \frac{1}{(1 - az)^2} + \frac{at_1 - c}{a} \cdot \frac{1}{1 - az} \quad (19.47)$$

El comportamiento asintótico queda determinado por  $a$  y  $b^d$ . Si  $a > b^d$ , domina el segundo término de (19.46):

$$T(k) \sim \left( t_1 + \frac{c}{a - b^d} \right) \cdot a^k \quad (19.48)$$

Si  $a < b^d$ , es el primer término de (19.46) el dominante:

$$T(k) \sim \frac{c}{b^d - a} \cdot b^{kd} \quad (19.49)$$

En caso que  $a = b^d$  debemos recurrir a (19.47), y es dominante el primer término:

$$T(k) \sim \frac{c}{a} \cdot k a^k \quad (19.50)$$

Las constantes indicadas son siempre diferentes de cero.

En términos de las variables originales, es  $k = \log_b n$  y  $a^k = a^{\log_b n} = b^{\log_b a \cdot \log_b n} = n^{\log_b a}$ :

$$t(n) \sim \begin{cases} \left( t_1 + \frac{c}{a - b^d} \right) \cdot n^{\log_b a} & \text{si } a > b^d \\ \frac{c}{a} n^{\log_b a} \log n & \text{si } a = b^d \\ \frac{c}{b^d - a} \cdot n^d & \text{si } a < b^d \end{cases}$$

Para los algoritmos que describimos tenemos las complejidades resumidas en el cuadro 19.2.

Nombre	$a$	$b$	$d$	Complejidad
Búsqueda binaria	1	2	0	$O(\log n)$
Ordenamiento por intercalación	2	2	1	$O(n \log n)$
Karatsuba	3	2	1	$O(n^{\log_2 3})$
Pavimentación	4	2	0	$O(n^2)$
	2	2	0	$O(n)$
	1	2	0	$O(n)$
Strassen	7	2	2	$O(n^{\log_2 7})$

Cuadro 19.2 – Complejidad de algunos algoritmos

Este tipo de recurrencias puede resolverse exactamente. Por ejemplo, Sedgewick y Flajolet [320] muestran que la solución a la recurrencia para el número de comparaciones en mergesort de  $n$  elementos diferentes:

$$C_n = C_{\lfloor n/2 \rfloor} + C_{\lceil n/2 \rceil} + n \quad C_1 = 0 \quad (19.51)$$

es:

$$C_n = n \log_2 n + n\theta(1 - \{\log_2 n\}) \quad (19.52)$$

donde:

$$\theta(x) = 1 + x - 2^x \quad (19.53)$$

Resulta  $\theta(0) = \theta(1) = 0$  y  $0 < \theta(x) < 0,086$  para  $0 < x < 1$ . Esta clase de comportamiento “periódico” complica el análisis preciso de muchos algoritmos.

Un desarrollo didáctico de resultados de este tipo se encuentra en el texto de Stein, Drysdale y Bogarth [336, apéndice A]. Una visión alternativa, incluyendo técnicas para acotar el caso de funciones forzantes diferentes, dan Bentley, Haken y Saxe [38]. Una extensión a estos resultados es el teorema de Akra-Bazzi [7]. Leighton [235] da la variante que reseñamos, extensiones interesantes da Roura [308], soluciones más precisas para versiones discretas (con techos/pisos) ofrecen Drmota y Szpankowski [102]. Para el caso común de recurrencias de la forma:

$$a(n) = \sum_{1 \leq k \leq s} r_k a(\lfloor n/m_k \rfloor) \quad a(1) = 1$$

donde  $r_k > 0$  y  $m_k \geq 2$  son enteros Erdős, Hildebrand, Odlyzko, Pudaite y Reznick [116] dan el comportamiento asintótico.

**Teorema 19.1** (Akra-Bazzi). *Sea una recurrencia de la forma:*

$$T(z) = g(z) + \sum_{1 \leq k \leq n} a_k T(b_k z + h_k(z)) \quad \text{para } z \geq z_0$$

donde  $z_0$ ,  $a_k$  y  $b_k$  son constantes, sujetas a las siguientes condiciones:

- Hay suficientes casos base.
- Para todo  $k$  se cumplen  $a_k > 0$  y  $0 < b_k < 1$ .
- Hay una constante  $c$  tal que  $|g(z)| = O(z^c)$ .
- Para todo  $k$  se cumple  $|h_k(z)| = O(z/(\log z)^2)$ .

Entonces, si  $p$  es tal que:

$$\sum_{1 \leq k \leq n} a_k b_k^p = 1$$

la solución a la recurrencia cumple:

$$T(z) = \Theta\left(z^p \left(1 + \int_1^z \frac{g(u)}{u^{p+1}} du\right)\right)$$

Frente a nuestro tratamiento tiene la ventaja de manejar divisiones desiguales ( $b_k$  diferentes), y explícitamente considera pequeñas perturbaciones en los términos, como lo son aplicar pisos o techos, a través de los  $h_k(z)$ . Diferencias con pisos y techos están acotados por una constante, mientras la cota del teorema permite que crezcan. Por ejemplo, la recurrencia correcta para el número de comparaciones en ordenamiento por intercalación es:

$$T(n) = T(\lfloor n/2 \rfloor) + T(\lceil n/2 \rceil) + n - 1$$

El teorema de Akra-Bazzi es aplicable. La recurrencia es:

$$T(n) = T(n/2 + h_+(n)) + T(n/2 + h_-(n)) + n - 1$$

Acá  $|h_{\pm}(n)| \leq 1/2$ , además  $a_{\pm} = 1$  y  $b_{\pm} = 1/2$ . Estos cumplen las condiciones del teorema, de:

$$\sum_{1 \leq k \leq 2} a_k b_k^p = 1$$

resulta  $p = 1$ , y tenemos la cota:

$$T(z) = \Theta\left(z \left(1 + \int_1^z \frac{u-1}{u^2} du\right)\right) = \Theta(z \ln z + 1) = \Theta(z \log z)$$

Otro ejemplo son los árboles de búsqueda aleatorizados (*Randomized Search Trees*, ver por ejemplo Aragon y Seidel [18], Martínez y Roura [249] y Seidel y Aragon [321]) en uno de ellos de tamaño  $n$  una búsqueda toma tiempo aproximado:

$$T(n) = \frac{1}{4} T(n/4) + \frac{3}{4} T(3n/4) + 1$$

Nuevamente es aplicable el teorema 19.1, de:

$$\frac{1}{4} \left(\frac{1}{4}\right)^p + \frac{3}{4} \left(\frac{3}{4}\right)^p = 1$$

obtenemos  $p = 0$ , y por tanto la cota

$$T(z) = \Theta\left(z^0 \left(1 + \int_1^z \frac{du}{u}\right)\right) = \Theta(\log z)$$

### 19.7.2. Quicksort

Quicksort, debido a Hoare [175], es otro algoritmo basado en dividir y conquistar, pero en este caso la división no es fija. Dado un rango de elementos de un arreglo a ser ordenado, se elige un elemento *pivote* de entre ellos y se reorganizan los elementos en el rango de forma que todos los elementos menores que el pivote queden antes de este, y todos los elementos mayores queden después. Con esto el pivote ocupa su posición final en el arreglo, y bastará ordenar recursivamente cada

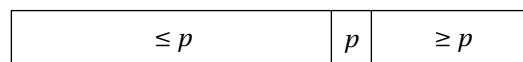


Figura 19.3 – Idea de Quicksort

uno de los dos nuevos rangos generados para completar el trabajo. La figura 19.4 indica una manera

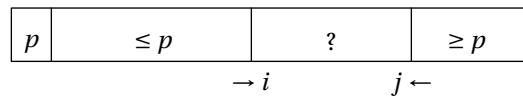


Figura 19.4 – Particionamiento en Quicksort

popular de efectuar esta *partición*: Se elige un pivote de forma aleatoria y el pivote elegido se intercambia con el primer elemento del rango (para sacarlo de en medio), luego se busca un elemento mayor que el pivote desde la izquierda y uno menor desde la derecha. Estos están fuera de orden, se

---

```

static double *a;

static int partition(const int lo, const int hi)
{
    int i = lo; j = hi + 1;

    for (;;) {
        while(a[++i] < a[lo])
            if(i == hi) break;
        while(a[lo] < a[--j])
            if(i == lo) break;
        if(i >= j) break;
        tmp = a[i]; a[i] = a[j]; a[j] = tmp;
    }
    return j;
}

static void qsr(const int lo, const int hi)
{
    int j;

    if(hi <= lo) return;
    j = partition(lo, hi);
    qsr(lo, j - 1);
    qsr(j + 1, hi);
}

void quicksort(double aa[], const int n)
{
    a = aa;
    qsr(0, n - 1);
}

```

---

Listado 19.1 – Versión simple de Quicksort

intercambian y se continúa de la misma forma hasta agotar el rango. Después se repone el pivote en su lugar, intercambiándolo con el último elemento menor que él. El rango finalmente queda como indica la figura 19.3. El listado 19.1 muestra una versión simple del programa, que elige siempre el primer elemento del rango como pivote. Evaluaremos el tiempo promedio de ejecución del algoritmo. Supondremos  $n$  elementos todos diferentes, que las  $n!$  permutaciones de los  $n$  elementos son igualmente probables, y que el pivote se elige al azar en cada etapa. En este caso está claro que el método de particionamiento planteado no altera el orden de los elementos en las particiones respecto del orden que tenían originalmente. Luego, los elementos en cada partición también son una permutación al azar.

Para efectos del análisis del algoritmo tomaremos como medida de costo el número promedio de comparaciones que efectúa Quicksort al ordenar un arreglo de  $n$  elementos. El trabajo adicional que se hace en cada partición será aproximadamente proporcional a esto, por lo que esta es una buena vara de medida. Al particionar, cada uno de los  $n - 1$  elementos fuera del pivote se comparan con

este exactamente una vez en el método planteado, y además es obvio que este es el mínimo número de comparaciones necesario para hacer este trabajo. Si llamamos  $k$  a la posición final del pivote, el costo de las llamadas recursivas que completan el ordenamiento será  $C(k-1) + C(n-k)$ . Si elegimos el pivote al azar la probabilidad de que  $k$  tenga un valor cualquiera entre 1 y  $n$  es la misma. Cuando el rango es vacío no se efectúan comparaciones. Estas consideraciones llevan a la recurrencia:

$$C(n) = n - 1 + \frac{1}{n} \sum_{1 \leq k \leq n-1} (C(k-1) + C(n-k)) \quad C(0) = 0$$

Por simetría podemos simplificar la suma, dado que estamos sumando los mismos términos en orden creciente y decreciente. Cambiando el rango de la suma y multiplicando por  $n$  queda:

$$nC(n) = n(n-1) + 2 \sum_{0 \leq k \leq n-1} C(k)$$

Ajustando los índices:

$$(n+1)C(n+1) = n(n+1) + 2 \sum_{0 \leq k \leq n} C(k) \quad C(0) = 0$$

Definimos la función generatriz ordinaria:

$$c(z) = \sum_{n \geq 0} C(n)z^n$$

Aplicando las propiedades de funciones generatrices ordinarias a la recurrencia queda la ecuación diferencial:

$$\begin{aligned} (zD + 1) \frac{c(z)}{z} &= ((zD)^2 + zD) \frac{1}{1-z} + \frac{2c(z)}{1-z} \quad c(0) = 0 \\ c'(z) &= \frac{2c(z)}{1-z} + \frac{2z}{(1-z)^3} \end{aligned}$$

La solución a esta ecuación es:

$$c(z) = -2 \frac{\ln(1-z)}{(1-z)^2} - \frac{2z}{(1-z)^2}$$

El primer término corresponde a la suma parcial de la secuencia de números harmónicos (derivamos su función generatriz en la sección 19.1), el segundo término da un coeficiente binomial:

$$\begin{aligned} C(n) &= 2 \sum_{0 \leq k \leq n} H_k - 2 \binom{n}{1} \\ &= 2 \sum_{0 \leq k \leq n} H_k - 2n \end{aligned}$$

Interesa obtener una fórmula más simple para la suma de los números harmónicos. Por la fórmula para la función generatriz de las sumas parciales:

$$H(z) = \sum_{n \geq 0} H_n z^n = \frac{1}{1-z} \ln \frac{1}{1-z}$$

con lo que la función generatriz de las sumas de números harmónicos es:

$$\frac{H(z)}{1-z} = \frac{1}{(1-z)^2} \ln \frac{1}{1-z} \tag{19.54}$$

Los coeficientes los conocemos de (19.10):

$$\begin{aligned} \sum_{0 \leq k \leq n} H_k &= (n+1)H_{n+1} - (n+1) \\ &= (n+1)H_n - n \end{aligned} \tag{19.55}$$

Esto da finalmente:

$$C(n) = 2(n+1)H_n - 4n$$

Vimos en el capítulo 18 que  $H_n = \ln n + O(1)$ , con lo que  $C(n) = 2n \ln n + O(n)$ .

Pero podemos hacer más. En el peor caso, al particionar en cada paso elegimos uno de los elementos extremos, con lo que las particiones son de largo 0 y  $n-1$ , lo que da lugar a la recurrencia:

$$C_{\text{peor}}(n) = n-1 + C_{\text{peor}}(n-1) \quad C_{\text{peor}}(0) = 0$$

Las técnicas estándar dan como solución:

$$\begin{aligned} C_{\text{peor}}(n) &= \frac{n(n-1)}{2} \\ &= \frac{1}{2}n^2 + O(n) \end{aligned}$$

El mejor caso es cuando en cada paso la división es equitativa, lo que lleva casi a la situación de dividir y conquistar analizada antes (sección 19.7.1), con  $a = 2$ ,  $b = 2$  y  $d = 1$ , cuya solución sabemos es  $C_{\text{mejor}}(n) = O(n \log n)$ . Un análisis más detallado, restringido al caso en que  $n = 2^k - 1$  de manera que los dos rangos siempre resulten del mismo largo, es como sigue. La recurrencia original se reduce a:

$$C_{\text{mejor}}(n) = n-1 + 2C_{\text{mejor}}((n-1)/2) \quad C_{\text{mejor}}(0) = 0$$

Con el cambio de variables:

$$n = 2^k - 1 \quad F(k) = C_{\text{mejor}}(2^k - 1)$$

esto se transforma en:

$$F(k) = 2^k - 2 + 2F(k-1) \quad F(0) = 0$$

cuya solución es:

$$\begin{aligned} F(k) &= k2^k + 2^{k+1} + 2 \\ C_{\text{mejor}}(n) &= (n+1)\log_2(n+1) + 2(n+1) + 2 \\ &= \frac{1}{\ln 2} n \ln n + O(n) \end{aligned}$$

La constante en este caso es aproximadamente 1,443, el mejor caso no es demasiado mejor que el promedio; pero el peor caso es mucho peor.

Una variante común es usar un método de ordenamiento simple para rangos chicos. Una opción es cortar la recursión no cuando el rango se reduce a un único elemento sino cuando cae bajo un cierto margen; y luego se ordena todo mediante inserción, que funciona muy bien si los datos vienen “casi ordenados”, como resulta de lo anterior. Para analizar esto se requieren medidas más ajustadas del costo de los métodos, y se cambian las condiciones de forma que para valores de  $n$  menor que el

límite se usa el costo del método alternativo. Esto puede hacerse, pero es bastante engoroso y no lo veremos acá.

Para evitar el peor caso (que se da cuando el pivote es uno de los elementos extremos) una opción es tomar una muestra de elementos y usar la mediana (el elemento del medio de la muestra) como pivote. La forma más simple de hacer esto es tomar tres elementos. Como además es frecuente que se invoque el procedimiento con un arreglo “casi ordenado” (o incluso ya ordenado), conviene tomar como muestra el primero, el último y un elemento del centro, de forma de elegir un buen pivote incluso en ese caso patológico. A esta idea se le conoce como *mediana de tres*. Esta estrategia disminuye un tanto la constante por efecto de una división más equitativa. Tiene la ventaja adicional que tener elementos menor que el pivote al comienzo del rango y mayor al final no es necesario comparar índices para determinar si se llegó al borde del rango. El análisis detallado se encuentra por ejemplo en Sedgewick y Flajolet [320].

Por el otro lado, McIlroy [252] muestra cómo lograr que siempre tome el máximo tiempo posible. Quicksort (haciendo honor a su nombre) es muy rápido ya que las operaciones en sus ciclos internos implican únicamente una comparación y un incremento o decremento de un índice. Es ampliamente usado, y como su peor caso es muy malo, vale la pena hacer un estudio detallado de la ingeniería del algoritmo, como hacen Bentley y McIlroy [39]. Debe tenerse cuidado con Quicksort por su peor caso, si un atacante puede determinar los datos puede hacer que el algoritmo consuma muchísimos recursos. Para evitar el peor caso se ha propuesto cambiar a Heapsort, debido a Williams [365] (garantizadamente  $O(n \log n)$ , pero mucho más lento que Quicksort) si se detecta un caso malo, como propone Musser [262].

# 20 Recurrencias

---

Es común encontrarse con situaciones en las cuales debemos resolver alguna *recurrencia*, vale decir, tenemos una ecuación que relaciona valores de una secuencia (generalmente adicionando algunos valores iniciales). Esto aparece tanto en la solución de problemas combinatorios como en el análisis de diversos algoritmos. Algunas de las técnicas que discutiremos se desarrollaron inicialmente para su aplicación en campos diversos como la economía o el control de procesos. Quienes hayan profundizado en el estudio de la solución de ecuaciones diferenciales hallarán paralelos sorprendentes (y divergencias importantes) con esa área. No disponemos de espacio para estudiar ese fenómeno en más detalle (ni es de nuestro interés inmediato).

## 20.1. Definición del problema

La situación general puede describirse:

$$f(a_n, a_{n+1}, \dots, a_{n+k}, n) = 0 \quad (20.1)$$

Si en (20.1) aparece la secuencia  $\langle a_n \rangle_{n \geq 0}$  completa, se le llama *de historia completa*, en caso contrario *de historia limitada*. Si aparecen  $a_n$  y  $a_{n+k}$ , se habla de una *recurrencia de orden k*. En general harán falta  $k$  valores para determinar la secuencia mediante una recurrencia de orden  $k$ , típicamente dados como  $a_0$  hasta  $a_{k-1}$ , de (20.1) podremos obtener  $a_k$ , con  $a_1$  a  $a_k$  tenemos  $a_{k+1}$ , y así sucesivamente. Es claro que hallar una expresión cerrada para los términos de tales secuencias será posible solo en situaciones especiales.

## 20.2. Recurrencias lineales

Una recurrencia se dice *lineal* si puede escribirse de la forma:

$$u_k(n)a_{n+k} + u_{k-1}(n)a_{n+k-1} + \dots + u_0(n)a_n = f(n) \quad (20.2)$$

donde  $u_i(n)$  y  $f(n)$  son funciones conocidas. Si tanto  $u_k$  como  $u_0$  son diferentes de cero, es una *recurrencia de orden k*. Si  $f(n) = 0$ , se dice que la recurrencia es *homogénea*, en caso contrario *no homogénea*. El estudio de las recurrencias lineales hace uso del álgebra lineal, para mayores detalles véanse por ejemplo Strang [340] o Treil [352].

Es claro que si las secuencias  $\langle x_n \rangle$  y  $\langle y_n \rangle$  satisfacen una recurrencia lineal homogénea, la combinación lineal  $\langle \alpha x_n + \beta y_n \rangle$  también la satisface. Esta es la razón del nombre. Si expresamos la recurrencia homogénea como:

$$a_{n+k} = u_{k-1}(n)a_{n+k-1} + u_{k-2}(n)a_{n+k-2} + \dots + u_0(n)a_n \quad (20.3)$$

con los vectores  $\mathbf{a}_n = (a_{n+k-1}, a_{n+k-2}, \dots, a_n)$  podemos expresar la recurrencia (20.3) como:

$$\mathbf{a}_{n+1} = \mathbf{U}_n \cdot \mathbf{a}_n \quad (20.4)$$

donde:

$$\mathbf{U}_n = \begin{pmatrix} u_{k-1}(n) & u_{k-2}(n) & \cdots & u_1(n) & u_0(n) \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \quad (20.5)$$

lo que nos permite expresar:

$$\mathbf{a}_n = \mathbf{U}_{n-1} \cdot \mathbf{U}_{n-2} \cdots \mathbf{U}_0 \cdot \mathbf{a}_0 \quad (20.6)$$

Esto dice que la solución de la ecuación lineal homogénea es la combinación lineal de  $k$  soluciones linealmente independientes: Podemos elegir los  $k$  componentes de  $\mathbf{a}_0$  independientemente, si ninguna de las matrices  $\mathbf{U}_n$  es singular vectores iniciales linealmente independientes darán vectores finales linealmente independientes. La solución general de la recurrencia lineal no homogénea puede expresarse como una solución particular y la combinación lineal de  $k$  soluciones linealmente independientes de la recurrencia homogénea.

En caso que  $\mathbf{U}_n$  sea una matriz constante  $\mathbf{U}$  (la recurrencia tiene coeficientes constantes), la ecuación (20.6) se reduce a:

$$\mathbf{a}_n = \mathbf{U}^n \cdot \mathbf{a}_0 \quad (20.7)$$

Técnicas eficientes para el cálculo de potencias (ver la sección 11.3) permiten obtener el vector  $\mathbf{a}_n$  rápidamente de (20.7). Esto ofrece una alternativa a las técnicas expuestas en el capítulo 14.

Una matriz  $A$  se dice *diagonalizable* si hay una matriz diagonal  $D$  y una matriz invertible  $P$  tales que  $A = PDP^{-1}$ . Calcular potencias de una matriz expresada de esta forma es particularmente simple, ya que  $A^n = P D^n P^{-1}$ , y la potencia de la matriz diagonal es simplemente las potencias de sus elementos. Los elementos de la matriz  $D$  resultan ser los valores propios de  $A$ , las soluciones de la ecuación  $\det(A - \lambda I) = 0$ . Esto da una forma alternativa de expresar la solución de la recurrencia (20.2) para el caso de coeficientes constantes.

### 20.3. Recurrencias lineales de primer orden

Un caso de particular interés práctico son las recurrencias lineales de primer orden, que podemos escribir:

$$a_{n+1} = u_n a_n + f_n \quad (20.8)$$

Vemos que si dividimos (20.8) por el *factor sumador*:

$$s_n = \prod_{0 \leq k \leq n} u_k \quad (20.9)$$

(lo que presupone que  $u_k \neq 0$  en el rango de interés) queda:

$$\frac{a_{n+1}}{s_n} - \frac{a_n}{s_{n-1}} = \frac{f_n}{s_n}$$

Sumando ambos lados obtenemos la solución.

La fórmula general es bastante engorrosa, ilustraremos la técnica mediante un ejemplo. Sea:

$$a_{n+1} = \frac{2(n+1)a_n + 5(n+1)!}{3} \quad a_0 = 5 \quad (20.10)$$

Reordenando un poco:

$$a_{n+1} - \frac{2(n+1)}{3} a_n = \frac{5(n+1)!}{3}$$

Vemos que el factor sumador es:

$$\begin{aligned} s_n &= \prod_{0 \leq k \leq n} \frac{2(n+1)}{3} \\ &= \left(\frac{2}{3}\right)^{n+1} (n+1)! \end{aligned}$$

Dividiendo la recurrencia por esto y sumando para  $0 \leq k \leq n-1$  resulta:

$$\begin{aligned} \frac{a_n}{(2/3)^n n!} - \frac{a_0}{s_{-1}} &= \frac{5}{3} \sum_{0 \leq k \leq n-1} \left(\frac{3}{2}\right)^{k+1} \\ \frac{a_n}{(2/3)^n n!} - \frac{5}{1} &= \frac{5}{3} \cdot \frac{3}{2} \cdot \frac{(3/2)^n - 1}{3/2 - 1} \\ \frac{a_n}{(2/3)^n n!} &= 5 + 5 \cdot ((3/2)^n - 1) \\ &= 5 \cdot (3/2)^n \\ a_n &= 5n! \end{aligned}$$

A veces esto sirve para simplificar sumas. Siguiendo esencialmente la estrategia de Rockett [305] calcularemos:

$$\sum_{0 \leq k \leq n} \binom{n}{k}^{-1} = \frac{1}{n!} \sum_{0 \leq k \leq n} k!(n-k)!$$

Nos concentraremos en la suma:

$$S_n = \sum_{0 \leq k \leq n} k!(n-k)! \tag{20.11}$$

$$\begin{aligned} &= \sum_{0 \leq k \leq n-1} k!(n-k)! + n! \\ &= \sum_{0 \leq k \leq n-1} k!(n-1-k)!((n+1)-(k+1)) + n! \\ &= (n+1) \sum_{0 \leq k \leq n-1} k!(n-1-k)! - \sum_{0 \leq k \leq n-1} k!(n-1-k)!(k+1) + n! \\ &= (n+1)S_{n-1} - \sum_{0 \leq k \leq n-1} (k+1)!(n-(k+1))! + n! \\ &= (n+1)S_{n-1} - \sum_{1 \leq k \leq n} k!(n-k)! + n! \\ &= (n+1)S_{n-1} - (S_n - n!) + n! \end{aligned}$$

$$2S_n = (n+1)S_{n-1} + 2n! \tag{20.12}$$

De la definición (20.11) es  $S_0 = 1$ . El factor sumador de (20.12) es  $2^{-n}(n+1)!$ :

$$\begin{aligned} \frac{2^{n+1}}{(n+1)!} S_n &= \frac{2^n}{n!} S_{n-1} + \frac{2^{n+1}}{n+1} \\ \frac{2^{n+1}}{(n+1)!} S_n - \frac{2}{1!} S_0 &= \sum_{1 \leq k \leq n} \frac{2^{k+1}}{k+1} \end{aligned}$$

Casualmente coincide con el término para  $k = 0$ :

$$\frac{2^{n+1}}{(n+1)!} S_n = \sum_{0 \leq k \leq n} \frac{2^{k+1}}{k+1}$$

O sea:

$$S_n = \frac{(n+1)!}{2^{n+1}} \sum_{0 \leq k \leq n} \frac{2^{k+1}}{k+1} \quad (20.13)$$

Con esto nuestra suma original es:

$$\sum_{0 \leq k \leq n} \binom{n}{k}^{-1} = \frac{n+1}{2^{n+1}} \sum_{0 \leq k \leq n} \frac{2^{k+1}}{k+1} \quad (20.14)$$

## 20.4. Recurrencias lineales de coeficientes constantes

Un caso particularmente importante es el de relaciones de recurrencias de la forma:

$$a_k u_{n+k} + a_{k-1} u_{n+k-1} + \cdots + a_0 u_n = f(n)$$

donde los  $a_i$  son constantes y  $f(n)$  es una función cualquiera. Esto se llama una *relación de recurrencia lineal de coeficientes constantes* (de orden  $k$ , si  $a_k \neq 0$ ). Si  $f(n) = 0$ , se dice *homogénea*. Se requieren  $k$  condiciones adicionales para fijar la solución, que generalmente toman la forma de *condiciones iniciales* dando los valores de  $u_0$  hasta  $u_{k-1}$ . Esto completa una *recurrencia lineal*. La recurrencia de Fibonacci que resolvimos antes es una recurrencia de segundo orden, lineal, de coeficientes constantes, homogénea. La recurrencia a la que nos llevó la Competencia de Ensayos de la Universidad de Miskatonic (sección 3.10) es de primer orden, lineal de coeficientes constantes, no homogénea.

Tratar el caso general es bastante engorroso, mostraremos el procedimiento mediante un ejemplo. De forma similar a la aplicación de funciones generatrices ordinarias presentada acá pueden aplicarse funciones generatrices exponenciales como lo hicimos en la sección 19.4.2 para los números de Fibonacci. Cuál se usa en un caso particular dependerá de lo que resulte más simple.

Consideremos la recurrencia:

$$a_{n+2} = 2a_{n+1} - 4a_n + 4n \cdot 2^n \quad a_0 = 5, a_1 = 0$$

Los primeros valores muestran comportamiento errático:

$$\langle 5, 0, -20, -32, 48, 320, 704, 768, 256, 1024, 9216, \dots \rangle$$

Por nuestra estrategia general, definimos:

$$A(z) = \sum_{n \geq 0} a_n z^n$$

Aplicando las propiedades de funciones generatrices ordinarias queda:

$$\frac{A(z) - 5}{z^2} = 2 \frac{A(z) - 5}{z} - 4A(z) + 4zD \frac{1}{1-2z}$$

Despejando y expresando en fracciones parciales:

$$\begin{aligned} A(z) &= \frac{5 - 30z + 60z^2 - 32z^3}{1 - 6z + 16z^2 - 24z^3 + 16z^4} \\ &= \frac{3 + i\sqrt{3}}{1 - (1 + i\sqrt{3})z} + \frac{3 - i\sqrt{3}}{1 - (1 - i\sqrt{3})z} + \frac{1}{(1 - 2z)^2} - \frac{2}{1 - 2z} \end{aligned}$$

Leemos coeficientes de estas series (geométrica y potencia de un binomio):

$$\begin{aligned} a_n &= (3 + i\sqrt{3}) \cdot (1 + i\sqrt{3})^n + (3 - i\sqrt{3}) \cdot (1 - i\sqrt{3})^n + (n+1) \cdot 2^n - 2 \cdot 2^n \\ &= (3 + i\sqrt{3}) \cdot (1 + i\sqrt{3})^n + (3 - i\sqrt{3}) \cdot (1 - i\sqrt{3})^n + (n-1) \cdot 2^n \end{aligned}$$

Es bien poco probable que hubiéramos adivinado esta solución...

Alternativamente, sabemos que las partes complejas son conjugadas:

$$\alpha \cdot r^n + \bar{\alpha} \cdot \bar{r}^n = 2\Re(\alpha \cdot r^n)$$

En nuestro caso, en términos de exponentiales complejas:

$$\begin{aligned} 3 + i\sqrt{3} &= 2\sqrt{3} \cdot \exp\left(\frac{\pi i}{6}\right) \\ 1 + i\sqrt{3} &= 2 \cdot \exp\left(\frac{\pi i}{3}\right) \end{aligned}$$

Uniendo las partes:

$$\begin{aligned} 2\Re((3 + i\sqrt{3}) \cdot (1 + i\sqrt{3})^n) &= 2\Re\left(2\sqrt{3} \cdot \exp\left(\frac{\pi i}{6}\right) \cdot 2^n \cdot \exp\left(\frac{n\pi i}{3}\right)\right) \\ &= 2^{n+2}\sqrt{3} \cos\left(\frac{\pi}{6} + \frac{n\pi}{3}\right) \end{aligned}$$

con lo que la solución es:

$$a_n = 2^{n+2}\sqrt{3} \cos\left(\frac{\pi}{6} + \frac{n\pi}{3}\right) + (n-1) \cdot 2^n$$

El término trigonométrico explica el comportamiento oscilatorio.

## 20.5. Método de repertorio

Una técnica útil para resolver ecuaciones lineales, introducida por Knuth y Schönhage [221], es lo que Knuth denomina *método del repertorio*. Describir el contexto formalmente es engoroso, lo ilustramos con una recurrencia tomada de Greene y Knuth [152] que concierne al número de comparaciones en quicksort eligiendo el pivote por mediana de tres:

$$C_n = n + 1 + \sum_{1 \leq k \leq n} \frac{\binom{k-1}{1} \binom{n-k}{1}}{\binom{n}{3}} (C_{k-1} + C_{n-k}) \quad (20.15)$$

Esta se explica porque elegimos 3 elementos entre  $n$ ; si el pivote resultante está en la posición final  $k$ , se eligió el menor de la muestra entre los  $k-1$  anteriores y el mayor entre los  $n-k$  posteriores. Es claro que la recurrencia no tiene sentido para  $n < 3$  (se elige el pivote como el elemento medio de una muestra de tres), requerimos  $C_1$  y  $C_2$  como valores iniciales ( $C_0$  nunca interviene).

Vemos que la suma es simétrica, y simplificamos. Reemplazamos  $n+1$  por una secuencia  $a_n$  en preparación para lo que sigue:

$$x_n = a_n + \frac{2}{\binom{n}{3}} \sum_{1 \leq k \leq n} (k-1)(n-k)x_{k-1} \quad (20.16)$$

La idea es armar un repertorio de secuencias  $x_n$  con sus correspondientes  $a_n$ , para construir la solución que nos interesa mediante una combinación lineal.

Eligiendo  $x_n = (n-1)^s$  resulta una suma manejable:

$$\begin{aligned}
 (n-1)^s &= a_n + \frac{12}{n^3} \sum_{1 \leq k \leq n} (n-k)(k-1)(k-2)^s \\
 &= a_n + \frac{12}{n^3} \sum_{1 \leq k \leq n} (n-k)(k-1)^{s+1} \\
 &= a_n + \frac{12}{n^3} \sum_{0 \leq k \leq n-1} (n-1-k)k^{s+1} \\
 &= a_n + \frac{12}{n^3} \cdot 1!(s+1)! \sum_{0 \leq k \leq n-1} \binom{n-1-k}{1} \binom{k}{s+1} \\
 &= a_n + \frac{12(s+1)!}{n^3} \binom{n}{s+3} \\
 &= a_n + \frac{12(s+1)!}{n^3} \cdot \frac{n^{s+3}}{(s+3)!} \\
 &= a_n + \frac{12(n-3)^s}{(s+1)^2}
 \end{aligned}$$

Acá usamos la identidad, simple de demostrar usando aceite de serpiente (sección 14.12):

$$\sum_{0 \leq k \leq n} \binom{n-k}{r} \binom{k}{s} = \binom{n+1}{r+s+1} \quad (20.17)$$

Resulta el cuadro 20.1. Buscamos  $a_n = n+1$ , con esta familia no basta, no hay  $a_n$  lineales.

$s$	$\mathbf{x}_n$	$\mathbf{a}_n$
0	1	-1
1	$n-1$	2
2	$(n-1)(n-2)$	$(2n^2+6n-26)/5$

Cuadro 20.1 – Familia para  $(n-1)^s$

De los resultados para quicksort (ver la sección 19.7.2) cabe esperar alguna expresión involucrando números harmónicos, intentemos la familia  $x_n = (n-1)^t H_n$ . Requeriremos:

$$\sum_{1 \leq k \leq n} k^r H_k$$

El plan es expandir la suma que define el número harmónico, intercambiar el orden de las sumas y

simplificar el resultado.

$$\begin{aligned}
 \sum_{1 \leq k \leq n} k^r H_k &= \sum_{1 \leq k \leq n} k^r \sum_{1 \leq j \leq k} \frac{1}{j} \\
 &= \sum_{1 \leq j \leq n} \frac{1}{j} \sum_{j \leq k \leq n} k^r \\
 &= \sum_{1 \leq j \leq n} \frac{1}{j} \left( \frac{(n+1)^{r+1}}{r+1} - \frac{j^{r+1}}{r+1} \right) \\
 &= \frac{(n+1)^{r+1}}{r+1} H_n - \frac{1}{r+1} \sum_{1 \leq j \leq n} \frac{j^{r+1}}{j} \\
 &= \frac{(n+1)^{r+1}}{r+1} H_n - \frac{1}{r+1} \sum_{1 \leq j \leq n} (j-1)^r \\
 &= \frac{(n+1)^{r+1}}{r+1} H_n - \frac{1}{r+1} \sum_{1 \leq j \leq n-1} j^r \\
 &= \frac{(n+1)^{r+1}}{r+1} H_{n+1} - \frac{(n+1)^{r+1}}{(r+1)(n+1)} - \frac{n^{r+1}}{(r+1)^2} \\
 &= \frac{(n+1)^{r+1}}{r+1} H_{n+1} - \frac{(n+1)^{r+1}}{(r+1)^2}
 \end{aligned}$$

O sea:

$$\sum_{1 \leq k \leq n} k^r H_k = \frac{(n+1)^{r+1}}{r+1} \left( H_{n+1} - \frac{1}{r+1} \right) \quad (20.18)$$

Dividiendo por  $r!$ , expresando en términos de coeficientes binomiales y simplificando obtenemos la agradable fórmula:

$$\sum_{1 \leq k \leq n} \binom{k}{r} H_k = \binom{n+1}{r+1} \left( H_{n+1} - \frac{1}{r+1} \right) \quad (20.19)$$

Con este resultado preliminar, podemos proceder:

$$\begin{aligned}
 (n-1)^t H_n &= a_n + \frac{12}{n^3} \sum_{1 \leq k \leq n} (n-k)(k-1)(k-2)^t H_{k-1} \\
 &= a_n + \frac{12}{n^3} \sum_{1 \leq k \leq n-1} (n-k-1)k^{t+1} H_k \\
 &= a_n + \frac{12}{n^3} \left( (n-t-2) \sum_{1 \leq k \leq n-1} k^{t+1} H_k - \sum_{1 \leq k \leq n-1} k^{t+2} H_k \right) \\
 &= a_n + \frac{12}{n^3} \left( (n-t-2) \frac{n^{t+2}}{t+2} H_n - (n-t-2) \frac{n^{t+2}}{(t+2)^2} - \frac{n^{t+3}}{t+3} H_n + \frac{n^{t+3}}{(t+3)^2} \right) \\
 &= a_n + \frac{12n^{t+3}}{n^3} \left( \frac{1}{(t+2)(t+3)} H_n - \frac{2t+5}{(t+2)^2(t+3)^2} \right) \\
 &= a_n + 12(n-3)^t \left( \frac{1}{(t+2)(t+3)} H_n - \frac{2t+5}{(t+2)^2(t+3)^2} \right)
 \end{aligned}$$

Resulta el cuadro 20.2. Como intuimos, obtenemos una expresión lineal con esta familia:  $(n+1)H_n$

$t$	$x_n$	$a_n$
0	$H_n$	$-H_n + 5/3$
1	$(n-1)H_n$	$2H_n + 7n/12 - 21/12$

Cuadro 20.2 – Familia para  $(n-1)^t H_n$ 

da  $7n/12 + 19/12$ . Combinando con la familia anterior, obtenemos la solución particular:

$$C_n = \frac{12}{7}(n+1)H_n + \frac{12}{7} \quad (20.20)$$

Pero necesitamos dos grados de libertad adicionales. Uno resulta de la sorprendente relación de la primera familia:

$$C'_n = n+1 \quad (20.21)$$

El segundo grado de libertad no es tan simple de ver. Pero estamos considerando la recurrencia:

$$n^3 x_n = 12 \sum_{1 < k < n} (n-k)(k-1)x_{k-1} \quad (20.22)$$

Definamos la función generatriz:

$$G(z) = \sum_{n \geq 1} x_n z^n$$

Un suave masaje (extender la suma a  $1 \leq k \leq n$  agrega términos que se anulan, desplazamos  $k$ , y evaluar para el siguiente  $n$ ) entrega:

$$(n+1)^3 x_{n+1} = 12 \sum_{0 \leq k \leq n} (n-k)k x_k \quad (20.23)$$

Al lado izquierdo de (20.23) tenemos la secuencia:

$$(n^2 - n)(n+1)x_{n+1} \rightsquigarrow ((zD)^2 - zD) G'(z) = z^2 G'''(z)$$

El lado derecho de (20.23) es la convolución de la secuencia  $\langle n \rangle_{n \geq 0}$  con  $\langle nx_n \rangle_{n \geq 0}$ , con lo que:

$$z^2 G'''(z) = 12 \frac{z}{(1-z)^2} \cdot z G'(z)$$

Simplificando resulta:

$$G'''(z) = \frac{12}{(1-z)^2} G'(z) \quad (20.24)$$

La forma de (20.24) sugiere una solución  $G(z) = (1-z)^\alpha$ , resultan las posibilidades  $\alpha = 0$  ( $G(z)$  constante,  $C_0$  es arbitrario),  $\alpha = -2$  (que entrega la ya conocida) y  $\alpha = 5$ , que da:

$$C''_n = [z^n](1-z)^5 = (-1)^n \binom{5}{n} \quad (20.25)$$

En consecuencia, combinando (20.20) con (20.21) y (20.25) para constantes  $c_1$  y  $c_2$  la solución completa es:

$$C_n = \frac{12}{7}(n+1)H_n + \frac{12}{7} + c_1(n+1) + c_2(-1)^n \binom{5}{n} \quad (20.26)$$

## 20.6. Recurrencia de Ricatti

Una recurrencia de la forma:

$$w_{n+1} = \frac{aw_n + b}{cw_n + d} \quad (20.27)$$

donde  $c \neq 0$  y  $ad - bc \neq 0$  se llama *recurrencia de Ricatti* (si  $c = 0$  es una recurrencia lineal de primer orden; si  $ad = bc$  se reduce a  $w_{n+1} = \text{constante}$ ). Incidentalmente, la recurrencia (19.28) para  $r$  que hallamos al analizar la búsqueda de Fibonacci en la sección 19.4.4 es una recurrencia de Ricatti.

Para resolver este tipo de recurrencias hay varias opciones, que exploraremos en lo que sigue.

### 20.6.1. Vía recurrencia de segundo orden

Seguimos el esquema de Brand [52]. Si en (20.27) substituimos  $y_n \mapsto cw_n + d$ , queda:

$$y_n = \alpha - \frac{\beta}{y_{n-1}} \quad (20.28)$$

donde:

$$\alpha = a + d$$

$$\beta = ad - bc$$

Claramente eso solo vale si  $ad - bc \neq 0$ . Substituyendo ahora:

$$y_n = \frac{x_{n+1}}{x_n} \quad (20.29)$$

resulta:

$$x_{n+2} - \alpha x_{n+1} + \beta x_n = 0 \quad (20.30)$$

Necesitamos dos valores iniciales para resolverla, podemos elegir bastante arbitrariamente  $x_0 = 1$ , dando  $x_1 = y_0$ , que a su vez podemos obtener de la condición inicial original.

Para un ejemplo, tomemos  $w_0 = 3$  y:

$$w_{n+1} = \frac{5w_n + 2}{3w_n + 4} \quad (20.31)$$

Siguiendo los pasos indicados:

$$\begin{aligned} 3w_{n+1} + 4 &= 3 \cdot \frac{5w_n + 2}{3w_n + 4} + 4 \\ &= 9 - \frac{14}{3w_n + 4} \end{aligned}$$

Substituyendo:

$$3w_n + 4 = \frac{x_{n+1}}{x_n}$$

y reordenando resulta:

$$x_{n+2} - 9x_{n+1} + 14x_n = 0 \quad (20.32)$$

Con las condiciones iniciales  $x_0 = 1$ ,  $x_1 = 3w_0 + 4 = 13$  la solución de (20.32) es:

$$x_n = \frac{11 \cdot 7^n - 6 \cdot 2^n}{5}$$

y finalmente:

$$w_n = \frac{11 \cdot 7^n + 2^{n+2}}{11 \cdot 7^n - 3 \cdot 2^{n+1}} \quad (20.33)$$

### 20.6.2. Reducción a una recurrencia de primer orden

Siguiendo a Mitchell [257] definamos la secuencia auxiliar:

$$x_n = \frac{1}{1 + \eta w_n} \quad (20.34)$$

Expresamos la recurrencia (20.27) en términos de  $x_n$ , y despejamos  $x_{n+1}$ :

$$x_{n+1} = \frac{(d\eta - c)x_n + c}{(b\eta^2 - (a-d)\eta - c)x_n + a\eta + c}$$

Buscamos que esta recurrencia sea lineal, o sea:

$$b\eta^2 - (a-d)\eta - c = 0$$

Arbitriariamente elegimos el signo positivo:

$$\eta = \frac{a-d + \sqrt{(a-d)^2 + 4bc}}{2b} \quad (20.35)$$

Esto lleva a la ecuación auxiliar:

$$x_{n+1} = \frac{(d\eta - c)x_n + c}{a\eta + c} \quad (20.36)$$

Esta es simple de resolver.

Aplicado al mismo ejemplo anterior, tenemos:

$$\eta = \frac{5 - 4 + \sqrt{(5-4)^2 + 4 \cdot 2 \cdot 3}}{2 \cdot 2} = \frac{3}{2}$$

La recurrencia auxiliar es:

$$\begin{aligned} x_{n+1} &= \frac{(4 \cdot \frac{3}{2} - 3)x_n + 3}{5 \cdot \frac{3}{2} + 3} \\ &= \frac{2x_n + 2}{7} \end{aligned} \quad (20.37)$$

De la condición inicial tenemos:

$$x_0 = \frac{1}{1 + \eta w_0} = \frac{2}{11} \quad (20.38)$$

La tradicional danza para resolver recurrencias entrega:

$$x_n = \frac{2}{5} - \frac{84}{385} \cdot \left(\frac{2}{7}\right)^n \quad (20.39)$$

De acá con (20.34) resulta:

$$w_n = \frac{11 \cdot 7^n + 2^{n+2}}{11 \cdot 7^n - 3 \cdot 2^{n+1}} \quad (20.40)$$

Tal como antes.

### 20.6.3. Transformación de Möbius

A una transformación de la forma:

$$w = \frac{a_{11}z + a_{12}}{a_{21}z + a_{22}} \quad (20.41)$$

donde  $a_{11}a_{22} - a_{12}a_{21} \neq 0$  (de lo contrario, la expresión se reduce a una constante) se le llama *transformación de Möbius*. Una de sus características interesantes es que forman un grupo con la composición de funciones, como es fácil demostrar. A nosotros puntualmente nos interesa lo siguiente: Sean  $A(z)$ ,  $B(z)$  transformaciones de Möbius.

$$A(z) = \frac{a_{11}z + a_{12}}{a_{21}z + a_{22}} \quad (20.42)$$

$$B(z) = \frac{b_{11}z + b_{12}}{b_{21}z + b_{22}} \quad (20.43)$$

La composición es:

$$A(B(z)) = \frac{(a_{11}b_{11} + a_{12}b_{21})z + (a_{11}b_{12} + a_{12}b_{22})}{(a_{21}b_{11} + a_{22}b_{21})z + (a_{21}b_{12} + a_{22}b_{22})} \quad (20.44)$$

Si representamos las transformaciones por las respectivas matrices de coeficientes, vemos que la composición corresponde al producto de las matrices. Lo que hace la recurrencia (20.27) es aplicar la transformación de Möbius repetidas veces:

$$w_n = A^n(w_0) \quad (20.45)$$

a lo que naturalmente corresponde el calcular la potencia de la matriz respectiva. Para cálculo numérico puede usarse entonces una técnica eficiente para calcular potencias, como las dadas en la sección 11.3.

En nuestro caso de matrices de  $2 \times 2$  los valores propios son simples de obtener:

$$(a_{11} - \lambda)(a_{22} - \lambda) - a_{12}a_{21} = 0 \quad (20.46)$$

La fórmula cuadrática da:

$$\lambda = \frac{a_{11} + a_{22} \pm \sqrt{(a_{11} + a_{22})^2 - 4(a_{11}a_{22} - a_{12}a_{21})}}{2} \quad (20.47)$$

Las columnas de la matriz  $\mathbf{P}$  a su vez son los vectores propios correspondientes:

$$\begin{pmatrix} a_{11} - \lambda_i & a_{12} \\ a_{21} & a_{22} - \lambda_i \end{pmatrix} \cdot \begin{pmatrix} p_{1i} \\ p_{2i} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad (20.48)$$

Por construcción, la matriz del sistema (20.48) es singular, y solo da una relación entre  $p_{1i}$  y  $p_{2i}$ . Podemos imponer cualquier condición que resulte cómoda. Conociendo  $\mathbf{D}$  y  $\mathbf{P}$  podemos calcular las potencias y así obtener la solución buscada.

Volviendo a nuestro manoseado ejemplo, tenemos:

$$\mathbf{A} = \begin{pmatrix} 5 & 2 \\ 3 & 4 \end{pmatrix} \quad (20.49)$$

Los valores propios son  $\lambda_1 = 7$  y  $\lambda_2 = 2$ , eligiendo valores  $p_{ij}$  enteros:

$$\mathbf{D} = \begin{pmatrix} 7 & 0 \\ 0 & 2 \end{pmatrix} \quad \mathbf{P} = \begin{pmatrix} 1 & 2 \\ 1 & -3 \end{pmatrix} \quad \mathbf{P}^{-1} = \frac{1}{5} \begin{pmatrix} 3 & 2 \\ 1 & -1 \end{pmatrix} \quad (20.50)$$

Podemos entonces calcular:

$$\begin{aligned} \mathbf{A}^n &= \mathbf{P} \cdot \mathbf{D}^n \cdot \mathbf{P}^{-1} \\ &= \frac{1}{5} \begin{pmatrix} 3 \cdot 7^n + 2^{n+1} & 2 \cdot 7^n - 2^{n+1} \\ 3 \cdot 7^n - 3 \cdot 2^n & 2 \cdot 7^n + 3 \cdot 2^n \end{pmatrix} \end{aligned} \quad (20.51)$$

Con esto es:

$$w_n = \frac{(3 \cdot 7^n + 2^{n+1}) w_0 + (7^n - 2^n)}{(2 \cdot 7^n - 2^{n+1}) w_0 + (2 \cdot 7^n + 3 \cdot 2^n)} \quad (20.52)$$

Nótese que esta solución muestra explícitamente la dependencia de la condición inicial. Con nuestra condición inicial  $w_0 = 3$  resulta nuevamente:

$$w_n = \frac{11 \cdot 7^n + 2^{n+2}}{11 \cdot 7^n - 3 \cdot 2^{n+1}} \quad (20.53)$$

## 21 El método simbólico

---

Vimos antes (capítulo 14) que las operaciones aritméticas entre funciones generatrices dan funciones generatrices que corresponden a combinaciones de los objetos que éstas representan. Expandiendo esta observación, veremos un marco en el cual derivar ecuaciones para las funciones generatrices de interés en problemas combinatorios es casi automático, como sistematizado por Flajolet y Sedgewick [126] y aplicado a análisis de algoritmos por Sedgewick y Flajolet [320]. Otra visión en la misma línea presenta Wilf [364]. Claro está que igual queda la tarea de extraer la información buscada de la ecuación resultante. Más adelante discutiremos herramientas para esta segunda tarea.

### 21.1. Un primer ejemplo

Consideremos primero el derivar una ecuación generatriz para el número de árboles binarios con  $n$  nodos, definidos diciendo que un árbol binario es una de las siguientes:

- Es *vacío*.
- Consta de un *nodo raíz* y dos subárboles binarios (izquierdo y derecho).

Una manera de modelar esto es usar la variable  $z$  para marcar los nodos, vía usar  $\beta$  para representar un árbol binario y  $|\beta|$  para su número de nodos, definir la función generatriz:

$$B(z) = \sum_{\beta} z^{|\beta|}$$

El coeficiente de  $z^n$  en  $B(z)$  es el número que nos interesa.

Directamente de la definición de árbol binario sabemos que hay un árbol binario vacío, que al no tener nodos aporta 1 a  $B(z)$ . Los demás se pueden dividir en un nodo raíz y dos subárboles binarios, vale decir:

$$\begin{aligned} B(z) &= 1 + \sum_{\beta_1, \beta_2} z^{1+|\beta_1|+|\beta_2|} \\ &= 1 + zB^2(z) \end{aligned}$$

Hay una íntima relación entre la definición recursiva y nuestra ecuación para la función generatriz. Lo que buscamos es sistematizar y extender esta observación.

Estamos interesados en colecciones de objetos. Formalmente:

**Definición 21.1.** Una *clase*  $\mathcal{A}$  es un conjunto numerable de *objetos*  $\alpha \in \mathcal{A}$ . A cada objeto  $\alpha$  se le asocia un *tamaño*,  $|\alpha| \in \mathbb{N}_0$ . El conjunto de objetos con un tamaño dado es finito.

Usaremos consistentemente letra caligráfica, como  $\mathcal{A}$ , para clases, y la misma letra para identificar nociones relacionadas. Así, para la clase  $\mathcal{A}$  generalmente usaremos  $a$  para un elemento de la clase y llamaremos  $a_n$  al número de objetos de la clase de tamaño  $n$ . Usaremos  $\mathcal{A}_n$  para referirnos al conjunto de objetos de la clase  $\mathcal{A}$  de tamaño  $n$ , con lo que  $a_n = |\mathcal{A}_n|$ . A las funciones generatrices ordinaria y exponencial correspondientes les llamaremos  $A(z)$  y  $\hat{A}(z)$ , respectivamente:

$$A(z) = \sum_{\alpha \in \mathcal{A}} z^{|\alpha|} = \sum_{n \geq 0} a_n z^n$$

$$\hat{A}(z) = \sum_{\alpha \in \mathcal{A}} \frac{z^{|\alpha|}}{|\alpha|!} = \sum_{n \geq 0} a_n \frac{z^n}{n!}$$

Nuestro siguiente objetivo es construir nuevas clases a partir de las que ya tenemos. Debe tenerse presente que como lo que nos interesa es contar el número de objetos de cada tamaño, basta construir objetos con distribución de tamaños adecuada (o sea, relacionados con lo que deseamos contar por una biyección). Comúnmente el tamaño de los objetos es el número de alguna clase de átomos que lo componen.

Las clases más elementales son  $\emptyset$ , la clase que no contiene objetos;  $\mathcal{E} = \{\epsilon\}$ , la clase que contiene únicamente el objeto vacío  $\epsilon$  (de tamaño nulo); y la clase que comúnmente llamaremos  $\mathcal{Z}$ , conteniendo un único objeto de tamaño uno (que llamaremos  $\zeta$  por consistencia). Luego definimos operaciones que combinan las clases  $\mathcal{A}$  y  $\mathcal{B}$  mediante *unión combinatoria*  $\mathcal{A} + \mathcal{B}$ , en que aparecen los  $\alpha$  y los  $\beta$  con sus tamaños (los objetos individuales se “decoran” con su proveniencia, de forma que  $\mathcal{A}$  y  $\mathcal{B}$  no necesitan ser disjuntos; pero generalmente nos preocuparemos que  $\mathcal{A}$  y  $\mathcal{B}$  sean disjuntos, o podemos usar el principio de inclusión y exclusión para contar los conjuntos de interés). Ocasionalmente restaremos objetos de una clase, lo que debe interpretarse sin decoraciones (estamos dejando fuera ciertos elementos, simplemente). Usaremos *producto cartesiano*  $\mathcal{A} \times \mathcal{B}$ , cuyos elementos son pares  $(\alpha, \beta)$  y el tamaño del par es  $|\alpha| + |\beta|$ . Otras operaciones son formar *secuencias* de elementos de  $\mathcal{A}$  (se anota  $\text{SEQ}(\mathcal{A})$ ), formar *conjuntos*  $\text{SET}(\mathcal{A})$  y *multiconjuntos*  $\text{MSET}(\mathcal{A})$  de elementos de  $\mathcal{A}$ . Consideraremos también la operación  $\text{CYC}(\mathcal{A})$ , que consiste en ordenar elementos de  $\mathcal{A}$  en un círculo (una secuencia conectando inicio y fin). Usaremos también la operación de *composición*, que anotaremos  $\mathcal{A} \circ \mathcal{B}$ , definida mediante para cada objeto  $\alpha \in \mathcal{A}$  construir un nuevo objeto substituyendo  $|\alpha|$  elementos de  $\mathcal{B}$  por sus átomos. Otra operación útil es *marcar* uno de los átomos de cada objeto, cosa que anotaremos  $\mathcal{A}^*$ . El tamaño de un objeto compuesto es simplemente la suma de los tamaños de los componentes. De incluir objetos de tamaño cero en estas construcciones pueden crearse infinitos objetos de un tamaño dado, lo que no es una clase según nuestra definición. Por ello estas construcciones son aplicables sólo si  $\mathcal{A}_0 = \emptyset$ .

Otro juego popular de notaciones para estas operaciones es  $\mathfrak{S}(\mathcal{A})$  para secuencia,  $\mathfrak{P}(\mathcal{A})$  para conjunto (de powerset),  $\mathfrak{M}(\mathcal{A})$  para multiconjunto  $\mathfrak{C}(\mathcal{A})$  para ciclo, y  $\theta \mathcal{A}$  para marcar un átomo.

Es importante recalcar las relaciones y diferencias entre las estructuras. En una secuencia es central el orden de las piezas que la componen. Ejemplo son las palabras, interesa el orden exacto de las letras (y estas pueden repetirse). En un conjunto solo interesa si el elemento está presente o no, no hay orden. En un conjunto un elemento en particular está o no presente, a un multiconjunto puede pertenecer varias veces.

En lo que sigue haremos distinción entre objetos rotulados y sin rotular. Para algunos ejemplos de la distinción véase la sección 14.6. Generalmente los rótulos se refieren a algún orden externo u otra marca que distingue a los elementos. Si un objeto se considera creado de átomos idénticos (intercambiables) corresponde considerarlos no rotulados; si un objeto está compuesto de átomos diferenciables podemos considerarlos rotulados secuencialmente, y estamos frente a objetos rotulados. Un punto que produce particular confusión es que tiene perfecto sentido hablar de secuencias de elementos sin rotular. La secuencia impone un orden, pero elementos iguales se consideran indistinguibles (en una palabra interesa el orden de las letras, pero al intercambiar dos letras iguales la palabra sigue siendo la misma). Recuerde la discusión de la sección 13.4.

## 21.2. Objetos sin rotular

Nuestro primer teorema relaciona las funciones generatrices ordinarias respectivas para algunas de las operaciones entre clases definidas antes. Las funciones generatrices de las clases  $\emptyset$ ,  $\mathcal{E}$  y  $\mathcal{Z}$  son, respectivamente, 0, 1 y  $z$ . En las derivaciones de las transferencias de ecuaciones simbólicas a ecuaciones para las funciones generatrices lo que nos interesa es contar los objetos entre manos, recurriremos a biyecciones para ello en algunos de los casos.

**Teorema 21.1** (Método simbólico, OGF). *Sean  $\mathcal{A}$  y  $\mathcal{B}$  clases de objetos, con funciones generatrices ordinarias respectivamente  $A(z)$  y  $B(z)$ . Entonces tenemos las siguientes funciones generatrices ordinarias:*

1. Para enumerar  $\mathcal{A} + \mathcal{B}$ :

$$A(z) + B(z)$$

2. Para enumerar  $\mathcal{A} \times \mathcal{B}$ :

$$A(z) \cdot B(z)$$

3. Para enumerar  $\text{SEQ}(\mathcal{A})$ :

$$\frac{1}{1 - A(z)}$$

4. Para enumerar  $\text{SET}(\mathcal{A})$ :

$$\prod_{\alpha \in \mathcal{A}} (1 + z^{|\alpha|}) = \prod_{n \geq 1} (1 + z^n)^{a_n} = \exp \left( \sum_{k \geq 1} \frac{(-1)^{k+1}}{k} A(z^k) \right)$$

5. Para enumerar  $\text{MSET}(\mathcal{A})$ :

$$\prod_{\alpha \in \mathcal{A}} \frac{1}{1 - z^{|\alpha|}} = \prod_{n \geq 1} \frac{1}{(1 - z^n)^{a_n}} = \exp \left( \sum_{k \geq 1} \frac{A(z^k)}{k} \right)$$

6. Para enumerar  $\text{CYC}(\mathcal{A})$ :

$$\sum_{n \geq 1} \frac{\phi(n)}{n} \ln \frac{1}{1 - A(z^n)}$$

*Demostración.* Usamos libremente resultados sobre funciones generatrices, capítulo 14, en las demostraciones de cada caso. Usaremos casos ya demostrados en las demostraciones sucesivas.

1. Si hay  $a_n$  elementos de  $\mathcal{A}$  de tamaño  $n$  y  $b_n$  elementos de  $\mathcal{B}$  de tamaño  $n$ , habrán  $a_n + b_n$  elementos de  $\mathcal{A} + \mathcal{B}$  de tamaño  $n$ .

Alternativamente, usando la notación de Iverson (ver la sección 1.5):

$$\sum_{\gamma \in \mathcal{A} \cup \mathcal{B}} z^{|\gamma|} = \sum_{\gamma \in \mathcal{A} \cup \mathcal{B}} ([\gamma \in \mathcal{A}] z^{|\gamma|} + [\gamma \in \mathcal{B}] z^{|\gamma|}) = \sum_{\alpha \in \mathcal{A}} z^{|\alpha|} + \sum_{\beta \in \mathcal{B}} z^{|\beta|} = A(z) + B(z)$$

2. Hay:

$$\sum_{0 \leq k \leq n} a_k b_{n-k}$$

maneras de combinar elementos de  $\mathcal{A}$  con elementos de  $\mathcal{B}$  cuyos tamaños sumen  $n$ , y este es precisamente el coeficiente de  $z^n$  en  $A(z) \cdot B(z)$ .

Alternativamente:

$$\sum_{\gamma \in \mathcal{A} \times \mathcal{B}} z^{|\gamma|} = \sum_{\substack{\alpha \in \mathcal{A} \\ \beta \in \mathcal{B}}} z^{|\alpha|+|\beta|} = \left( \sum_{\alpha \in \mathcal{A}} z^{|\alpha|} \right) \cdot \left( \sum_{\beta \in \mathcal{B}} z^{|\beta|} \right) = A(z) \cdot B(z)$$

3. Hay una manera de obtener la secuencia de largo 0 (aporta el objeto vacío  $\epsilon$ ), las secuencias de largo 1 son simplemente los elementos de  $\mathcal{A}$ , las secuencias de largo 2 son elementos de  $\mathcal{A} \times \mathcal{A}$ , y así sucesivamente. O sea, las secuencias se representan mediante:

$$\mathcal{E} + \mathcal{A} + \mathcal{A} \times \mathcal{A} + \mathcal{A} \times \mathcal{A} \times \mathcal{A} + \dots$$

Por la segunda parte y la serie geométrica (14.13), la función generatriz correspondiente es:

$$1 + A(z) + A^2(z) + A^3(z) + \dots = \frac{1}{1 - A(z)}$$

4. La clase de los subconjuntos finitos de  $\mathcal{A}$  queda representada por el producto simbólico:

$$\prod_{\alpha \in \mathcal{A}} (\mathcal{E} + \{\alpha\})$$

ya que al distribuir los productos de todas las formas posibles aparecen todos los subconjuntos de  $\mathcal{A}$ . Directamente obtenemos entonces:

$$\prod_{\alpha \in \mathcal{A}} (1 + z^{|\alpha|}) = \prod_{n \geq 0} (1 + z^n)^{a_n}$$

Otra forma de verlo es que cada elemento de tamaño  $n$  aporta un factor  $1 + z^n$ , si hay  $a_n$  de estos el aporte total es  $(1 + z^n)^{a_n}$ . Esta es la primera parte de lo aseverado. Aplicando logaritmo:

$$\begin{aligned} \sum_{\alpha \in \mathcal{A}} \ln(1 + z^{|\alpha|}) &= - \sum_{\alpha \in \mathcal{A}} \sum_{k \geq 1} \frac{(-1)^k z^{|\alpha|k}}{k} \\ &= - \sum_{k \geq 1} \frac{(-1)^k}{k} \sum_{\alpha \in \mathcal{A}} z^{|\alpha|k} \\ &= \sum_{k \geq 1} \frac{(-1)^{k+1} A(z^k)}{k} \end{aligned}$$

Exponenciando lo último resulta equivalente a la segunda parte.

5. Para cada objeto  $\alpha \in \mathcal{A}$  esto se traduce en una secuencia de  $|\alpha|$  elementos de  $\mathcal{B}$  a ser reemplazados por los átomos de  $\alpha$ , con lo que la función generatriz respectiva es:

$$\sum_{\alpha \in \mathcal{A}} B(z)^{|\alpha|}$$

que es lo prometido.

6. Podemos considerar un multiconjunto finito como la combinación de una secuencia para cada tipo de elemento:

$$\prod_{\alpha \in \mathcal{A}} \text{SEQ}(\{\alpha\})$$

La función generatriz buscada es:

$$\prod_{\alpha \in \mathcal{A}} \frac{1}{1 - z^{|\alpha|}} = \prod_{n \geq 0} \frac{1}{(1 - z^n)^{a_n}}$$

Esto provee la primera parte. Nuevamente aplicamos logaritmo para simplificar:

$$\begin{aligned} \ln \prod_{\alpha \in \mathcal{A}} \frac{1}{1 - z^{|\alpha|}} &= - \sum_{\alpha \in \mathcal{A}} \ln(1 - z^{|\alpha|}) \\ &= \sum_{\alpha \in \mathcal{A}} \sum_{k \geq 1} \frac{z^{k|\alpha|}}{k} \\ &= \sum_{k \geq 1} \frac{1}{k} \sum_{\alpha \in \mathcal{A}} z^{k|\alpha|} \\ &= \sum_{k \geq 1} \frac{A(z^k)}{k} \end{aligned}$$

7. Esta situación es más compleja de tratar, la discutiremos en la sección 21.2.3 más abajo.  $\square$

La utilidad del teorema 21.1 es que de cómo construir la clase de objetos que nos interesa da directamente una ecuación satisfecha por la función generatriz. Claro que igual resta extraer los coeficientes, tarea en la cual la fórmula de inversión de Lagrange (teorema 17.8) es invaluable.

### 21.2.1. Algunas aplicaciones

La clase de los árboles binarios  $\mathcal{B}$  es por definición es la unión disjunta del árbol vacío y la clase de tuplas de un nodo (la raíz) y dos árboles binarios. O sea:

$$\mathcal{B} = \mathcal{E} + \mathcal{Z} \times \mathcal{B} \times \mathcal{B}$$

de donde directamente igual que antes obtenemos:

$$B(z) = 1 + zB^2(z)$$

Con el cambio de variable  $u(z) = B(z) - 1$  queda:

$$u(z) = z(1 + u(z))^2$$

Es aplicable la fórmula de inversión de Lagrange, teorema 17.8, con  $\phi(u) = (u + 1)^2$  y  $f(u) = u$ :

$$\begin{aligned} [z^n] u(z) &= \frac{1}{n} [u^{n-1}] \phi(u)^n \\ &= \frac{1}{n} [u^{n-1}] (u + 1)^{2n} \\ &= \frac{1}{n} [u^{n-1}] \sum_{k \geq 0} \binom{2n}{k} u^k \\ &= \frac{1}{n} \binom{2n}{n-1} \end{aligned}$$

Tenemos, como  $u(z) = B(z) - 1$  y sabemos que  $b_0 = 1$ :

$$b_n = \begin{cases} \frac{1}{n} \binom{2n}{n-1} = \frac{1}{n+1} \binom{2n}{n} & \text{si } n \geq 1 \\ 1 & \text{si } n = 0 \end{cases}$$

Casualmente la expresión simplificada para  $n \geq 1$  da el valor correcto  $b_0 = 1$ . A estos números ya los habíamos mencionado en (14.62), son los números de Catalan. Es  $b_n = C_n$ .

Sea ahora  $\mathcal{A}$  la clase de *árboles con raíz ordenados*, formados por un nodo raíz conectado a las raíces de una secuencia de árboles ordenados. La idea es que la raíz tiene hijos en un cierto orden. Simbólicamente:

$$\mathcal{A} = \mathcal{Z} \times \text{SEQ}(\mathcal{A})$$

El método simbólico entrega directamente la ecuación:

$$A(z) = \frac{z}{1 - A(z)}$$

Nuevamente es aplicable la fórmula de inversión de Lagrange, con  $\phi(A) = (1 - A)^{-1}$  y  $f(A) = A$ :

$$\begin{aligned} [z^n] A(z) &= \frac{1}{n} [A^{n-1}] \phi(A)^n \\ &= \frac{1}{n} [A^{n-1}] (1 - A)^{-n} \\ &= \frac{1}{n} \binom{2n-2}{n-1} \\ &= C_{n-1} \end{aligned}$$

Otra vez números de Catalan. Un combinatorista de verdad considerará esto como el desafío de encontrar una biyección entre árboles binarios y árboles ordenados, nosotros nos contentaremos con consignar el resultado.

La manera obvia de representar  $\mathbb{N}_0$  es mediante secuencias de marcas, como  $|||$  para 4; simbólicamente  $\mathbb{N}_0 = \text{SEQ}(\mathcal{Z})$ . Para calcular el número de multiconjuntos de  $k$  elementos tomados entre  $n$ , un multiconjunto queda representado por las cuentas de los  $n$  elementos de que se compone, y eso corresponde a:

$$\mathbb{N}_0 \times \cdots \times \mathbb{N}_0 = (\text{SEQ}(\mathcal{Z}))^n$$

Para obtener el número que nos interesa:

$$\binom{n}{k} = [z^k] (1 - z)^{-n} = (-1)^n \binom{-n}{k} = \binom{n+k-1}{n}$$

Este resultado ya lo dedujimos en el capítulo 13.

Consideremos *árboles 2-3*, constando de un único nodo, o de un nodo conectado a 2 o 3 árboles 2-3. Estos son de interés como estructuras de datos, dado que es fácil mantenerlos balanceados, de forma que todas las hojas estén a la misma distancia de la raíz. Vemos que de un árbol 2-3 balanceado obtenemos uno mayor reemplazando simultáneamente todas las hojas por dos o tres nodos. Si consideramos el tamaño del árbol 2-3 como el número de sus hojas, descritas por la clase  $\mathcal{D}$ , esto lleva a la ecuación simbólica:

$$\mathcal{D} = \mathcal{Z} + \mathcal{D} \circ (\mathcal{Z}^2 + \mathcal{Z}^3)$$

que nos da la ecuación funcional:

$$D(z) = z + D(z^2 + z^3) \quad (21.1)$$

Es claro que substituir  $s$  veces partiendo de la estimación inicial  $D(z) = z$  nos entrega hasta el coeficiente de  $z^{2^s}$ . Resulta:

$$D(z) = z + z^2 + z^3 + z^4 + 2z^5 + 2z^6 + 3z^7 + 4z^8 + 5z^9 + 8z^{10} + 14z^{11} + 23z^{12} + 32z^{13} + 43z^{14} + \dots$$

El comportamiento de los coeficientes de soluciones de ecuaciones como (21.1) es bastante extraño, Odlyzko [270] demuestra que oscilan y da rangos.

Los *árboles con raíz* constan de un nodo raíz conectado a una colección de árboles con raíz. La clase  $\mathcal{R}$  correspondiente cumple:

$$\mathcal{R} = \mathcal{Z} \times \text{MSET}(\mathcal{R})$$

Para la función generatriz queda:

$$R(z) = z \exp\left(\sum_{k \geq 1} \frac{R(z^k)}{k}\right) \quad (21.2)$$

Ciertamente es una ecuación harto fea, pero puede usarse para obtener sucesivamente los  $r_n$ .

Una manera general de atacar ecuaciones como (21.2) es ver que da  $R$  en términos de  $R$ , y comenzar con alguna aproximación para ir refinándola. De partida, vemos que  $r_0 = 0$ , con lo que tenemos una aproximación inicial  $R^{(0)}(z) = 0$ . Substituyendo en (21.2) obtenemos  $R^{(1)}(z) = z$ . Como al substituir  $R^{(1)}(z)$  en (21.2) ya no aparecerán nuevos términos en  $z$ , sabemos que  $r_1 = 1$ . De la misma forma, cuando substituyamos  $R^{(n)}(z)$  en (21.2) ya no aparecerán nuevas contribuciones al coeficiente de  $z^n$ , y este proceso converge según definimos en el capítulo 17. No tiene sentido retener más términos al calcular  $R^{(n)}(z)$ , los demás no influyen sobre el coeficiente de  $z^n$ . Armado con un paquete de álgebra simbólica o mucha paciencia se pueden calcular términos adicionales:

$$R(z) = z + z^2 + 2z^3 + 4z^4 + 9z^5 + 20z^6 + 48z^7 + 115z^8 + \dots \quad (21.3)$$

Se pueden extraer estimaciones asintóticas de (21.2), ver por ejemplo a Flajolet y Sedgewick [126] o a Knuth [219], pero las técnicas a emplear escapan con mucho a nuestro ámbito. Ya Pólya [291] encontró:

$$r_n \sim 0,4399 \cdot 2,9558^n \cdot n^{-3/2}$$

Una *combinación* de  $n$  es expresarlo como una suma. Por ejemplo, hay 8 combinaciones de 4:

$$4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 3 = 1 + 2 + 1 = 1 + 1 + 2 = 1 + 1 + 1 + 1$$

Llameemos  $c(n)$  al número de combinaciones de  $n$ .

A la clase de los naturales podemos representarla como de secuencias de marcas. Por ejemplo, 5 es  $|||||$ . Son secuencias no vacías, el primer natural es 1. Así:

$$\mathbb{N} = \mathcal{Z} \times \text{SEQ}(\mathcal{Z})$$

Otra forma de representar al natural  $n$  es mediante una bolsa de  $n$  piedritas, que sugiere:

$$\mathbb{N} = \mathcal{Z} \times \text{MSET}(\mathcal{Z})$$

Las reglas de transferencia del teorema 21.1 en este caso particular dan la misma función generatriz para ambas:

$$N(z) = \frac{z}{1-z}$$

A su vez, una combinación no es más que una secuencia de naturales:

$$\mathcal{C} = \text{SEQ}(\mathbb{N})$$

Directamente resulta:

$$\begin{aligned} C(z) &= \sum_{n \geq 0} c(n)z^n \\ &= \frac{1}{1 - N(z)} \\ &= \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{1-2z} \\ c(n) &= \frac{1}{2} [n=0] + \frac{1}{2} \cdot 2^n \\ &= \frac{1}{2} [n=0] + 2^{n-1} \end{aligned}$$

Esto es consistente con  $c(4) = 8$  obtenido arriba.

### 21.2.2. Palabras que no contienen un patrón dado

Nos interesan secuencias que no contengan un patrón dado. Un ejemplo simple es secuencias binarias sin ceros seguidos. Llamemos  $\mathcal{B}_{00}$  a esta clase. Un elemento de  $\mathcal{B}_{00}$  puede ser vacío o 0, o es 1 o 01 seguido por un elemento de  $\mathcal{B}_{00}$ . O sea:

$$\mathcal{B}_{00} = \mathcal{E} + \{0\} + \{1, 01\} \times \mathcal{B}_{00}$$

Si  $z$  marca cada símbolo, para la respectiva función generatriz ordinaria  $B_{00}(z)$ :

$$B_{00}(z) = 1 + z + (z + z^2)B_{00}(z)$$

Despejando:

$$B_{00}(z) = \frac{1+z}{1-z-z^2}$$

Resulta ser  $[z^n] B_{00}(z) = F_n + F_{n+1} = F_{n+2}$ , un número de Fibonacci.

Si ahora buscamos que no contenga  $k$  ceros seguidos, podemos expresar:

$$\mathcal{B}_{0^k} = \mathcal{P}_{<k} + \mathcal{P}_{<k} \times \{1\} \times \mathcal{B}_{0^k}$$

Acá  $\mathcal{P}_{<k}$  es la clase de secuencias de menos de  $k$  ceros:

$$\mathcal{P}_{<k} = \mathcal{E} + \{0\} + \{0\}^2 + \cdots + \{0\}^{k-1}$$

Las respectivas funciones generatrices ordinarias cumplen:

$$\begin{aligned} P_{<k}(z) &= 1 + z + z^2 + \cdots + z^{k-1} \\ &= \frac{1-z^k}{1-z} \\ B_{0^k}(z) &= \frac{1-z^k}{1-z} (1 + z B_{0^k}(z)) \end{aligned}$$

Despejando:

$$B_{0^k}(z) = \frac{1 - z^k}{1 - 2z + z^{k+1}} \quad (21.4)$$

Podemos extraer información adicional de acá. Los coeficientes de  $B_{0^k}(z)$  son el número de strings que no contienen  $0^k$ , el coeficiente de  $z^n$  dividido por  $2^n$  es la proporción del total:

$$\begin{aligned} B_{0^k}(z) &= \sum_{n \geq 0} \{\# \text{ de largo } n \text{ sin } 0^k\} z^n \\ B_{0^k}(z/2) &= \sum_{n \geq 0} \{\# \text{ de largo } n \text{ sin } 0^k\} / 2^n z^n \\ B_{0^k}(1/2) &= \sum_{n \geq 0} \{\# \text{ de largo } n \text{ sin } 0^k\} / 2^n \\ &= \sum_{n \geq 0} \Pr(\text{No hay } 0^k \text{ en los primeros } n) \\ &= \sum_{n \geq 0} \Pr(\text{Primer } 0^k \text{ termina después de } > n) \\ &= \text{Posición esperada del fin de los primeros } k \text{ ceros} \end{aligned}$$

A esto se le llama *tiempo de espera* (en inglés, *waiting time*). Resulta:

**Teorema 21.2.** *El tiempo de espera para los primeros  $k$  ceros en un string binario al azar es:*

$$B_{0^k}(1/2) = 2^{k+1} - 2 \quad (21.5)$$

O sea, en promedio hay que esperar 30 bits hasta hallar 0000. La pregunta obvia es si esto vale también para otros patrones de largo cuatro, por ejemplo 0001. Resulta que no es así. Consideremos la primera vez que aparece 000. Es igualmente probable que continúe 0000 o 0001. Si 0000 no calza es 0001, y para 0000 debemos esperar al menos 4 bits más. Si 0001 no calza, es porque es 0000 y el próximo bit puede completar 0001.

Consideremos un patrón  $p$  de largo  $k$  arbitrario tomados entre  $s$  símbolos entonces. Sea  $\mathcal{B}_p$  la clase de strings que no contienen  $p$ , y sea  $\mathcal{T}_p$  la clase de strings que terminan en  $p$ , pero en los cuales  $p$  no aparece nunca antes del final. Es claro que  $\mathcal{B}_p$  y  $\mathcal{T}_p$  son disjuntos. Si agregamos un símbolo a un string en  $\mathcal{B}_p$ , el resultado es un string no vacío en  $\mathcal{B}_p$  o en  $\mathcal{T}_p$ . O sea:

$$\mathcal{B}_p + \mathcal{T}_p = \mathcal{E} + \mathcal{B}_p \times \{0, 1, \dots, s - 1\}$$

Esto nos da la ecuación funcional para las respectivas funciones generatrices ordinarias:

$$B_p(z) + T_p(z) = 1 + szB_p(z) \quad (21.6)$$

Hace falta determinar  $T_p$ . Es similar a  $\mathcal{B}_p \times \{p\}$ , pero debemos considerar que un elemento de  $\mathcal{B}_p$  puede terminar en “casi”  $p$ , con lo que solo le falta una cola.

El desarrollo que sigue es básicamente de Odlyzko [271]. Escribiremos  $|x|$  para el largo del string  $x$  (el número de símbolos que lo componen). Para describir la manera en que dos strings se traslanan definimos la *correlación* entre los string  $x$  e  $y$  (posiblemente de distinto largo) como el polinomio  $c_{xy}(t)$  de grado  $|x| - 1$  tal que el coeficiente de  $t^k$  se determina ubicando  $y$  bajo  $x$  de manera que el primer carácter de  $y$  cae bajo el  $k$ -ésimo carácter de  $x$ . El coeficiente es 1 si ambos son iguales donde traslanan, 0 en caso contrario. Por ejemplo, si  $x = \text{cabcbcabc}$  e  $y = \text{abcabcde}$ , resulta  $c_{xy}(t) = t^4 + t$ , como muestra el cuadro 21.1. Nótese que en general  $c_{xy}(t) \neq c_{yx}(t)$  (en el ejemplo es  $c_{yx}(t) = 0$ ). De particular interés es la *autocorrelación*  $c_x(t) = c_{xx}(t)$ , la correlación de un string consigo mismo. En el ejemplo,  $c_x(t) = t^6 + t^3 + 1$ .

Cuadro 21.1 – Cálculo de  $c_{xy}(t) = t^4 + t$

Fijemos un patrón  $p$  de largo  $k$ , y escribamos:

$$B_p(z) = \sum_{n \geq 0} b_n z^n$$

$$T_p(z) = \sum_{n \geq 0} t_n z^n$$

Consideremos uno de los  $b_n$  strings de largo  $n$  que no terminan en  $p$ , y adosemos  $p$  al final. Sea  $n+r$  la posición en la cual por primera vez termina  $p$  en el resultado, donde  $0 < r \leq k$ . Como  $p$  también aparece al final, deben coincidir el prefijo de largo  $k-r$  de  $p$  y el sufijo de largo  $k-r$  de  $p$ , o sea,  $[t^{k-r}] c_p(t) = 1$ .

Para un ejemplo, sea el patrón  $p = \text{aaba}$  y el string  $x = \text{ababbaab} \in \mathcal{B}_p$ . Es  $k = |p| = 4$  y  $n = |x| = 8$ . Vemos que  $xp = \text{ababba}\color{red}{\text{aaba}}\color{blue}{\text{aba}}$ , o sea,  $r = 1$  (hay un traslapo de  $k - r = 4 - 1 = 3$  entre el principio del patrón y el final del string). Tenemos un miembro de  $\mathcal{T}_p$  de largo  $n + r = 9$  y una cola de largo  $k - r = 3$ , determinados en forma única por  $x$  y  $p$ . Esta descomposición solo es posible cuando  $[t^{k-r}] c_p(t) = 1$ .

Nos interesa contar estos string. Hay  $t_{n+r}$  de ellos, la descomposición descrita es una biyección. Vale decir, como los coeficientes de  $c_p$  son cero o uno:

$$b_n = \sum_{0 \leq r \leq k} t_{n+r} \left[ t^{k-r} \right] c_p(t) \quad (21.7)$$

Multiplicando (21.7) por  $z^{n+k}$  y sumando para  $n \geq 0$  (recordar que  $k = |p| \geq \deg(c_p(t)) + 1$ ) da:

$$B_p(z)z^k = \sum_{n \geq 0} z^{n+k} \sum_{0 \leq r \leq k} t_{n+r} \left[ t^{k-r} \right] c_p(t)$$

Esta es la convolución de  $T_p(z)$  con  $c_p(z)$ :

$$B_p(z)z^k = T_p(z)c_p(z) \quad (21.8)$$

Uniendo las piezas anteriores tenemos un resultado de Solov'ev [328]:

**Teorema 21.3.** Sea  $p$  un patrón de largo  $k$  formado por  $s$  símbolos, con autocorrelación  $c_p(z)$ . Entonces el número de strings de largo  $n$  que no contienen el patrón  $p$  tiene función generatriz ordinaria:

$$B_p(z) = \frac{c_p(z)}{(1-sz)c_p(z) + z^k} \quad (21.9)$$

*El tiempo de espera para el patrón  $p$  está dado por:*

$$W_p = s^k c_p(1/s) \quad (21.10)$$

*Demostración.* La ecuación (21.9) es la solución del sistema de ecuaciones (21.6) y (21.8). El tiempo de espera es como se discutió antes para el patrón  $0^k$ , la expresión dada resulta de substituir  $z = 1/s$  en (21.9).  $\square$

Incidentalmente, al ser  $c_p$  un polinomio de coeficientes enteros de grado menor a  $k$ , por (21.10) el tiempo de espera siempre es un entero.

Completando la discusión previa, tenemos  $c_{0000}(z) = 1 + z + z^2 + z^3$  y  $c_{0001}(z) = 1$ . El tiempo de espera para el patrón  $p$  está dado por  $2^4 c_p(1/2)$ . Para nuestros dos patrones, por las fórmulas desarrolladas antes:

$$B_{0000}(z) = \frac{1 - z^4}{1 - 2z + z^5} \quad (21.11)$$

$$W_{0000} = 30 \quad (21.12)$$

$$B_{0001}(z) = \frac{1}{1 - 2z + z^4} \quad (21.13)$$

$$W_{0001} = 16 \quad (21.14)$$

Por técnicas similares se pueden manejar conjuntos de patrones.

### 21.2.3. Construcción ciclo

El tratamiento de  $\text{Cyc}(\mathcal{A})$  en el teorema 21.1 requiere considerar simetrías en la secuencia subyacente. Por ejemplo, el ciclo  $(abcd)$  resulta de las cuatro secuencias  $abcd$ ,  $bcda$ ,  $cdab$  y  $dabc$ ; pero el ciclo  $(abab)$  resulta solo de las dos  $abab$  y  $baba$ . Por ahora hablaremos de secuencias y ciclos de símbolos, para luego aplicar lo aprendido a clases y sus funciones generatrices. Usaremos conceptos de funciones aritméticas y el anillo de Dirichlet en lo sucesivo, véase la sección 8.2.

Nuestro desarrollo sigue a Flajolet y Soria [127]. Llamemos *secuencia primitiva* a una secuencia que no es la repetición de una secuencia más corta. O sea,  $abaab$  es primitiva,  $abab = (ab)^2$  no lo es. La secuencia más corta tal que la secuencia dada se puede escribir como una repetición de ella la llamamos la *raíz* de la secuencia. En el ejemplo, la raíz de  $abaab$  es  $abaab$ , ya que es primitiva; la raíz de  $abab$  es  $ab$ . Sea  $s$  el número de símbolos en el alfabeto sobre el cual se consideran las secuencias. Si llamamos  $p_n$  al número de secuencias primitivas de largo  $n$ , como toda secuencia es la repetición de una secuencia primitiva, debe ser:

$$s^n = \sum_{d|n} p_d$$

El lado izquierdo es el número total de secuencias de largo  $n$ , el lado derecho cuenta este mismo número como secuencias primitivas de largo  $d$  que se repiten para dar el largo  $n$ . Inversión de Möbius, teorema 8.19, entrega:

$$p_n = \sum_{d|n} \mu(d) s^{n/d}$$

Necesitamos extender este resultado a las funciones generatrices respectivas.

**Lema 21.4** (Inversión de Möbius). *Sean secuencias  $\langle u_n \rangle_{n \geq 0}$  y  $\langle v_n \rangle_{n \geq 0}$  tales que para  $n \geq 1$ :*

$$u_n = \sum_{d|n} v_d$$

*Entonces las funciones generatrices ordinarias respectivas  $U(z)$  y  $V(z)$  cumplen:*

$$U(z) = \sum_{n \geq 1} V(z^n)$$

$$V(z) = \sum_{n \geq 1} \mu(n) U(z^n)$$

*Demostración.* Primero, usando la convención de Iverson:

$$\begin{aligned}
 U(z) &= \sum_{n \geq 1} u_n z^n \\
 &= \sum_{n \geq 1} \sum_{a \geq 1} \sum_{b \geq 1} [ab = n] v_a z^a z^{nb} \\
 &= \sum_{a \geq 1} \sum_{b \geq 1} v_a z^a z^{nb} \\
 &= \sum_{b \geq 1} \sum_{a \geq 1} v_a (z^b)^a \\
 &= \sum_{b \geq 1} V(z^b)
 \end{aligned}$$

De la misma forma:

$$\begin{aligned}
 V(z) &= \sum_{n \geq 1} \sum_{a \geq 1} \sum_{b \geq 1} [ab = n] \mu(a) u_b z^n \\
 &= \sum_{a \geq 1} \mu(a) \sum_{b \geq 1} u_b z^{ab} \\
 &= \sum_{a \geq 1} \mu(a) U(z^a)
 \end{aligned}$$

□

Queda claro que si  $\alpha(n)$  tiene inversa de Dirichlet  $\alpha^{-1}(n)$  y:

$$\begin{aligned}
 u_n &= \sum_{d|n} \alpha(n/d) v_d \\
 v_n &= \sum_{d|n} \alpha^{-1}(n/d) u_d
 \end{aligned}$$

entonces:

$$U(z) = \sum_{n \geq 1} \alpha(n) V(z^n) \quad (21.15)$$

$$V(z) = \sum_{n \geq 1} \alpha^{-1}(n) U(z^n) \quad (21.16)$$

Igual que en el caso de secuencias podemos hablar de *ciclos primativos* y sus *raíces*, nos interesa la relación entre secuencias y ciclos. La figura 21.1 muestra algunos ciclos de largo seis con sus raíces.

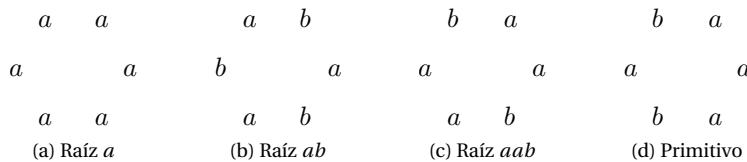


Figura 21.1 – Ciclos de largo seis

Sea  $\omega$  una secuencia primitiva de largo  $l$ , y consideremos el ciclo formado por  $r$  copias de  $\omega, \omega^r$ . Si lo rotamos en un múltiplo de  $l$  posiciones obtenemos el original. Si lo rotamos en menos de  $l$  posiciones, el efecto es dividir  $\omega = \alpha\beta$  y trasladar  $\alpha$  al final, queda  $\beta(\alpha\beta)^{r-1}\alpha = (\beta\alpha)^r$ , nuevamente un ciclo con raíz de largo  $l$ . Esto ocurre al rotar en cualquier número de posiciones que no es un múltiplo de  $l$ . Si la secuencia es primitiva, todas las rotaciones de la misma también lo son. Vale

decir, hay un mapa 1 a  $l$  de secuencias primitivas de largo  $l$  a ciclos primitivos de largo  $l$ . A su vez, todo ciclo es la repetición de un ciclo primitivo (su raíz).

Traduzcamos lo anterior a funciones generatrices ahora. Consideraremos primeramente secuencias de al menos un  $\mathcal{A}$ . Si además del tamaño total nos interesa el número de  $\mathcal{A}$  componentes, usando una clase auxiliar  $\mathcal{U}$  con un único elemento de tamaño uno podemos representar la clase  $\mathcal{S}$  que nos interesa como:

$$\mathcal{S} = \text{SEQ}_{\geq 1}(\mathcal{U} \times \mathcal{A})$$

De esto, usando  $u$  para contar el número de  $\mathcal{U}$  participantes (vale decir, el número de  $\mathcal{A}$  que componen nuestra secuencia) el método simbólico da:

$$S(z, u) = \frac{uA(z)}{1 - uA(z)}$$

La función generatriz  $S_p(z, u)$  del número de secuencias primitivas formadas por  $\mathcal{A}$  queda determinado por la ecuación implícita:

$$S(z, u) = \sum_{n \geq 1} S_p(z^n, u^n)$$

de donde por el lema 21.4:

$$S_p(z, u) = \sum_{n \geq 1} \mu(n) \frac{u^n A(z^n)}{1 - u^n A(z^n)} \quad (21.17)$$

Pero nos interesa la función generatriz de los ciclos primitivos,  $C_p(z, u)$ . Por lo discutido antes, esto se obtiene de  $S_p(z, u)$  haciendo el reemplazo  $u^l \rightarrow u^l/l$ , y esto a su vez integrando término a término se obtiene como:

$$\begin{aligned} C_p(z, u) &= \int_0^u S_p(z, v) \frac{dv}{v} \\ &= \sum_{n \geq 1} \frac{\mu(n)}{n} \ln \frac{1}{1 - u^n A(z^n)} \end{aligned} \quad (21.18)$$

Construimos ciclos completos repitiendo ciclos primitivos, lo que corresponde a la inversa de Dirichlet de (21.18):

$$C(z, u) = \sum_{n \geq 1} \frac{\phi(n)}{n} \ln \frac{1}{1 - u^n A(z^n)} \quad (21.19)$$

Substituyendo  $u = 1$  obtenemos la ecuación prometida.

Resta demostrar que en el anillo de Dirichlet:

$$\left( \frac{\mu(n)}{n} \right)^{-1} = \frac{\phi(n)}{n}$$

La identidad de Gauß (teorema 8.23) dice:

$$n = \sum_{d|n} \phi(d)$$

Por inversión de Möbius:

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$$

que es equivalente a lo que buscábamos demostrar.

#### 21.2.4. Polinomios irreductibles en $\mathbb{F}_q$

Recordamos del capítulo 10 que los polinomios  $\mathbb{F}_q[x]$  para  $q$  la potencia de un primo son un dominio euclíadiano, por lo que por la teoría de la sección 9.2, en particular el teorema 9.10, nos asegura que hay factorización única (salvo unidades) en  $\mathbb{F}_q[x]$ . Para obviar las unidades, consideremos polinomios mónicos.

Si para el polinomio  $\alpha(x) \in \mathbb{F}_q[x]$  consideramos su grado como tamaño, vemos que multiplicar polinomios es simplemente sumar sus tamaños. Podemos entonces considerar la clase  $\mathcal{P}$  de polinomios mónicos en  $\mathbb{F}_q[x]$  con  $|\alpha(x)| = \deg(\alpha)$ , y combinar polinomios corresponde a multiplicarlos. Es claro que hay  $q^n$  polinomios mónicos de grado  $n$ , o sea la función generatriz ordinaria que cuenta polinomios mónicos es:

$$P(z) = \sum_{n \geq 0} q^n z^n = \frac{1}{1 - qz}$$

Consideremos la clase  $\mathcal{I}$  de polinomios mónicos irreductibles, contados por la función generatriz ordinaria:

$$I(z) = \sum_{n \geq 0} N_n z^n$$

Factorización única significa que todo polinomio corresponde a un multiconjunto de polinomios irreductibles:

$$\mathcal{P} = \text{MSET}(\mathcal{I}) \quad (21.20)$$

Resulta interesante contar con una forma de resolver ecuaciones implícitas como (21.20).

**Teorema 21.5.** Sean  $\mathcal{A}$  y  $\mathcal{B}$  clases de objetos no rotulados relacionadas mediante:

$$\mathcal{A} = \text{MSET}(\mathcal{B})$$

Entonces las funciones generatrices ordinarias respectivas cumplen:

$$B(z) = \sum_{k \geq 1} \frac{\mu(k)}{k} \ln A(z^k) \quad (21.21)$$

*Demostración.* El método simbólico da:

$$A(z) = \exp \left( \sum_{k \geq 1} \frac{B(z^k)}{k} \right)$$

Tomando logaritmos:

$$\begin{aligned} \ln A(z) &= \sum_{r \geq 1} \frac{B(z^r)}{r} \\ &= \sum_{r \geq 1} \frac{1}{r} \sum_{s \geq 1} b_s z^{rs} \end{aligned}$$

Extraemos coeficientes:

$$\begin{aligned} n[z^n] \ln A(z) &= \sum_{r \geq 1} \frac{n}{r} \sum_{s \geq 1} b_s z^{rs} \\ &= \sum_{rs=n} sb_s \end{aligned}$$

Este es exactamente el caso del lema 21.4, lo que entrega lo enunciado.  $\square$

Con el teorema 21.5 queda de (21.20):

$$I(z) = \sum_{k \geq 1} \frac{\mu(k)}{k} \frac{1}{1 - qz^k}$$

Tenemos nuevamente el resultado del teorema 10.22:

$$N_n = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d$$

### 21.3. Objetos rotulados

En la discusión previa solo interesaba el tamaño de los objetos, no su disposición particular. Consideraremos ahora objetos rotulados, donde importa cómo se compone el objeto de sus partes (los átomos están numerados, o se ubican en orden).

El objeto más simple con partes rotuladas son las permutaciones (biyecciones  $\sigma: [n] \rightarrow [n]$ , podemos considerarlas secuencias de átomos numerados). Para la función generatriz exponencial tenemos, ya que hay  $n!$  permutaciones de  $n$  elementos:

$$\sum_{\sigma} \frac{z^{|\sigma|}}{|\sigma|!} = \sum_{n \geq 0} n! \frac{z^n}{n!} = \frac{1}{1-z}$$

Lo siguiente más simple de considerar es colecciones de ciclos rotulados. Por ejemplo, escribimos  $(1\ 3\ 2)$  para el objeto en que viene 3 luego de 1, 2 sigue a 3, y a su vez 1 sigue a 2. Así  $(2\ 1\ 3)$  es solo otra forma de anotar el ciclo anterior, que no es lo mismo que  $(3\ 1\ 2)$ . Interesa definir formas consistentes de combinar objetos rotulados. Por ejemplo, al combinar el ciclo  $(1\ 2)$  con el ciclo  $(1\ 3\ 2)$  resultará un objeto con 5 rótulos, y debemos ver cómo los distribuimos entre las partes. El cuadro 21.2 reseña las posibilidades al respetar el orden de los elementos asignados a cada parte. Es

$$\begin{array}{cccc} (1\ 2)(3\ 5\ 4) & (2\ 3)(1\ 5\ 4) & (3\ 4)(1\ 5\ 2) & (4\ 5)(1\ 3\ 2) \\ (1\ 3)(2\ 5\ 4) & (2\ 4)(1\ 3\ 5) & (3\ 5)(1\ 4\ 2) & \\ (1\ 4)(2\ 5\ 3) & (2\ 5)(1\ 3\ 4) & & \\ (1\ 5)(2\ 4\ 3) & & & \end{array}$$

Cuadro 21.2 – Combinando los ciclos  $(1\ 2)$  y  $(1\ 3\ 2)$

claro que lo que estamos haciendo es elegir un subconjunto de 2 rótulos de entre los 5 para asignárselos al primer ciclo. El combinar dos clases de objetos  $\mathcal{A}$  y  $\mathcal{B}$  de esta forma lo anotaremos  $\mathcal{A} \star \mathcal{B}$ . Otra operación común es la *composición*, anotada  $\mathcal{A} \circ \mathcal{B}$ . La idea es elegir un elemento  $\alpha \in \mathcal{A}$ , luego elegir  $|\alpha|$  elementos de  $\mathcal{B}$ , y reemplazar los  $\mathcal{B}$  por las partes de  $\alpha$ , en el orden que están rotuladas; para finalmente asignar rótulos a los átomos que conforman la estructura completa respetando el orden de los rótulos al interior de los  $\mathcal{B}$ . Ocasionalmente es útil *marcar* uno de los componentes del objeto, operación que anotaremos  $\mathcal{A}^\bullet$ . Otra notación común para esta operación es  $\Theta\mathcal{A}$ . Usaremos también la construcción  $MSET(\mathcal{A})$ , que podemos considerar como una secuencia de elementos numerados obviando el orden. Cuidado, muchos textos le llaman  $SET()$  a esta operación.

Tenemos el siguiente teorema:

**Teorema 21.6** (Método simbólico, EGF). *Sean  $\mathcal{A}$  y  $\mathcal{B}$  clases de objetos, con funciones generatrices exponenciales  $\hat{A}(z)$  y  $\hat{B}(z)$ , respectivamente. Entonces tenemos las siguientes funciones generatrices exponenciales:*

1. Para enumerar  $\mathcal{A}^*$ :

$$zD\widehat{A}(z)$$

2. Para enumerar  $\mathcal{A} + \mathcal{B}$ :

$$\widehat{A}(z) + \widehat{B}(z)$$

3. Para enumerar  $\mathcal{A} \star \mathcal{B}$ :

$$\widehat{A}(z) \cdot \widehat{B}(z)$$

4. Para enumerar  $\mathcal{A}^*$ :

$$z\widehat{A}'(z)$$

5. Para enumerar  $\mathcal{A} \circ \mathcal{B}$ :

$$\widehat{A}(\widehat{B}(z))$$

6. Para enumerar  $\text{SEQ}(\mathcal{A})$ :

$$\frac{1}{1 - \widehat{A}(z)}$$

7. Para enumerar  $\text{MSET}(\mathcal{A})$ :

$$e^{\widehat{A}(z)}$$

8. Para enumerar  $\text{CYC}(\mathcal{A})$ :

$$-\ln(1 - \widehat{A}(z))$$

*Demostración.* Usaremos casos ya demostrados en las demostraciones sucesivas.

1. El objeto  $\alpha \in \mathcal{A}$  da lugar a  $|\alpha|$  objetos al marcar cada uno de sus átomos, lo que da la función generatriz exponencial:

$$\sum_{\alpha \in \mathcal{A}} |\alpha| \frac{z^{|\alpha|}}{|\alpha|!}$$

Esto es lo indicado.

2. Nuevamente trivial.

3. El número de objetos  $\gamma$  que se obtienen al combinar  $\alpha \in \mathcal{A}$  con  $\beta \in \mathcal{B}$  es:

$$\binom{|\alpha| + |\beta|}{|\alpha|}$$

y tenemos la función generatriz exponencial:

$$\sum_{\gamma \in \mathcal{A} \star \mathcal{B}} \frac{z^{|\gamma|}}{|\gamma|!} = \sum_{\substack{\alpha \in \mathcal{A} \\ \beta \in \mathcal{B}}} \binom{|\alpha| + |\beta|}{|\alpha|} \frac{z^{|\alpha|+|\beta|}}{(|\alpha|+|\beta|)!} = \left( \sum_{\alpha \in \mathcal{A}} \frac{z^{|\alpha|}}{|\alpha|!} \right) \cdot \left( \sum_{\beta \in \mathcal{B}} \frac{z^{|\beta|}}{|\beta|!} \right) = \widehat{A}(z) \cdot \widehat{B}(z)$$

4. Si tomamos un objeto  $\alpha \in \mathcal{A}$  de tamaño  $|\alpha|$ , estamos creando  $|\alpha|$  nuevos objetos al marcar cada uno de sus componentes. La función generatriz resultante es:

$$\sum_{\alpha \in \mathcal{A}} |\alpha| \frac{z^{|\alpha|}}{|\alpha|!} = z \hat{A}'(z)$$

5. Tomemos  $\alpha \in \mathcal{A}$ , de tamaño  $n = |\alpha|$ , y  $n$  elementos de  $\mathcal{B}$  en orden a ser reemplazados por las partes de  $\alpha$ . Esa secuencia de  $\mathcal{B}$  es representada por:

$$\mathcal{B} \star \mathcal{B} \star \cdots \star \mathcal{B}$$

con función generatriz exponencial:

$$\hat{B}^n(z)$$

Sumando sobre las contribuciones:

$$\sum_{\alpha \in \mathcal{A}} \frac{\hat{B}^{|\alpha|}(z)}{|\alpha|!}$$

Esto es lo prometido.

6. Primeramente, para  $\text{SEQ}(\mathcal{Z})$ , como hay  $n!$  secuencias de largo  $n$ :

$$\sum_{n \geq 0} n! \frac{z^n}{n!} = \frac{1}{1-z}$$

Aplicando composición se obtiene lo indicado.

7. Hay un único multiconjunto de  $n$  elementos rotulados (se rotulan simplemente de 1 a  $n$ ), con lo que  $\text{MSET}(\mathcal{Z})$  corresponde a:

$$\sum_{n \geq 0} \frac{z^n}{n!} = \exp(z)$$

Al aplicar composición resulta lo anunciado.

Otra demostración es considerar el multiconjunto de  $\mathcal{A}$ , descrito por  $\mathcal{M} = \text{MSET}(\mathcal{A})$ . Si marcamos uno de los átomos de  $\mathcal{M}$  estamos marcando uno de los  $\mathcal{A}$ , el resto sigue formando un multiconjunto de  $\mathcal{A}$ :

$$\mathcal{M}^\bullet = \mathcal{A}^\bullet \star \mathcal{M}$$

Por lo anterior:

$$zM'(z) = zA'(z)M(z)$$

Hay un único multiconjunto de tamaño 0, o sea  $M(0) = 1$ ; y hemos impuesto la condición que no hay objetos de tamaño 0 en  $\mathcal{A}$ , vale decir,  $A(0) = 0$ . Así la solución a la ecuación diferencial es:

$$M(z) = \exp(A(z))$$

8. Consideraremos un ciclo de  $\mathcal{A}$ , o sea  $\mathcal{C} = \text{CYC}(\mathcal{A})$ . Si marcamos los  $\mathcal{C}$ , estamos marcando uno de los  $\mathcal{A}$ , y el resto es una secuencia:

$$\mathcal{C}^\bullet = \mathcal{A}^\bullet \star \text{SEQ}(\mathcal{A})$$

Esto se traduce en la ecuación diferencial:

$$z\hat{C}'(z) = zA'(z) \frac{1}{1-A(z)}$$

Integrando bajo el entendido  $C(0) = 0$  con  $A(0) = 0$  se obtiene lo indicado.  $\square$

### 21.3.1. Rotulado o no rotulado, esa es la cuestión...

Después de las exposiciones anteriores el amable lector estará comprensiblemente confundido respecto de cuándo considerar rotulados los objetos entre manos. Como regla general, se deben considerar no rotulados los objetos en los cuales piezas iguales son intercambiables. Al considerar un canasto de frutas, como en el primer ejemplo de la sección 14.6, consideramos que solo es relevante el número de las frutas de los distintos tipos. En los términos presentes, son multiconjuntos de objetos no rotulados, y la clase canasto (número par de manzanas, número de plátanos divisible por cinco, a lo más cuatro naranjas, opcionalmente una sandía) se representa simbólicamente como:

$$\mathcal{C} = \text{MSET}(\mathcal{Z} \times \mathcal{Z}) \times \text{MSET}(\mathcal{Z} \times \mathcal{Z} \times \mathcal{Z} \times \mathcal{Z} \times \mathcal{Z}) \times \text{MSET}_{\leq 4}(\mathcal{Z}) \times \text{MSET}_{\leq 1}(\mathcal{Z})$$

Aplicando las reglas de transferencia del teorema 21.1 resulta la función generatriz ordinaria:

$$\begin{aligned} C(z) &= \frac{1}{1-z^2} \cdot \frac{1}{1-z^5} \cdot (1+z+z^2+z^3+z^4) \cdot (1+z) \\ &= \frac{1}{(1-z)^2} \end{aligned}$$

y en consecuencia el número de canastos con  $n$  frutas es:

$$[z^n] C(z) = n + 1$$

como habíamos deducido antes.

Las permutaciones son secuencias de elementos distinguibles, por lo que se consideran objetos rotulados. La clase de permutaciones queda entonces representada por la expresión simbólica:

$$\mathcal{P} = \text{SEQ}(\mathcal{Z})$$

Las reglas del teorema 21.6 dan la función generatriz exponencial:

$$\hat{P}(z) = \frac{1}{1-z}$$

de donde el número de permutaciones de  $n$  elementos es:

$$n! [z^n] \hat{P}(z) = n!$$

como ya sabíamos.

Hay situaciones en las cuales los objetos en sí son indistinguibles, pero los consideramos rotulados por sus posiciones. Un ejemplo popular considera un buque que hace señales mediante 12 banderas de colores blanco, rojo, azul y negro. Se restringen las señales a tener un número par de banderas blancas e impar de rojas. Se pregunta cuántas señales diferentes puede dar, suponiendo que tiene banderas suficientes de cada color. Esto puede responderse por las técnicas de la sección 13.4, pero resulta engorroso. Si consideramos cada color de bandera como el multiconjunto de esa bandera rotuladas por su posición, la regla de distribución de rótulos de la operación  $\star$  exactamente corresponde a barajar las banderas de los distintos colores. Considerando entonces objetos rotulados, la clase de señales queda descrita simbólicamente por:

$$\mathcal{S} = \text{MSET}_{\text{even}}(\mathcal{Z}) \star \text{MSET}_{\text{odd}}(\mathcal{Z}) \star \text{MSET}(\mathcal{Z}) \star \text{MSET}(\mathcal{Z})$$

El teorema 21.6 da la función generatriz exponencial (el multiconjunto de número par de elementos da los términos pares de la serie para la exponencial, multiconjuntos con número impar de elementos da los términos impares; y esto a su vez da coseno y seno hiperbólicos):

$$\hat{S}(z) = \cosh z \sinh z e^{2z}$$

$$= \frac{e^{4z} - 1}{4}$$

y el número de señales que pueden formarse con 12 banderas es:

$$12! [z^{12}] \widehat{S}(z) = 12! \frac{1}{4} \frac{4^{12}}{12!} = 4^{11}$$

### 21.3.2. Algunas aplicaciones de objetos rotulados

Un primer ejemplo simple es determinar el número de organizaciones circulares de  $n$  elementos. Al ser diferentes, podemos considerarlos rotulados. Quedan representadas simbólicamente por  $\text{CYC}(\mathcal{Z})$ , con función generatriz exponencial:

$$\ln \frac{1}{1-z}$$

Como es una función generatriz exponencial, interesa:

$$n! [z^n] \ln \frac{1}{1-z} = n! [z^n] \sum_{n \geq 1} \frac{z^n}{n} = (n-1)!$$

Las permutaciones podemos representarlas como secuencias rotuladas,  $\text{SEQ}(\mathcal{Z})$ , con función generatriz exponencial:

$$\frac{1}{1-z}$$

La función generatriz exponencial para colecciones de ciclos  $\text{MSET}(\text{CYC}(\mathcal{Z}))$  es:

$$\exp(-\ln(1-z)) = \frac{1}{1-z}$$

Vale decir, hay tantas maneras de distribuir  $n$  elementos en ciclos como hay permutaciones de esos  $n$  elementos. Volveremos a esto en el capítulo 26.

Sea  $\mathcal{D}$  la clase de los desarreglos. Como las permutaciones son elementos que se mantienen fijos (podemos representarlos como su conjunto) y elementos que no están en sus posiciones (desarreglos), podemos expresar:

$$\text{SEQ}(\mathcal{Z}) = \mathcal{D} \star \text{SET}(\mathcal{Z})$$

O sea:

$$\frac{1}{1-z} = \widehat{D}(z) \cdot e^z$$

Como antes.

Podemos modificar los operadores, por ejemplo anotar  $\text{MSET}_{\geq 1}(\mathcal{A})$  para conjuntos de al menos un  $\mathcal{A}$ , con ajustes a sus expansiones sugeridas por la demostración del teorema del caso. Hay identidades evidentes, como  $\text{SEQ}_{\geq 1}(\mathcal{A}) = \mathcal{A} \star \text{SEQ}(\mathcal{A})$  que pueden simplificar los desarrollos.

Una permutación consta de sus puntos fijos y el desarreglo de los restantes. Si tiene exactamente  $k$  puntos fijos:

$$\mathcal{D} \star \text{MSET}_k(\mathcal{Z})$$

Representando un multiconjunto de  $k$  elementos como secuencia obviando el orden, esto da la función generatriz exponencial:

$$\frac{e^{-z}}{1-z} \cdot \frac{z^k}{k!}$$

Extraemos coeficientes:

$$\begin{aligned} n! [z^n] \frac{z^k e^{-z}}{k!(1-z)} &= \frac{n!}{k!} [z^{n-k}] \frac{e^{-z}}{1-z} \\ &= \frac{n!}{k!} \exp|_{n-k}(-1) \end{aligned}$$

Para contar todas las maneras de particionar un conjunto tenemos la expresión simbólica:

$$\text{MSET}(\text{MSET}_{\geq 1}(\mathcal{Z}))$$

que se traduce directamente en la función generatriz exponencial de los *números de Bell* [31]:

$$\hat{B}(z) = e^{e^z - 1} \quad (21.22)$$

Para obtener una fórmula explícita para  $B_n$  salimos del espacio estricto de las series formales. Las manipulaciones se justifican ya que las series involucradas convergen uniformemente para todo  $z$ .

$$\begin{aligned} \hat{B}(z) &= \frac{e^{e^z}}{e} \\ &= \frac{1}{e} \sum_{r \geq 0} \frac{e^{rz}}{r!} \\ &= \frac{1}{e} \sum_{r \geq 0} \frac{1}{r!} \sum_{s \geq 0} \frac{(rz)^s}{s!} \\ &= \frac{1}{e} \sum_{s \geq 0} \frac{z^s}{s!} \sum_{r \geq 0} \frac{r^s}{r!} \end{aligned}$$

El número de Bell  $B_n$  es el coeficiente de  $z^n/n!$  en esto:

$$B_n = \frac{1}{e} \sum_{r \geq 0} \frac{r^n}{r!} \quad (21.23)$$

El resultado (21.23) se conoce como *ecuación de Dobinski* [97].

Derivando (21.22) obtenemos la ecuación diferencial, cuyo valor inicial resulta directamente de la función generatriz:

$$\hat{B}'(z) = e^z \hat{B}(z) \quad \hat{B}(0) = 1 \quad (21.24)$$

El lado izquierdo es un desplazamiento, el derecho corresponde a una convolución binomial:

$$B_{n+1} = \sum_{0 \leq k \leq n} \binom{n}{k} B_k \quad B_0 = 1 \quad (21.25)$$

El lector interesado verificará que el truco *zDlog* aplicado a (21.22) lleva a la misma recurrencia (21.25).

Un ejemplo clásico es considerar árboles rotulados, formados por un nodo raíz conectados a un conjunto de árboles. Esto lleva directamente a:

$$\mathcal{T} = \mathcal{Z} \star \text{MSET}(\mathcal{T})$$

que se traduce en la ecuación para la función generatriz  $\hat{T}(z)$ :

$$\hat{T}(z) = z e^{\hat{T}(z)}$$

Inversión de Lagrange da directamente la afamada fórmula de Cayley:

$$\begin{aligned}\frac{t_n}{n!} &= \frac{1}{n} [u^{n-1}] e^{nu} \\ &= \frac{1}{n} \cdot \frac{n^{n-1}}{(n-1)!} \\ t_n &= n^{n-1}\end{aligned}$$

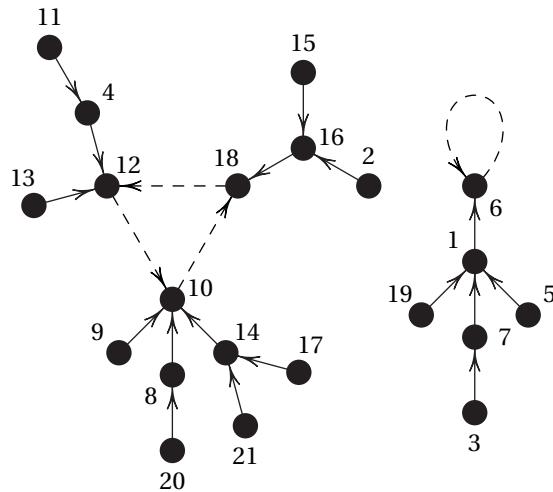


Figura 21.2 – Una función de [21] a [21]

Consideremos una función de  $[n] \rightarrow [n]$ , como por ejemplo la graficada en la figura 21.2 vía indicar por flechas el valor de la función. Vemos que los valores se organizan en árboles, y a su vez estos en ciclos. Esto se describe mediante las ecuaciones simbólicas:

$$\begin{aligned}\mathcal{T} &= \mathcal{Z} \star \text{MSET}(\mathcal{T}) \\ \mathcal{F} &= \text{MSET}(\text{CYC}(\mathcal{T}))\end{aligned}$$

Esto lleva a las ecuaciones funcionales:

$$\begin{aligned}\widehat{T}(z) &= ze^{\widehat{T}(z)} \\ \widehat{F}(z) &= \exp(-\ln(1 - \widehat{T}(z))) \\ &= \frac{1}{1 - \widehat{T}(z)}\end{aligned}$$

Podemos aplicar inversión de Lagrange, teorema 17.8, con  $\phi(u) = e^u$  y  $f(u) = (1 - u)^{-1}$ :

$$\begin{aligned} \frac{f_n}{n!} &= \frac{1}{n} [u^{n-1}] ((1-u)^{-2} e^{nu}) \\ &= \frac{1}{n} [u^{n-1}] \sum_{k \geq 0} (k+1) u^k e^{nu} \\ &= \frac{1}{n} \sum_{k \geq 0} (k+1) [u^{n-k-1}] e^{nu} \\ &= \frac{1}{n} \sum_{k \geq 0} (k+1) \frac{n^{n-k-1}}{(n-k-1)!} \\ f_n &= (n-1)! \sum_{k \geq 0} (k+1) \frac{n^{n-k-1}}{(n-k-1)!} \end{aligned}$$

No es precisamente una fórmula bonita, pero no fue difícil de deducir.

### 21.3.3. Operaciones adicionales

Hay operaciones adicionales que son de interés ocasional. La definición de la siguiente operación es un tanto bizarra, pero pronto la aplicaremos. Sean  $\mathcal{A}$  y  $\mathcal{B}$  clases de objetos, con  $\alpha \in \mathcal{A}$  y  $\beta \in \mathcal{B}$ . Definimos el *producto cajonado* (en el inglés original *boxed product*, término bastante poco descriptivo) entre  $\alpha$  y  $\beta$ , que se anota  $\alpha^\square \star \beta$ , combinando  $\alpha$  y  $\beta$  y rotulando el resultado de forma que el mínimo rótulo se asigna a la parte  $\alpha$ . Por ejemplo:

$$(2, 1, 3)^\square \star (2, 1) = \{(2, 1, 3, 5, 4), (2, 1, 4, 5, 3), (2, 1, 5, 4, 3), (3, 1, 4, 5, 2), (3, 1, 5, 4, 2), (4, 1, 5, 3, 2)\}$$

Lo que estamos haciendo es elegir  $|\alpha| - 1$  rótulos de entre  $|\alpha| + |\beta| - 1$ . Extendemos esta operación a las clases respectivas uniendo los conjuntos resultantes. Si llamamos  $n = |\alpha| + |\beta|$ ,  $k = |\alpha|$  (y por tanto  $n - k = |\beta|$ ) el número de nuevos objetos de tamaño  $n$  creados así es:

$$\sum_{1 \leq k \leq n} \binom{n-1}{k-1} a_k b_{n-k} = \sum_{0 \leq k \leq n-1} \binom{n-1}{k} a_{k+1} b_{n-1-k}$$

Esta es la convolución binomial de las secuencias  $\langle a_{n+1} \rangle_{n \geq 0}$  y  $\langle b_n \rangle_{n \geq 0}$ , pero desplazada en una posición a la derecha. Desplazamiento a la derecha es derivar, con lo que desplazar a la izquierda es integrar:

$$\mathcal{A}^\square \star \mathcal{B} \xleftarrow{\text{egf}} \int_0^z D\hat{A}(u) \cdot \hat{B}(u) du$$

Pongamos en uso esta operación. Una *permutación alternante* es tal que:

$$a_1 < a_2 > a_3 < \dots$$

Consideremos primero las que tienen un número impar de elementos, clase  $\mathcal{T}$ . Si nos fijamos en su máximo, vemos que divide la permutación en forma única en una permutación alternante de largo impar, el máximo, y una permutación alternante de largo impar.

La operación  $a_i \mapsto n+1-a_i$  es claramente una biyección entre permutaciones, y hace que el máximo pase a ser el mínimo. Podemos además interpretar la combinación  $[\square, (\square, \dots, \square), (\square, \dots, \square)]$  como ubicando el primer elemento entre las secuencias. Con estas biyecciones en mente, podemos contar la clase  $\mathcal{T}$  de permutaciones alternantes de largo impar mediante:

$$\mathcal{T} = \mathcal{Z} + \mathcal{Z}^\square \star (\mathcal{T} \star \mathcal{T}) \tag{21.26}$$

lo que lleva a la ecuación:

$$\widehat{T}(z) = z + \int_0^z u' \cdot \widehat{T}^2(u) du$$

y a la ecuación diferencial:

$$\widehat{T}'(z) = 1 + \widehat{T}^2(z) \quad \widehat{T}(0) = 0$$

de donde:

$$\widehat{T}(z) = \tan z \tag{21.27}$$

Si consideramos las permutaciones alternantes de largo par (terminan en una subida), clase  $\mathcal{S}$ , vemos que su máximo las divide en una permutación alternante de largo impar que termina en una bajada (descrita por  $\mathcal{T}$ ), el máximo, y una permutación alternante de largo par que termina en subida (descrita por  $\mathcal{S}$ ):

$$\mathcal{S} = \mathcal{E} + \mathcal{Z}^\square \star (\mathcal{T} \star \mathcal{S}) \tag{21.28}$$

Esto da lugar a la ecuación:

$$\widehat{S}(z) = 1 + \int_0^z u' \cdot \widehat{S}(u) \widehat{T}(u) du$$

con solución:

$$\widehat{S}(z) = \sec z \tag{21.29}$$

Obtenemos el curioso resultado de André [13] (ver también Stanley [331]) para los números  $E_n$  que cuentan permutaciones alternantes:

$$\widehat{E}(z) = \sec z + \tan z \tag{21.30}$$

Los coeficientes son los *números de Euler*, quien había llegado a los  $E_{2n+1}$  por otro camino.

Una manera de obtener una recurrencia es observar:

$$\begin{aligned} \widehat{E}'(z) &= \sec^2 z + \tan z \sec z \\ \widehat{E}^2(z) &= \tan^2 z + 2 \tan z \sec z + \sec^2 z \\ &= 2 \tan z \sec z + 2 \sec^2 z - 1 \\ &= 2\widehat{E}'(z) - 1 \end{aligned}$$

Usando las propiedades de funciones generatrices exponenciales vemos que cumplen la recurrencia:

$$2E_{n+1} = [n=1] + \sum_{0 \leq k \leq n} \binom{n}{k} E_k E_{n-k} \quad E_0 = 1 \tag{21.31}$$

## 21.4. Un problema de Moser y Lambek

En 1959, Leo Moser y Joe Lambek plantearon [268]:

**Teorema 21.7.** *Hay una única forma de particionar  $\mathbb{N}_0$  en conjuntos  $\mathcal{A}$  y  $\mathcal{B}$  tales que el número de maneras en que se puede representar  $n \in \mathbb{N}_0$  como sumas  $n = a_1 + a_2$  con  $a_1 \neq a_2$  y  $a_1, a_2 \in \mathcal{A}$  es igual al número de representaciones como  $n = b_1 + b_2$  con  $b_1 \neq b_2$  y  $b_1, b_2 \in \mathcal{B}$ .*

*Demostración.* Definamos funciones generatrices:

$$A(z) = \sum_{a \in \mathcal{A}} z^a \quad B(z) = \sum_{b \in \mathcal{B}} z^b$$

Como  $\mathcal{A}$  y  $\mathcal{B}$  particionan  $\mathbb{N}_0$ , los coeficientes son 0 o 1:

$$A(z) + B(z) = \frac{1}{1-z}$$

Para las maneras en que se puede escribir  $n$  como suma de dos  $\mathcal{A}$  distintos:

$$\sum_{\substack{a_1 \neq a_2 \\ a_1, a_2 \in \mathcal{A}}} z^{a_1 + a_2} = \frac{1}{2} (A^2(z) - A(z^2))$$

De la misma forma podemos expresar el caso de  $\mathcal{B}$ , e interesa que sean las mismas:

$$\begin{aligned} A^2(z) - A(z^2) &= B^2(z) - B(z^2) \\ A(z^2) - B(z^2) &= A^2(z) - B^2(z) \\ &= (A(z) - B(z)) \cdot (A(z) + B(z)) \\ &= \frac{A(z) - B(z)}{1-z} \end{aligned}$$

O equivalentemente:

$$A(z) - B(z) = (A(z^2) - B(z^2))(1-z)$$

Substituyendo  $z \rightsquigarrow z^2, z^4, \dots, z^{2^{n-1}}$  obtenemos:

$$A(z) - B(z) = (A(z^{2^n}) - B(z^{2^n})) \prod_{0 \leq k \leq n-1} (1 - z^{2^k}) \quad (21.32)$$

lo que indica:

$$A(z) - B(z) = \prod_{k \geq 0} (1 - z^{2^k}) \quad (21.33)$$

Como series formales (ver la sección 17.4) la secuencia al lado derecho de (21.32) converge a la expresión (21.33).

Los términos del lado derecho de (21.33) tienen coeficientes  $\pm 1$ , con lo que determinan en forma única los coeficientes de  $A(z)$  y  $B(z)$ , que son cero o uno. El conjunto  $\mathcal{A}$  son los que tienen un número par de unos en su expansión binaria.  $\square$

## 21.5. Contando secuencias

Muchas situaciones llevan a enfrentar problemas de contar secuencias con ciertas restricciones. Veremos algunos ejemplos representativos.

¿Cuántas palabras de largo  $n$  formadas únicamente por las 5 vocales pueden formarse, si deben contener un número par de vocales fuertes ('a', 'e' y 'o')?

De las solicitadas podemos formar 1 de largo 0, 2 de largo 1,  $2 \cdot 2 + 3 \cdot 3 = 13$  de largo 2. Estos valores sirven para verificar luego.

Definamos las clases  $\mathcal{U}$  para palabras con un número par de vocales fuertes, y  $\mathcal{V}$  si tienen un número impar, con las respectivas funciones generatrices  $U(z)$  y  $V(z)$  donde  $z$  cuenta el número de vocales. Podemos definir el sistema de ecuaciones simbólicas:

$$\mathcal{U} = \mathcal{E} + \{i, u\} \times \mathcal{U} + \{a, e, o\} \times \mathcal{V}$$

$$\mathcal{V} = \{a, e, o\} \times \mathcal{U} + \{i, u\} \times \mathcal{V}$$

El método simbólico entrega:

$$U(z) = 1 + 2zU(z) + 3zV(z)$$

$$V(z) = 3zU(z) + 2zV(z)$$

Resolvemos el sistema de ecuaciones para  $U(z)$ , que es lo único que realmente interesa, y descomponemos en fracciones parciales:

$$U(z) = \frac{1}{2} \cdot \frac{1}{1-5z} + \frac{1}{2} \cdot \frac{1}{1+z}$$

Podemos leer los  $u_n$  de esto último, que son simplemente dos series geométricas:

$$u_n = \frac{1}{2} (5^n + (-1)^n)$$

Esto coincide con los valores obtenidos antes.

Volvamos nuevamente a la situación de las secuencias de unos y ceros sin ceros seguidos, pero ahora interesa contar no solo el largo sino simultáneamente el número de unos. Para la clase  $\mathcal{S}$  de tales secuencias obtuvimos:

$$\mathcal{S} = \mathcal{E} + \{0\} + \mathcal{S} \times \{1, 10\}$$

Si usamos  $x$  para marcar los ceros, e  $y$  para el número total de símbolos, obtenemos para la función generatriz  $S(x, y)$ :

$$S(x, y) = 1 + y + (xy + xy^2)S(x, y)$$

Despejando:

$$S(x, y) = \frac{1+y}{1-x(y+y^2)}$$

Podemos expandir como serie geométrica en  $x(y+y^2)$ :

$$S(x, y) = \sum_{r \geq 0} x^r y^r (1+y)^{r+1}$$

El número de estas secuencias de largo  $n$  con  $k$  unos es:

$$\begin{aligned} [x^k y^n] \sum_{r \geq 0} x^r y^r (1+y)^{r+1} &= [y^n] y^k (1+y)^{k+1} \\ &= [y^{n-k}] (1+y)^{k+1} \\ &= \binom{k+1}{n-k} \end{aligned}$$

Pero  $n - k$  es el número de ceros. Podemos interpretar esto como diciendo que debemos distribuir  $n - k$  ceros en las  $k + 1$  posiciones separadas por los  $k$  unos.



## 22 Familias de números famosas

---

Hay ciertas familias de números que aparecen frecuentemente en problemas combinatorios. En muchos casos es directo obtener recurrencias para los números que interesan, y funciones generatrices dan entonces forma de llegar a expresiones explícitas o relaciones adicionales. Aplicamos el método simbólico (desarrollado en el capítulo 21) donde es posible, dado que simplifica inmensamente los desarrollos. Un recurso indispensable es la enciclopedia de secuencias de enteros [327], que registra muchos miles de secuencias, cómo se generan y da referencias al respecto.

### 22.1. Subconjuntos y multiconjuntos

Para obtener el número de subconjuntos de  $k$  elementos tomados entre  $n$ , podemos razonar en forma afín a la demostración del teorema 21.1 para conjuntos: Cada elemento aporta 0 o 1 al tamaño de un subconjunto, por lo que la función generatriz para los subconjuntos de un conjunto de  $n$  elementos no es más que:

$$(1 + z)^n$$

y el número de interés es entonces directamente:

$$\binom{n}{k} = [z^k] (1 + z)^n$$

como ya sabíamos.

Otra situación interesante son los multiconjuntos. Siguiendo nuevamente el razonamiento de la demostración del teorema 21.1, el aporte de cada elemento es:

$$1 + z + z^2 + \dots = \frac{1}{1 - z}$$

con lo que el número de multiconjuntos de  $k$  elementos tomados entre  $n$  es simplemente:

$$\binom{\binom{n}{k}}{k} = [z^k] \left( \frac{1}{1 - z} \right)^n = (-1)^k \binom{-n}{k} = \binom{n+k-1}{n-1}$$

### 22.2. Números de Fibonacci y de Lucas

Consideremos el problema de cubrir un rectángulo de  $n \times 1$  con cuadrados y dominós (rectángulos de  $2 \times 1$ ). Esto da lugar a la ecuación simbólica para la clase R:

$$\mathcal{R} = \mathcal{E} + \mathcal{R} \times (\mathcal{Z} + \mathcal{Z} \times \mathcal{Z}) \tag{22.1}$$

de la cual tenemos:

$$\begin{aligned} R(z) &= 1 + R(z)(z + z^2) \\ R(z) &= \frac{1}{1 - z - z^2} \end{aligned} \tag{22.2}$$

Vemos que (22.2) se parece a la función generatriz (19.21) de los números de Fibonacci. Como  $F_0 = 0$ :

$$R(z) = \frac{F(z) - F_0}{z}$$

y en consecuencia:

$$r_n = F_{n+1} \tag{22.3}$$

Un problema relacionado es el número de brazaletes (organizaciones circulares) que pueden formarse con cuadrados y dominós (sin considerar simetrías). Sea  $L_n$  el número de brazaletes de largo  $n$ , se les conoce como *números de Lucas*. Vemos que un brazalete de largo  $n$  tiene dos formas posibles:

- Las posiciones  $n$  y 1 están cubiertas por un dominó, las restantes  $n - 2$  posiciones pueden cubrirse de  $r_{n-2}$  formas.
- Las posiciones  $n$  y 1 no están cubiertas por un dominó, es simplemente unir por sus extremos una de las  $r_n$  maneras de cubrir un rectángulo.

Así tenemos:

$$\begin{aligned} L_n &= r_n + r_{n-2} \quad \text{para } n \geq 3 \\ &= F_{n+1} + F_{n-1} \end{aligned} \tag{22.4}$$

De (22.4) vemos que cumplen la recurrencia (3.32) de los números de Fibonacci. Por (22.4) sabemos que  $L_1 = F_2 + F_0 = 1$  y  $L_2 = F_3 + F_1 = 3$ , usamos (22.5) para calcular  $L_0 = 2$ . Así:

$$L_{n+2} = L_{n+1} + L_n \quad L_0 = 2, L_1 = 1 \tag{22.5}$$

La danza tradicional para resolver recurrencias entrega la particularmente elegante solución:

$$L_n = \tau^n + \phi^n \tag{22.6}$$

Benjamin y Quinn [35] describen una variedad de problemas combinatorios en que aparecen números de Fibonacci y de Lucas. Muestran ingeniosas biyecciones para explicar identidades entre estos números, como (3.34) que dimos como ejemplo de inducción.

### 22.3. Números de Catalan

Ya vimos que los números de Catalan  $C_n$  cuentan el número de secuencias de  $2n$  paréntesis balanceados (sección 14.7.1) y que el número de árboles binarios con  $n$  hojas es  $C_{n-1}$  (sección 14.10). Si llamamos  $\mathcal{C}$  la clase de secuencias de paréntesis balanceados, tenemos la relación simbólica:

$$\mathcal{C} = \mathcal{E} + (\mathcal{C})\mathcal{C}$$

Al usar  $z$  para marcar un par de paréntesis (sus posiciones exactas realmente no interesan), esto da:

$$C(z) = 1 + zC^2(z) \tag{22.7}$$

Vimos que esto da la función generatriz:

$$C(z) = \frac{1 - \sqrt{1 - 4z}}{2z} \quad (22.8)$$

de la que obtenemos la fórmula explícita:

$$C_n = \frac{1}{n+1} \binom{2n}{n} \quad (22.9)$$

Consideremos ahora la manera de dividir un polígono convexo (vale decir, toda diagonal cae completamente en su interior) en triángulos mediante diagonales. La figura 22.1 muestra que para el pentágono hay cinco triangulaciones. Podemos considerar un polígono convexo triangulado como

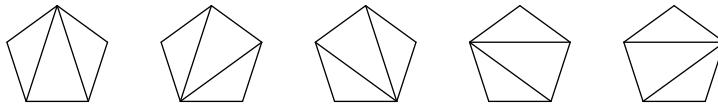


Figura 22.1 – División del pentágono en triángulos

un polígono triangulado, un triángulo y otro polígono triangulado. El caso extremo es el “polígono” con dos vértices (una línea) que tiene una única triangulación (en cero triángulos). Si representamos la clase de triangulaciones por  $\mathcal{T}$  y los triángulos por  $\mathcal{Z}$ , tenemos la expresión simbólica:

$$\mathcal{T} = \mathcal{E} + \mathcal{T} \times \mathcal{Z} \times \mathcal{T} \quad (22.10)$$

con la correspondiente ecuación funcional:

$$T(z) = 1 + z T^2(z) \quad (22.11)$$

La solución es nuevamente los números de Catalan; solo que expresa el número de triangulaciones en términos del número de triángulos, no de lados del polígono. Vemos que un polígono de  $n$  lados se divide en  $n - 2$  triángulos, con lo que finalmente el número de triangulaciones de un polígono de  $n$  lados es  $C_{n-2}$ .

La función generatriz (22.8), en consecuencia los coeficientes (22.9), aparecen con regularidad. Stanley [332, 334] lista un total de 205 interpretaciones combinatorias de los números de Catalan. A (22.8) se le ha llamado la función generatriz más famosa de la combinatoria.

## 22.4. Números de Motzkin

Donaghey y Shapiro [99] indican una estrecha relación entre los números de Motzkin y los de Catalan, por lo que debieran aparecer con frecuencia similar. Una de las tantas estructuras que cuentan es el número de maneras en que pueden dibujarse cuerdas entre puntos sobre una circunferencia de manera que no se intersecten al interior ni sobre la circunferencia. La figura 22.2 muestra que  $m_5 = 21$ . Analizando la situación de la figura 22.2 podemos construir una recurrencia para  $m_n$ . Si elegimos uno de los  $n$  puntos este puede participar en alguna cuerda o no. Si no participa, es como si no existiera, esa situación aporta  $m_{n-1}$  casos. Si ese punto participa en una cuerda, sus dos extremos quedan excluidos, y quedan por tender cuerdas entre los demás  $n - 2$  puntos, de forma que no crucen la cuerda entre manos. Vale decir, la cuerda corta el círculo en dos, una parte de  $k$  nodos y otra de  $n - k - 2$  nodos, las formas de tender cuerdas entre ellas se pueden combinar a gusto:

$$m_n = m_{n-1} + \sum_{0 \leq k \leq n-2} m_k m_{n-k-2}$$

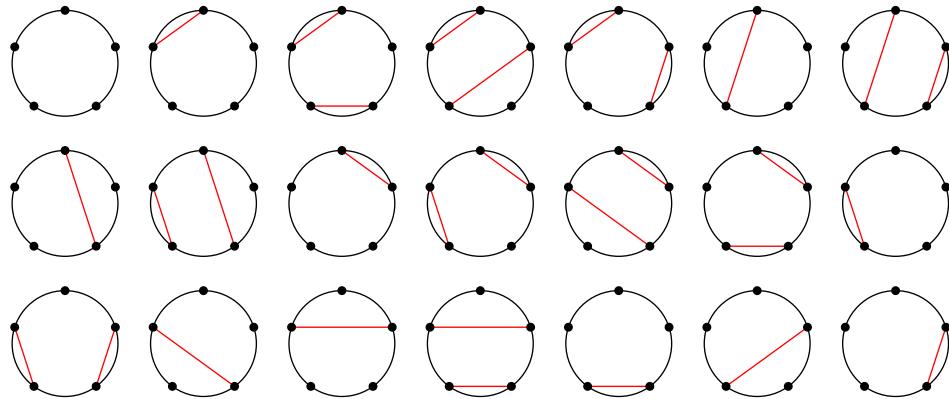


Figura 22.2 – Cuerdas entre cinco puntos sobre la circunferencia

Como condiciones de contorno tenemos  $m_0 = m_1 = 1$  (con la recurrencia entregan los valores conocidos  $m_2 = 2$  y  $m_3 = 4$ ). Resulta:

$$m_{n+2} = m_{n+1} + \sum_{0 \leq k \leq n} m_k m_{n-k} \quad m_0 = m_1 = 1 \quad (22.12)$$

Aplicando las reglas con la función generatriz ordinaria  $M(z)$  y simplificando queda:

$$M(z) = 1 + zM(z) + z^2 M^2(z) \quad (22.13)$$

de donde:

$$M(z) = \frac{1 - z - \sqrt{1 - 2z - 3z^2}}{2z^2} \quad (22.14)$$

(elegimos el signo negativo ya que  $M(0) = m_0 = 1$ ). Expandiendo en serie:

$$M(z) = 1 + z + 2z^2 + 4z^3 + 9z^4 + 21z^5 + 51z^6 + 127z^7 + 323z^8 + 835z^9 + 2188z^{10} + \dots$$

Alternativamente, si  $\mathcal{M}$  es la clase de las maneras de tender cuerdas, podemos descomponerla en ningún punto (aporta  $\mathcal{E}$ ); agregar un punto que no participa en ninguna cuerda (aporta  $\mathcal{Z} \times \mathcal{M}$ ) y tender una cuerda, lo que da cuenta de dos puntos y divide en dos conjuntos de puntos entre los cuales tender cuerdas (aporta  $\mathcal{Z} \times \mathcal{Z} \times \mathcal{M} \times \mathcal{M}$ ). En total:

$$\mathcal{M} = \mathcal{E} + \mathcal{Z} \times \mathcal{M} + \mathcal{Z} \times \mathcal{Z} \times \mathcal{M} \times \mathcal{M} \quad (22.15)$$

Esto lleva nuevamente a la ecuación funcional (22.13).

## 22.5. Números de Schröder

De interés ocasional son los números de Schröder, quien los planteó como el segundo de sus cuatro problemas [317], ver también a Stanley [330]. Tenemos  $n$  símbolos (por ejemplo,  $x$ ) e interesa saber de cuántas formas se pueden “parentizar”, donde la regla es más fácil de explicar recursivamente:  $x$  mismo es una parentización; y si lo son  $\sigma_1$  a  $\sigma_k$  con  $k \geq 2$ , también lo es  $(\sigma_1 \sigma_2 \cdots \sigma_k)$ . Por ejemplo,  $((xx)x(xxx))(xx)$  es una parentización de  $xxxxxxxx$ . El método simbólico aplicado a esta descripción recursiva lleva a:

$$\mathcal{S} = \mathcal{Z} + \text{SEQ}_{\geq 2}(\mathcal{S}) \quad (22.16)$$

y a la ecuación funcional:

$$S(z) = z + \frac{S^2(z)}{1 - S(z)}$$

No es aplicable directamente la fórmula de inversión de Lagrange, pero podemos resolver la cuadrática:

$$2S^2(z) - (z + 1)S(z) + z = 0 \quad (22.17)$$

lo que al descartar la solución espuria da:

$$S(z) = \frac{1}{4} \left( 1 + z - \sqrt{1 - 6z + z^2} \right) \quad (22.18)$$

Expandiendo en serie:

$$S(z) = z + z^2 + 3z^3 + 11z^4 + 45z^5 + 197z^6 + 903z^7 + 4279z^8 + 20793z^9 + 103049z^{10} + \dots$$

La ecuación (22.18) es incómoda. Derivando (22.17) y despejando  $S'(z)$ :

$$S'(z) = \frac{S(z) - 1}{4S(z) - z - 1} \quad (22.19)$$

Observamos de (22.18) que:

$$4S(z) - z - 1 = \sqrt{1 - 6z + z^2}$$

Amplificando la fracción en (22.19) por esto, substituyendo el resultado de despejar  $S^2(z)$  de (22.17) y simplificando:

$$(z^2 - 6z + 1)S'(z) - (z - 3)S(z) = -z + 1 \quad (22.20)$$

Substituyendo la serie de potencias  $S(z)$  en (22.20) e igualando coeficientes de  $z^n$  resulta la recurrencia para  $n \geq 1$  (esto permite evitar las situaciones especiales que introduce el lado derecho de (22.20)):

$$(n+2)s_{n+2} - 3(2n+1)s_{n+1} + (n-1)s_n = 0 \quad (22.21)$$

Expandiendo (22.18) tenemos  $s_1 = s_2 = 1$  como puntos de partida.

Acá obtuvimos una ecuación diferencial lineal manipulando la ecuación funcional para la función generatriz, y de ella extrajimos una recurrencia, más cómoda para calcular los coeficientes que la función generatriz. Esto puede extenderse al caso general de ecuaciones funcionales algebraicas, como muestra Bostan, Chyzak, Salvy y Schost [51].

Otra opción es el camino siguiente:

$$\frac{S(z)}{z} = 1 + \frac{S(z)}{z} \frac{S(z)}{1 - S(z)}$$

Despejando  $S/z$  resulta:

$$S(z) = z \frac{1 - S(z)}{1 - 2S(z)}$$

donde sí es aplicable inversión de Lagrange. El resultado es complicado, y lo omitiremos.

{1}	{2, 3, 4}
{1, 2}	{3, 4}
{1, 3}	{2, 4}
{1, 4}	{2, 4}
{1, 2, 3}	{4}
{1, 2, 4}	{3}
{1, 3, 4}	{2}

Cuadro 22.1 – Las 7 particiones de 4 elementos en 2 clases

## 22.6. Números de Stirling de segunda especie

Interesa el número de maneras de dividir el conjunto {1, 2, 3, 4} en dos clases, como ilustra el cuadro 22.1. Esto muestra que hay 7 particiones de 4 elementos en 2 clases. El número de maneras de dividir un conjunto en clases lo da el *número de Stirling de segunda especie*, se anota  $\{n\}_k$  para el número de formas de dividir un conjunto de  $n$  elementos en  $k$  particiones. Cabe hacer notar que esta notación, originada por Karamata [195], es relativamente común (uno de sus campeones es Knuth, por ejemplo [150, 213]), aunque hay una gran variedad de notaciones, algunas con signo. Claramente para los números de Bell vistos en la sección 21.3:

$$B_n = \sum_{1 \leq k \leq n} \{n\}_k \quad (22.22)$$

Una aplicación es contar el número de funciones sobre de  $[n]$  a  $[k]$ : Corresponde a particionar el dominio en las preimágenes de cada elemento del rango, y podemos asignar valores de la función a cada una de las  $k$  particiones de  $k!$  maneras, con lo que  $\{n\}_k k!$  es el valor buscado.

Para obtener  $\{n\}_k$ , consideremos dos grupos de particiones:

**Aquellas en que  $n$  está solo:** Corresponden a tomar  $k - 1$  particiones de los demás  $n - 1$  elementos, hay  $\{n-1\}_{k-1}$  de estas.

**Aquellas en que  $n$  está con otros elementos:** Se construyen en base a  $k$  clases de los restantes  $n - 1$  elementos vía agregar  $n$  a cada clase, hay  $k \cdot \{n-1\}_k$  de estas.

Estas dos opciones son excluyentes y exhaustivas, y:

$$\{n\}_k = \{n-1\}_{k-1} + k \{n-1\}_k \quad (22.23)$$

Donde:

$$\begin{cases} \{n\}_0 = [n=0] \\ \{n\}_n = 1 \end{cases}$$

Si además decetramos:

$$\begin{cases} \{n\}_k = 0 & n < 0 \\ \{n\}_k = 0 & k < 0 \\ \{n\}_k = 0 & k > n \end{cases}$$

la recurrencia *siempre* se cumple. Una tabla de los números de Stirling de segunda especie en forma de triángulo (como el triángulo de Pascal del cuadro 19.1) comienza como ilustra el cuadro 22.2.

$n = 0 :$	1					
$n = 1 :$	0 1					
$n = 2 :$	0 1 1					
$n = 3 :$	0 1 3 1					
$n = 4 :$	0 1 7 6 1					
$n = 5 :$	0 1 15 25 10 1					
$n = 6 :$	0 1 31 90 65 15 1					

Cuadro 22.2 – Números de Stirling de segunda especie

Podemos optar entre tres funciones generatrices: Multiplicar por  $u^k$  y sumar sobre  $k$ , multiplicar por  $z^n$  y sumar sobre  $n$  o multiplicar por  $u^k z^n$  sumar sobre ambos índices. Al sumar sobre  $k$  el factor  $k$  resulta en una derivada, se optaría por sumar solo sobre  $n$ , que da ecuaciones más simples de tratar. Resulta eso sí una recurrencia para la función generatriz del caso. El desarrollo es largo, y lo omitiremos, vea el texto de Wilf [364].

Es más simple aplicar el método simbólico. Para obtener el número de particiones de  $n$  elementos en  $k$  clases partimos de la expresión simbólica:

$$\mathcal{S} = \text{MSET}(\mathcal{U} \times \text{MSET}_{\geq 1}(\mathcal{Z}))$$

en la que  $\mathcal{U}$  contiene un único elemento de tamaño uno (usado para contabilizar el número de clases asociándolo a la variable  $u$ , mientras  $z$  cuenta el número de elementos total), lo que lleva a la función generatriz mixta (exponencial en  $z$ , los elementos están rotulados; y ordinaria en  $u$ , las clases no lo están):

$$S(z, u) = e^{u(e^z - 1)} \tag{22.24}$$

De acá:

$$\begin{aligned} \binom{n}{k} &= n! [z^n u^k] S(u, z) \\ &= n! [z^n] \frac{(e^z - 1)^k}{k!} \\ &= \frac{n!}{k!} [z^n] \sum_{0 \leq r \leq k} (-1)^{k-r} \binom{k}{r} e^{rz} \\ &= \frac{n!}{k!} \sum_{0 \leq r \leq k} (-1)^{k-r} \binom{k}{r} \frac{r^n}{n!} \\ &= \sum_{0 \leq r \leq k} \frac{(-1)^{k-r} r^n}{r!(k-r)!} \end{aligned} \tag{22.25}$$

## 22.7. Números de Stirling de primera especie

Interesa el número de maneras de organizar  $n$  elementos en  $k$  ciclos. Simbólicamente, con  $\mathcal{U}$  para los ciclos y  $\mathcal{Z}$  para elementos:

$$\mathcal{C} = \text{MSET}(\mathcal{U} \times \text{CYC}(\mathcal{Z}))$$

de donde el método simbólico entrega directamente la función generatriz mixta (exponencial en  $z$ , los elementos están rotulados; y ordinaria en  $u$ , los ciclos no lo están):

$$C(z, u) = \exp\left(u \ln \frac{1}{1-z}\right) = (1-z)^{-u} \quad (22.26)$$

Los coeficientes se conocen como *números de Stirling de primera especie* y se anota  $[n]_k$  (nuevamente notación impulsada por Knuth [213]). Se lee “ $n$  ciclo  $k$ ” (en inglés se expresa  $n$  cycle  $k$ ).

Para derivar una recurrencia para ellos, consideraremos cómo podemos construir una organización de  $n$  objetos con  $k$  ciclos a partir de  $n-1$  objetos. Al agregar el nuevo objeto, podemos ponerlo en un ciclo por sí mismo, lo que puede hacer de una única manera partiendo de cada una de las  $[n-1]_{k-1}$  organizaciones de  $n-1$  elementos con  $k-1$  ciclos. La otra opción es insertarlo en alguno de los  $k$  ciclos ya existentes. Si suponemos  $n-1$  elementos y  $k$  ciclos:

$$(a_1 a_2 \dots a_{j_1})(a_{j_1+1} a_{j_1+2} \dots a_{j_2}) \dots (a_{j_{k-1}+1} a_{j_{k-1}+2} \dots a_{n-1})$$

En ella podemos insertar el nuevo elemento antes de cada elemento, agregándolo al ciclo al que este pertenece; insertar el elemento al final del ciclo es lo mismo que ubicarlo al comienzo de éste, por lo que esto no aporta nuevas opciones. De esta forma para cada caso hay  $n-1$  posibilidades de insertar el nuevo elemento:

$$[n]_k = (n-1) \begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} \quad (22.27)$$

Para condiciones de contorno, tenemos:

$$\begin{bmatrix} n \\ 0 \end{bmatrix} = [n=0] \quad \begin{bmatrix} n \\ n \end{bmatrix} = 1$$

Si además decetramos:

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{cases} 0 & n < 0 \\ 0 & k < 0 \\ 0 & k > n \end{cases}$$

la recurrencia *siempre* se cumple.

En forma de triángulo à la Pascal tenemos el cuadro 22.3. Hay fórmulas explícitas, pero son

$n = 0 :$					1
$n = 1 :$			0		1
$n = 2 :$		0		1	1
$n = 3 :$	0		2		1
$n = 4 :$	0	6		11	6
$n = 5 :$	0	24	50		10
$n = 6 :$	0	120	274	225	85
					15
					1

Cuadro 22.3 – Números de Stirling de primera especie

complicadas y las omitiremos.

## 22.8. Números de Lah

Los números de Lah [228] cuentan el número de maneras de ordenar  $n$  elementos en  $k$  secuencias. Se les ha llamado “números de Stirling de tercera especie” por analogía a los anteriores, y Petkovšek y Pisanski [282] les dan la notación  $\begin{bmatrix} n \\ k \end{bmatrix}$  que usaremos. También es común  $L_{n,k}$ . Queda representado por la expresión simbólica:

$$\mathcal{L} = \text{MSET}(\mathcal{U} \times \text{SEQ}_{\geq 1}(\mathcal{Z}))$$

y el método simbólico da la función generatriz mixta (elementos rotulados, secuencias sin rotular):

$$L(z, u) = e^{u((1-z)^{-1}-1)} = e^{uz(1-z)^{-1}} \quad (22.28)$$

Podemos extraer una fórmula explícita de (22.28):

$$\begin{bmatrix} n \\ k \end{bmatrix} = n! \left[ u^k z^n \right] \exp(uz(1-z)^{-1}) \quad (22.29)$$

$$= n! [z^n] \frac{z^k (1-z)^{-k}}{k!} \quad (22.30)$$

$$= \frac{n!}{k!} [z^{n-k}] (1-z)^{-k} \quad (22.31)$$

$$= \frac{n!}{k!} (-1)^{n-k} \binom{-k}{n-k} \quad (22.32)$$

$$= \frac{n!}{k!} \binom{n-1}{k-1} \quad (22.33)$$

Para derivar una recurrencia para estos números, usamos la misma técnica anterior. Veamos cómo podemos construir  $k$  secuencias tomadas entre  $n$  elementos partiendo con las configuraciones de  $n-1$  elementos. Hay dos posibilidades exhaustivas y excluyentes:  $n$  forma una secuencia por sí sola, cosa que puede hacerse de una única forma partiendo con cada una de las  $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$  configuraciones con  $n-1$  elementos y  $k-1$  secuencias; o podemos agregar  $n$  a alguna de  $k$  secuencias en configuraciones de  $n-1$  elementos. Podemos agregar un nuevo elemento a una secuencia de largo  $e$  de  $e+1$  formas (antes del primero, o después de cada uno de los  $e$  elementos). Como los largos de las secuencias suman  $n-1$ , en total creamos  $(n+k-1) \begin{bmatrix} n-1 \\ k \end{bmatrix}$  nuevas configuraciones. Resulta:

$$\begin{bmatrix} n \\ k \end{bmatrix} = (n+k-1) \begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} \quad (22.34)$$

Para condiciones de contorno tenemos:

$$\begin{bmatrix} n \\ 0 \end{bmatrix} = [n=0] \quad \begin{bmatrix} n \\ n \end{bmatrix} = 1$$

Si además decetramos:

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{cases} 0 & n < 0 \\ 0 & k < 0 \\ 0 & k > n \end{cases}$$

la recurrencia *siempre* se cumple.

Al estilo del triángulo de Pascal tenemos el cuadro 22.4.

$n = 0 :$	1					
$n = 1 :$	0 1					
$n = 2 :$	0 1 1					
$n = 3 :$	0 6 6 1					
$n = 4 :$	0 24 36 12 1					
$n = 5 :$	0 120 240 120 20 1					
$n = 6 :$	0 720 1800 1200 300 30 1					

Cuadro 22.4 – Números de Lah

## 22.9. Potencias, números de Stirling y de Lah

Las potencias factoriales aparecen con bastante regularidad al calcular con diferencias finitas, como muestran entre otros Graham, Knuth y Patashnik [150]. Como vimos en la sección 1.6 hay paralelos entre las diferencias finitas y la derivada, y entre la sumatoria y la integral. Este tipo de relaciones se explotan en el cálculo umbral [307].

Interesa expresar la potencia  $z^n$  en términos de los  $z^k$ , o sea obtener los coeficientes  $S(n, k)$  en la expansión siguiente:

$$z^n = \sum_{0 \leq k \leq n} S(n, k) z^k$$

Cuando  $k < 0$  o  $k > n$  debe ser  $S(n, k) = 0$ , con lo que los límites en realidad son superfluos. Además, para  $n = 0$  resulta  $S(0, 0) = 1$ , es  $S(n, 0) = 0$  si  $n > 0$  y es claro que  $S(n, n) = 1$ .

Escribamos:

$$\begin{aligned} z^{n+1} &= \sum_k S(n, k) z^k \cdot z \\ &= \sum_k S(n, k) (z^{k+1} + kz^k) \\ &= \sum_k (S(n, k-1) + kS(n, k)) z^k \end{aligned}$$

Comparando coeficientes de esto con la expansión de  $z^{n+1}$ :

$$S(n+1, k) = kS(n, k) + S(n, k-1)$$

Tenemos las condiciones de contorno:

$$S(n, 0) = [n = 0] \quad S(n, n) = 1$$

El lector astuto reconocerá esto como la recurrencia (22.23), tenemos:

$$z^n = \sum_k \left\{ \begin{matrix} n \\ k \end{matrix} \right\} z^k \tag{22.35}$$

Veamos ahora los coeficientes  $C(n, k)$  en:

$$z^{\bar{n}} = \sum_k C(n, k) z^k$$

Con esto:

$$\begin{aligned} z^{\overline{n+1}} &= \sum_k C(n, k) z^k (z+n) \\ &= \sum_k (C(n, k) z^{k+1} + nC(n, k) z^k) \\ &= \sum_k (C(n, k-1) + nC(n, k)) z^k \end{aligned}$$

Comparando coeficientes con la expansión de  $z^{\overline{n+1}}$ :

$$C(n+1, k) = nC(n, k) + C(n, k-1)$$

con condiciones de contorno:

$$C(n, 0) = [n=0] \quad C(n, n) = 1$$

Esto coincide con los números de Stirling de primera especie, o sea es:

$$z^{\overline{n}} = \sum_k \begin{Bmatrix} n \\ k \end{Bmatrix} z^k \quad (22.36)$$

En vista que nos ha ido tan bien con esto, consideremos los coeficientes  $L(n, k)$  en:

$$z^{\overline{n}} = \sum_k L(n, k) z^k$$

Aplicando la misma estrategia:

$$\begin{aligned} z^{\overline{n+1}} &= \sum_k L(n, k) z^k (z+n) \\ &= \sum_k L(n, k) (z^{k+1} + n + k) \\ &= \sum_k (L(n, k-1) + (n+k)L(n, k)) z^k \end{aligned}$$

Comparar coeficientes da:

$$L(n+1, k) = (n+k)L(n, k) + L(n, k-1)$$

con condiciones de borde:

$$L(n, 0) = [n=0] \quad L(n, n) = 1$$

Esta es la recurrencia (22.34) de los números de Lah:

$$z^{\overline{n}} = \sum_k \begin{Bmatrix} n \\ k \end{Bmatrix} z^k \quad (22.37)$$

Podemos usar la identidad  $(-z)^m = (-1)^m z^{\overline{m}}$  y viceversa para obtener de (22.35), (22.36) y (22.37):

$$z^n = \sum_k (-1)^{n-k} \begin{Bmatrix} n \\ k \end{Bmatrix} z^{\overline{k}} \quad (22.38)$$

$$z^{\overline{n}} = \sum_k (-1)^{n-k} \begin{Bmatrix} n \\ k \end{Bmatrix} z^k \quad (22.39)$$

$$z^{\overline{n}} = \sum_k (-1)^{n-k} \begin{Bmatrix} n \\ k \end{Bmatrix} z^{\overline{k}} \quad (22.40)$$

La impresionante colección de identidades (22.35) a (22.40) cumple la promesa dada por el título.

## 22.10. Desarreglos

Ya calculamos el número de desarreglos (permutaciones sin puntos fijos) como ejemplo del uso del principio de inclusión y exclusión en el capítulo 15 y como ejemplo del método simbólico en la sección 21.3. Acá veremos técnicas alternativas.

Llamamos  $D_n$  al número de desarreglos de  $n$  elementos. Valores de  $D_n$  son interesantes para contrastar nuestros resultados luego:  $D_0 = 1$  (hay una única manera de ordenar cero elementos, y en esa ningún elemento está en su posición),  $D_1 = 0$  (un elemento puede ordenarse de una manera solamente, y ese siempre está en su posición),  $D_2 = 1$  (solo (2 1)),  $D_3 = 2$  (son (3 1 2) y (2 3 1)).

Para obtener una recurrencia para los  $D_n$ , consideremos la permutación de  $n$  elementos con exactamente  $k$  puntos fijos. Podemos elegir los  $k$  puntos fijos de  $\binom{n}{k}$  maneras, ninguno de los  $n - k$  elementos restantes está en su ubicación, pueden distribuirse de  $D_{n-k}$  formas. O sea, hay exactamente  $\binom{n}{k} \cdot D_{n-k}$  permutaciones con  $k$  puntos fijos. Toda permutación tiene puntos fijos (0, 1, ...,  $n$  de ellos) y hay un total de  $n!$  permutaciones, con lo que para  $n \geq 0$ :

$$n! = \sum_{0 \leq k \leq n} \binom{n}{k} \cdot D_{n-k} \quad (22.41)$$

El lado derecho de (22.41) es la convolución binomial de las secuencias  $\langle 1 \rangle_{n \geq 0}$  y  $\langle D_n \rangle_{n \geq 0}$ :

$$\hat{D}(z) = \sum_{n \geq 0} D_n \frac{z^n}{n!}$$

Aplicamos las propiedades de funciones generatrices exponenciales a (22.41) para obtener:

$$\hat{D}(z) = \frac{e^{-z}}{1-z} \quad (22.42)$$

De (22.42):

$$\begin{aligned} D_n &= n! [z^n] \hat{D}(z) \\ &= n! \sum_{0 \leq k \leq n} \frac{(-1)^k}{k!} \end{aligned}$$

En términos de la exponencial truncada definida por (15.11) resulta (15.12):

$$D_n = n! \cdot \exp|_n(-1)$$

Tenemos:

$$\hat{D}(z) = 1 + \frac{1}{2!} z^2 + \frac{2}{3!} z^3 + \frac{9}{4!} z^4 + \frac{44}{5!} z^5 + \frac{265}{6!} z^6 + \frac{1854}{7!} z^7 + \frac{14833}{8!} z^8 + \frac{133496}{9!} z^9 + \dots$$

Otra forma es derivar directamente una recurrencia para los  $D_n$ . Consideremos  $n$  personas que eligen entre  $n$  sombreros de manera que ninguna se lleva el suyo. Numeramos a las personas y los respectivos sombreros de 1 a  $n$ . La persona  $n$  puede elegir el sombrero equivocado de  $n - 1$  maneras, supongamos que elige el sombrero  $k$ . Ahora hay dos posibilidades: Si la persona  $k$  toma el sombrero  $n$ , podemos eliminar los sombreros (y las personas)  $n$  y  $k$  de consideración, y el problema se reduce a distribuir los  $n - 2$  sombreros restantes entre las otras  $n - 2$  personas. Si la persona  $k$  no toma el sombrero  $n$ , podemos renombrar ese como  $k$  (no lo toma  $k$  porque ahora le corresponde) y quedan por distribuir los  $n - 1$  sombreros restantes sin que a nadie le toque el suyo. Al revés, de un par de desarreglos de  $n - 1$  y  $n - 2$  elementos podemos construir  $n - 1$  desarreglos de  $n$  elementos (podemos elegir  $k$  arriba de  $n - 1$  maneras en ambos casos). Obtenemos:

$$D_n = (n - 1)(D_{n-1} + D_{n-2}) \quad (n \geq 2) \quad D_0 = 1, D_1 = 0 \quad (22.43)$$

Para resolver (22.43), definimos una función generatriz exponencial, ya que el factor  $n - 1$  se compensa parcialmente con  $(n - 1)!$  en el denominador. Para  $n \geq 1$  podemos escribir:

$$D_{n+1} = nD_n + nD_{n-1} \quad (22.44)$$

Las propiedades de las funciones generatrices exponenciales dan:

$$\begin{aligned}\hat{D}'(z) &\xrightarrow{\text{egf}} \langle D_{n+1} \rangle_{n \geq 0} \\ z\hat{D}'(z) &\xrightarrow{\text{egf}} \langle nD_n \rangle_{n \geq 0}\end{aligned}$$

Falta el segundo término del lado derecho de (22.44):

$$\sum_{n \geq 1} nD_{n-1} \frac{z^n}{n!} = z \sum_{n \geq 1} D_{n-1} \frac{z^{n-1}}{(n-1)!} = z\hat{D}(z)$$

Otra forma de ver esto es que la secuencia  $\langle D_{n-1} \rangle_{n \geq 0}$  corresponde a la antiderivada de  $\hat{D}(z)$  (correr una posición a la derecha), y al multiplicar por  $n$  (que corresponde al operador  $zD$ ) la derivada y la antiderivada se cancelan. Combinando las anteriores:

$$\begin{aligned}\hat{D}'(z) &= z\hat{D}'(z) + z\hat{D}(z) \quad \hat{D}(0) = D_0 = 1 \\ \frac{\hat{D}'(z)}{\hat{D}(z)} &= \frac{z}{1-z}\end{aligned}$$

La solución de esta ecuación diferencial es nuevamente (22.42).

Aún otra manera de enfrentar este problema es masajear la recurrencia (22.44) para obtener una recurrencia más simple de resolver:

$$\begin{aligned}D_n - nD_{n-1} &= -D_{n-1} + (n-1)D_{n-2} \\ &= -(D_{n-1} - (n-1)D_{n-2}) \\ (-1)^n (D_n - nD_{n-1}) &= (-1)^{n-1} (D_{n-1} - (n-1)D_{n-2})\end{aligned} \quad (22.45)$$

Vale decir, el lado izquierdo de (22.45) es independiente de  $n$ . Como  $D_0 = 1$  y  $D_1 = 0$ , con  $n = 1$  vemos que vale 1. Esto da la recurrencia:

$$D_n = nD_{n-1} + (-1)^n \quad D_0 = 1 \quad (22.46)$$

Nuevamente el factor  $n$  sugiere una función generatriz exponencial:

$$\begin{aligned}\sum_{n \geq 1} D_n \frac{z^n}{n!} &= \sum_{n \geq 1} nD_{n-1} \frac{z}{n!} + \sum_{n \geq 1} (-1)^n \frac{z^n}{n!} \\ \hat{D}(z) - D_0 &= z \sum_{n \geq 1} D_{n-1} \frac{z^{n-1}}{(n-1)!} + e^{-z} - 1 \\ &= z\hat{D}(z) + e^{-z} - 1\end{aligned}$$

Con  $D_0 = 1$  esto se simplifica a (22.42), y tenemos (15.12) una vez más.

## 22.11. Resultados de competencias con empate

Interesa saber cuántos resultados finales pueden producirse en un campeonato entre  $n$  participantes si pueden producirse empates, vale decir pueden haber varios primeros puestos, y en general

varios en cada puesto. No hay puestos vacantes, si hay participantes en el puesto  $j$ , los hay en todos los puestos  $1 \leq i \leq j$ . A estos números se les llama *números de Bell ordenados*, como los números de Bell vistos en la sección 21.3 cuentan el número total de particiones sin especificar el orden de las mismas, acá las estamos ordenando. Good [144] trata estos números en gran detalle.

Llámemos  $R_n$  al número de posibilidades indicado. Claramente  $R_0 = 1$ ,  $R_1 = 1$ ,  $R_2 = 3$ .

Si hay  $k$  en primer lugar, habrán  $n - k$  que se distribuyen de la misma forma desde el segundo lugar, o sea, hay  $R_{n-k}$  distribuciones de los demás. Como a los  $k$  campeones los estamos eligiendo entre los  $n$ , y pueden haber de 1 a  $n$  en primer lugar, resulta la recurrencia:

$$R_n = \sum_{1 \leq k \leq n} \binom{n}{k} R_{n-k} \quad (22.47)$$

Para  $n \geq 1$  podemos completar la suma en (22.47):

$$2R_n = \sum_{0 \leq k \leq n} \binom{n}{k} R_{n-k}$$

Para  $n = 0$  tenemos:

$$\sum_{0 \leq k \leq 0} \binom{0}{k} R_{0-k} = R_0$$

En vista de esto, como  $R_0 = 1$ , la recurrencia completa, válida para  $n \geq 0$ , es:

$$2R_n = [n = 0] + \sum_{0 \leq k \leq n} \binom{n}{k} R_{n-k} \quad (22.48)$$

Como (22.48) es la convolución binomial de las secuencias  $\langle 1 \rangle_{n \geq 0}$  y  $\langle R_n \rangle_{n \geq 0}$ , definimos:

$$\widehat{R}(z) = \sum_{n \geq 0} R_n \frac{z^n}{n!} \quad (22.49)$$

Con (22.48) tenemos así:

$$\begin{aligned} 2\widehat{R}(z) &= 1 + \widehat{R}(z)e^z \\ \widehat{R}(z) &= \frac{1}{2 - e^z} \end{aligned} \quad (22.50)$$

Expandiendo en serie:

$$\widehat{R}(z) = 1 + z + \frac{3}{2!}z^2 + \frac{13}{3!}z^3 + \frac{75}{4!}z^4 + \frac{541}{5!}z^5 + \frac{4683}{6!}z^6 + \frac{47293}{7!}z^7 + \frac{545835}{8!}z^8 + \dots$$

Alternativamente, por el método simbólico:

$$\mathcal{R} = \text{SEQ}(\text{SET}_{\geq 1}(\mathcal{Z}))$$

y directamente obtenemos (22.50).

Podemos expandir (22.50) como serie geométrica:

$$\begin{aligned} \widehat{R}(z) &= \frac{1}{2} \sum_{k \geq 0} \frac{e^{kz}}{2^k} \\ &= \frac{1}{2} \sum_{k \geq 0} \frac{1}{2^k} \left( \sum_{n \geq 0} \frac{(kz)^n}{n!} \right) \\ &= \sum_{n \geq 0} \frac{z^n}{n!} \sum_{k \geq 0} \frac{k^n}{2^{k+1}} \end{aligned}$$

De acá tenemos:

$$R_n = \sum_{k \geq 0} \frac{k^n}{2^{k+1}} \quad (22.51)$$

Difícilmente habríamos adivinado esta expresión (con la idea de demostrarla luego por inducción).

## 22.12. Particiones de enteros

En el siglo XX tema de investigaciones importantes en teoría de números involucraban la teoría de las particiones de enteros, un área en la que Euler fue pionero. Acá veremos solo un par de resultados curiosos, que ya demostró Euler.

### 22.12.1. Particiones en general

Sea  $p(n)$  el número de formas de escribir  $n$  como suma. Tenemos:

$$\begin{aligned} p(1) &= 1 & 1 \\ p(2) &= 2 & 2 = 1 + 1 \\ p(3) &= 3 & 3 = 1 + 1 + 1 = 2 + 1 \\ p(4) &= 4 & 4 = 1 + 1 + 1 + 1 = 2 + 1 + 1 = 2 + 2 = 3 + 1 \\ &\vdots \end{aligned}$$

Tratamos esto mediante el método simbólico, una partición de  $n$  corresponde a un multiconjunto de  $\mathbb{N}$ , o sea nos interesa  $MSET(\mathbb{N})$ . Cada número aparece una vez en  $\mathbb{N}$ , así:

$$P(z) = \sum_{n \geq 1} p(n)z^n = \prod_{n \geq 1} \frac{1}{1 - z^n} \quad (22.52)$$

### 22.12.2. Sumandos diferentes e impares

Poniendo como condición que los sumandos no se pueden repetir tenemos subconjuntos de  $\mathbb{N}$ , interesa  $SET(\mathbb{N})$ . Anotamos  $p_d(n)$  para el número de estas particiones, por *different* en inglés, y distinguimos así la función generatriz también:

$$P_d(z) = \sum_{n \geq 0} p_d(n)z^n = \prod_{n \geq 1} (1 + z^n) \quad (22.53)$$

Este producto podemos expresarlo de otra forma:

$$P_d(z) = \prod_{n \geq 1} \frac{1 - z^{2n}}{1 - z^n} = \prod_{n \geq 0} \frac{1}{1 - z^{2n+1}} \quad (22.54)$$

Este producto corresponde a sumandos impares, si escribimos  $p_o(n)$  por el número de particiones en sumandos impares (de *odd* en inglés), tenemos:

$$p_d(n) = p_o(n) \quad (22.55)$$

Curioso resultado (22.55), obtenido únicamente considerando las funciones generatrices del caso. Y ni siquiera evaluamos ninguna de (22.52), (22.53) o (22.54).



## 23 Propiedades adicionales

---

De manera muy similar a como contabilizamos las estructuras de un tamaño dado mediante funciones generatrices podemos representar el total de alguna característica. Dividiendo por el número de estructuras del tamaño respectivo tenemos el promedio del valor de interés. Esto suele ser relevante como medida del rendimiento promedio de algún algoritmo o estructura de datos.

Veremos dos maneras complementarias de atacar esta clase de situaciones. Partiremos por una representación directa, más sencilla de aplicar en muchos casos, pero que entrega información limitada. Luego mostraremos una técnica que permite obtener estadísticas detalladas.

### 23.1. Funciones generatrices cumulativas

Para precisar, consideremos una clase de objetos  $\mathcal{A}$ . Como siempre el número de objetos de tamaño  $n$  lo anotaremos  $a_n$ , con función generatriz:

$$A(z) = \sum_{\alpha \in \mathcal{A}} z^{|\alpha|} \quad (23.1)$$

$$= \sum_{n \geq 0} a_n z^n \quad (23.2)$$

Consideremos no sólo el número de objetos, sino alguna característica, cuyo valor para el objeto  $\alpha$  anotaremos  $\chi(\alpha)$ . Es natural definir la *función generatriz cumulativa*:

$$C(z) = \sum_{\alpha \in \mathcal{A}} \chi(\alpha) z^{|\alpha|} \quad (23.3)$$

Vale decir, los coeficientes son la suma de la medida  $\chi$  para un tamaño dado:

$$[z^n]C(z) = \sum_{|\alpha|=n} \chi(\alpha) \quad (23.4)$$

Así tenemos el valor promedio para objetos de tamaño  $n$ :

$$\mathbb{E}_n[\chi] = \frac{[z^n]C(z)}{[z^n]A(z)} \quad (23.5)$$

La discusión precedente es aplicable si tenemos objetos no rotulados entre manos. Si corresponden objetos rotulados, podemos definir las respectivas funciones generatrices exponenciales:

$$\widehat{A}(z) = \sum_{\alpha \in \mathcal{A}} \frac{z^{|\alpha|}}{|\alpha|!} \quad (23.6)$$

$$= \sum_{n \geq 0} a_n \frac{z^n}{n!} \quad (23.7)$$

$$\widehat{C}(z) = \sum_{\alpha \in \mathcal{A}} \chi(\alpha) \frac{z^{|\alpha|}}{|\alpha|!} \quad (23.8)$$

Nuevamente, como los factoriales en los coeficientes se cancelan:

$$\mathbb{E}_n[\chi] = \frac{[z^n]\widehat{C}(z)}{[z^n]\widehat{A}(z)} \quad (23.9)$$

Para un primer ejemplo trivial, consideremos secuencias binarias y determinemos el número promedio de ceros en las secuencias de largo  $n$ . Estos son secuencias de objetos sin rotular (intercambiar un par de ceros no cambia la secuencia). Podemos describir la clase de las secuencias de interés como:

$$\mathcal{S} = \mathcal{E} + \mathcal{S} \times \{0, 1\} \quad (23.10)$$

Para la función generatriz respectiva:

$$S(z) = \sum_{\sigma \in \mathcal{S}} z^{|\sigma|} \quad (23.11)$$

el método simbólico lleva directamente a:

$$S(z) = 1 + 2zS(z)$$

con solución:

$$S(z) = \frac{1}{1 - 2z} \quad (23.12)$$

de donde vemos que:

$$[z^n]S(z) = 2^n$$

Como esperábamos.

Si llamamos  $\zeta(\sigma)$  al número de ceros en la secuencia  $\sigma$ , vemos que el número total de ceros en todas las secuencias de largo  $|\sigma| + 1$  que pueden crearse a partir de  $\sigma$  es simplemente  $2\zeta(\sigma) + 1$  (añadir 1 aporta  $\zeta(\sigma)$  ceros al total, agregar 0 aporta  $\zeta(\sigma) + 1$ ). Siguiendo la descripción de la clase podemos derivar una ecuación para  $C(z)$ :

$$C(z) = \sum_{\sigma \in \mathcal{S}} \zeta(\sigma) z^{|\sigma|} \quad (23.13)$$

$$\begin{aligned} &= \zeta(\epsilon) + \sum_{\sigma \in \mathcal{S}} (2\zeta(\sigma) + 1) z^{|\sigma|+1} \\ &= 2z \sum_{\sigma \in \mathcal{S}} \zeta(\sigma) z^{|\sigma|} + z \sum_{\sigma \in \mathcal{S}} z^{|\sigma|} \\ &= 2zC(z) + zS(z) \end{aligned} \quad (23.14)$$

Con (23.12) podemos resolver (23.14):

$$C(z) = \frac{z}{(1 - 2z)^2} \quad (23.15)$$

De acá: usando la convención de Iverson (ver la sección 1.5):

$$\begin{aligned} [z^n]C(n) &= [z^n] \frac{z}{(1 - 2z)^2} \\ &= \begin{cases} 0 & \text{si } n = 0 \\ [z^{n-1}](1 - 2z)^{-2} & \text{si } n > 0 \end{cases} \\ &= [n > 0] n \cdot 2^{n-1} \\ &= n 2^{n-1} \end{aligned}$$

Combinando con lo anterior:

$$\begin{aligned} E_n[\zeta] &= \frac{[z^n]C(z)}{[z^n]S(z)} \\ &= \frac{n}{2} \end{aligned} \tag{23.16}$$

Tal como esperábamos.

---

```

1 void sort(double a[], const int n)
2 {
3     int i, j;
4     double tmp;
5
6     for(i = 1; i < n; i++) {
7         tmp = a[i];
8         for(j = i - 1; j >= 0 && tmp < a[j]; j--)
9             a[j + 1] = a[j];
10            a[j + 1] = tmp;
11    }
12 }
```

---

Listado 23.1 – Ordenamiento por inserción

Una de las áreas principales de aplicación de la combinatoria es el análisis detallado de algoritmos, como ilustra nuestro siguiente ejemplo. Analizaremos el algoritmo de ordenamiento por inserción, mostrado en el listado 23.1. Interesa particularmente el número de veces que se ejecuta la línea 9. Es claro que este número es  $O(n^2)$ , pero interesa una descripción más precisa.

Si suponemos que todos los valores son diferentes, esto se reduce a analizar la permutación de los valores. Vemos que para un valor dado de  $i$  los valores previos ya han sido ordenados, con lo que el valor de  $a[i]$  se compara con los valores anteriores que son mayores a él, y éstos se mueven una posición hacia arriba en el arreglo en la línea 9. En una permutación  $\pi$  se dice que hay una *inversión* si  $\pi(i) > \pi(j)$  con  $i < j$ . La parte central del análisis es entonces determinar el número de inversiones en permutaciones de  $n$  elementos. Para poder hablar de rendimiento promedio, debemos indicar la distribución de las permutaciones a ordenar. Una suposición simple es que todas las permutaciones son igualmente probables.

Anotemos  $\iota(\pi)$  para el número de inversiones de la permutación  $\pi$ , y definamos la función generatriz cumulativa:

$$I(z) = \sum_{\pi \in \mathcal{P}} \iota(\pi) \frac{z^{|\pi|}}{|\pi|!} \tag{23.17}$$

En particular, nos interesa el número promedio de inversiones para permutaciones de tamaño  $n$ .

Podemos describir permutaciones mediante la expresión simbólica:

$$\mathcal{P} = \mathcal{E} + \mathcal{P} \star \mathcal{Z} \tag{23.18}$$

Vale decir, una permutación es vacía o es una permutación combinada con un elemento adicional. Dada la permutación  $\pi$  construimos permutaciones de largo  $|\pi| + 1$  añadiendo un nuevo elemento vía la operación  $\star$ . Estamos creando  $|\pi| + 1$  nuevas permutaciones, cada una de las cuales conserva las inversiones que tiene, y agrega entre 0 y  $|\pi|$  nuevas inversiones dependiendo del valor elegido como último. El total de inversiones en el conjunto de permutaciones así creado a partir de  $\pi$  es:

$$(|\pi| + 1)\iota(\pi) + \sum_{0 \leq k \leq |\pi|} k = (|\pi| + 1)\iota(\pi) + \frac{|\pi|(|\pi| + 1)}{2} \tag{23.19}$$

Con esto tenemos la descomposición para la función generatriz cumulativa (la permutación de cero elementos no tiene inversiones):

$$I(z) = \sum_{\pi \in \mathcal{P}} \iota(\pi) \frac{z^{|\pi|}}{|\pi|!} \quad (23.20)$$

$$= \iota(\epsilon) + \sum_{\pi \in \mathcal{P}} \left( (|\pi|+1)\iota(\pi) + \frac{|\pi|(|\pi|+1)}{2} \right) \frac{z^{|\pi|+1}}{(|\pi|+1)!} \quad (23.21)$$

$$= \sum_{\pi \in \mathcal{P}} \iota(\pi) \frac{z^{|\pi|+1}}{|\pi|!} + \frac{1}{2} \sum_{\pi \in \mathcal{P}} \frac{z^{|\pi|+1}}{|\pi|!} |\pi|$$

Como hay  $k!$  permutaciones de tamaño  $k$ , sumando sobre tamaños resulta:

$$\begin{aligned} &= zI(z) + \frac{1}{2} z \sum_{k \geq 0} kz^k \\ &= zI(z) + \frac{z^2}{2(1-z)^2} \end{aligned} \quad (23.22)$$

Despejando:

$$I(z) = \frac{1}{2} \frac{z^2}{(1-z)^3} \quad (23.23)$$

Obtenemos el número promedio de inversiones directamente, ya que hay  $n!$  permutaciones de tamaño  $n$ , y el promedio casualmente es el coeficiente de  $z^n$  en la función generatriz exponencial:

$$E_n[l] = [z^n] I(z) \quad (23.24)$$

$$\begin{aligned} &= \frac{1}{2} \binom{n}{2} \\ &= \frac{n(n-1)}{4} \end{aligned} \quad (23.25)$$

En consecuencia, en promedio al ordenar  $n$  elementos el método de inserción mueve  $n(n-1)/4$  elementos. Esto también resulta ser el número promedio de comparaciones de elementos, ver el listado 23.1.

Podemos definir árboles binarios como un *nodo externo* (simbolizado por  $\square$ ) o un *nodo interno* (simbolizado por  $\bullet$ ) conectado a dos árboles binarios (izquierdo y derecho). Así podemos expresar la clase de árboles binarios como:

$$\mathcal{A} = \square + \bullet \times \mathcal{A} \times \mathcal{A} \quad (23.26)$$

Con  $|\alpha|$  el número de nodos internos del árbol binario  $\alpha$  y  $\boxed{\alpha}$  su número de nodos externos, por inducción estructural:

$$\boxed{\alpha} = |\alpha| + 1 \quad (23.27)$$

Si consideramos como medida de tamaño el número de nodos internos, la descripción simbólica (23.26) da la ecuación funcional:

$$A(z) = 1 + zA^2(z) \quad (23.28)$$

que entrega:

$$A(z) = \frac{1 - \sqrt{1 - 4z}}{2z} \quad (23.29)$$

que sabemos de (14.61) da los números de Catalan:

$$a_n = C_n = \frac{1}{n+1} \binom{2n}{n} \quad (23.30)$$

En un árbol binario, la *altura* de un nodo es la distancia de la raíz. Se define el *largo de camino interno* (en inglés *internal path length*) del árbol como la suma de las alturas de los nodos internos, lo anotamos  $\pi(\alpha)$ . El *largo de camino externo* (en inglés *external path length*) del árbol es la suma de las alturas de los nodos externos, que anotamos  $\xi(\alpha)$ . Si buscamos en un árbol binario en el que los nodos en el subárbol izquierdo son menores que la raíz, y ésta a su vez menor que los nodos en el subárbol derecho,  $\pi(\alpha)$  es la suma de los costos para buscar los  $|\alpha|$  nodos internos, mientras  $\xi(\alpha)$  es la suma de los costos para buscar los  $|\alpha| + 1$  nodos externos, partiendo cada vez de la raíz. Si almacenamos datos en los nodos internos en la forma de árboles binarios de búsqueda, nodos externos corresponden a búsquedas fallidas

Calculemos el promedio de los largos de camino en árboles binarios de  $n$  nodos internos. De partida, ambas medidas son cero para el árbol que sólo tiene un nodo externo. De la descripción del árbol binario  $\alpha$  como nodo raíz y subárboles izquierdo y derecho ( $\alpha_l$  y  $\alpha_r$ , respectivamente), como al agregar una raíz la altura de cada nodo aumenta en uno (y la suma de las alturas aumenta en el número de nodos considerados), podemos escribir:

$$\pi(\alpha) = \pi(\alpha_l) + |\alpha_l| + \pi(\alpha_r) + |\alpha_r| \quad (23.31)$$

$$\begin{aligned} \xi(\alpha) &= \xi(\alpha_l) + \boxed{\alpha_l} + \xi(\alpha_r) + \boxed{\alpha_r} \\ &= \xi(\alpha_l) + |\alpha_l| + 1 + \xi(\alpha_r) + |\alpha_r| + 1 \end{aligned} \quad (23.32)$$

Esto lleva directamente a las ecuaciones funcionales para las funciones generatrices cumulativas, al considerar el árbol con un nodo externo y los demás:

$$I(z) = \sum_{\alpha \in \mathcal{A}} \pi(\alpha) z^{|\alpha|} \quad (23.33)$$

$$= \pi(\square) + \sum_{\substack{\alpha_l \in \mathcal{A} \\ \alpha_r \in \mathcal{A}}} (\pi(\alpha_l) + |\alpha_l| + \pi(\alpha_r) + |\alpha_r|) z^{|\alpha_l| + |\alpha_r| + 1}$$

$$= \sum_{\substack{\alpha_l \in \mathcal{A} \\ \alpha_r \in \mathcal{A}}} (\xi(\alpha_l) + |\alpha_l| + 1 + \xi(\alpha_r) + |\alpha_r| + 1) z^{|\alpha_l| + |\alpha_r| + 1} \quad (23.34)$$

$$E(z) = \sum_{\alpha \in \mathcal{A}} \xi(\alpha) z^{|\alpha|} \quad (23.35)$$

$$= \xi(\square) + \sum_{\substack{\alpha_l \in \mathcal{A} \\ \alpha_r \in \mathcal{A}}} (\xi(\alpha_l) + |\alpha_l| + 1 + \xi(\alpha_r) + |\alpha_r| + 1) z^{|\alpha_l| + |\alpha_r| + 1}$$

$$= \sum_{\substack{\alpha_l \in \mathcal{A} \\ \alpha_r \in \mathcal{A}}} (\xi(\alpha_l) + |\alpha_l| + 1 + \xi(\alpha_r) + |\alpha_r| + 1) z^{|\alpha_l| + |\alpha_r| + 1} \quad (23.36)$$

Consideremos las sumas resultantes, por ejemplo:

$$\begin{aligned} \sum_{\substack{\alpha_l \in \mathcal{A} \\ \alpha_r \in \mathcal{A}}} \pi(\alpha_l) z^{|\alpha_l| + |\alpha_r| + 1} &= z \sum_{\alpha_l \in \mathcal{A}} \pi(\alpha_l) z^{|\alpha_l|} \cdot \sum_{\alpha_r \in \mathcal{A}} z^{|\alpha_r|} \\ &= z I(z) A(z) \end{aligned}$$

Otro tipo de suma es:

$$\begin{aligned} \sum_{\substack{\alpha_l \in \mathcal{A} \\ \alpha_r \in \mathcal{A}}} |\alpha_l| z^{|\alpha_l|+|\alpha_r|+1} &= z \sum_{\alpha_l \in \mathcal{A}} |\alpha_l| z^{|\alpha_l|} \cdot \sum_{\alpha_r \in \mathcal{A}} z^{|\alpha_r|} \\ &= z^2 A'(z) A(z) \end{aligned}$$

Acá usamos:

$$z A'(z) = \sum_{\alpha \in \mathcal{A}} |\alpha| z^{|\alpha|}$$

Finalmente:

$$\begin{aligned} \sum_{\substack{\alpha_l \in \mathcal{A} \\ \alpha_r \in \mathcal{A}}} z^{|\alpha_l|+|\alpha_r|+1} &= z \sum_{\alpha_l \in \mathcal{A}} z^{|\alpha_l|} \cdot \sum_{\alpha_r \in \mathcal{A}} z^{|\alpha_r|} \\ &= z A^2(z) \end{aligned}$$

En (23.34) los primeros tipos de suma se repiten dos veces (una vez al sumar sobre  $\alpha_l$  y una vez al sumar sobre  $\alpha_r$ ):

$$I(z) = 2z I(z) A(z) + 2z^2 A(z) A'(z) \quad (23.37)$$

Despejando  $I(z)$ :

$$\begin{aligned} I(z) &= \frac{2z^2 A(z) A'(z)}{1 - 2z A(z)} \\ &= \frac{1 - 3z - (1-z)\sqrt{1-4z}}{z(1-4z)} \end{aligned} \quad (23.38)$$

Por el teorema de Bender (teorema 29.3) tenemos que:

$$\begin{aligned} [z^n] I(z) &\sim \lim_{z \rightarrow 1/4} \left( \frac{1 - 3z - (1-z)\sqrt{1-4z}}{z} \right) \cdot 4^n \\ &\sim 4^n \end{aligned} \quad (23.39)$$

Nos interesa el promedio, para lo que según (23.67) requerimos además:

$$\begin{aligned} [z^n] A(z) &= C_n \\ &= \frac{1}{n+1} \binom{2n}{n} \\ &\sim \frac{4^n n^{-3/2}}{\sqrt{\pi}} \end{aligned}$$

(lo último de la fórmula de Stirling (18.18) para factoriales con la expresión (13.5) para coeficientes binomiales). Con esto el promedio buscado es:

$$\begin{aligned} E_n[\pi] &= \frac{[z^n] I(z)}{[z^n] A(z)} \\ &\sim \sqrt{\pi} n^{3/2} \end{aligned} \quad (23.40)$$

El costo promedio de búsquedas exitosas en el árbol resulta así:

$$\frac{E_n[\pi]}{n} \sim \sqrt{\pi n} \quad (23.41)$$

Para  $E(z)$  tenemos de forma similar:

$$E(z) = 2zE(z)A(z) + 2z^2 A(z)A'(z) + 2zA^2(z)$$

Despejando:

$$\begin{aligned} E(z) &= \frac{2z^2 A(z)A'(z) + 2zA^2(z)}{1 - 2zA(z)} \\ &= \frac{1 - \sqrt{1 - 4z}}{1 - 4z} \end{aligned} \quad (23.42)$$

Esto es sencillo de manejar usando (14.30) y aproximando el coeficiente binomial mediante la fórmula de Stirling (18.18):

$$\begin{aligned} [z^n]E(z) &= [z^n] \frac{1}{1 - 4z} - [z^n](1 - 4z)^{-1/2} \\ &= 4^n - \binom{-1/2}{n} (-4)^n \\ &= 4^n - \frac{1}{4^n} \binom{2n}{n} \cdot 4^n \\ &\sim 4^n \left(1 - \sqrt{\frac{2}{\pi n}}\right) \end{aligned} \quad (23.43)$$

Para el costo promedio de las  $n + 1$  posibles búsquedas fallidas resulta:

$$\begin{aligned} \frac{E_n[\xi]}{n+1} &= \frac{[z^n]E(z)}{(n+1)[z^n]A(z)} \\ &\sim \sqrt{\pi n} \end{aligned} \quad (23.44)$$

Interesa analizar el comportamiento de árboles binarios de búsqueda, particularmente el costo promedio de búsquedas exitosas y fallidas. Árboles binarios de búsqueda normalmente se crean insertando sucesivamente los elementos a buscar, con lo que un modelo razonable es considerar que se insertan elementos de claves diferentes y que todas las permutaciones de los datos son igualmente probables. Nótese que estas son las mismas estructuras que consideramos antes, pero la distribución es diferente.

Al elegir la raíz estamos dividiendo los restantes valores en dos subárboles, estos valores vienen intercalados. Si los tamaños de los subárboles izquierdo y derecho son  $|\alpha_l|$  y  $|\alpha_r|$ , respectivamente, el mismo árbol binario de búsqueda resulta del siguiente número de permutaciones diferentes:

$$\binom{|\alpha_l| + |\alpha_r|}{|\alpha_l|}$$

y sabemos que este coeficiente binomial es máximo cuando  $|\alpha_l| = |\alpha_r|$ . Vale decir, construir árboles binarios de búsqueda insertando elementos en orden aleatorio da resultados más balanceados que árboles elegidos al azar.

Suponemos además que la probabilidad de buscar cada uno de los datos es la misma, y además que búsquedas fallidas tienen la misma probabilidad para cada rango de claves antes, entre cada par de elementos y luego del último. El costo de una búsqueda exitosa es la altura del nodo interno que contiene el dato buscado, el de una búsqueda fallida es la altura del nodo externo en que termina.

Bajo los supuestos indicados, el primer elemento de la permutación de  $n$  elementos (digamos que es  $k$ ) es la raíz del árbol, los elementos menores que  $k$  forman el subárbol izquierdo mientras los elementos mayores integran el subárbol derecho. Dado que todas las permutaciones se suponen igualmente probables, también lo son las permutaciones de los elementos que forman los subárboles. Sabemos que la función generatriz para permutaciones es:

$$\hat{P}(z) = \sum_{\sigma \in \mathcal{P}} \frac{z^{|\sigma|}}{|\sigma|!} \quad (23.45)$$

$$= \frac{1}{1-z} \quad (23.46)$$

Tenemos la función generatriz cumulativa del largo de camino interno:

$$\hat{I}(z) = \sum_{\sigma \in \mathcal{P}} \pi(\sigma) \frac{z^{|\sigma|}}{|\sigma|!} \quad (23.47)$$

Descomponemos según la raíz:

$$\hat{I}(z) = \sum_{\substack{\sigma_l \in \mathcal{P} \\ \sigma_r \in \mathcal{P}}} \binom{|\sigma_l| + |\sigma_r|}{|\sigma_l|} \frac{z^{|\sigma_l| + |\sigma_r| + 1}}{(|\sigma_l| + |\sigma_r| + 1)!} (\pi(\sigma_l) + \pi(\sigma_r) + |\sigma_l| + |\sigma_r|) \quad (23.48)$$

Derivamos para simplificar la suma:

$$\begin{aligned} \hat{I}'(z) &= \sum_{\substack{\sigma_l \in \mathcal{P} \\ \sigma_r \in \mathcal{P}}} \frac{z^{|\sigma_l|}}{|\sigma_l|!} \frac{z^{|\sigma_r|}}{|\sigma_r|!} (\pi(\sigma_l) + |\sigma_l| + \pi(\sigma_r) + |\sigma_r|) \\ &= 2\hat{I}(z)\hat{P}(z) + 2z\hat{P}(z)\hat{P}'(z) \\ &= \frac{2\hat{I}(z)}{1-z} + \frac{2z}{(1-z)^2} \end{aligned} \quad (23.49)$$

Condición inicial es que  $\hat{I}(0) = 0$ , ya que el árbol con un único nodo externo tiene  $\pi(\square) = 0$ . La solución de la ecuación diferencial (23.49) es:

$$\hat{I}(z) = \frac{2}{(1-z)^2} \ln \frac{1}{1-z} - \frac{2z}{(1-z)^3} \quad (23.50)$$

Esta es esencialmente la función generatriz (19.54) de la suma de números harmónicos, (19.55) da los coeficientes:

$$E_n[\pi] = 2(n+1)(H_{n+1} - 1) - 2n \quad (23.51)$$

$$\sim 2n \ln n \quad (23.52)$$

El costo promedio de una búsqueda exitosa es así:

$$\frac{E_n[\pi]}{n} \sim 2 \ln n \quad (23.53)$$

De forma similar tratamos búsquedas fallidas:

$$\hat{E}(z) = \sum_{\sigma \in \mathcal{P}} \xi(\sigma) \frac{z^{|\sigma|}}{|\sigma|!} \quad (23.54)$$

$$= \sum_{\substack{\sigma_l \in \mathcal{P} \\ \sigma_r \in \mathcal{P}}} \binom{|\sigma_l| + |\sigma_r|}{|\sigma_l|} \frac{z^{|\sigma_l| + |\sigma_r| + 1}}{(|\sigma_l| + |\sigma_r| + 1)!} (\xi(\sigma_l) + |\sigma_l| + 1 + \xi(\sigma_r) + |\sigma_r| + 1) \quad (23.55)$$

$$\begin{aligned} \hat{E}'(z) &= \sum_{\substack{\sigma_l \in \mathcal{P} \\ \sigma_r \in \mathcal{P}}} \frac{z^{|\sigma_l|}}{|\sigma_l|!} \frac{z^{|\sigma_r|}}{|\sigma_r|!} (\xi(\sigma_l) + \xi(\sigma_r) + |\sigma_l| + 1 + |\sigma_r| + 1) \\ &= 2\hat{E}(z)\hat{P}(z) + 2z\hat{P}(z)\hat{P}'(z) + 2\hat{P}^2(z) \\ &= \frac{2\hat{E}(z)}{1-z} + \frac{2}{(1-z)^3} \end{aligned} \quad (23.56)$$

Nuevamente, como  $\xi(\square) = 0$  es  $\hat{E}(0) = 0$ . Solución de la ecuación diferencial es:

$$\hat{E}(z) = \frac{2}{(1-z)^2} \ln \frac{1}{1-z} \quad (23.57)$$

De (19.55) tenemos los coeficientes:

$$[z^n]E(z) = 2(n+1)(H_{n+1} - 1)$$

El costo promedio de una búsqueda fallida resulta ser:

$$\frac{E_n[\xi]}{n+1} = 2(H_{n+1} - 1) \quad (23.58)$$

$$\sim 2 \ln n \quad (23.59)$$

## 23.2. Generatrices multivariadas

Una manera distinta de atacar el problema general que hemos planteado es usar funciones generatrices multivariadas. Consideraremos una clase  $\mathcal{A}$ , con objetos  $\alpha \in \mathcal{A}$  de tamaño  $|\alpha|$ ; y a su vez un parámetro, cuyo valor para  $\alpha$  es  $\chi(\alpha)$ . Como hasta ahora usaremos la indeterminada  $z$  para contabilizar tamaños, y usaremos la indeterminada  $u$  para marcar el valor del parámetro de interés. Si los átomos que componen  $\alpha$  son indistinguibles, es natural definir la función generatriz ordinaria:

$$A(z, u) = \sum_{\alpha \in \mathcal{A}} z^{|\alpha|} u^{\chi(\alpha)} \quad (23.60)$$

De la misma forma, si los átomos son distinguibles es apropiada la función generatriz exponencial:

$$\hat{A}(z, u) = \sum_{\alpha \in \mathcal{A}} \frac{z^{|\alpha|}}{|\alpha|!} u^{\chi(\alpha)} \quad (23.61)$$

Es común que nos interese el valor promedio de  $\chi(\alpha)$  para objetos de tamaño dado. Nótese que:

$$\frac{\partial A}{\partial u} = \sum_{\alpha \in \mathcal{A}} \chi(\alpha) u^{\chi(\alpha)-1} z^{|\alpha|} \quad (23.62)$$

Así podemos calcular los valores promedios a partir de los coeficientes de las siguientes sumas:

$$\sum_{\alpha \in \mathcal{A}} z^{|\alpha|} = A(z, 1) \quad (23.63)$$

$$\sum_{\alpha \in \mathcal{A}} \chi(\alpha) z^{|\alpha|} = \frac{\partial A}{\partial u} \Big|_{u=1} \quad (23.64)$$

Vemos que (23.63) no es más que la función generatriz (23.1) del número de objetos, mientras (23.64) es la función generatriz cumulativa (23.3).

En aras de brevedad, usaremos la notación:

$$A_z(z, u) = \frac{\partial A}{\partial z} \quad A_u(z, u) = \frac{\partial A}{\partial u} \quad (23.65)$$

En esto el subíndice indica el argumento de la función (o sea, primer y segundo argumento respectivamente en el ejemplo). Para derivadas parciales superiores anotamos por ejemplo:

$$A_{zz}(z, u) = \frac{\partial^2 A}{\partial z^2} \quad A_{uz}(z, u) = \frac{\partial^2 A}{\partial z \partial u} \quad A_{zu}(z, u) = \frac{\partial^2 A}{\partial u \partial z}$$

Nótese que el orden de los subíndices es el orden en que se deriva.

En particular, extraer los coeficientes de  $z^n$  de las sumas mencionadas entrega los valores necesarios:

$$E_n[\chi] = \frac{\sum_{|\alpha|=n} \chi(\alpha)}{a_n} \quad (23.66)$$

$$= \frac{[z^n] A_u(z, 1)}{[z^n] A(z, 1)} \quad (23.67)$$

Exactamente el mismo razonamiento se aplica a funciones generatrices exponenciales (los denominadores  $n!$  se cancelan).

La ventaja de esta línea de desarrollo frente al de la sección 23.1 es que la función generatriz multivariada contiene la distribución completa de los valores. En particular, vemos que la función generatriz de probabilidad (ver 16.2.1) de la medida  $\chi$  para objetos de tamaño  $n$  está dada por:

$$G_n(u) = \frac{[z^n] A(z, u)}{[z^n] A(z, 1)} \quad (23.68)$$

Aplicando (16.45) vemos que:

$$\text{var}_n[\chi] = G_n''(1) + G_n'(1) - (G_n'(1))^2 \quad (23.69)$$

$$= \frac{[z^n] A_{uu}(z, 1)}{[z^n] A(z, 1)} + \frac{[z^n] A_u(z, 1)}{[z^n] A(z, 1)} - \left( \frac{[z^n] A_u(z, 1)}{[z^n] A(z, 1)} \right)^2 \quad (23.70)$$

Cabe resaltar que en (23.70) se producirán importantes cancelaciones por la resta, se requieren valores precisos para los coeficientes para poder usarla. Esta fórmula se aplica sin cambios a funciones generatrices exponenciales, los factoriales de los denominadores se cancelan como ocurría en (23.9).

Repetiendo el primer ejemplo, obtengamos el número promedio de 0 en secuencias binarias de largo  $n$ . Estas secuencias quedan descritas por la expresión simbólica (compare con (23.10)):

$$\mathcal{S} = \text{SEQ}(\{0\} + \{1\}) \quad (23.71)$$

Usando  $z$  para tamaño (número total de símbolos) y  $u$  para el número de ceros, la función generatriz correspondiente a  $\{0\} + \{1\}$  es:

$$zu + z = z(1 + u) \quad (23.72)$$

con lo que al aplicar el método simbólico resulta:

$$S(z, u) = \frac{1}{1 - z(1 + u)} \quad (23.73)$$

Aplicando la técnica explicitada por (23.67) a (23.73) tenemos:

$$\begin{aligned} S(z, 1) &= \frac{1}{1 - 2z} \\ S_u(z, u) &= \frac{z}{(1 - z(1 + u))^2} \\ S_{uu}(z, 1) &= \frac{z}{(1 - 2z)^2} \end{aligned}$$

Nuevamente tenemos (23.16) para el promedio:

$$\begin{aligned} [z^n]S(z, 1) &= [z^n]\frac{1}{1 - 2z} = 2^n \\ [z^n]S_u(z, 1) &= [z^n]\frac{z}{(1 - 2z)^2} = n2^{n-1} \end{aligned}$$

En consecuencia, el número promedio de ceros es:

$$\frac{[z^n]S_u(z, 1)}{[z^n]S(z, 1)} = \frac{n2^{n-1}}{2^n} = \frac{n}{2} \quad (23.74)$$

Tal como esperábamos.

Vamos por la varianza:

$$\begin{aligned} S_{uu}(z, u) &= \frac{2z^2}{(1 - z - zu)^3} \\ S_{uu}(z, 1) &= \frac{2z^2}{(1 - 2z)^3} \\ [z^n]S_{uu}(z, 1) &= \frac{1}{2}\binom{n}{2}2^n \\ &= n(n-1)2^{n-2} \end{aligned}$$

Con (23.70) resulta la varianza del número de ceros en secuencias binarias de largo  $n$ :

$$\begin{aligned} \text{var}_n[\zeta] &= \frac{n(n-1)2^{n-2}}{2^n} + \frac{n2^{n-1}}{2^n} - \left(\frac{n2^{n-1}}{2^n}\right)^2 \\ &= \frac{n}{4} \end{aligned} \quad (23.75)$$

Un ejemplo más complejo es el algoritmo obvio para hallar el máximo de un arreglo, ver el listado 23.2. Todas las operaciones se efectúan  $n$  veces, salvo las actualizaciones a la variable  $m$ . Es evidente que el número de veces que se actualiza  $m$  es  $O(n)$ , pero interesa una respuesta más precisa.

---

```

1  double maximum(const double a[], const int n)
2  {
3      int i;
4      double m;
```

```

5
6     m = a[0];
7     for (i = 1; i < n; i++)
8         if (a[i] > m)
9             m = a[i];
10    return m;
11 }
```

---

Listado 23.2 – Hallar el máximo

Necesitamos un modelo para responder a la pregunta. Si suponemos que todos los valores son diferentes, y que todas las maneras de ordenarlos son igualmente probables, estamos buscando el número promedio de máximos de izquierda a derecha de permutaciones. Podemos describir la clase de permutaciones simbólicamente como en (23.18):

$$\mathcal{P} = \mathcal{E} + \mathcal{P} \star \mathcal{Z} \quad (23.76)$$

Si llamamos  $\chi(\sigma)$  al número de máximos de izquierda a derecha en la permutación  $\sigma$ , la función generatriz de probabilidad de que una permutación de tamaño  $n$  tenga  $k$  máximos de izquierda a derecha es:

$$M(z, u) = \sum_{\sigma \in \mathcal{P}} \frac{z^{|\sigma|}}{|\sigma|!} u^{\chi(\sigma)} \quad (23.77)$$

Esto casualmente es la función generatriz exponencial bivariada correspondiente a la clase (23.76).

Como el último elemento de la permutación es un máximo de izquierda a derecha si es el máximo de todos ellos, usando la convención de Iverson (ver la sección 1.5) podemos expresar el número de máximos de izquierda a derecha en la permutación resultante de  $\sigma \star (1)$  si se asigna el rótulo  $j$  al elemento nuevo como:

$$\chi(\sigma) + [j = |\sigma| + 1] \quad (23.78)$$

con lo que:

$$M(z, u) = \sum_{\sigma \in \mathcal{P}} \sum_{1 \leq j \leq |\sigma|+1} \frac{z^{|\sigma|+1}}{(|\sigma|+1)!} u^{\chi(\sigma)+[j=|\sigma|+1]} \quad (23.79)$$

$$\begin{aligned} &= \sum_{\sigma \in \mathcal{P}} \frac{z^{|\sigma|+1}}{(|\sigma|+1)!} u^{\chi(\sigma)} \sum_{1 \leq j \leq |\sigma|+1} u^{[j=|\sigma|+1]} \\ &= \sum_{\sigma \in \mathcal{P}} \frac{z^{|\sigma|+1}}{(|\sigma|+1)!} u^{\chi(\sigma)(|\sigma|+u)} \end{aligned} \quad (23.80)$$

Derivando respecto de  $z$ :

$$\begin{aligned} M_z(z, u) &= \sum_{\sigma \in \mathcal{P}} \frac{z^{|\sigma|}}{|\sigma|!} u^{\chi(\sigma)(|\sigma|+u)} \\ &= zM_z(z, u) + uM(z, u) \end{aligned}$$

Vale decir:

$$(1 - z)M_z(z, u) - uM(z, u) = 0 \quad (23.81)$$

En (23.81) la variable  $u$  interviene como parámetro, esta es una ecuación diferencial ordinaria. Como  $M(0, u) = 1$ , la solución es:

$$M(z, u) = \left( \frac{1}{1-z} \right)^u \quad (23.82)$$

$$= \sum_{n,k} \begin{bmatrix} n \\ k \end{bmatrix} \frac{z^n}{n!} u^k \quad (23.83)$$

Aparecen los números de Stirling de primera especie (22.26), o sea, hay tantas permutaciones de  $n$  elementos con  $k$  máximos de izquierda a derecha como permutaciones con  $k$  ciclos. Derivando respecto de  $u$ :

$$M_u(z, 1) = \frac{1}{1-z} \ln \frac{1}{1-z}$$

Reconocemos la función generatriz (19.3) de los números harmónicos, y el número promedio de asignaciones a  $m$  buscando el máximo entre  $n$  elementos resulta ser:

$$\mathbb{E}_n[\chi] = [z^n] M_u(z, 1) = H_n \quad (23.84)$$

$$= \ln n + \gamma + O(1/n) \quad (23.85)$$

Lo último de la expansión asintótica (18.13).

Para usar (16.45) calculamos:

$$M_{uu}(z, 1) = \frac{\ln^2(1-z)}{1-z} \quad (23.86)$$

Esta es la función (19.4) que analizamos en la sección 19.2. Con la definición de números harmónicos generalizados (19.5) resulta la elegante fórmula:

$$[z^n] M_{uu}(z, 1) = H_n^2 - H_n^{(2)} \quad (23.87)$$

Tenemos lo necesario para calcular la varianza:

$$\begin{aligned} \text{var}_n[\chi] &= [z^n] M_{uu}(z, 1) + [z^n] M_u(z, 1) - ([z^n] M_u(z, 1))^2 \\ &= H_n^2 - H_n^{(2)} + H_n - H_n \\ &= H_n - H_n^{(2)} \end{aligned} \quad (23.88)$$

Ilustramos el cálculo de los largos promedio de camino interno y externo en árboles binarios. Expresamos la clase de árboles binarios como en (23.26):

$$\mathcal{A} = \square + \bullet \times \mathcal{A} \times \mathcal{A} \quad (23.89)$$

Como al agregar una raíz la altura de cada nodo aumenta en uno (y la suma de las alturas aumenta en el número de nodos) podemos escribir para el largo de camino interno:

$$I(z, u) = 1 + z \sum_{\substack{\alpha_l \in \mathcal{A} \\ \alpha_r \in \mathcal{A}}} z^{|\alpha_l|} u^{\pi(\alpha_l) + |\alpha_l|} z^{|\alpha_r|} u^{\pi(\alpha_r) + |\alpha_r|} \quad (23.90)$$

$$\begin{aligned} &= 1 + z \left( \sum_{\alpha \in \mathcal{A}} (zu)^{|\alpha|} u^{\pi(\alpha)} \right)^2 \\ &= 1 + z I^2(zu, u) \end{aligned} \quad (23.91)$$

Derivando respecto de  $u$ :

$$\begin{aligned} I_u(z, u) &= 2zI(zu, u)(zI_z(zu, u) + I_u(zu, u)) \\ I_u(z, 1) &= 2zI(z, 1)(zI_z(z, 1) + I_u(z, 1)) \\ I_u(z, 1) &= \frac{2z^2 I(z, 1) I_z(z, 1)}{1 - 2zI(z, 1)} \end{aligned}$$

Pero  $I(z, 1) = A(z)$ , donde  $A(z)$  está dada por (23.29), con lo que  $I_z(z, 1) = A'(z)$ , y resulta:

$$\begin{aligned} I_u(z, 1) &= \frac{2z^2 A(z) A'(z)}{1 - 2zA(z)} \\ &= \frac{1 - 3z - (1-z)\sqrt{1-4z}}{z-4z^2} \end{aligned} \tag{23.92}$$

Esto es nuevamente (23.38).

De forma parecida podemos tratar el largo de camino externo. Siguiendo la misma descomposición del árbol, como  $\boxed{\alpha} = |\alpha| + 1$ :

$$E(z, u) = \sum_{\alpha \in \mathcal{A}} z^{|\alpha|} u^{\xi(\alpha)} \tag{23.93}$$

$$\begin{aligned} &= 1 + z \sum_{\substack{\alpha_l \in \mathcal{A} \\ \alpha_r \in \mathcal{A}}} z^{|\alpha_l|+|\alpha_r|} u^{\xi(\alpha_l)+(|\alpha_l|+1)+\xi(\alpha_r)+(|\alpha_r|+1)} \\ &= 1 + z \left( \sum_{\alpha \in \mathcal{A}} z^{|\alpha|} u^{\xi(\alpha)+|\alpha|+1} \right)^2 \\ &= 1 + zu^2 \left( \sum_{\alpha \in \mathcal{A}} (zu)^{|\alpha|} u^{\xi(\alpha)} \right)^2 \\ &= 1 + zu^2 E^2(zu, u) \end{aligned} \tag{23.94}$$

Como antes, derivando ambos lados respecto de  $u$ :

$$\begin{aligned} E_u(z, u) &= 2zuE^2(zu, u) + 2zu^2E(zu, u)(zE_z(zu, u) + E_u(zu, u)) \\ E_u(z, 1) &= 2zE^2(z, 1) + 2zE(z, 1)(zE_z(z, 1) + E_u(z, 1)) \end{aligned}$$

Despejando, como  $E(z, 1) = A(z)$ :

$$\begin{aligned} E_u(z, 1) &= \frac{2zA^2(z) + 2z^2 A(z) A'(z)}{1 - 2zA(z)} \\ &= \frac{1 - \sqrt{1-4z}}{1-4z} \end{aligned} \tag{23.95}$$

Nuevamente (23.42), que da el promedio asintótico (23.44).

Si construimos árboles binarios insertando claves en orden aleatorio, la distribución es diferente. Para el largo de camino interno tenemos:

$$\hat{I}(z, u) = \sum_{\alpha \in \mathcal{P}} \frac{z^{|\alpha|}}{|\alpha|!} u^{\pi(\alpha)} \tag{23.96}$$

$$= 1 + \sum_{\substack{\alpha_l \in \mathcal{P} \\ \alpha_r \in \mathcal{P}}} \binom{|\alpha_l|+|\alpha_r|}{|\alpha_l|} \frac{z^{|\alpha_l|+|\alpha_r|+1}}{(|\alpha_l|+|\alpha_r|+1)!} u^{\pi(\alpha_l)+\alpha_l+\pi(\alpha_r)+\alpha_r} \tag{23.97}$$

Para simplificar, derivamos respecto de  $z$ :

$$\begin{aligned}\widehat{I}_z(z, u) &= \sum_{\substack{\alpha_l \in \mathcal{P} \\ \alpha_r \in \mathcal{P}}} \binom{|\alpha_l| + |\alpha_r|}{|\alpha_l|} \frac{z^{|\alpha_l| + |\alpha_r|}}{(|\alpha_l| + |\alpha_r|)!} u^{\pi(\alpha_l) + \alpha_l + \pi(\alpha_r) + \alpha_r} \\ &= \sum_{\substack{\alpha_l \in \mathcal{P} \\ \alpha_r \in \mathcal{P}}} \frac{(zu)^{|\alpha_l|}}{|\alpha_l|!} u^{\pi(\alpha_l)} \cdot \frac{(zu)^{|\alpha_r|}}{|\alpha_r|!} u^{\pi(\alpha_r)} \\ &= \widehat{I}^2(zu, u)\end{aligned}\tag{23.98}$$

Nos interesan las derivadas  $\widehat{I}_u(z, 1)$  y  $\widehat{I}_{uu}(z, 1)$ , ya sabemos que  $\widehat{I}(z, 1) = (1 - z)^{-1}$ . Tenemos:

$$\widehat{I}_{zu}(z, u) = 2\widehat{I}(zu, u)(z\widehat{I}_z(zu, u) + \widehat{I}_u(zu, u))\tag{23.99}$$

$$\begin{aligned}\widehat{I}_{zvu}(z, u) &= 2(z\widehat{I}_z(zu, u) + \widehat{I}_u(zu, u))^2 \\ &\quad + 2\widehat{I}(zu, u)(z^2\widehat{I}_{zz}(zu, u) + z\widehat{I}_{zu}(zu, u) + z\widehat{I}_{uz}(zu, u) + \widehat{I}_{uu}(zu, u))\end{aligned}\tag{23.100}$$

Por el teorema de Schwartz (también conocido como teorema de Clairaut, ver textos de cálculo, como Zakon [367] o Thomson, Bruckner y Bruckner [349, teorema 12.5]) si las derivadas son continuas se cumple que:

$$f_{xy}(x, y) = f_{yx}(x, y)$$

En general, podemos permutar el orden de derivación a gusto si alguna de las derivadas de interés es continua. En nuestro caso, al ser  $[z^n]\widehat{I}(z, u)$  un polinomio en  $u$  y  $\widehat{I}(z, 1) = (1 - z)^{-1}$ , que tiene infinitas derivadas continuas en  $z = 0$ , las derivadas que nos interesan en  $z = 0$ ,  $u = 1$  siempre existen y son continuas. Reordenando derivadas en (23.99) y (23.100), evaluando para  $u = 1$  resulta:

$$\widehat{I}_{uz}(z, 1) = 2\widehat{I}(z, 1)(z\widehat{I}_z(z, 1) + \widehat{I}_u(z, 1))$$

$$\widehat{I}_{uuz}(z, 1) = 2(z\widehat{I}_z(z, 1) + \widehat{I}_u(z, 1))^2 + 2\widehat{I}(z, 1)(z^2\widehat{I}_{zz}(z, 1) + 2z\widehat{I}_{uz}(z, 1) + \widehat{I}_{uu}(z, 1))$$

Despejando:

$$\widehat{I}_{uz}(z, 1) = \frac{2\widehat{I}_u(z, 1)}{1 - z} + \frac{2z}{(1 - z)^3}\tag{23.101}$$

Condiciones iniciales para las ecuaciones diferenciales (23.101) y su similar de (23.100) da la condición  $[z^0]\widehat{I}(z, u) = 1$ , de donde  $\widehat{I}_u(0, 1) = 0$ , con lo que:

$$\widehat{I}_u(z, 1) = 2\frac{1}{(1 - z)^2} \ln \frac{1}{1 - z} - \frac{z}{(1 - z)^2}\tag{23.102}$$

y también, reemplazando (23.102) en (23.100) y resolviendo la ecuación diferencial resultante, donde nuestra condición anterior ahora da  $\widehat{I}_{uu}(0, 1) = 0$ :

$$\widehat{I}_{uu}(z, 1) = \frac{1}{(1 - z)^3} \left( 4(1 + z) \ln^2 \frac{1}{1 - z} - 4(1 + z) \ln \frac{1}{1 - z} + 2z^2 + 4z \right)\tag{23.103}$$



## 24 Grafos

---

Un grafo corresponde a una abstracción de la situación en la cual hay objetos (*vértices*), algunos de los cuales están conectados entre sí (mediante *arcos*). El interés es razonar solo con el hecho que existen o no conexiones entre los vértices. Esta área es una de las más antiguas entre lo que se conoce como matemáticas discretas, con un amplio rango de aplicaciones. Los grafos (y estructuras afines) sirven para abstraer y representar objetos del más variado tipo, desde redes de transporte hasta rangos de validez de valores al analizar el código de un programa, pasando por aplicaciones como asignación de horarios.

Como modelan una variedad de situaciones, estudiamos algoritmos para efectuar operaciones comunes sobre grafos. Demostraremos que son correctos, y daremos un somero análisis de su rendimiento.

### 24.1. Algunos ejemplos de grafos

Aplicaciones de grafos son circuitos eléctricos, donde interesa cómo están conectados entre sí los componentes (ver un ejemplo en la figura 24.1) y representaciones de redes de transporte, como

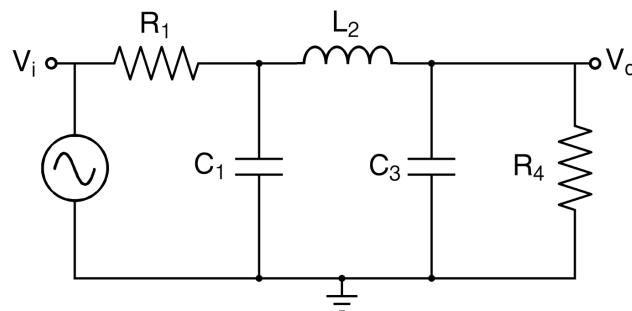


Figura 24.1 – Diagrama de circuito de un filtro de paso bajo de tercer orden [244]

el esquema 24.2 de la red de metro de Londres en 1908.

En computación los grafos son ubicuos porque son una forma cómoda de representar relaciones entre objetos, como programas o personas. Un arco puede representar que dos personas se llevan bien (o no), que un ramo debe tomarse antes de otro, o que una función llama a otra. Muchas estructuras de datos, particularmente las enlazadas, pueden representarse mediante grafos, y muchos problemas de optimización importantes se modelan mediante grafos. También sirven como notación gráfica de algunos modelos de computación. Una advertencia: A pesar de ser un área bastante antigua de las matemáticas, aún no hay consenso en la notación o la nomenclatura. Curiosamente, recién en 1936 Kőnig publicó el primer texto sobre teoría de grafos [223], cuando el

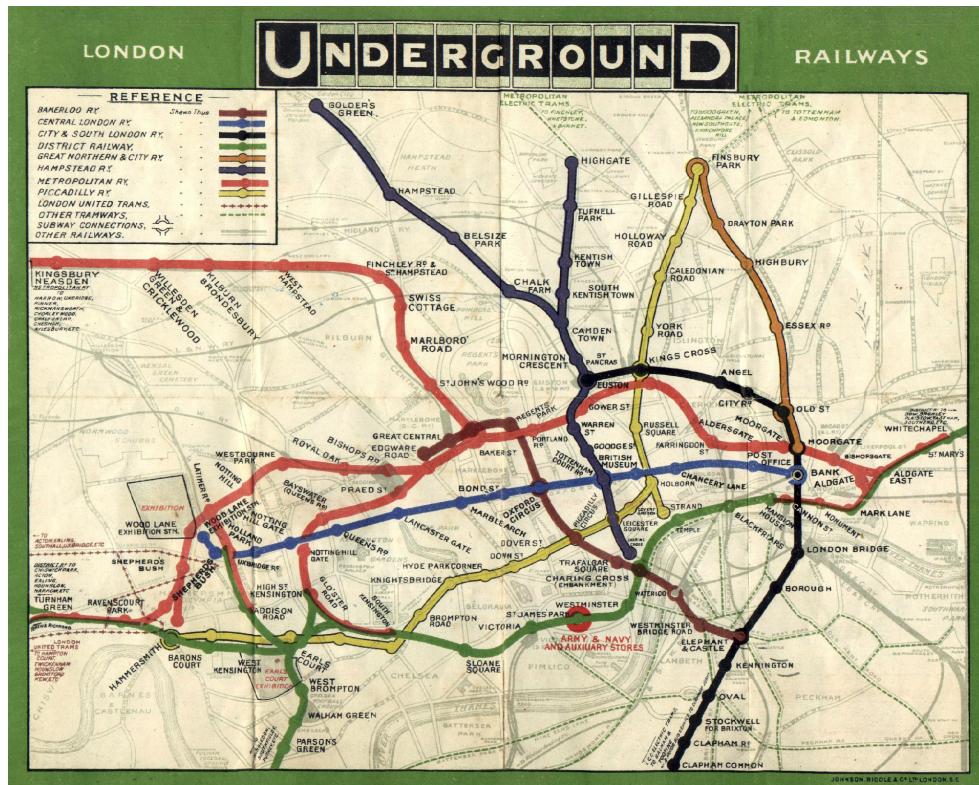


Figura 24.2 – Esquema del metro de Londres (1908) [242]

área data de la época de Euler (1707–1783). En caso de duda, revise las definiciones dadas por el autor. Acá usaremos básicamente la notación y nomenclatura de uno de los textos estándar del área, el de Diestel [91]. Un tratamiento más accesible para no especialistas es el de Ore [276].

Formalmente:

**Definición 24.1.** Un grafo  $G = (V, E)$  consta de:

**V:** Conjunto finito no vacío de vértices.

**E:** Conjunto de arcos, pares de vértices pertenecientes a  $V$ . Un arco  $\{a, b\} \in E$  consta de  $a, b \in V$ .

Para nuestros efectos no interesa el caso de conjuntos infinitos de vértices. Al número de vértices de un grafo se le llama su *orden*. Consideramos en esta definición que un arco conecta un par de vértices diferentes (sin importar el orden), y no pueden haber varios arcos uniendo el mismo par de vértices. A veces para abreviar se anota  $ab$  por el arco  $\{a, b\}$ . En tal caso  $ab = ba$ .

Dos vértices contenidos en un arco se llaman *adyacentes* o *vecinos*. Al número de arcos en que participa un vértice se llama su *grado*. Si todos los vértices del grafo tienen el mismo grado, el grafo se llama *regular*, que para el vértice  $v$  se anota  $\delta(v)$ . Un arco que contiene al vértice  $v$  se dice *incide* en él. Dos arcos que tienen un vértice en común también se llaman *adyacentes*. Si de un grafo  $G = (V, E)$  se eliminan arcos o vértices (con los arcos que los contienen) el resultado  $G' = (V', E')$  es un *subgrafo* de  $G$ . El *vecindario* de  $v$  son los vértices adyacentes a él, anotamos  $N_G(v) = \{v_1, v_2, \dots, v_k\}$  si  $\{v, v_i\} \in E$ . Normalmente omitiremos el subíndice que identifica al grafo cuando es claro del contexto.

Para evitar notación engorrosa, identificaremos el grafo  $G = (V, E)$  con su conjunto de vértices o arcos. Así, diremos simplemente  $v \in G$  para indicar  $v \in V$ ,  $uv \in G$  cuando  $\{u, v\} \in E$  o  $G \setminus uv$  para el grafo  $G' = (V, E \setminus \{u, v\})$ .

Se dice que el grafo  $G' = (V', E')$  es un *subgrafo* del grafo  $G = (V, E)$  si  $V' \subseteq V$  y  $E' \subseteq E$ . Decir que  $G'$  es un grafo hace que los vértices que aparecen en  $E'$  están en  $V'$ , y hace también que  $V' \neq \emptyset$ .

Variantes de grafos son *multigrafos*, en los cuales se permiten varios arcos entre el mismo par de vértices, e incluso arcos que comienzan y terminan en el mismo vértice. Muchas de nuestras conclusiones se aplican a ellos también, pero no los trataremos explícitamente.

Como los grafos son empleados en muchas áreas, los nombres suelen ajustarse al área bajo estudio, por ejemplo a veces se les llama *redes*. Los vértices pueden llamarse también *nodos* o *puntos*, y hay quienes hablan de *aristas* en vez de arcos. Nosotros excluimos la posibilidad  $V = \emptyset$ , dado que resulta un contraejemplo trivial a muchos teoremas importantes. Al dejar fuera este caso muchos resultados se pueden expresar en forma más simple, sin embargo esta convención no es universal. En general, hay consenso en el significado de los términos, pero el tratamiento de casos excepcionales varía.

Al dibujar grafos se representan los vértices mediante puntos y los arcos mediante líneas que los unen. Los vértices normalmente no se identifican. Notar que  $u$  conectado con  $v$  o  $v$  conectado con  $u$ , para el caso significa lo mismo. No importa la ruta o el largo del arco, ni si accidentalmente cruza otros. Sólo el hecho que un par de vértices están conectados importa.

**Ejemplo 24.1.** Definición de un grafo.

$G$  dado por:

$$V = \{a, b, c, d, z\}$$

$$E = \{\{a, d\}, \{b, z\}, \{c, d\}, \{d, z\}\}$$

Gráficamente está dado por la figura 24.3.

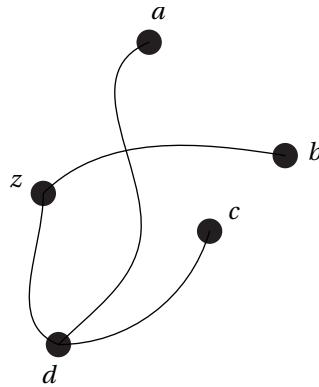


Figura 24.3 – Un grafo

## 24.2. Representación de grafos

Un dibujo es útil para seres humanos, pero bastante inútil para razonar con él o para el uso en computadoras. Veremos algunas opciones adicionales.

### 24.2.1. Lista de adyacencia

La *lista de adyacencia* es una tabla donde para cada vértice se listan los vértices adyacentes. Para el caso del grafo de la figura 24.3 se tiene la lista de adyacencia en el cuadro 24.1.

V	Ady
a	d
b	z
c	d
d	a, c, z
z	b, d

Cuadro 24.1 – Lista de adyacencia para el grafo de la figura 24.3

### 24.2.2. Matriz de adyacencia

Representar un grafo mediante una *matriz de adyacencia* corresponde a definir una matriz cuyos índices son los vértices, y los elementos son 1 o 0 dependiendo de si los vértices del caso están conectados o no. El grafo de la figura 24.3 queda representado en el cuadro 24.2. Es claro que esta

	a	b	c	d	z
a	0	0	0	1	0
b	0	0	0	0	1
c	0	0	0	1	0
d	1	0	1	0	1
z	0	1	0	1	0

Cuadro 24.2 – Matriz de adyacencia del grafo de la figura 24.3

matriz es simétrica (vale decir,  $a[i, j] = a[j, i]$ ) ya que  $i$  conectado a  $j$  es lo mismo que  $j$  conectado a  $i$ . Los elementos en la diagonal son todos cero porque no hay arcos que conectan vértices consigo mismos.

Los multigrafos permiten rizos (en inglés *loops*) que conectan vértices consigo mismos. En tal caso la diagonal no necesariamente es ceros. Si hay más de un arco entre un par de vértices, es natural considerar que la entrada de la matriz es el número de arcos entre los vértices. Igualmente, si consideramos que el arco tiene dirección (va de  $u$  a  $v$ ), resulta una matriz no necesariamente simétrica (estamos representando *grafos dirigidos*, que se discuten en mayor detalle en el capítulo 25).

### 24.2.3. Representación enlazada

Una opción es representar los vértices por nodos con punteros que lo conectan a sus vecinos. Como el número de vecinos no necesariamente es el mismo (o siquiera razonablemente acotado) es natural que cada nodo tenga una lista de punteros a los vecinos (terminan siendo las listas de adyacencia).

### 24.2.4. Representación implícita

En muchas aplicaciones el grafo nunca existe como estructura de datos, se van generando (y descartando) los vértices vecinos conforme se requieren. Un ejemplo de esta situación se da cuando un programa juega al ajedrez: Los nodos son posiciones de las piezas, y dos nodos son adyacentes si

son posiciones relacionadas mediante una movida. El grafo del caso es finito, pero tan grande que es totalmente impracticable generarlo completo (y aún menos almacenarlo). Se van generando los vértices conforme los requiera el programa.

### 24.3. Isomorfismo entre grafos

Intuitivamente, si dos grafos pueden dibujarse de la misma forma, los consideraremos iguales. Sin embargo, como los conjuntos de vértices (y en consecuencia, arcos) no serán los mismos, esta idea debe interpretarse de otra forma.

**Definición 24.2.** Si  $G_1 = (V_1, E_1)$  y  $G_2 = (V_2, E_2)$  son grafos se dice que son *isomorfos* si existe una biyección  $\alpha: V_1 \rightarrow V_2$  tal que  $\{\alpha(u), \alpha(v)\} \in E_2$  exactamente cuando  $\{u, v\} \in E_1$ . En tal caso se anota  $G_1 \cong G_2$ .

Nótese que esto es coherente con lo que indicamos antes, en que los vértices no se identifican. Cuando hablamos de un grafo en realidad estamos refiriéndonos a una clase de grafos isomorfos.

Una regla simple que resulta de la definición es que el número de vértices y arcos es el mismo entre grafos isomorfos. Al buscar isomorfismos solo deben considerarse como candidatos vértices del mismo grado, y vértices adyacentes deberán mapear a vértices adyacentes. La figura 24.4 muestra un par de grafos isomorfos, indicando las correspondencias entre vértices. Otro par de grafos isomorfos

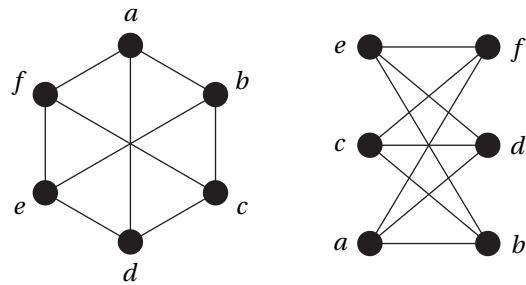


Figura 24.4 – Ejemplo de isomorfismo entre grafos

dan la figura 24.5. De los ejemplos se nota que incluso para grafos más bien chicos no es posible

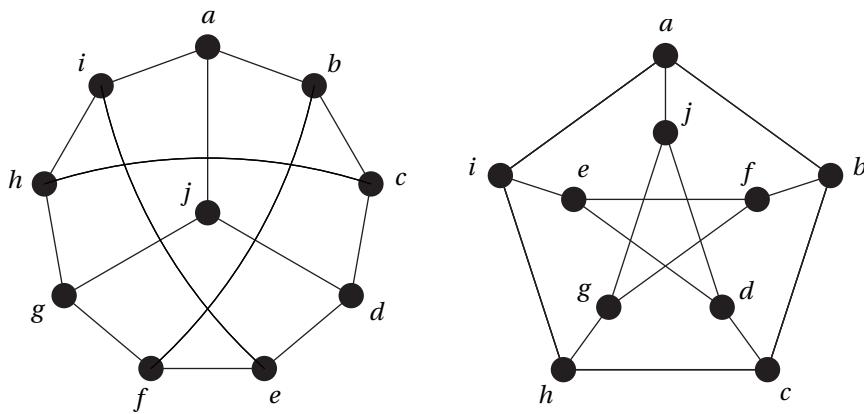


Figura 24.5 – Dos formas de dibujar el grafo de Petersen [200, 280]

determinar a simple vista si son isomorfos. Resulta que el problema de determinar si dos grafos son isomorfos es NP-completo, una categoría de problemas difíciles introducida por Cook [78] para los cuales no se conocen algoritmos que tomen un tiempo razonable. Para la definición precisa véanse textos de algoritmos y teoría de autómatas, como [4, 179, 277], y a Garey y Johnson [141] para un tratamiento detallado. El problema de isomorfismo de grafos fue uno de los primeros problemas clásicos demostrado NP-completo.

#### 24.4. Algunas familias de grafos especiales

Algunos grafos se repiten en aplicaciones, o son útiles para ejemplos y casos de estudio. Se les dan nombres y notación especiales.

- $P_n$ : Camino simple de  $n$  vértices, donde  $n \geq 2$ , ver la figura 24.6. Tiene  $n - 1$  arcos, los vértices son de grados 1 y 2.

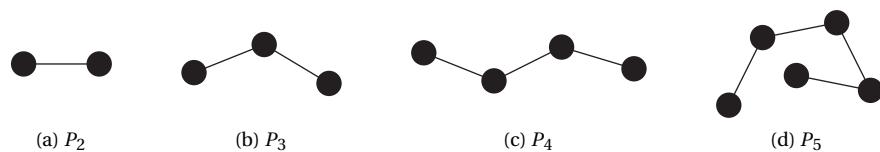


Figura 24.6 – Algunos grafos  $P_n$

- $C_n$ : Ciclo de  $n$  vértices, donde el vértice  $i$  está conectado con los vértices  $i - 1$  e  $i + 1$  módulo  $n$ . Para que sea realmente un ciclo, es  $n \geq 3$ . Tiene  $n$  arcos, es regular de grado 2. Ver figura 24.7.

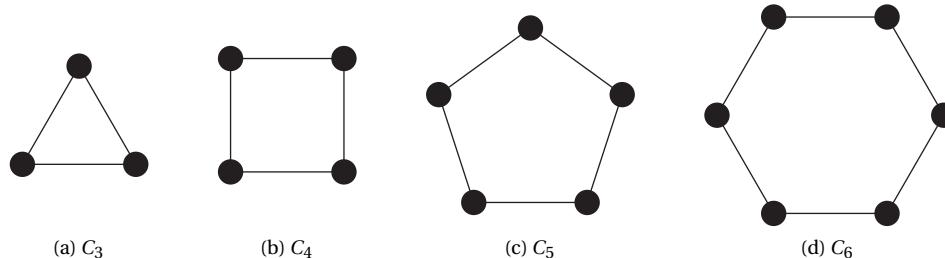
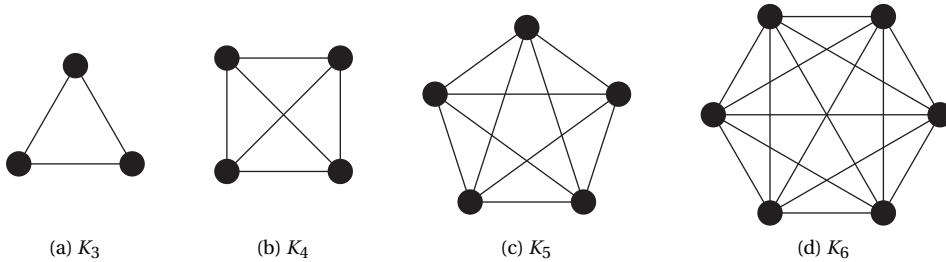
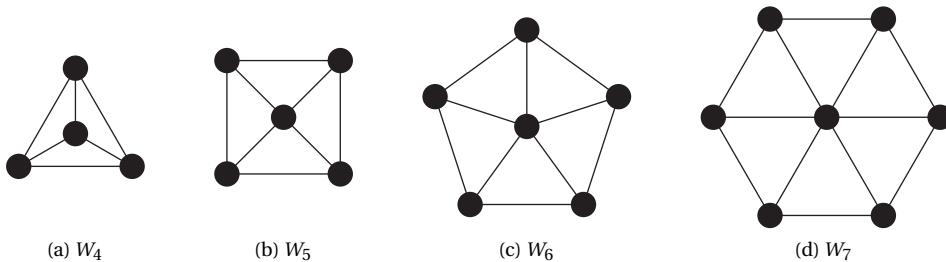


Figura 24.7 – Algunos grafos  $C_n$

- $K_n$ : Grafo completo de  $n$  vértices cada uno conectado con todos los demás, con  $n \geq 1$ . Tiene  $n(n - 1)/2$  arcos, es regular de grado  $n - 1$ . La figura 24.8 muestra algunos ejemplos.
- $W_n$ : Rueda (en inglés *wheel*) de  $n$  vértices, que consiste en un grafo  $C_{n-1}$  más un “centro” conectado a cada vértice del ciclo. Nótese que algunos autores llaman  $W_n$  a  $W_{n+1}$  (solo cuentan los vértices de afuera). Tiene  $2(n - 1)$  arcos,  $n - 1$  vértices de grado 3 y uno de grado  $n - 1$ . Algunas ruedas muestran la figura 24.9.
- $Q_n$ : Cubo de orden  $n$ . Donde:

**Vértices:** Secuencias de  $n$  símbolos  $\{0, 1\}$ .

Figura 24.8 – Algunos grafos  $K_n$ Figura 24.9 – Algunos grafos  $W_n$ 

**Arcos:** Conectan a todos los pares de vértices que difieren en un símbolo.

Nótese que el número de vértices es  $2^n$ . Tiene  $n2^{n-1}$  arcos, es regular de grado  $n$ . La figura 24.10 muestra algunos grafos  $Q_n$ .

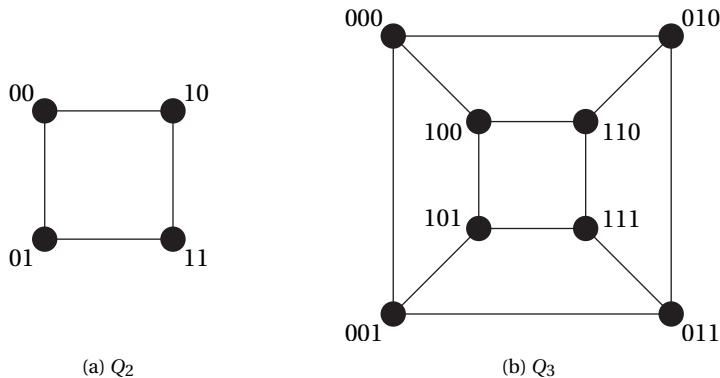


Figura 24.10 – Algunos cubos

Resulta que  $C_3 \cong K_3$ ,  $Q_2 \cong C_4$  y  $W_4 \cong K_4$ .

## 24.5. Algunos resultados simples

Algunos teoremas simples de demostrar son sorprendentemente útiles.

**Teorema 24.1.** *Sea  $G = (V, E)$  un grafo, entonces:*

$$\sum_{v \in V} \delta(v) = 2 \cdot |E|$$

*Demostración.* Consideremos  $S \subseteq V \times E$  tal que  $(v, e) \in S$  siempre que  $v \in e$ . Contando los elementos de  $S$  “por filas” y “por columnas” (ver la discusión respectiva en el capítulo 13) tenemos:

**Por filas:** Cada vértice aparece una vez por cada arco en el cual participa:

$$|S| = \sum_{v \in V} \delta(v)$$

**Por columnas:** Cada vértice aparece dos veces (una por cada extremo del arco):

$$|S| = \sum_{e \in E} 2 = 2 \cdot |E|$$

Estas dos expresiones deben ser iguales, lo que corresponde precisamente a lo que se quería demostrar.  $\square$

**Lema 24.2** (Handshaking). *El número de vértices de grado impar en un grafo es par.*

*Demostración.* Sean  $V_o$  los vértices de grado impar y  $V_e$  los vértices de grado par del grafo. Entonces:

$$\sum_{v \in V_o} \delta(v) + \sum_{v \in V_e} \delta(v) = 2 \cdot |E|$$

El lado derecho de esta ecuación es par. El segundo término del lado izquierdo es una suma de números pares, por lo que es par. Con esto, el primer término debe ser par, pero es la suma de números impares. Esto significa que hay un número par de estos, que es exactamente lo que se quería demostrar.  $\square$

## 24.6. Secuencias gráficas

Nos interesa resolver problemas como el siguiente:

**Ejemplo 24.2.** ¿Es posible tener grafos con vértices de grados 1, 2, 2, 3, 4?

Es factible dibujar este grafo, ver figura 24.11.

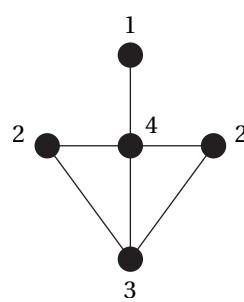


Figura 24.11 – Un grafo con grados 1, 2, 2, 3 y 4

Diremos que una secuencia de enteros es *gráfica* si corresponde a los grados de los vértices de un grafo. Hay algunas condiciones simples, como que el número de vértices de grado impar debe ser par (lema 24.2) y que el grado máximo debe ser menor que el número de vértices. Para determinar si una secuencia es gráfica veremos primero cómo reorganizar los arcos sin afectar los grados de los vértices. Esto lo usaremos para modificar grafos de forma que responder la pregunta sea más fácil.

**Definición 24.3.** En un grafo  $G = (V, E)$  un *2-switch* respecto de los arcos  $uv, xy \in E$  (donde  $ux, vy \notin E$ ) reemplaza esos arcos por  $ux$  y  $vy$ . Denotamos  $G \xrightarrow{2s} H$  si se puede obtener  $H$  de  $G$  mediante una secuencia finita de 2-switch.

Para ilustración véase la figura 24.12. Nótese que si  $G \xrightarrow{2s} H$  entonces también  $H \xrightarrow{2s} G$ , ya que

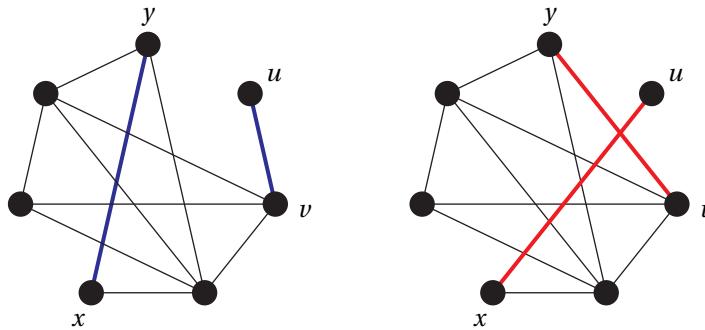


Figura 24.12 – La operación 2-switch entre los arcos  $uv$  y  $xy$

podemos aplicar la secuencia en el orden inverso. En realidad, esta es una relación de equivalencia (es reflexiva, ya que no hacer nada equivale a aplicar 0 2-switch; es claro que es transitiva; y es simétrica porque podemos aplicar una secuencia de 2-switch al revés en orden inverso). Antes de demostrar el teorema de Berge, vemos que podemos ordenar los arcos de forma que conecten los vértices en orden de grado decreciente:

**Lema 24.3.** *Sea  $G$  un grafo de orden  $n$ , con  $\delta_G(v_i) = d_i$  tal que  $d_1 \geq d_2 \geq \dots \geq d_n$ . Entonces hay un grafo  $G'$  tal que  $G \xrightarrow{2s} G'$  con  $N_{G'}(v_1) = \{v_2, v_3, \dots, v_{d_1+1}\}$ .*

*Demuestração.* Consideremos un grafo con los vértices ordenados según grado decreciente en que lo indicado no se cumple, o sea, hay un primer vértice  $v_i$  con  $2 \leq i \leq d_1 + 1$  tal que  $v_1 v_i \notin E$ . Demostremos que un 2-switch corrige esto para ese vértice, repitiendo el proceso logramos lo prometido.

Como  $\delta_G(v_1) = d_1$ , hay  $v_j$  con  $j \geq d_1 + 2$  tal que  $v_1 v_j \in E$ . Debe ser  $d_i \geq d_j$ , ya que  $i < j$ . Como  $v_1 v_j \in E$ , es  $d_j = \delta_G(v_j) \geq 1$ . Así sabemos que  $v_j$  es adyacente a  $v_1$  y a  $d_j - 1$  otros vértices, mientras  $v_i$  es adyacente a  $d_i$  vértices que no incluyen a  $v_1$ . Como por el orden de los vértices  $d_i \geq d_j > d_j - 1$ , los conjuntos  $N(v_i)$  y  $N(v_j) \setminus \{v_1\}$  no pueden coincidir (por ser de tamaños diferentes); o sea hay algún  $t \neq 1$  tal que  $v_i v_t \in E$  pero  $v_j v_t \notin E$ . Aplicando un 2-switch a  $v_1 v_j$  y  $v_i v_t$  (son arcos  $v_1 v_j$  y  $v_i v_t$  y no están unidos  $v_1$  con  $v_i$  ni  $v_j$  con  $v_t$ , con lo que esta operación es válida) ninguno de los vértices involucrados cambia de grado y se intercambian  $v_i$  con  $v_j$  en el vecindario de  $v_1$ . Aplicando repetidas veces esta operación obtendremos lo prometido.  $\square$

Ahora podemos demostrar:

**Teorema 24.4** (Berge, 1973). *Dos grafos  $G$  y  $H$  sobre el mismo conjunto de vértices  $V$  satisfacen  $\delta_G(v) = \delta_H(v)$  para todo  $v \in V$  si y solo si  $G \xrightarrow{2s} H$ .*

*Demostración.* Demostramos implicancia en ambos sentidos. Ya vimos que al aplicar un 2-switch el grado de los vértices no cambia, con lo que si  $G \xrightarrow{2s} H$  entonces los vértices tienen los mismos grados en ambos.

Para demostrar necesidad, aplicamos inducción sobre el número de vértices en  $G$ . La base,  $|V| = 1$  es trivial. Para inducción, por el lema 24.3, si elegimos el vértice  $v$  de grado máximo en  $G$  y  $H$ , hay grafos  $G'$  y  $H'$  tales que  $G \xrightarrow{2s} G'$  y  $H \xrightarrow{2s} H'$  y tales que  $N_{G'}(v) = N_{H'}(v)$ . Si eliminamos  $v$  de  $G'$  y  $H'$  obteniendo grafos  $G''$  y  $H''$ , ambos tienen los mismos grados ya que estamos eliminando los mismos arcos de  $G'$  y  $H'$ . Por la hipótesis de inducción,  $G'' \xrightarrow{2s} H''$ , y por tanto también  $G' \xrightarrow{2s} H'$ . Esto basta para demostrar lo aseverado, dado que es una relación de equivalencia.  $\square$

Con estas herramientas estamos en posición de atacar nuestro problema original.

**Definición 24.4.** Sea  $\langle d_1, d_2, d_3, \dots, d_n \rangle$  una secuencia descendente de números naturales, o sea,  $d_1 \geq d_2 \geq d_3 \geq \dots \geq d_n$ . Tal secuencia se dice *gráfica* si hay un grafo  $G = (V, E)$  con  $V = \{v_1, v_2, \dots, v_n\}$  tal que  $d_i = \delta(v_i)$ .

Entonces<sup>1</sup>:

**Teorema 24.5** (Havel-Hakimi). *Una secuencia  $d_1 \geq d_2 \geq d_3 \geq \dots \geq d_n$  (con  $d_1 \geq 1$  y  $n \geq 2$ ) es gráfica si y solo si lo es la secuencia siguiente ordenada de mayor a menor:*

$$d_2 - 1, d_3 - 1, \dots, d_{d_1+1} - 1, d_{d_1+2}, d_{d_1+3}, \dots, d_n$$

*Demostración.* Demostramos implicancias en ambas direcciones. Para el recíproco, consideremos un grafo  $G$  de orden  $n - 1$  con vértices y grados:

$$\delta_G(v_2) = d_2 - 1, \dots, \delta_G(v_{d_1+1}) = d_{d_1+1} - 1, \delta_G(v_{d_1+2}) = d_{d_1+2}, \dots, \delta_G(v_n) = d_n.$$

Agregue el vértice  $v_1$  con arcos  $v_1 v_i$  para  $2 \leq i \leq d_1 + 1$  para dar el grafo  $H$ , que cumple  $\delta_H(v_1) = d_1$ , y  $\delta_H(v_i) = d_i$  para todo  $2 \leq i \leq n$ .

Para el directo, suponga un grafo  $G$  tal que  $\delta_G(v_i) = d_i$  para  $1 \leq i \leq n$ . Por el lema 24.3 podemos suponer que  $N_G(v_1) = \{v_2, \dots, v_{d_1+1}\}$ . Si eliminamos el vértice  $v_1$  de  $G$  obtenemos un grafo con la secuencia de grados indicada.  $\square$

Aplicando repetidas veces el teorema de Havel-Hakimi, teorema 24.5, podemos determinar rápidamente si una secuencia es o no gráfica. Por ejemplo, considérese la secuencia  $\langle 4, 4, 4, 3, 2, 1 \rangle$ . Tenemos:

$$\begin{aligned} \langle 4, 4, 4, 3, 2, 1 \rangle &\text{ es gráfica si y solo si } \langle 3, 3, 2, 1, 1 \rangle \text{ es gráfica} \\ &\text{ es gráfica si y solo si } \langle 2, 1, 1, 0 \rangle \text{ es gráfica} \\ &\text{ es gráfica si y solo si } \langle 0, 0, 0 \rangle \text{ es gráfica} \end{aligned}$$

Esta última corresponde al grafo de tres vértices y sin arcos, por lo que es gráfica.

El teorema de Havel-Hakimi da una forma de construir un grafo con los grados prescritos: Se ordenan los grados de mayor a menor, luego el vértice  $v_1$  está conectado con  $v_2$  a  $v_{d_1+1}$ , el vértice  $v_2$  se conecta con los siguientes desde  $v_{d_1+2}$  hasta completar su grado, y así sucesivamente. Donde

---

<sup>1</sup>Según Allenby y Slomson [10, página 159], Havel [170] publicó este resultado en checo, Hakimi [158] es independiente del resultado previo.

en el proceso se reordenan los grados deben reordenarse los vértices de la misma manera. Para un ejemplo de este proceso, tomemos:

$$\begin{aligned}
 & \langle 8, 8, 6, 5, 4, 3, 3, 3, 1, 1 \rangle \rightarrow \langle 7, 5, 4, 3, 2, 2, 2, 0, 1 \rangle & v_{10} \text{ pasa a } v_9 \\
 & \quad \langle 7, 5, 4, 3, 2, 2, 2, 1, 0 \rangle \\
 & \quad \rightarrow \langle 4, 3, 2, 1, 1, 1, 0, 0 \rangle \\
 & \quad \rightarrow \langle 2, 1, 0, 0, 1, 0, 0 \rangle & v_8 \text{ pasa a } v_6 \\
 & \quad \langle 2, 1, 1, 0, 0, 0, 0 \rangle \\
 & \rightarrow \langle 0, 0, 0, 0, 0, 0 \rangle
 \end{aligned}$$

La última secuencia es gráfica (son seis vértices aislados). Los comentarios indican los cambios de posición que sufrieron los vértices: Se intercambiaron  $v_9$  con  $v_{10}$ ; luego  $v_6$  fue a  $v_7$ ,  $v_7$  a  $v_8$  y  $v_8$  pasó a  $v_6$ . La figura 24.13 muestra el grafo resultante.

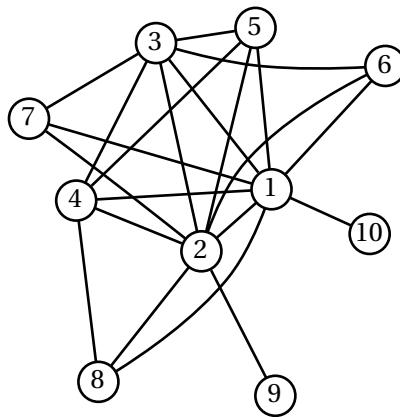


Figura 24.13 – Un grafo con vértices de grados  $\langle 8, 8, 6, 5, 4, 3, 3, 3, 1, 1 \rangle$

**Definición 24.5.**  $G = (V, E)$  es un grafo. Entonces se define:

**Camino:** Es una secuencia de vértices  $\langle v_1, v_2, \dots, v_n \rangle$  tal que  $v_i, v_{i+1}$  son adyacentes (*walk* en inglés).

**Camino simple:** Es un camino en los que los  $v_i$  son todos distintos (en inglés, *path*).

**Ciclo:** Es un camino  $\langle v_1, v_2, \dots, v_n, v_1 \rangle$ , en el cual no se repite más que el primer y último vértice. Se llama  $r$ -ciclo (ciclo de largo  $r$ ) si tiene  $r$  arcos y  $r$  vértices.

**Círculo:** Un camino cerrado  $\langle v_1, v_2, \dots, v_n, v_1 \rangle$  (pueden repetirse vértices). Algunos les llaman círculos, y llaman *ciclos simples* a lo que nosotros llamamos ciclos.

**Definición 24.6.** Sea  $G = (V, E)$  un grafo. Definimos la relación  $\sim$  entre vértices, tal que  $x \sim y$  si  $x$  e  $y$  están en un camino de  $G$ , o sea  $x = v_1, v_2, \dots, v_k = y$  es un camino.

Es fácil ver que  $\sim$  es una relación de equivalencia:

**Reflexiva:**  $x \sim x$ . Un camino de 0 arcos cumple con la definición.

**Simétrica:**  $x \sim y \implies y \sim x$ : Esto es  $x = v_1, \dots, v_k = y \implies y = v_k, \dots, v_1 = x$ , que claramente es cierto.

**Transitiva:**  $(x \sim y) \wedge (y \sim z) \implies x \sim z$ . Esto es decir:

$$x = v_1, \dots, v_k = y = u_1, \dots, u_k = z$$

Esto es un camino que de  $x$  va a  $z$ ,  $x \sim z$ .

**Definición 24.7.** Sea  $G = (V, E)$  un grafo. Si  $V_1, V_2, \dots, V_k$  son las clases de equivalencia de  $\sim$ , y  $E_1, E_2, \dots, E_k$  conjuntos de arcos tales que  $E_i$  contiene solo vértices de  $V_i$ , a los grafos  $G_i = (V_i, E_i)$  se les llama *componentes conexos* de  $G$ . Si  $G$  tiene un único componente conexo es llamado *conexo*.

En el grafo de la figura 24.14 se distinguen vértices a los cuales no se puede acceder desde algunos de los otros vértices. Este grafo tiene dos componentes conexos.

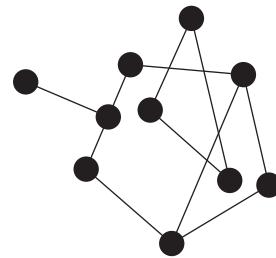


Figura 24.14 – Un grafo con dos componentes conexos

Un resultado simple es la relación entre el número de vértices y arcos en grafos conexos.

**Teorema 24.6.** *Todo grafo  $G = (V, E)$  tiene a lo menos  $|V| - |E|$  componentes conexos.*

Nótese que para  $K_n$  esto nos dice que tiene al menos  $n(3 - n)/2$  componentes conexos, y para  $n > 3$  esto es negativo. La cota no es para nada ajustada.

*Demostración.* Usamos inducción sobre el número de arcos.

**Base:** En un grafo con 0 arcos, cada vértice es un componente conexo, y hay  $|V| - 0 = |V|$  componentes conexos.

**Inducción:** Suponemos que la hipótesis vale para todo grafo de  $n$  arcos, y demostramos que vale para todo grafo de  $n + 1$  arcos, con  $n \geq 0$ . Considérese un grafo  $G = (V, E)$  con  $n + 1$  arcos. Eliminamos un arco arbitrario  $ab$  del grafo, dejando el grafo  $G'$  con  $n$  arcos. Por la hipótesis,  $G'$  tiene a lo menos  $|V| - n$  componentes conexos. Reponemos el arco eliminado, con lo que tenemos de vuelta el grafo original  $G$ . Si  $a$  y  $b$  pertenecían al mismo componente conexo de  $G'$ ,  $G$  tiene el mismo número de componentes conexos de  $G'$ , que es a lo menos  $|V| - n$  por hipótesis. Si  $a$  y  $b$  pertenecen a componentes conexos distintos de  $G'$ ,  $G$  tiene un componente conexo menos que  $G'$ , ya que el arco  $ab$  une esos dos componentes conexos de  $G'$  en uno solo en  $G$ . Como  $G'$  tenía a lo menos  $|V| - n$  componentes conexos,  $G$  tiene entonces a lo menos uno menos que esto, vale decir  $|V| - n - 1 = |V| - (n + 1)$ . Esto demuestra el paso de inducción.  $\square$

Algunos puntos se deben notar de esta demostración. Primeramente, usamos inducción sobre el número de arcos. Esto es común en demostraciones en grafos, al igual que inducción sobre el número de vértices. Sólo si ninguna de estas dos estrategias sirve vale la pena considerar otras opciones.

Por otro lado, usamos la táctica de eliminar un arco y reponerlo en nuestra demostración. Esta es la forma más sencilla de evitar errores lógicos comunes, ya que asegura que el elemento que queremos agregar es posible y lleva en la dirección correcta. Si se usa inducción en grafos (ya sea sobre arcos o vértices), siempre conviene usar esta idea de encoger-expandir.

**Corolario 24.7.** *Todo grafo conexo de  $n$  vértices tiene a lo menos  $n - 1$  arcos.*

*Demostración.* Usamos la misma estrategia de la demostración del teorema 24.6: Partiendo con  $|V|$  vértices aislados ( $|V|$  componentes conexos), cada vez que agregamos un arco disminuye el número de componentes conexos en 0 o 1. Si siempre elegimos un arco que conecta componentes conexos distintos, al agregar  $n - 1$  arcos queda un único componente conexo.  $\square$

**Definición 24.8.** Sea  $G = (V, E)$  un grafo. Entonces:

- Un camino simple que visita todos los vértices es un *camino hamiltoniano*. Un ciclo que contiene todos los vértices del grafo es llamado *ciclo hamiltoniano*.
- Un camino que pasa exactamente una vez por cada arco es denominado *camino de Euler*. Un circuito que pasa exactamente una vez por cada arco se llama *circuito de Euler*.

Determinar si hay un camino o ciclo hamiltoniano es NP-completo. Incluso tiene la distinción de ser uno de los 21 problemas identificados inicialmente como tales por Karp [197].

En cambio, un camino (o circuito) de Euler es sencillo de hallar. Si consideramos vértices cualquiera hay dos opciones:

1. Comienzo en un vértice, termino en otro.
2. Comienzo en un vértice, termino en el mismo.

Si inicio y fin son diferentes (es un camino de Euler):

- Inicio: *Salgo* una vez, *paso* por él (entro y salgo) varias veces, lo que significa que  $\delta(\text{inicio})$  es impar.
- Fin: *Llego* una vez, *paso* por él (entro y salgo) varias veces, con lo que también  $\delta(\text{fin})$  es impar.
- Otros vértices: *Paso* por él (entro y salgo) varias veces, por lo que  $\delta(\text{otro})$  es par.

Si inicio y fin son el mismo (es un circuito de Euler):

- Inicio (y fin): *Salgo* una vez, *paso* por él (entro y salgo) varias veces, *llego* una vez, y  $\delta(\text{inicio})$  es par.
- Otros vértices: *Paso* por él (entro y salgo) varias veces, con lo que  $\delta(\text{otro})$  es siempre par.

Estas dos son las únicas posibilidades, y por tanto es condición necesaria para la existencia de un camino de Euler en un grafo conexo el que o todos los vértices sean de grado par (en tal caso podemos comenzar en cualquiera de ellos, terminamos en el mismo, es un *circuito de Euler*), o que hayan exactamente dos vértices de grado impar (comenzamos en uno de ellos, terminamos en el otro, es un *camino de Euler*). Más adelante demostraremos que estas condiciones son suficientes, y daremos algoritmos para encontrar un camino (o circuito) de Euler.

**Ejemplo 24.3.** Puentes de Königsberg

Supóngase que se desea dar un paseo por la ciudad de Königsberg, pasando una única vez por cada uno de los siete puentes, situados según la figura 24.15. ¿Es posible realizar esta tarea?

La respuesta es no, como demostró Euler en 1735, dando inicio al estudio de lo que hoy es la teoría de grafos. Representando los sectores unidos por los puentes en un grafo como en la misma figura 24.15, se aprecia claramente que hay más de dos vértices de grado impar. Debido a esto no es posible que exista un camino de Euler que permita cumplir con la tarea requerida. Si bien la representación no es un grafo propiamente tal – es un multigrafo pues hay vértices que están conectados por más de un arco – aún así los principios son aplicables.

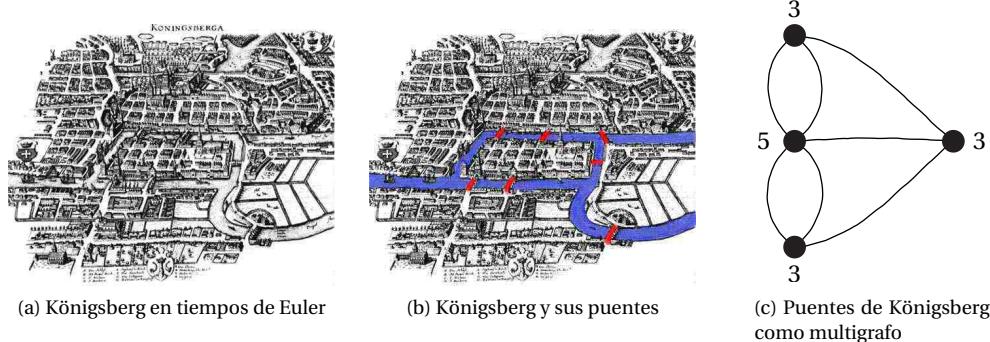


Figura 24.15 – Puentes de Königsberg [269]

Del resultado siguiente Euler demostró la necesidad en 1736, Hierholzer [174] demostró suficiencia recién en 1873. Igual se atribuye a Euler.

**Teorema 24.8** (Euler). *Sea  $G$  un grafo conexo. Entonces hay un camino de Euler si y solo si hay exactamente dos vértices de grado impar (y todo camino de Euler comienza en uno de ellos y termina en el otro), y hay un circuito de Euler si y solo si todos los vértices son de grado par.*

*Demostración.* Demostramos implicancia en ambas direcciones. Que las condiciones son necesarias ya lo vimos antes, demostramos ahora que son suficientes por inducción fuerte sobre el número de arcos de  $G$ .

**Base:** Si  $G$  tiene un único arco, la conclusión es trivial.

**Inducción:** Sea un grafo  $G$  con  $n + 1$  arcos, todos cuyos vértices son de grado par o hay exactamente dos vértices de grado impar. La estrategia general es eliminar un arco, y analizar por separado las situaciones en las cuales esta operación divide el grafo en dos componentes conexos y aquellas en que sigue siendo conexo.

Consideremos primero el caso en que todos los vértices de  $G$  son de grado par. Elijamos un vértice  $x$  y un arco  $e = xy$ . Si eliminamos el arco  $e$ , obtenemos un nuevo grafo  $G'$ , en el cual ahora  $x$  e  $y$  son los únicos vértices de grado impar. Entonces  $G'$  es conexo, ya que si no fuera conexo  $x$  e  $y$  en  $G'$  pertenecerían a componentes conexos diferentes, y en  $G'$  los vértices  $x$  e  $y$  serían los únicos de grado impar en sus respectivos componentes conexos. Esto es absurdo, contradice al lema 24.2. Por inducción, como  $G'$  es conexo y tiene  $n$  arcos, hay un camino de Euler que comienza en  $x$  y termina en  $y$ ; al reponer el arco  $xy$  hay entonces un circuito de Euler (el camino anterior junto con este arco).

Supongamos ahora que  $G$  tiene exactamente dos vértices de grado impar, llamémosles  $x$  e  $y$ . Consideremos primero el caso en que  $x$  e  $y$  son adyacentes. Eliminando el arco  $xy$  tenemos un grafo  $G'$  con  $n$  arcos, y todos sus vértices son de grado par. Si  $G'$  es conexo, tiene un circuito de Euler, y agregando el arco  $xy$  a este tenemos un camino de Euler que comienza en  $x$  y termina en  $y$ . Si  $G'$  no es conexo, tiene dos componentes conexos, llamémoslos  $G_1$  y  $G_2$ . Pero tanto  $G_1$  como  $G_2$  tienen solo vértices de grado par, y tienen menos de  $n$  arcos, con lo que cada uno de ellos tiene un circuito de Euler, que podemos suponer comienza y termina en  $x$  (respectivamente  $y$ ). Conectando estos dos circuitos mediante el arco  $xy$  obtenemos un camino de Euler para  $G$ , que comienza en  $x$  y termina en  $y$ . Si no hay un arco que conecte a  $x$  e  $y$ , debe haber un arco  $xz$  para algún vértice  $z$ . Eliminando este arco, tenemos un grafo  $G'$  con  $n$  arcos en el cual hay exactamente dos vértices de grado impar,  $z$  e  $y$ . Por inducción, si  $G'$  es conexo hay un camino de Euler que comienza en  $z$  y termina en  $y$ , reponiendo el arco  $xz$  tenemos un camino de Euler que comienza en  $x$  y termina en  $y$ . Si  $G'$  no es conexo, tendrá componentes conexos  $G_1$  (que contiene a  $x$ ) y  $G_2$ . Entonces  $z$  estará en  $G_2$  (en caso contrario,  $G'$  sería conexo), e  $y$  estará en  $G_2$  también (de otra forma, sería el único vértice de grado impar en  $G_1$ ). O sea,  $G_1$  tiene solo vértices de grado par, y  $G_2$  tiene exactamente dos vértices de grado impar ( $y$  y  $z$ ). Por inducción, hay un circuito de Euler en  $G_1$ , que podemos suponer comienza y termina en  $x$ , y un camino de Euler en  $G_2$ , que comienza en  $z$  y termina en  $y$ . Reponiendo el arco  $xz$  tenemos un camino de Euler que comienza en  $x$ , recorre  $G_1$  para volver a  $x$ , luego pasa a  $G_2$  por  $xz$  y sigue el camino de Euler en  $G_2$  para terminar en  $y$ .  $\square$

La demostración del teorema 24.8 no da muchas luces sobre cómo hallar el camino (circuito) de Euler. Curiosamente, Euler mismo nunca dio un método para hallar tal camino o circuito. Una técnica elegante da el algoritmo de Fleury [129]: Si hay vértices de grado impar, comience en uno de ellos, en caso contrario elija uno cualquiera. En cada paso, elija un arco desde el vértice actual y atráveselo, luego lo elimina del grafo. Al hacer esto, debe tener cuidado que el grafo resultante sea conexo (salvo que no tenga alternativa).

Una técnica más eficiente para hallar un circuito de Euler se debe a Hierholzer [174]: Parta de un vértice  $v$  cualquiera y siga un camino sin repetir arcos a través del grafo hasta volver a  $v$ . Es imposible quedar sin posibilidades de continuar, ya que los vértices son de grado par, de llegar a un vértice tiene que haber al menos un arco que permita salir; y como hay un número finito de vértices tarde o temprano retornaremos al inicio. Si esto no visita todos los arcos, elija algún vértice  $v'$  en el circuito construido que tenga arcos no visitados, y comience el proceso nuevamente desde  $v'$ , integrando luego el nuevo circuito en el anterior.

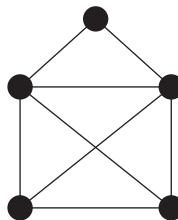


Figura 24.16 – Dibuja una casita

**Ejemplo 24.4.** Se pide dibujar la figura 24.16 en un papel, de manera que el lápiz no se levante en ningún momento del papel y no dibuje dos veces el mismo trazo. ¿Es posible realizar esto?

La respuesta es sí, puesto que hay exactamente dos vértices de grado impar. Debemos elegir uno de ellos como punto de partida, y terminaremos en el otro.

**Ejemplo 24.5.** Un cubo de queso cortado en  $3 \times 3$ .

Un ratón comienza en una de las esquinas, come ese cubito y sigue con uno de los vecinos (no en diagonal). ¿Puede comerse todo el queso terminando con el cubo del centro? Los arcos en la figura 24.17 muestran las movidas legales.

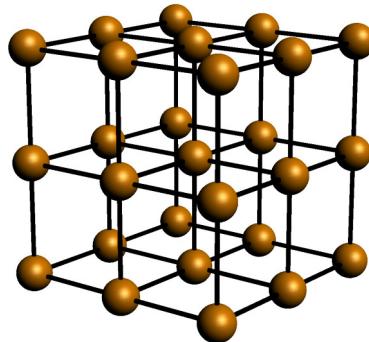


Figura 24.17 – Queso cortado en nueve cubitos

La respuesta a esto es no. Considere el grafo de la figura 24.18, en el cual se han coloreado de

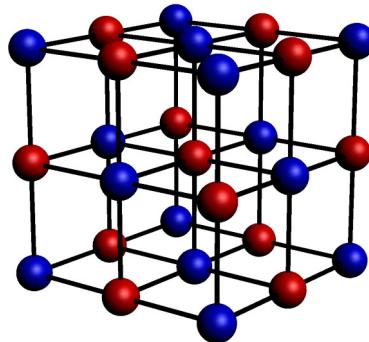


Figura 24.18 – Cubitos de queso de colores

rojo y azul vértices adyacentes. Se ve que hay 14 vértices azules y 13 rojos. En cualquier camino que nuestro roedor siga irá alternando colores, por lo que si comienza en una de las esquinas, que son azules, necesariamente terminará en un cubito azul de comerse todo el queso. Pero el cubito central es rojo.

## 24.7. Árboles

En muchas aplicaciones aparecen grafos conexos sin enlaces redundantes (sin ciclos). Esta idea es capturada por la definición siguiente.

**Definición 24.9.** El grafo  $T = (V, E)$  es un *árbol* si:

**T1:**  $T$  es conexo.

**T2:** No hay ciclos en  $T$ .

Aclaramos que los árboles binarios vistos en el ramo Estructuras de Datos, *no son árboles*. Acá no hay raíz, hijos ni descendientes, y aún menos “hijos izquierdos” y “derechos”, solo *vecinos*. Y como estos son grafos, no hay árboles sin nodos.

**Definición 24.10.** En un árbol  $T = (V, E)$  un vértice  $v \in V$  se llama *hoja* si tiene grado uno. En caso contrario es un *vértice interno*.

Buena parte de la importancia de los árboles reside en que tienen una colección de propiedades interesantes, como las siguientes.

**Teorema 24.9.** Si  $T = (V, E)$  es un árbol entonces:

**T3:** Para cualquier par de vértices en  $V$  hay un único camino simple entre ellos.

**T4:** Al agregar un arco a  $T$  se forma un ciclo.

**T5:** Al eliminar un arco de  $T$ , quedan dos componentes conexos que son árboles.

**T6:** Un árbol con al menos dos vértices tiene al menos dos hojas.

**T7:**  $|E| = |V| - 1$ .

*Demostración.* Demostramos cada una de las aseveraciones por turno.

**T3:** Supongamos que  $T = (V, E)$  es un árbol y que hay dos vértices  $x, y$  con más de un camino simple que los conecta, digamos:

$$x = u_1, u_2, \dots, u_r = y$$

$$x = v_1, v_2, \dots, v_s = y$$

Sea ahora  $i$  el *menor* índice tal que  $v_{i+1} \neq u_{i+1}$ ; y sea  $j$  el *mayor* índice tal que  $u_{j-1} \neq v_{k-1}$ , pero  $u_j = v_k$  para algún  $k$ . Vea la figura 24.19. Se nota que  $v_i, v_{i+1}, \dots, v_{k-1}, v_k, u_{j-1}, u_{j-2}, u_{i+1}, u_i, u_1, v_1$

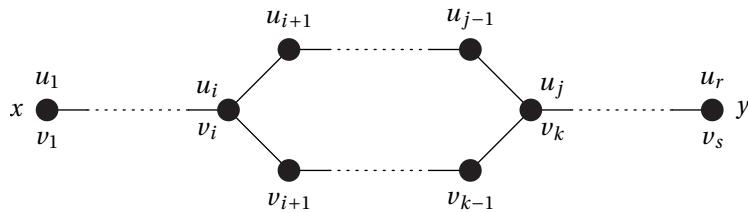


Figura 24.19 – Esquema de vértices en la parte T3 del teorema 24.9

son un ciclo, pero siendo  $T$  un árbol no tiene ciclos. Esta contradicción completa la demostración de esta parte.

**T4:** Al agregar un arco  $xy$  al árbol, este junto con el camino entre  $x$  e  $y$  (que existe porque  $T$  es conexo) forman un ciclo.

**T5:** Consideremos un arco  $xy$  del árbol. Si lo eliminamos, ya no hay caminos entre  $x$  e  $y$  (por T3 hay un único camino entre  $x$  e  $y$ , precisamente este arco). Luego el grafo resultante tiene dos componentes conexos, cada uno conexo y sin ciclos. Ambos son árboles.

**T6:** Consideremos un camino de largo máximo en  $T$ , con vértices  $v_1, v_2, \dots, v_m$ . Entonces  $m \geq 2$ , dado que un árbol con al menos dos vértices tiene que tener al menos un arco. No pueden haber arcos  $v_1 v_i$  para  $i \geq 2$ , ya que de otra forma tendríamos un ciclo  $v_1, \dots, v_i, v_1$ . Tampoco puede haber un arco  $uv_1$ , ya que de haberlo tendríamos un camino más largo  $u, v_1, \dots, v_m$ . O sea,  $v_1$  es una hoja. De forma similar,  $v_m$  es una hoja, y hay al menos dos hojas.

Nótese que el caso extremo de dos hojas se da en un camino.

**T7:** Queremos demostrar que  $|E| = |V| - 1$ . Usamos inducción sobre el número de vértices. En un árbol con un único vértice, la aseveración se cumple. Supongamos ahora que la aseveración se cumple para todos los árboles con  $n$  vértices, y consideremos un árbol con  $n + 1$  vértices. Elijamos una hoja  $x$  (por T6 hay al menos dos hojas), hay un único arco  $xy$  que incluye a  $x$ . Al eliminar el vértice  $x$  de  $T$  junto con el arco  $xy$  queda un árbol de  $n$  vértices, que por inducción tiene  $n - 1$  arcos. Al reponer el vértice  $y$  y el arco, el número de arcos y el de vértices aumenta en uno, y tenemos el resultado.  $\square$

La parte T7 y el corolario 24.7 dicen que un árbol es el grafo conexo con mínimo número de arcos para ese conjunto de vértices. Es común querer conectar los vértices de un grafo con el mínimo número de arcos:

**Definición 24.11.** Sea  $G = (V, E)$  un grafo conexo. A un árbol  $T = (V, E')$ , donde  $E' \subseteq E$  se le llama *árbol recubridor* (en inglés, *spanning tree*) de  $G$ .

**Ejemplo 24.6.** Dibujar los árboles no isomorfos de 6 vértices.

La mejor forma de solucionar esto es empezar a dibujar los grafos, partiendo por el caso en que se encuentre un vértice de grado máximo, es decir, de grado 5. Véase la figura 24.20a. Luego los árboles con grado máximo 4 (figura 24.20b), los de grado 3 (figura 24.20c), y finalmente los de grado máximo 2 (figura 24.20d). Estos son la solución a nuestro problema. Hay un total de 6 árboles no

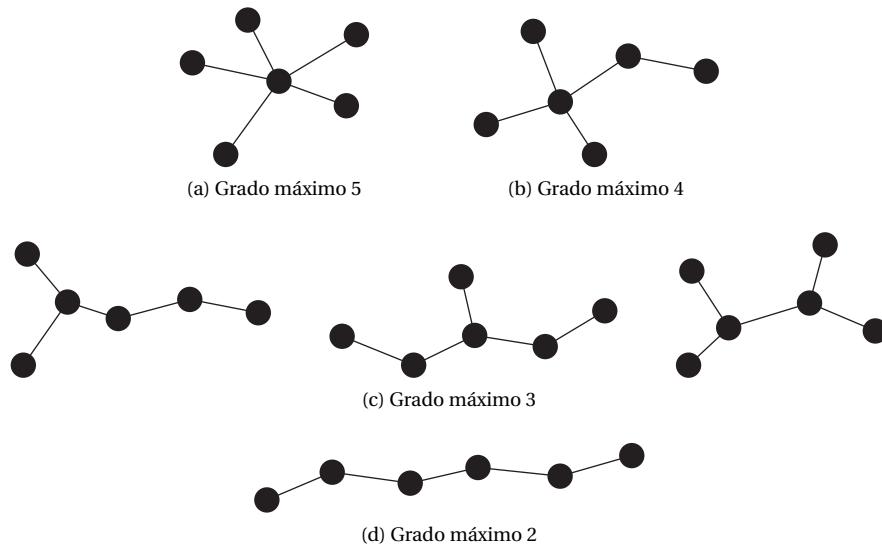


Figura 24.20 – Los 6 árboles con 6 vértices

isomorfos de 6 vértices. Obtener el número de árboles para cualquier número de vértices es uno de los problemas abiertos famosos de la teoría de grafos.

## 24.8. Árboles con raíz

Veremos algunas aplicaciones de árbol con un vértice especial designado como raíz. Esto aparece en aplicaciones en las cuales hay una jerarquía, como al representar un organigrama. Así *no* son isomorfos los árboles con raíz (el vértice en blanco marca el distinguido como raíz) mostrados en la figura 24.21, a pesar de ser isomorfos si los consideramos como árboles (no distinguimos raíces). Aparte de la raíz distinguimos *vértices internos* con  $\delta(v) \geq 2$ , y *hojas* con  $\delta(v) = 1$ . Normalmente

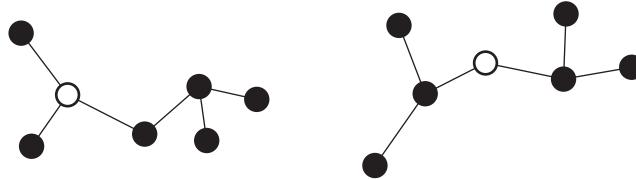


Figura 24.21 – Ejemplos de árbol con raíz

dibujaremos la raíz y debajo de ella sus vecinos, y así sucesivamente hasta llegar a las hojas.

En muchas aplicaciones encontraremos que la raíz y los vértices internos tienen el mismo grado. Si tienen grado  $m$  se habla de *árboles m-arios*.

Podemos enumerar los vértices de un árbol con raíz, analizando su distancia desde la raíz, donde la distancia es el largo (número de arcos) del camino entre la raíz y el vértice considerado:

**Nivel 0:** La raíz.

**Nivel 1:** Los vecinos de la raíz.

**Nivel 2:** Los vecinos de vértices en el nivel 1, salvo los que están en el nivel 0.

...

**Nivel  $n$ :** Los vecinos de los vértices en el nivel  $n - 1$ , salvo los que están en nivel  $n - 2$ .

Esto motiva la siguiente definición:

**Definición 24.12.** La *altura* del árbol con raíz es el máximo  $k$  para el que el nivel  $k$  no es vacío.

La interpretación como una jerarquía similar a una genealogía sugiere:

**Definición 24.13.** Sea  $T$  un árbol con raíz  $r$ . Si hay un camino de  $r$  a  $v$  que pasa por  $u$ , se dice que  $u$  es *ancestro* de  $v$ , y  $v$  es un *descendiente* de  $u$ . Si  $u$  y  $v$  son vecinos, se dice que  $u$  es el *padre* de  $v$ , y que  $v$  es *hijo* de  $u$ .

La enumeración en niveles que da lugar a la definición de altura sugiere el algoritmo 24.1 para recorrer un árbol con raíz. Se invoca el procedimiento recorrer inicialmente con la raíz. En este algoritmo podemos considerar visitar (procesar de alguna forma) cada vértice la primera o la última vez que pasamos por él, dando lugar a recorridos en *preorden* o en *postorden*, alternativas que suelen presentarse por separado. Cual se elija (o incluso si se usan ambos) dependerá de la aplicación. Como no hay orden definido entre los hijos de un vértice, en caso de haber varios elegimos uno arbitrariamente.

**Teorema 24.10.** Si el número máximo de hijos de los vértices de un árbol con raíz es  $d$  y su altura es  $h$  entonces el árbol tiene a lo más  $d^h$  hojas.

---

 Algoritmo 24.1: Recorrer árboles con raíz
 

---

```

procedure recorrer( $v$ )
    if  $v$  es hoja then
        Visitar  $v$ 
    else
        Visitar  $v$  en preorden
        for  $x$  hijo de  $v$  do
            recorrer( $x$ )
        end
        Visitar  $v$  en postorden
    end

```

---

*Demostración.* La demostración es por inducción fuerte sobre  $h$ .

**Base:** Cuando  $h = 0$  hay un único vértice (la raíz es hoja) y hay  $1 \leq d^0 = 1$  hojas.

**Inducción:** Supongamos que todos los árboles de altura menor o igual a  $h$  tienen a lo más  $d^h$  hojas.

Consideremos un árbol de altura  $h + 1$ . Este es la raíz y a lo más  $d$  árboles de altura a lo más  $h$ , cada uno de los cuales aporta a lo más  $d^h$  hojas, para un total de a lo más  $d \cdot d^h = d^{h+1}$  hojas.  $\square$

**Corolario 24.11.** *Un árbol en el cual cada nodo tiene a lo más  $d$  hijos y que tiene  $r$  hojas tiene altura a lo menos de  $\log_d r$ .*

En particular, árboles binarios (que como ya se comentó realmente no son árboles, pero tienen suficiente en común con ellos para los efectos presentes) con  $r$  hojas tienen altura a lo menos  $\log_2 r$ , y árboles binarios de altura  $h$  tienen a lo más  $2^h$  hojas.

## 24.9. Árboles ordenados

Una situación afín a los árboles con raíz se da cuando hay un orden entre los hijos de un vértice. Así, hay un primer, segundo, tercero, etc. hijo. Muchas situaciones son naturales de modelar de esta forma.

### 24.9.1. Árboles de decisión

Un árbol de decisión representa una secuencia de decisiones y los resultados de estas. Se comienza en la raíz, cada vértice interno representa una decisión, y las hojas son resultados finales. Un camino entre la raíz y una hoja representa una ejecución del procedimiento, a través de la secuencia de decisiones y sus resultados que el camino representa.

**Ejemplo 24.7.** Búsqueda de monedas falsas.

Tenemos una moneda  $O$  (la sabemos buena) y  $r$  otras monedas, una de las cuales puede ser falsa (puede que sea más pesada o más liviana que la moneda  $O$ ). ¿Cuál es el número mínimo de pesadas (comparar el peso de dos colecciones de monedas) para determinar si hay una falsa y saber exactamente cuál es?

Un nodo del árbol de decisiones puede representarse como en la figura 24.22, para cada pesada hay tres opciones: La izquierda es más liviana, son iguales, la derecha es más liviana.

Las hojas que debemos obtener (resultados finales del proceso) son las siguientes:

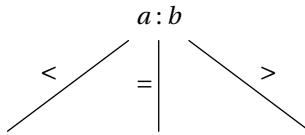


Figura 24.22 – Vértice del árbol de decisión al pesar monedas

- Todas buenas.
- #1 Pesada.
- #1 Liviana.
- (Muchas alternativas omitidas)
- # $r$  Pesada.
- # $r$  Liviana.

Hay  $2r + 1$  resultados, con lo que se requieren a lo menos  $\lceil \log_3(2r + 1) \rceil$  pesadas. Pueden ser más que esto, solo hemos demostrado que es imposible hacerlo con menos.

#### 24.9.2. Análisis de algoritmos de ordenamiento

Supongamos un método de ordenamiento basado en comparaciones. Una pregunta obvia es: ¿Cuántas comparaciones se requieren para ordenar  $n$  elementos?

El suponer que todos los elementos son diferentes hace más duro resolver el problema, con lo que nos concentraremos en ese caso. El ordenar  $n$  elementos involucra determinar en qué orden están (o, lo que es lo mismo, han de ubicarse). Modelamos un algoritmo de ordenamiento especificando cuáles de los elementos originales se comparan en cada paso, y organizamos los distintos caminos que sigue el algoritmo como ramas de un árbol con raíz. Cada vértice representa el resultado de comparar dos elementos con las opciones  $<$ ,  $>$ . Pueden aparecer comparaciones redundantes o incluso contradictorias en el árbol. Las hojas son órdenes de los  $n$  elementos de entrada (aunque también es posible que aparezcan entre las hojas situaciones imposibles, al especificar el camino desde la raíz situaciones contradictorias).

**Ejemplo 24.8.** Comparamos tres elementos  $\{a, b, c\}$ , todos distintos.

Como se ve en la figura 24.23, tomando cada comparación  $x: y$  como un vértice cuyos resultados son  $x < y$  o  $x > y$ , el árbol tiene 6 hojas, que corresponden a las  $3!$  formas de ordenar 3 objetos.

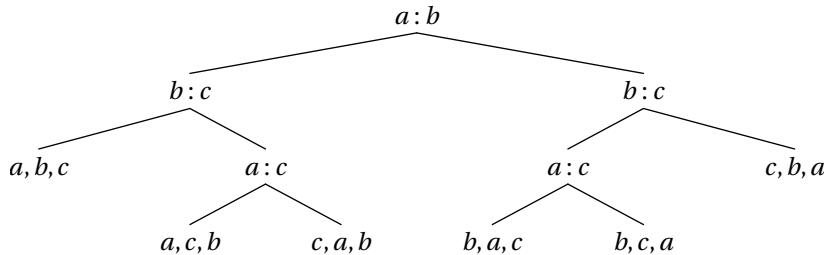


Figura 24.23 – Árbol de decisión al ordenar 3 objetos

Esto muestra que la altura del árbol de decisión (el número de comparaciones requeridas en el peor caso) es  $\lceil \log_2 n! \rceil$ . Aproximamos el factorial en la sección 18.5 como  $\ln n! = n \ln n - n + O(1)$ . Por nuestro análisis el número de comparaciones requerido es entonces  $\Omega(n \log n)$ .

#### 24.9.3. Generar código

Una aplicación interesante de árboles ordenados se da al generar código para expresiones aritméticas mediante la técnica de Sethi y Ullman [322]. Considerando un modelo de máquina que tiene cierto número de registros de propósito general, con operaciones aritméticas tradicionales que toman sus argumentos de dos registros cualquiera y dejan el resultado en alguno cualquiera. Lo que interesa es generar código óptimo para expresiones aritméticas en esta clase de máquinas.

Por ejemplo, la expresión  $a * x + b * y + c * (-u + v)$  queda representada por el árbol de la figura 24.24. Los números que adornan los vértices del árbol representan el número de registros

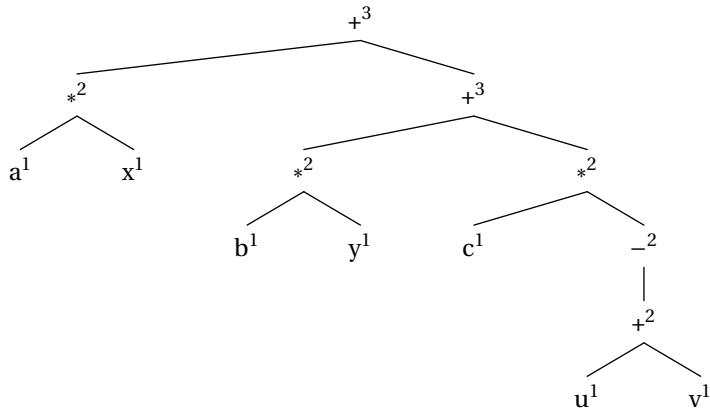


Figura 24.24 – Árbol sintáctico de una expresión

requeridos para calcular el valor de ese vértice (se les llama *números de Sethi-Ullman*, en honor a los inventores del algoritmo que discutiremos).

Al calcular una expresión vista de esta forma como un árbol nada puede ganarse calculando parte de una rama, seguir con otra, para luego volver a completar la primera. El caso más simple es el de una variable o constante, basta cargar el valor en un registro libre. Consideremos ahora una operación cualquiera dentro del árbol, suponiendo operaciones con dos argumentos (las ideas se pueden extender sin problemas a casos en que hay más de dos parámetros). Toma los valores de sus argumentos de dos registros. Para calcular estas expresiones más complejas, supongamos que evaluar los operandos requiere  $m$  y  $n$  registros respectivamente. Se dan dos casos:

**Caso  $m = n$ :** De ser así, la estrategia consiste en calcular el argumento izquierdo (se usan  $m$  registros en el proceso, queda el resultado en uno de ellos). Luego calculamos el argumento derecho, usando  $m$  registros más, lo que con el registro usado para almacenar temporalmente el valor del operando izquierdo hace un total de  $m + 1$  registros. Finalmente calculamos el valor buscado, sin usar registros adicionales.

**Caso  $m \neq n$ :** Consideremos  $m < n$ , el otro caso es totalmente simétrico. En este caso calculamos primero aquel argumento que requiere más registros, (el derecho en nuestro caso), usando  $n$  registros, y dejando el resultado en uno de ellos. Luego calculamos el otro argumento (el izquierdo en nuestro caso), para lo que se requieren  $m < n$  registros, reusando los que quedaron libres del cálculo anterior. En total, se requieren  $n$  registros.

El algoritmo para generar código óptimo en este caso particular (este tipo de arquitecturas y expresiones sin subexpresiones repetidas) resulta inmediato de la discusión anterior:

1. Calcule los números de Sethi-Ullman para los vértices del árbol en un recorrido en postorden.
2. Considere cada vértice en un recorrido en postorden. Si es una variable o constante, cargue su valor en algún registro libre. Si es una operación, calcule primero aquel argumento que requiere más registros, luego el otro, y efectúe la operación.

Si faltan registros, la solución es guardar en una variable temporal el contenido de aquel registro que no se usará por más tiempo, para reponerlo cuando se necesite. Esto resulta óptimo, ya que minimiza el número de instrucciones adicionales (cada operación requiere al menos una instrucción, y nuestro algoritmo usa exactamente una instrucción por operación si no quedamos cortos de registros). Nótese también que basta con operaciones que trabajen entre dos registros (origen y destino), no hacen falta operaciones con dos orígenes y un destino para el resultado. Eso sí pueden hacer falta operaciones simétricas, con efectos por ejemplo  $a \leftarrow a - b$  y  $a \leftarrow b - a$  (aunque pueden obtenerse sus efectos con una secuencia de dos operaciones, por ejemplo calculando  $a \leftarrow a - b$  y cambiando el signo).

```

 $r0 \leftarrow u$ 
 $r1 \leftarrow v$ 
 $r0 \leftarrow r0 + r1$ 
 $r0 \leftarrow -r0$ 
 $r1 \leftarrow c$ 
 $r0 \leftarrow r0 * r1$ 
 $r1 \leftarrow b$ 
 $r2 \leftarrow y$ 
 $r1 \leftarrow r1 * r2$ 
 $r0 \leftarrow r0 + r1$ 
 $r1 \leftarrow a$ 
 $r2 \leftarrow x$ 
 $r1 \leftarrow r1 * r2$ 
 $r0 \leftarrow r0 + r1$ 

```

Cuadro 24.3 – Código óptimo para la expresión ejemplo

Para el árbol de la figura 24.24 resulta el código del cuadro 24.3. El formato de las instrucciones es por ejemplo  $r0 \leftarrow r1 - r2$ , para indicar que al registro  $r0$  se le asigna el valor  $r1 - r2$ . Sólo se aceptan operaciones entre registros, traer datos de memoria a un registro y llevar datos de un registro a memoria. Lamentablemente en situaciones más realistas (registros de uso específico, instrucciones que no solo operan entre registros, subexpresiones comunes, aplicar identidades algebraicas) la situación es bastante más compleja y no hay algoritmos tan simples y eficientes.

## 24.10. Grafos planares

Un grafo se dice *planar* si puede dibujarse en un plano sin que se crucen arcos. Un caso particular del siguiente resultado dio Descartes en 1639, el caso general se debe a Euler en 1751. Eppstein lista 19 demostraciones en [113], la brillante demostración siguiente es de von Staudt [335].

**Teorema 24.12** (Fórmula de Euler). *Sea  $G = (V, E)$  un grafo planar conexo dibujado en el plano. Definimos  $f$  como el número de caras del grafo (las áreas separadas por arcos, incluyendo el área infinita fuera del grafo),  $e = |E|$  y  $v = |V|$ . Entonces:*

$$v - e + f = 2$$

*Demostración.* Sea  $G$  un grafo planar conexo, dibujado en el plano. Definimos el *dual* de  $G$  como el multigrafo  $G^*$ , cuyos vértices son las caras de  $G$  y cuyos arcos pasan por los puntos medios de los arcos de  $G$  que separan las caras, vea la figura 24.25. El multigrafo  $G^*$  es conexo, ya que podemos ir de

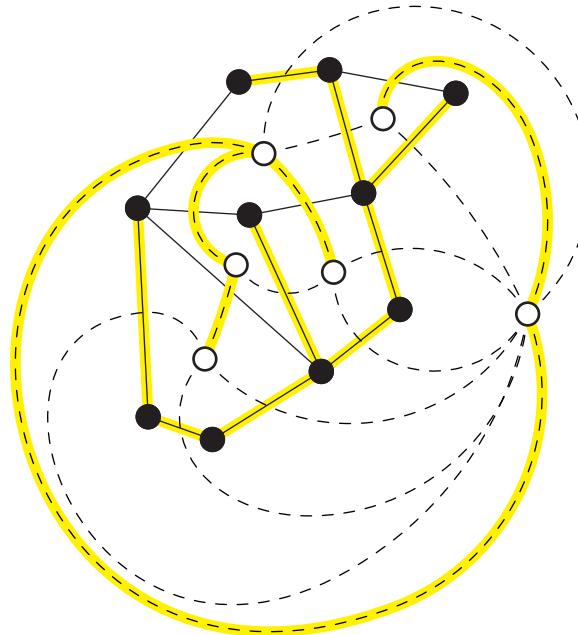


Figura 24.25 – Ilustración de la demostración de la fórmula de Euler

cualquiera de las caras de  $G$  a cualquiera otra atravesando arcos. Consideremos un árbol recubridor de  $G^*$ , llamémosle  $T^*$ . Si eliminamos los arcos de  $G$  cortados por arcos de  $T^*$ , queda un grafo que llamaremos  $T$ . Como  $T^*$  es un árbol, no tiene ciclos y no puede cortar  $G$  en componentes conexos, así que  $T$  es conexo. Por el otro lado,  $T$  no tiene ciclos, ya que podemos ir de cualquiera de los vértices de  $G^*$  a cualquier otro a través de arcos de  $T^*$ . O sea,  $T$  también es un árbol. Por construcción, el número de arcos de  $G$  es la suma del número de arcos de  $T$  con el número de arcos de  $T^*$ :

$$(v - 1) + (f - 1) = e$$

Esto es lo que se quería probar. □

Llamemos  $k$ -cara a una cara acotada por  $k$  arcos, y sea  $f_k$  el número de  $k$ -caras en  $G$ . Del lema 24.2 sabemos que:

$$2e = \sum_{x \in V} \delta(x)$$

De forma similar tenemos:

$$f = \sum_k f_k \quad 2e = \sum_k k f_k$$

El número promedio de lados por cara es:

$$\bar{f} = \frac{2e}{f}$$

Con esto podemos demostrar que  $K_5$  y  $K_{3,3}$  ( $K_{3,3}$  es el grafo formado por dos conjuntos de tres vértices, en el cual todos los vértices de un conjunto están conectados con todos los vértices del otro pero no hay conexiones dentro de los conjuntos, ver la figura 24.26) no son planares. Consideremos

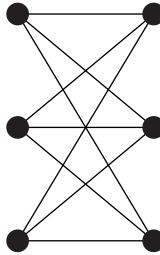


Figura 24.26 – El grafo  $K_{3,3}$

$K_5$ , con  $v = 5$  y  $e = \binom{5}{2} = 10$ . Para un supuesto dibujo de  $K_5$  en el plano calculamos  $f = 2 + e - v = 7$ ; el número promedio de lados por cara sería  $\bar{f} = 2 \cdot 10/7 < 3$ , lo que es ridículo. De forma similar, para  $K_{3,3}$  resultan  $v = 6$ ,  $e = 9$  y  $f = 5$ , con lo que  $\bar{f} = 2 \cdot 9/5 < 4$ . Es fácil verificar (ver la figura 24.26) que  $K_{3,3}$  no tiene ciclos de largo tres, así que esto es imposible.

Como toda cara tiene al menos tres lados, y al sumar sobre todas las caras los arcos se cuentan dos veces, tenemos:

$$2e \geq 3f$$

Substituyendo en la fórmula de Euler:

$$\begin{aligned} e + 2 &\leq v + \frac{2e}{3} \\ e &\leq 3v - 6 \end{aligned} \tag{24.1}$$

O sea, los grafos planares son ralos, tienen mucho menos que los arcos posibles.

Otra conclusión inmediata viene de combinar el teorema 24.1 con (24.1):

$$\begin{aligned} \sum_i \delta(v_i) &= 2e \\ \bar{\delta} &= \frac{2e}{v} \\ &\leq \frac{6v - 12}{v} \\ &< 6 \end{aligned} \tag{24.2}$$

Por lo tanto, tienen que haber vértices de grado menor a seis en todo grafo planar.

**Teorema 24.13.** *Hay cinco sólidos regulares.*

*Demostración.* Si tomamos el sólido, eliminamos una de sus caras y extendemos sus aristas en un plano, obtenemos un grafo planar al tomar los vértices del sólido como vértices del grafo, y las aristas como arcos. Un ejemplo lo da el dodecaedro (sólido con 12 caras pentagonales), figura 24.27. Podemos aplicar la fórmula de Euler al grafo resultante. Sean las caras del sólido de  $p$  lados, y se

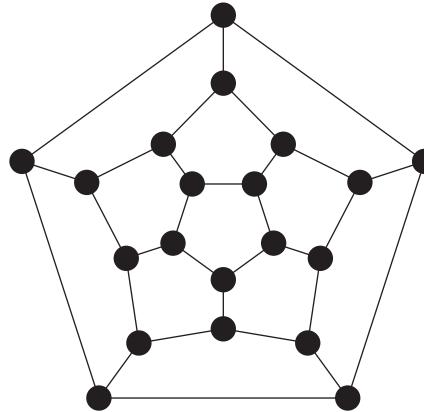


Figura 24.27 – El grafo del dodecaedro

encuentran  $q$  aristas en cada vértice. Por lo anterior,  $pf = 2e$ . Además, como cada arista conecta dos vértices,  $qv = 2e$ . Substituyendo estos en la fórmula de Euler resulta:

$$\begin{aligned} \frac{2e}{p} + \frac{2e}{q} - e &= 2 \\ \frac{1}{p} + \frac{1}{q} &= \frac{1}{2} + \frac{1}{e} \end{aligned} \tag{24.3}$$

Por otro lado, debe ser  $p \geq 3$  y  $q \geq 3$ , las caras deben tener al menos tres lados y deben encontrarse al menos tres aristas en un vértice. Si  $p$  y  $q$  fueran ambos mayores que tres, quedaría:

$$\frac{1}{p} + \frac{1}{q} \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

Esto contradice a (24.3), por tanto debe ser  $p = 3$  o  $q = 3$ . Si  $p = 3$ , de (24.3) resulta:

$$\frac{1}{q} - \frac{1}{6} = \frac{1}{e} \tag{24.4}$$

Como (24.4) debe ser positivo, solo están las posibilidades  $q = 3, 4, 5$ . Estas dan, respectivamente  $e = 6, 12, 30$ . De la misma forma,  $q = 3$  da opciones  $p = 3, 4, 5$  que dan  $e = 30, 12, 6$ . Esto da las cinco

$\{p, q\}$	$f$	$e$	$v$	Nombre
$\{3, 3\}$	4	6	4	tetraedro
$\{4, 3\}$	6	12	8	cubo
$\{3, 4\}$	8	12	6	octaedro
$\{5, 3\}$	12	30	20	dodecaedro
$\{3, 5\}$	20	30	12	icosaedro

Cuadro 24.4 – Poliedros regulares

combinaciones listadas en el cuadro 24.4, que resultan ser todas posibles.  $\square$

Un problema famoso, planteado en 1852 por Francis Guthrie, es demostrar que bastan cuatro colores para pintar un mapa de forma que no hayan regiones del mismo color con fronteras (líneas, no simplemente puntos) en común. Esto es equivalente a demostrar que bastan cuatro colores para colorear todos los grafos planares: Considere cada región a colorear como un vértice del grafo, y conecte regiones vecinas con arcos. Este grafo claramente es planar, y un coloreo de él corresponde a una asignación de colores a las regiones. La primera demostración fue publicada por Appel y Haken [14, 15]. La demostración parte de que todo posible contraejemplo contiene uno de 1936 mapas irreductibles, y verificar que todos ellos pueden colorearse con cuatro colores. Esta tarea se hizo mediante un programa de computador, lo que produjo un motín entre los matemáticos (ver por ejemplo Swart [343]), e intentos de una nueva manera de ver lo que significa “demostración” (Tymoczko [357]). Fue el primer teorema importante en cuya demostración el computador resulta indispensable, es de suponer que es por esto que Petkovsek, Wilf y Zeilberger [283] tienen tanto cuidado de indicar que sus técnicas de demostración de identidades con sumatorias (que requieren el apoyo del computador, es común que deban revisar centenares de opciones) dan lugar a un “certificado”, que permite verificar el resultado manualmente.

Algunos detalles de la historia del problema y de las técnicas empleadas por Appel y Haken discute Thomas [348], desde entonces se han publicado demostraciones adicionales (todas apoyadas de una forma u otra por el computador, con lo que desafortunadamente no aplacan los recelos).

## 24.11. Algoritmos de búsqueda en grafos

En muchas aplicaciones se requiere recorrer un grafo en forma completa (visitar cada uno de sus vértices), o al menos encontrar algún vértice que cumpla ciertas condiciones especiales. Esto lleva a considerar algoritmos de búsqueda en grafos (aunque tal vez un mejor nombre sería algoritmos de recorrido).

### 24.11.1. Búsqueda en profundidad

La idea de este algoritmo es partir de un vértice, visitar algún vecino de este y continuar de allí hasta llegar a un vértice ya visitado o no poder continuar, para luego retornar al vértice anterior y continuar con su siguiente vecino. Se le llama *búsqueda en profundidad* porque la estrategia esbozada avanza a través del grafo todo lo que puede antes de considerar alternativas. En inglés se llama *Depth First Search*, abreviado *DFS*.

#### Ejemplo 24.9. Búsqueda en profundidad

Consideremos el grafo de la figura 24.28. El grafo de la figura 24.29 fue recorrido siguiendo el algoritmo búsqueda en profundidad. Se partió desde el vértice 1, y desde allí se recorrió y enumeró el resto de los vértices, eligiendo uno al azar como vecino a considerar luego. En rojo quedan registrados los arcos por los cuales se pasó.

Búsqueda en profundidad recorre un árbol recubridor del grafo. En general entrega un componente conexo del grafo, para encontrar todos los componentes conexos basta con repetir la búsqueda partiendo cada vez de un vértice aún no visitado hasta agotar los vértices. Ver el algoritmo 24.2 para una versión recursiva, que se invoca como  $DFS(v)$  para un vértice del grafo. Se usan marcas *considerado* y *visitado* en este algoritmo (y sus sucesores) para evitar caer en ciclos infinitos: Un vértice *considerado* pero no *visitado* está pendiente; si está *visitado* ya fue procesado y no requiere más atención. El algoritmo 24.3 es una versión que usa un *stack* explícitamente (resultado de eliminar la recursión). Debe tenerse cuidado de no incluir los vértices varias veces, por eso se marcan como considerados cuando se agregan al *stack*.

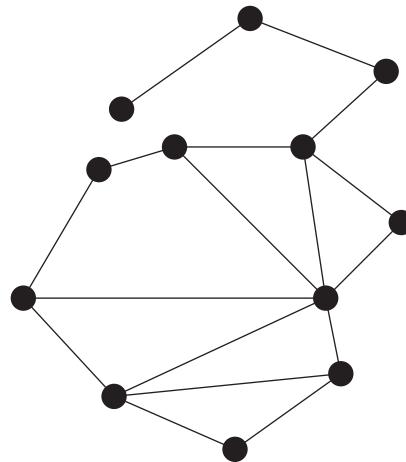


Figura 24.28 – Grafo para ejemplos de recorrido

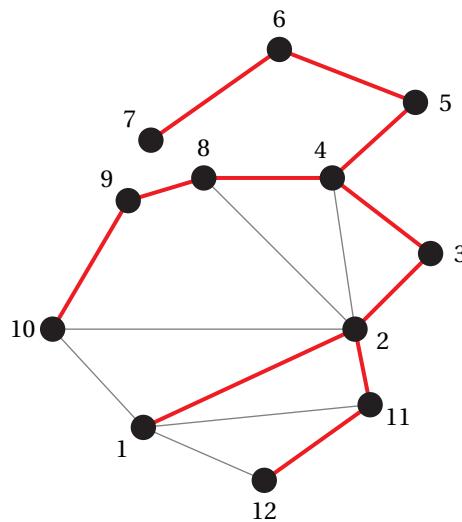


Figura 24.29 – El grafo de la figura 24.28 recorrido en profundidad

---

Algoritmo 24.2: Búsqueda en profundidad, versión recursiva

---

```

procedure DFS(x)
    Marque x considerado
    if x no visitado then
        Marque x visitado
        foreach y adyacente a x, no visitado y no considerado do
            Marque y considerado
            DFS(y)
        end
    end

```

---

---

Algoritmo 24.3: Búsqueda en profundidad, versión no recursiva

---

```

procedure DFS(x)
  variables S: Stack de vértices
  Marque x considerado
  push(S, x)
  while S no vacío do
    x  $\leftarrow$  pop(S)
    if x no visitado then
      Marque x visitado
      foreach y adyacente a x, no visitado y no considerado do
        Marque y considerado
        push(S, y)
      end
    end
  end

```

---

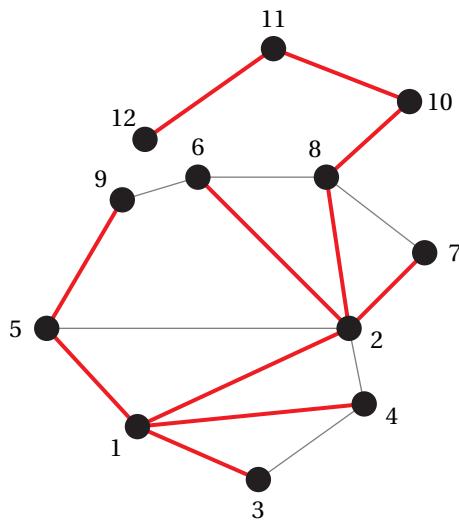


Figura 24.30 – El grafo de la figura 24.28 recorrido a lo ancho

**24.11.2. Búsqueda a lo ancho**

Acá se visitan los vecinos del punto de partida, y recién cuando se han visitado todos ellos se avanza a los vecinos de estos. Por la forma en que avanza en el grafo se le llama *búsqueda a lo ancho*, en inglés *Breadth First Search*, que se abrevia *BFS*. Una manera simple de manejar primero todos los vecinos, y recién después los vecinos de estos, es ingresar los nodos en una cola de espera (*queue* en inglés).

**Ejemplo 24.10.** Búsqueda a lo ancho

Tomando el grafo del ejemplo de búsqueda en profundidad (ver figura 24.28), ahora se enumeran los vértices y se marcan los arcos recorridos, pero ahora con el método de búsqueda a lo ancho. Véase la figura 24.30.

Más formalmente el algoritmo para buscar a lo ancho es el [24.4](#). Usamos marcas para asegurar-

---

Algoritmo 24.4: Búsqueda a lo ancho

---

```

procedure BFS( $x$ )
variables  $Q$ : Queue de vértices
    Marque  $x$  considerado
    enqueue( $Q, x$ )
    while  $Q$  no vacío do
         $x \leftarrow$  dequeue( $Q$ )
        if  $x$  no visitado then
            Marque  $x$  visitado
            foreach  $y$  adyacente a  $x$ , no visitado y no considerado do
                Marque  $y$  considerado
                enqueue( $Q, y$ )
            end
        end
    end

```

---

nos de no agregar el mismo nodo varias veces.

#### 24.11.3. Búsqueda a lo ancho versus búsqueda en profundidad

Si comparamos los dos procedimientos (algoritmos [24.3](#) y [24.4](#)) se ve que la única diferencia es el orden en que se procesan los vértices. En el peor caso, se exploran todos los vértices y se recorren todos los arcos, y la complejidad es simplemente  $O(|V| + |E|)$  para ambos. Podemos resumir las características de ambos algoritmos como sigue:

- Ambos llegan a todos los vértices del componente conexo.
- Los programas son similares, aunque búsqueda en profundidad (recursivo) es un tanto más simple de programar.
- Complejidad (equivalente a tiempo de ejecución) similares.

La pregunta entonces es cómo elegir entre los dos.

- Si interesa una solución cualquiera: Usar búsqueda en profundidad.
- Si interesa “la mejor” (por lo general referida a cercanía de vértices): Usar búsqueda a lo ancho.

Pero un análisis más profundo de los dos algoritmos muestra que tienen una estructura común: Guardan vértices para considerarlos más adelante en alguna estructura, la única diferencia es si se procesan en orden de llegada (al buscar a lo ancho) o se atiende primero al último en llegar (búsqueda en profundidad). Claramente podemos usar algún otro criterio para elegir el siguiente vértice a considerar, no solamente el momento en que nos encontramos con él por primera vez. Esto da lugar a una gama de métodos de búsqueda heurísticos.

## 24.12. Colorear vértices

Hay muchas situaciones en las cuales interesa encontrar una asignación que respeta restricciones dadas. Una forma de representar estas es modelando las entidades a recibir asignaciones como vértices, las asignaciones como colores de los vértices, las restricciones entre asignaciones como arcos entre los vértices, y buscamos asignar colores a los vértices de forma que vértices vecinos siempre tengan colores diferentes.

**Ejemplo 24.11.** Consideremos la situación en que deseamos programar seis charlas, cada una de una hora. Hay interesados en asistir a varias de ellas, en particular, hay interesados en las charlas 1 y 2, en las 1 y 4, en 1 y 6, en 2 y 6, en 3 y 5, en 4 y 5, en 5 y 6. Debemos programar las charlas en el mínimo número de horas.

Podemos modelar esto mediante un grafo, conectando las charlas que tienen asistentes en común, véase la figura 24.31. Por ejemplo, podemos asignar las charlas  $v_1$  y  $v_3$  a la hora 1,  $v_2$  y  $v_4$  a la

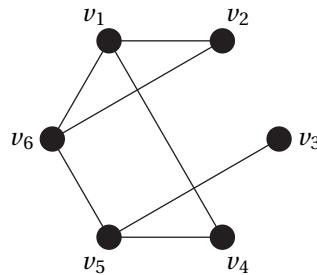


Figura 24.31 – Grafo representando charlas

hora 2,  $v_5$  a la hora 3, y finalmente  $v_6$  a la hora 4. Si representamos la hora 1 con color azul, la 2 con rojo, la 3 con amarillo y la 4 con verde, se obtiene lo que muestra la figura 24.32.

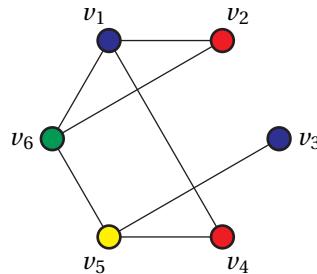


Figura 24.32 – Asignación de horas a charlas como colores

En términos matemáticos, hemos particionado los vértices del grafo en cuatro, de forma que no hayan vértices adyacentes en ninguna de las partes. Una forma de representar esta situación usa la función  $c: V \rightarrow [4]$  que a cada vértice (charla) le asigna una hora. Generalmente hablamos de colores de los vértices, no de horas asignadas, aunque claramente la naturaleza exacta de los objetos  $\{1, 2, 3, 4\}$  es irrelevante. Podemos hablar de colores azul, rojo, amarillo, verde, o de hora 1, hora 2, hora 3, hora 4. Lo único que importa es que vértices vecinos tienen colores diferentes.

**Definición 24.14.** Un *coloreo de vértices* de un grafo  $G = (V, E)$  es una función  $c: V \rightarrow \mathbb{N}$  tal que  $c(x) \neq c(y)$  siempre que  $xy \in E$ .

**Definición 24.15.** El *número cromático* de un grafo  $G = (V, E)$ , escrito  $\chi(G)$ , es el mínimo entero  $k$  tal que el grafo tiene un colooreo de  $k$  colores.

Volviendo a nuestro ejemplo, la asignación de horas de la figura 24.32 corresponde a un colooreo con 4 colores. Pero probando un poco con 3 horas vemos que podemos asignar  $v_1$  y  $v_5$  a la hora 1,  $v_2$  y  $v_3$  a la hora 2, y dejar  $v_4$  y  $v_6$  para la hora 3. Ver la figura 24.33. Por lo demás, se requieren al menos

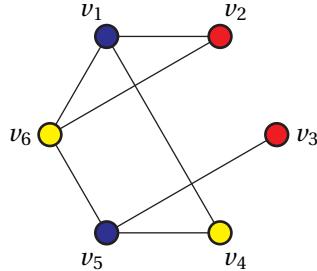


Figura 24.33 – Otra asignación de horas a charlas

3 colores ya que  $v_1$ ,  $v_2$  y  $v_6$  están conectados entre sí. Hemos demostrado que el número cromático de este grafo es 3.

En general, para demostrar que el número cromático de un grafo es  $k$  se requiere:

1. Encontrar un colooreo con  $k$  colores.
2. Demostrar que es imposible hacerlo con menos de  $k$  colores.

Este problema es NP-completo, uno de los 21 problemas identificados inicialmente como intratables por Karp [197].

#### Ejemplo 24.12. Números cromáticos

Veamos cuántos colores se necesitan para colorear el grafo de la figura 24.34.

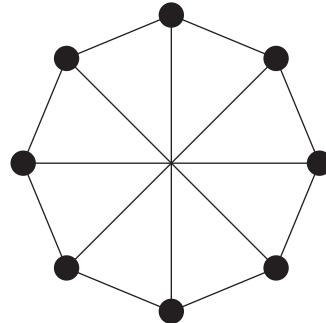


Figura 24.34 – Grafo a colorear

Como el grafo contiene ciclos de largo impar (por ejemplo el de la figura 24.35), se desprende la necesidad de al menos 3 colores. La figura 24.36 muestra un colooreo con 3 colores, por lo que el número cromático del grafo es precisamente 3.

#### Ejemplo 24.13. Números cromáticos: Otro caso.

Consideremos el grafo de la figura 24.37.

Dado que son 6 vértices, el número de colores es a lo más 6. En la figura 24.38a se marca un ciclo

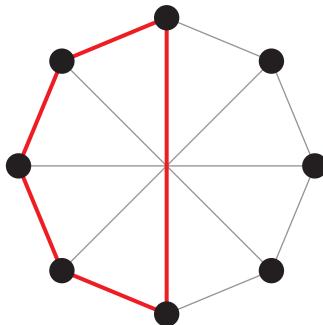


Figura 24.35 – Un ciclo de largo impar en el grafo de la figura 24.34

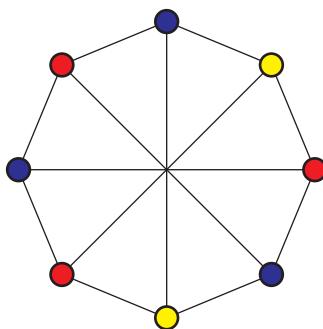


Figura 24.36 – Un colooreo con tres colores del grafo de la figura 24.34

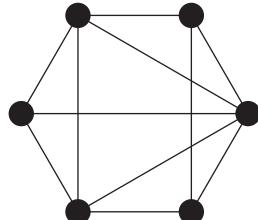


Figura 24.37 – Otro grafo a colorear

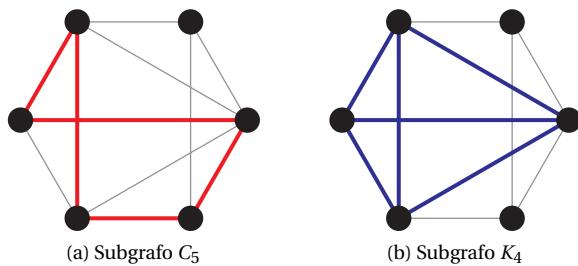


Figura 24.38 – Subgrafos del grafo de la figura 24.37

impar en rojo, lo que indica que necesitan a lo menos 3 colores. Pero se ve en azul en la figura 24.38b que el grafo tiene  $K_4$  como subgrafo, lo que indica que el número de colores tiene que ser a lo menos 4. La figura 24.39 muestra un coloreo con 4 colores, el número cromático es 4.

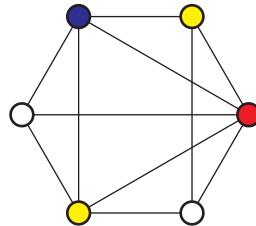


Figura 24.39 – Coloreo con cuatro colores del grafo de la figura 24.37

Como se comentó antes, muchos problemas de asignación de recursos pueden modelarse mediante coloreo de grafos. Por esta razón el encontrar soluciones óptimas (coloreo usando  $\chi(G)$  colores) o al menos buenas (pocos más que  $\chi(G)$  colores) tienen inmensa importancia práctica. Siendo un problema NP-completo la investigación se concentra en hallar soluciones a casos especiales o hallar métodos aproximados.

Por ejemplo, al compilar código para un programa interesa guardar los más valores posibles en los registros del procesador, de forma de que acceder a ellos sea más rápido, compárese con la sección 24.9.3. Una manera de hacer esto da Chaitin [68] vía construir un grafo (*el grafo de interferencia*) cuyos vértices son los valores y hay un arco entre un par de valores si sus vidas (desde el instante de creación hasta el último uso) se traslanan. El mínimo número de registros requeridos es simplemente el número cromático del grafo de interferencia, y un coloreo mínimo es una asignación de valores a esos registros. Se obtiene un coloreo ordenando los vértices en orden de grado decreciente y aplicando el algoritmo voraz. Esto es rápido y da un coloreo suficientemente bueno en la práctica.

Delahaye [88] indica que el popular puzzle Sudoku puede interpretarse como completar un coloreo de un grafo de 81 vértices con 9 colores.

#### 24.12.1. El algoritmo voraz para colorear grafos

Encontrar el número cromático de un grafo es un problema NP-completo. Sin embargo, hay una forma simple de construir un coloreo de vértices usando un número “razonable” de colores. La idea es ir asignando colores a los vértices de forma de usar siempre el primer color que no produce conflictos. El algoritmo representa los colores asignados a los vértices mediante el arreglo  $c$  (índices son los vértices). Usamos el “color” 0 para indicar que el vértice aún no ha sido coloreado. El conjunto  $S$  recoge los colores de los vecinos del vértice bajo consideración.

Por ejemplo, el coloreo de la figura 24.32 resulta aplicando el algoritmo 24.5 a los vértices del grafo de la figura 24.31 en orden del número del vértice. El coloreo de la figura 24.36 resulta de asignar colores azul, rojo, amarillo mediante el algoritmo voraz partiendo del vértice superior y avanzando en sentido contra reloj. El lector podrá entretenérse usando este algoritmo para colorear el grafo de la figura 24.28 siguiendo ya sea el orden de la figura 24.29 o de la figura 24.30, y de hallar el número cromático.

El algoritmo 24.5 es corto de vista, por lo que el coloreo que entrega no necesariamente es bueno. Sin embargo, puede producir el coloreo con el mínimo número de colores, dependiendo del orden en que se consideren los vértices. Lo malo es que si hay  $n$  vértices son  $n!$  órdenes diferentes a considerar. A pesar de esto, el algoritmo es útil en teoría y en la práctica. Demostraremos un teorema usando esta estrategia.

---

Algoritmo 24.5: Coloreo voraz

---

```

procedure GreedyColoring( $G$ )
   $n \leftarrow$  Número de vértices de  $G$ 
  for  $i \leftarrow 1$  to  $n$  do
     $c[v_i] \leftarrow 0$ 
  end
   $c[v_1] \leftarrow 1$ 
  for  $i \leftarrow 2$  to  $n$  do
     $S \leftarrow \emptyset$ 
    for  $j \leftarrow 1$  to  $i - 1$  do
      if  $v_j$  es adyacente a  $v_i$  y no ha sido coloreado then
         $S \leftarrow S \cup \{c[v_j]\}$ 
      end
    end
     $c[v_i] \leftarrow$  primer color no en  $S$ 
  end

```

---

**Teorema 24.14.** Si  $G$  es un grafo de grado máximo  $k$ , entonces:

1.  $\chi(G) \leq k + 1$ .
2. Si  $G$  no es regular, entonces  $\chi(G) \leq k$ .

*Demostración.* Como el coloreo de cada componente conexo es independiente del resto del grafo, basta discutir la situación de un grafo conexo. Demostramos cada aseveración por turno.

1. Sea  $v_1, v_2, \dots, v_n$  un orden de los vértices de  $G$ . Si aplicamos el algoritmo de coloreo voraz, al considerar un vértice cualquiera tendrá a lo más  $k$  vecinos con colores ya asignados. Si contamos con  $k + 1$  colores, siempre habrá uno que podamos asignarle.
2. Para este caso consideraremos los vértices en un orden especial. Como el grafo no es regular, habrá al menos un vértice cuyo grado es menor a  $k$ . Llamémosle  $v_n$  a uno de ellos. Numeremos los vecinos de  $v_n$  como  $v_{n-1}, v_{n-2}, \dots$  (hay a lo más  $k - 1$  de estos). Una vez agotados los vecinos de  $v_n$ , numeramos los vecinos de  $v_{n-1}$  distintos de  $v_n$ ; nuevamente habrá a lo más  $k - 1$  de estos. Continuamos de esta forma, siempre dejando fuera de consideración los que ya tienen número asignado. Si ahora aplicamos el algoritmo voraz, siempre que considere un vértice tendrá a lo más  $k - 1$  vecinos ya coloreados, y se requerirán a lo más  $k$  colores.  $\square$

La demostración del primer caso parece poco inteligente, pero considerar el grafo  $K_{k+1}$ , regular de grado  $k$ , muestra que en realidad es lo mejor que puede hacerse. Por el otro lado, el grafo bipartito completo  $K_{n,n}$  es regular de grado  $n$ , pero  $\chi(K_{n,n}) = 2$ .

Esta demostración sugiere la heurística de ordenar los vértices por grado decreciente y luego aplicar el algoritmo voraz como manera de obtener una buena coloración.

## 24.13. Colorear arcos

Una situación análoga al coloreo de vértices se produce si coloreamos arcos de forma que no hayan arcos adyacentes (que comparten vértices) del mismo color. Formalmente:

**Definición 24.16.** Dado un grafo  $G = (V, E)$  un *coloreo de arcos* es una función  $c: E \rightarrow \mathbb{N}$  tal que  $c(e_1) \neq c(e_2)$  si  $e_1 \neq e_2$  y  $e_1 \cap e_2 \neq \emptyset$ .

Acá tenemos una partición de los arcos  $E_1 \cup E_2 \cup \dots \cup E_n$  tal que los arcos en  $E_i$  no tienen vértices en común. La nomenclatura difiere, hay autores que le llaman *número cromático de arcos* al mínimo número de colores en un coloreo de arcos, otros le llaman el *índice cromático* del grafo. Se anota  $\chi'(G)$  o  $\chi_1(G)$ , aunque la noción (y la notación) es mucho menos usada que el número cromático. Nosotros le llamaremos índice cromático, y anotaremos  $\chi'(G)$ .

El índice cromático es 2 para un ciclo de orden par, y 3 para un ciclo de orden impar. Esto provee cotas para el índice cromático de grafos que contienen los anteriores. Obviamente el índice cromático es a lo menos el grado máximo de un vértice.

Un bonito ejemplo es el coloreo de arcos del grafo de Frucht [136] dado en la figura 24.40. Como hay vértices de grado 3 (en realidad es un grafo 3-regular), es imposible un coloreo con menos colores, y su índice cromático es 3.

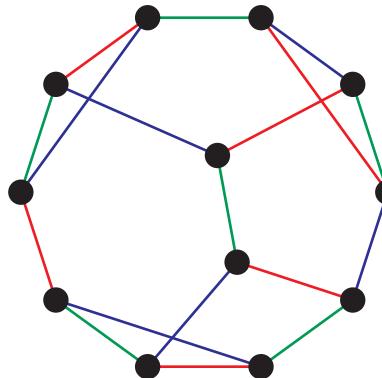


Figura 24.40 – Un coloreo de arcos del grafo de Frucht

Aplicaciones de esto ocurren en muchos problemas de asignar recursos y tareas de manera que no interfieran en el tiempo (ver por ejemplo el texto de Skiena [326]). Al programar la primera ronda de un torneo de fútbol (donde compiten “todos contra todos”) debe hallarse un calendario de forma que a nadie se le solicite estar jugando dos partidos a la vez, pero que también use el mínimo de tiempo (si hay  $N$  equipos en competencia, son  $N(N - 1)/2$  los partidos a jugar, con lo que la solución obvia de programar un partido por semana tomaría demasiado tiempo). Esto se modela mediante un grafo en el que los vértices son los equipos participantes, mientras los arcos son partidos que deben jugarse. El coloreo de arcos entonces asigna fechas a los partidos, de forma que ningún equipo esté jugando dos partidos la misma fecha. Es de suponer que el problema real a resolver por la ANFP es mucho más complejo, al tratar de lograr que todos los fines de semana haya un partido entretenido.

## 24.14. Grafos bipartitos

Un caso especial muy importante son los grafos para los cuales  $\chi(G) = 2$ . En este caso, los vértices se dividen en dos grupos  $V_1$  y  $V_2$  que corresponden a los coloreados con los colores 1 y 2, respectivamente, y los arcos unen uno de cada grupo. En consecuencia, estos grafos se llaman *bipartitos*. Aplicamos esta idea en el ejemplo 24.5 del ratón que come queso. Para representar un grafo bipartito escribiremos  $G = (V_1 \cup V_2, E)$ , bajo el entendido que  $V_1$  y  $V_2$  son las particiones de los vértices según color. Hay muchas situaciones que se pueden modelar de esta forma, veremos algunos ejemplos pronto. Un caso importante es cuando cada vértice de  $V_1$  está conectado con todos los vértices de

$V_2$ . Así obtenemos el *grafo bipartito completo*, que se anota  $K_{m,n}$  si  $|V_1| = m$  y  $|V_2| = n$ . Nótese que  $K_{2,2} \cong C_4$ .

Algunos ejemplos muestran las figuras 24.41 y 24.42. Por razones obvias a los grafos  $K_{1,n}$  se les suele llamar *estrellas*.

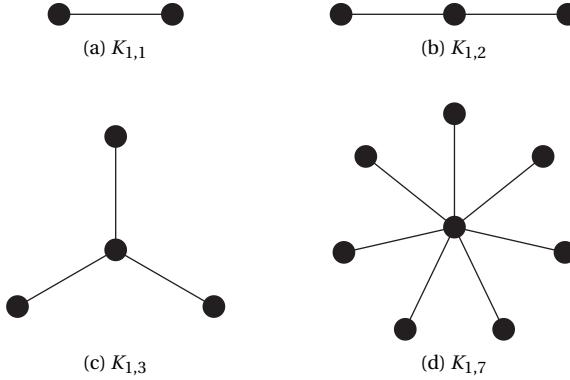


Figura 24.41 – Algunas estrellas

Para grafos bipartitos tenemos:

**Teorema 24.15.** *Un grafo es bipartito si y solo si no tiene ciclos de largo impar.*

*Demostración.* Demostramos implicancias en ambas direcciones.

Si hay un ciclo de largo impar, se requieren tres colores solo para colorear ese ciclo, y  $\chi(G) \geq 3$ . Por el otro lado, si no hay ciclos de largo impar, construiremos un ordenamiento de los vértices que produce un colorado con dos colores. Elijamos un vértice cualquiera, llamémoslo  $v_1$ , y le asignamos el nivel 0. A los vecinos de  $v_1$  les llamamos  $v_2, \dots, v_r$ , les asignamos el nivel 1. A los vecinos de los vértices de nivel 1 que no están ya numerados les asignamos el nivel 2, ..., a los vecinos no numerados de los vértices de nivel  $l - 1$  les asignamos el nivel  $l$ . De esta forma completamos un componente conexo de  $G$ , y procesamos a los demás componentes conexos de la misma forma. Lo crucial de este orden es que un vértice del nivel  $l$  solo tiene vecinos en los niveles  $l - 1$  y  $l + 1$ . Para ver esto, supongamos que hay dos vértices conectados en el mismo nivel. Siguiendo sus conexiones hacia atrás a través de los distintos niveles, encontraremos caminos simples hacia un vértice común, que tendrán el mismo largo, ver la figura 24.43. Pero estos forman un ciclo de largo impar junto con el arco entre los vértices del mismo nivel que supusimos conectados.  $\square$

Una manera tal vez más simple de entender lo anterior (y, a la pasada, dar un algoritmo para determinar si un grafo es bipartito y obtener las particiones) es tomar un vértice cualquiera y pintarlo de rojo, sus vecinos colorearlos de azul, y así sucesivamente ir pintando vértices vecinos aún no coloreados del color contrario (esto corresponde a búsqueda a lo ancho). Si esto termina con todos los vértices coloreados (recomenzando con otro aún no coloreado si se acabaron los vecinos) el grafo es bipartito, si encontramos conflictos (vecinos del mismo color) no lo es. Esto es una aplicación de los algoritmos de recorrido de grafos, y la complejidad es simplemente  $O(|V| + |E|)$ .

**Lema 24.16.** *Sea  $G = (X \cup Y, E)$  un grafo bipartito con arcos entre  $X$  e  $Y$ . Entonces:*

$$\sum_{x \in X} \delta(x) = \sum_{y \in Y} \delta(y) = |E|$$

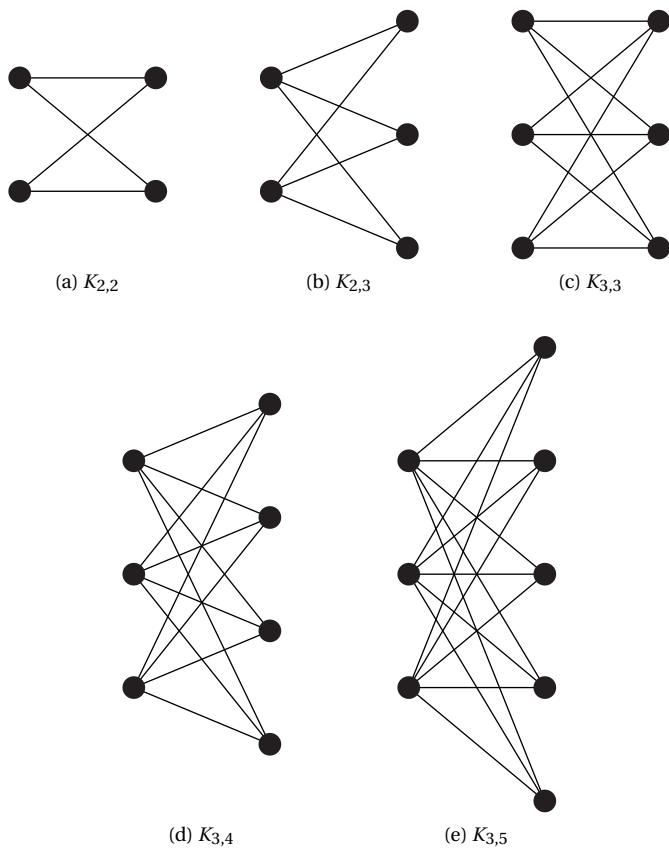


Figura 24.42 – Algunos grafos bipartitos completos

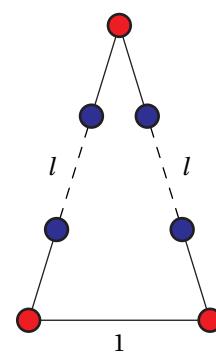


Figura 24.43 – Un ciclo de largo  $2l + 1$  si hay conexiones cruzadas

*Demostración.* Cada arco tiene un vértice en  $X$ , y la primera suma es el número total de arcos vistos desde  $X$ . Lo mismo respecto a la segunda suma e  $Y$ .  $\square$

**Teorema 24.17.** *El índice cromático de un grafo bipartito es su grado máximo.*

*Demostración.* Sea el grafo  $G = (V, E)$ . Usamos inducción sobre el número de arcos  $m = |E|$ .

**Base:** Cuando  $m = 1$ , hay un único arco, y el grado máximo es 1. Claramente basta un color en este caso.

**Inducción:** Supongamos ahora que es cierto para todos los grafos bipartitos de  $m$  arcos y grado máximo  $k$ . Consideremos un grafo bipartito  $G = (X \cup Y, E)$  con  $m + 1$  arcos y grado máximo  $k$ . Elegimos un arco  $xy \in E$ , y consideramos el grafo  $G' = (X \cup Y, E')$  donde  $E' = E \setminus xy$ . El grafo  $G'$  tiene  $m$  arcos, y por inducción admite un colooreo de arcos con  $k$  colores. En  $G$ , tanto  $x$  como  $y$  tienen grado a lo más  $k$ ; y al eliminar el arco  $xy$ , en  $G'$  es  $\delta(x) \leq k - 1$ . De la misma forma  $\delta(y) \leq k - 1$ . Luego tanto  $x$  como  $y$  participan en a lo más  $k - 1$  arcos y por tanto están rodeados por a lo más  $k - 1$  colores.

Ahora sea  $\alpha$  un color no adyacente a  $x$  y  $\beta$  un color no adyacente a  $y$  (los llamaremos *libres* en  $x$  e  $y$ , respectivamente). Estos colores deben existir por lo anterior. Se pueden presentar dos casos:

**Caso simple:** Podemos elegir  $\alpha = \beta$ . Tomamos ese color para el arco y asunto resuelto.

**Caso complejo:** No podemos elegir  $\alpha = \beta$ . Entonces hay un arco  $xy_1$  de color  $\beta$  (de caso contrario  $\beta$  estaría libre en  $x$  y podría elegir  $\alpha = \beta$  como en el caso anterior). Puede haber un arco  $x_1y_1$  de color  $\alpha$ , un arco  $x_1y_2$  de color  $\beta$  y así sucesivamente (vamos de  $X$  a  $Y$  mediante arcos de color  $\beta$ , y de  $Y$  a  $X$  a través de arcos de color  $\alpha$ ). Este proceso de crear un camino debe terminar, ya que el grafo tiene un número finito de vértices, y no puede formar un ciclo ya que no hay arco de color  $\alpha$  en  $x$ . Como ilustra la figura 24.44, luego de

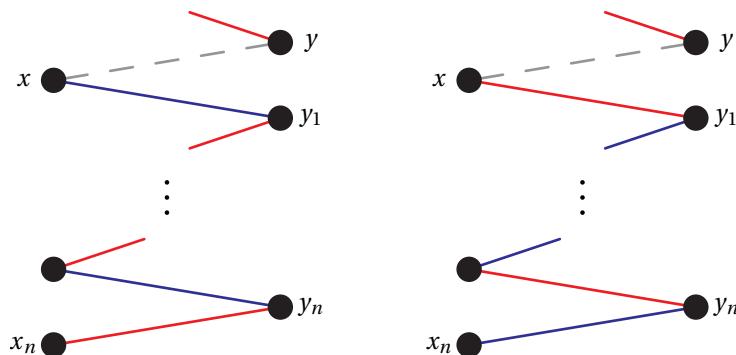


Figura 24.44 – Cómo operar en el teorema 24.17

este proceso podemos intercambiar los colores  $\alpha$  y  $\beta$ , cayendo en el caso simple.

Por inducción, el resultado vale para todos los grafos bipartitos.  $\square$

Esta técnica de zig-zag e intercambio vale la pena tenerla presente, bastantes demostraciones se basan en ella.

### 24.14.1. Matchings

Supongamos la situación en que hay un conjunto  $X$  de personas y un conjunto  $Y$  de trabajos. Una pregunta con implicancias obvias es la siguiente: ¿Cómo asignamos personas a las tareas, de forma que el número máximo de personas queda asignada a una tarea para la que está calificada? Esta pregunta la traduciremos al lenguaje de grafos bipartitos. La relación “estar calificado” da un grafo bipartito  $G = (X \cup Y, E)$ : El arco  $xy$  indica que la persona  $x$  está calificada para la tarea  $y$ . Una asignación de tareas a personas corresponde a un *matching* en el sentido técnico que definiremos ahora. Otras aplicaciones de estas ideas ocurren en una gran variedad de áreas, llegando a la economía. Cabe hacer notar que los conjuntos  $X$  e  $Y$  no necesariamente son de la misma cardinalidad. Bajo nuestra interpretación tiene perfecto sentido considerar situaciones en que hay más (o menos) tareas a asignar que personas, tareas para las que no hay calificados, y personas que no están calificadas para ninguna de las tareas.

**Definición 24.17.** Sea  $G = (V, E)$  un grafo. Un *matching* es un subconjunto  $M \subseteq E$  de arcos tal que no hay vértices en común entre dos arcos. El *tamaño* del *matching* es el número de arcos en él. Un *matching* de  $G$  se dice *maximal* si no hay *matchings* de mayor tamaño en  $G$ . Un *matching*  $M$  se dice que *satura* a los vértices  $U \subseteq V$  si todos los vértices de  $U$  participan en  $M$ .

El caso más importante de lo anterior se da en grafos bipartitos, como se comentó antes. Por ejemplo, la figura 24.45 muestra dos *matchings* de un grafo, donde los arcos en  $M$  están marcados. El *matching*  $M_2$  es mayor, en el sentido que contiene más arcos. No puede haber uno mayor, ya

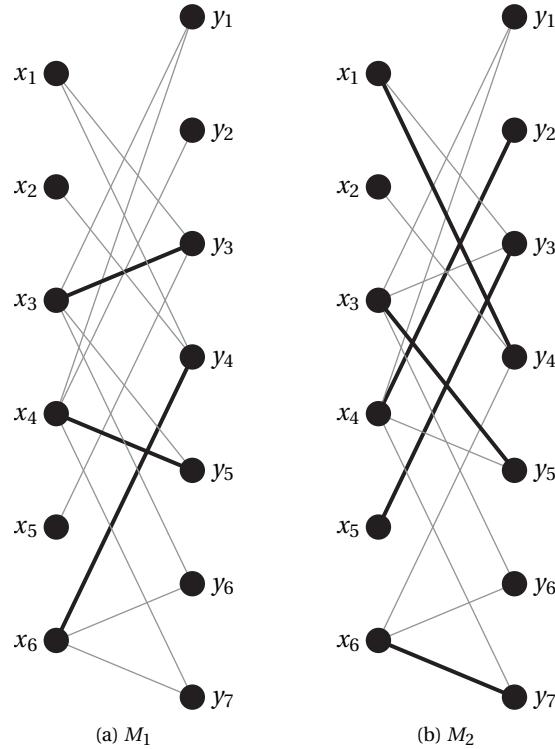


Figura 24.45 – Matchings en un grafo bipartito

que si consideramos el conjunto  $\{x_1, x_2, x_5\}$ , en total solo están capacitados para  $\{y_3, y_4\}$ , por lo que necesariamente quedará uno de los tres sin trabajo asignado. Esto motiva lo siguiente.

**Definición 24.18.** Sea  $G = (X \cup Y, E)$  un grafo bipartito. Un *matching* es *completo* si  $|M| = |X|$  (vale decir, *satura* a  $X$ ).

Analicemos primero las condiciones bajo las cuales hay *matchings* completos. Supongamos un grafo bipartito  $G = (X \cup Y, E)$ , y para todo  $A \subseteq X$  definimos el conjunto de vértices vecinos (*neighbors* en inglés) como:

$$N(A) = \{y: xy \in E \text{ para algún } x \in A\}$$

En un *matching* completo el conjunto de tareas asignadas a los integrantes de  $A$  es un subconjunto de  $N(A)$ , debe ser  $|N(A)| \geq |A|$  para todo  $A \subseteq X$ . En nuestro ejemplo es  $N(\{x_1, x_2, x_5\}) = \{y_3, y_4\}$ , y como  $|N(\{x_1, x_2, x_5\})| < |\{x_1, x_2, x_5\}|$  no hay *matching* completo posible.

Resulta que esta condición se cumpla para todo subconjunto de  $X$  es necesario y suficiente para la existencia de un *matching* completo, como demostraremos a continuación.

**Teorema 24.18 (Hall).** Sea  $G = (X \cup Y, E)$  un grafo bipartito. Entonces hay un matching completo de  $G$  si y solo si para todo  $A \subseteq X$  tenemos  $|N(A)| \geq |A|$ .

*Demostración.* Demostramos implicancia en ambos sentidos. Para simplificar la discusión, seguiremos hablando de trabajos, calificación para los mismos y trabajos asignados.

Si hay un *matching* completo, para cada subconjunto  $A \subseteq X$  tenemos en  $N(A)$  al menos los trabajos asignados a los integrantes de  $A$ , o sea  $|N(A)| \geq |A|$ .

Al revés, supongamos que para todo  $A \subseteq X$  se cumple  $|N(A)| \geq |A|$ , y consideremos un *matching* maximal  $M$  de  $G$ . Demostraremos por contradicción que  $M$  es completo. Si  $M$  no es completo, demostraremos cómo construir un nuevo *matching*  $M'$  tal que  $|M'| = |M| + 1$ , lo que contradice a que  $M$  era maximal. Llamaremos  $A_M(B)$  al conjunto de personas a las que el *matching*  $M$  asigna los trabajos en  $B \subseteq Y$ .

Como  $M$  no es completo, hay  $x_0 \in X$  que no participa en  $M$ . Por hipótesis  $x_0$  está calificado al menos para un trabajo, el conjunto de tareas para las que está calificado  $x_0$  es  $N(\{x_0\})$ . Consideremos el conjunto  $X_0 = A_M(N(\{x_0\}))$  (vale decir, las personas que tienen asignados los trabajos para los que está calificado  $x_0$ ). Junto con  $x_0$  son  $|X_0| + 1$  personas, que por hipótesis están calificadas en conjunto al menos para  $|X_0| + 1$  trabajos. Esto significa que hay al menos una persona en  $X_0$  que está calificada para un trabajo que no está en  $N(\{x_0\})$ , y que no tiene ese trabajo asignado. Si agregamos las personas (de haberlas) que tienen asignados esos trabajos a  $X_0$  construimos un conjunto  $X_1$ . Aplicando el mismo proceso nuevamente a  $X_1$  construimos un conjunto  $X_2$ , y así sucesivamente. Este proceso debe terminar, ya que los conjuntos  $X_i$  no pueden crecer en forma indefinida. Pero el proceso termina por hallar trabajos que no están asignados. Tomando uno de ellos y trazando el proceso hacia atrás tenemos un camino que parte de  $x_0$ , va a  $Y$  por una tarea sin asignar, vuelve a  $X$  por una tarea asignada, ..., y finalmente pasa de  $X$  a  $Y$  por una tarea sin asignar. Este camino tiene un arco más fuera de  $M$  que en  $M$ , intercambiando las tareas asignadas con las sin asignar en él da un *matching* mayor que  $M$ . Pero habíamos supuesto que  $M$  es maximal, una contradicción. Por tanto, si  $M$  es maximal bajo la hipótesis dada, es completo.  $\square$

La demostración del teorema de Hall motiva la siguiente:

**Definición 24.19.** Sea  $G = (X \cup Y, E)$  un grafo bipartito, y  $M$  un *matching* de  $G$ . Un camino en  $G$  se llama *alternante para*  $M$  si alterna arcos de  $M$  con arcos que no están de  $M$ . Un camino alternante se llama *aumentante para*  $M$  si comienza y termina en vértices que no participan en  $M$  (el primer y el último arco del camino no están en  $M$ ).

Nuestra discusión previa indicaría que de  $A$  a lo más  $|N(A)|$  podrán encontrar trabajo. Esto lleva a:

**Definición 24.20.** Sea  $G = (X \cup Y, E)$  un grafo bipartito. La *deficiencia* de  $G$  es:

$$d = \max_{A \subseteq X} \{|A| - |N(A)|\}$$

Siempre podemos tomar  $A = \emptyset$ , y en tal caso  $|A| - |N(A)| = 0$ , con lo que la deficiencia nunca es negativa.

Con esto podemos demostrar:

**Teorema 24.19.** Sea  $G = (X \cup Y, E)$  un grafo bipartito de deficiencia  $d$ . Entonces el matching maximal  $M$  de  $G$  cumple  $|M| = |X| - d$ .

*Demostración.* Primeramente, si  $A \subseteq X$  es un conjunto para el cual  $d = |A| - |N(A)|$ , a lo menos  $d$  elementos de  $A$  quedarán sin  $Y$  asignado, y así ningún *matching* puede tener más que el tamaño indicado. Basta entonces demostrar que hay un *matching* de ese tamaño.

Sea  $D$  un conjunto de vértices nuevos con  $|D| = d$ . Definimos el grafo  $G^* = (X^* \cup Y^*, E^*)$  mediante:

$$\begin{aligned} X^* &= X \\ Y^* &= Y \cup D \\ E^* &= E \cup \{xy : x \in X \wedge y \in D\} \end{aligned}$$

Estamos agregando un nuevo conjunto de trabajos  $D$  para los que todos están calificados. Entonces  $G^*$  cumple con las condiciones del teorema de Hall y tiene un *matching* completo  $M^*$ . Pero  $M^*$  incluye todos los vértices de  $D$ , ya que si  $A$  es un conjunto para el cual  $d = |A| - |N(A)|$  es máximo, la única forma de parear todos los elementos de  $A$  es incluir los elementos de  $D$  en el pareo. Eliminando los arcos que incluyen vértices de  $D$  de  $M^*$  obtenemos un *matching* de tamaño  $|X| - d$ .  $\square$

El teorema 24.19 no es particularmente útil para encontrar un *matching* maximal, ni ayuda a la hora de hallar su tamaño ya que considera analizar los  $2^{|X|}$  subconjuntos de  $X$  para determinar la deficiencia. Una forma práctica de encontrar *matchings* maximales las da el siguiente teorema.

**Teorema 24.20** (Lema de Berge). *Sea  $G = (X \cup Y, E)$  un grafo bipartito, y  $M$  un matching de  $G$ . Si  $M$  no es maximal,  $G$  contiene un camino aumentante para  $M$ .*

*Demostración.* Sea  $M^*$  un *matching* maximal de  $G$ , y sea  $F = M^* \Delta M$  el conjunto de arcos en que están en  $M^*$  o  $M$ , pero no en ambos. Los arcos en  $F$  y los vértices que contienen forman un grafo bipartito cuyos vértices tienen grado 1 o 2, por lo que sus componentes conexos son caminos y ciclos. Pero en todo camino o ciclo los arcos de  $M$  alternan con arcos no de  $M$ , por lo que en todo ciclo el número de arcos en  $M$  debe ser igual al número de arcos no en  $M$  (al ser  $G$  bipartito, no tiene ciclos de largo impar). Como  $|M^*| > |M|$ , hay más arcos de  $M^*$  que arcos de  $M$  en  $F$ . Por lo tanto, hay al menos un componente conexo de  $F$  que es un camino con más arcos en  $M^*$  que en  $M$ , y este es un camino aumentante para  $M$ .  $\square$

Esto sugiere la siguiente estrategia para hallar un *matching* maximal:

1. Comience con un *matching*  $M$  cualquiera (un arco por sí solo sirve).
2. Busque un camino aumentante para  $M$ .

3. Si encontró un camino aumentante, construya un *matching*  $M'$  mejor intercambiando arcos que pertenecen al *matching* con los que no de la forma usual, y vuelva al paso (2) con  $M'$  en vez de  $M$ .
4. Si no hay camino aumentante,  $M$  es maximal.

Para hallar un camino aumentante, podemos usar búsqueda a lo ancho. Comenzando con un vértice  $x_0$  que no tiene trabajo asignado construimos un árbol de caminos aumentantes “parciales” desde  $x_0$  como sigue:

1. En el nivel 1 inserte los vértices  $y_1, y_2, \dots, y_k$  adyacentes a  $x_0$ . Si alguno de estos vértices no tiene *match*, digámoslo  $y_i$ , deténgase. En este caso  $\langle x_0, y_i \rangle$  es un camino aumentante.
2. Si todos los vértices en el nivel 1 tienen *match*, inserte vértices  $x_1, x_2, \dots, x_k$ , los *matches* de  $y_1, y_2, \dots, y_k$ , en el nivel 2.
3. En el nivel 3, inserte los vértices adyacentes a los de nivel 2 que no tienen *match* con ellos. Si alguno de ellos no tiene *match*, deténgase: El camino desde  $x_0$  hasta él es un camino aumentante.
4. Si todos los vértices de nivel 3 tienen *match*, inserte sus *matches* en el nivel 4, ...

Claramente este proceso puede terminar porque no hay vértices a insertar en un nivel impar. En tal caso, no hemos hallado un camino aumentante, y habrá que intentar otro punto de partida. Si ninguno de los vértices sin *match* resulta en un camino aumentante, el *match* que tenemos es maximal.

Consideremos el *matching* en el grafo bipartito de la figura 24.46a. El vértice  $x_2$  no tiene *match*;

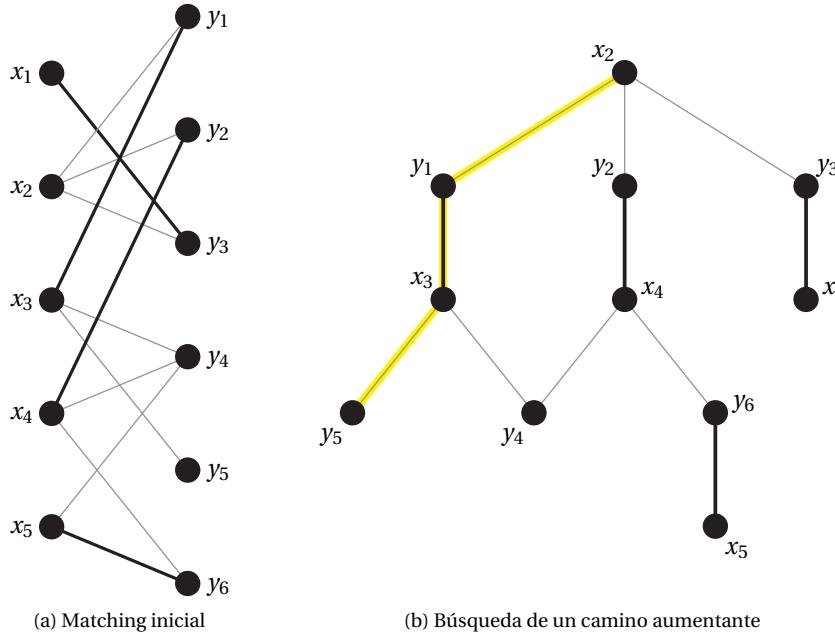


Figura 24.46 – Aumentando un matching

la figura 24.46b muestra el “árbol” construido a partir de ese vértice según la estrategia descrita, indicando un camino aumentante identificado en el proceso; y finalmente la figura 24.47 da el

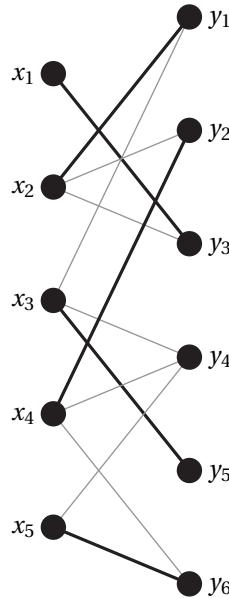


Figura 24.47 – Matching resultante

*matching* que resulta de intercambiar los arcos pertenecientes al *matching* inicial con los que no aparecen en él. Si todos los caminos desde el vértice elegido son como el camino  $\langle x_2 \ y_2 \ x_4 \ y_6 \ x_5 \rangle$ , con el mismo número de arcos en  $M$  y fuera de él, quiere decir que desde ese vértice no hay camino aumentante.

Un algoritmo mejor es el de Hopcroft-Karp [178], que usa la misma estrategia básica, pero identifica todas las extensiones posibles en paralelo.

#### 24.14.2. Transversales de familias de conjuntos finitos

Una situación de interés se da cuando tenemos varios conjuntos que se intersectan, y buscamos encontrar un representante único para cada conjunto.

**Ejemplo 24.14.** En la Universidad de Miskatonic todo se resuelve en comités de sus académicos. Hay seis profesores que participan en los distintos comités, los profesores Atwood, Dexter, Ellery, Freeborn, Halsey y Upham. Están organizados en los siguientes comités:

Académico: Atwood, Upham

Investigación: Atwood, Dexter, Upham

Administración: Dexter, Upham

Estacionamientos: Ellery, Freeborn, Halsey

Se decide que cada comité envíe un representante al nuevo Comité de Comités de la Universidad, y cada uno puede representar solo a un comité. Si un integrante pertenece a varios comités, asiste como representante de uno de ellos solamente. En el ejemplo, Atwood puede representar al comité académico o al de investigación, pero no ambos. ¿Es posible crear este comité?

Dados los miembros de los distintos comités, esto se puede lograr de diferentes formas. Por ejemplo, podemos elegir a Atwood, Dexter, Ellery y Freeborn. Sin embargo, si el comité de estacionamientos estuviera formado solo por Dexter y Ellery, no se puede formar el Comité de Comités.

La forma general de este problema se expresa más claramente usando la noción de *familia de conjuntos*. Tenemos la familia  $\mathcal{F} = \{\mathcal{S}_i : i \in \mathcal{I}\}$  de conjuntos (usamos  $\mathcal{I}$  como el conjunto de los

índices, básicamente los nombres de los conjuntos), no necesariamente diferentes, y buscamos un representante  $s_i$  para cada  $i \in \mathcal{I}$ , tales que cada  $s_i \in \mathcal{S}_i$  y son todos diferentes. Tal conjunto de representantes distintos se llama *transversal* de  $\mathcal{F}$ . Nuestro problema es entonces hallar condiciones que aseguren que la familia  $\mathcal{F}$  tenga un transversal. Esto tiene perfecto sentido incluso cuando  $\mathcal{I}$  es infinito, pero acá nos restringimos a familias finitas. En nuestro ejemplo, el conjunto índice  $\mathcal{I}$  no es más que los nombres de los comités, y  $\mathcal{S}_i$  son los integrantes del comité  $i$ .

En realidad, esto no es más que una forma disfrazada del problema de hallar un *matching*. Para ver esto, construimos un grafo bipartito cuyas partes corresponden a los conjuntos y a los elementos, y hay arcos que unen a los elementos con los conjuntos a los que pertenecen. La figura 24.48 muestra la situación de los comités de la Universidad de Miskatonic.

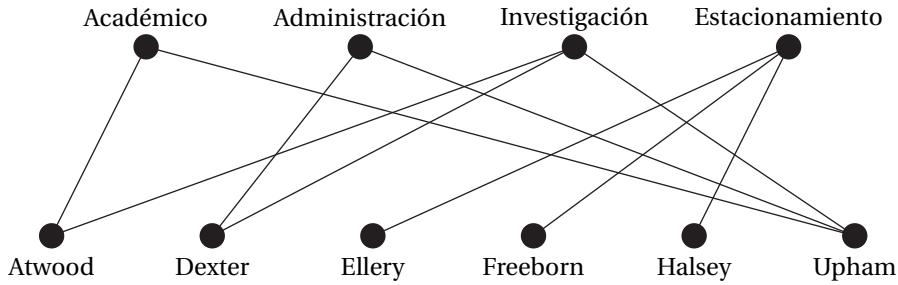


Figura 24.48 – Comités de la Universidad de Miskatonic

Formalmente, definimos  $G = (X \cup Y, E)$  mediante:

$$\begin{aligned} X &= \mathcal{I} && \text{(los nombres de los conjuntos)} \\ Y &= \bigcup_{i \in \mathcal{I}} \mathcal{S}_i && \text{(todos los elementos de los conjuntos)} \end{aligned}$$

y el arco  $iy$  está en  $E$  si  $y \in \mathcal{S}_i$ . Entonces un transversal de  $\mathcal{F}$  no es más que un *matching* completo de  $G$ . En estos términos la condición de Hall es fácil de expresar. Un subconjunto  $\mathcal{H}$  de  $\mathcal{I}$  es una subfamilia de  $\mathcal{F}$ , y  $N(\mathcal{H})$  es simplemente los miembros de todos esos conjuntos:

$$N(\mathcal{H}) = \bigcup_{i \in \mathcal{H}} \mathcal{S}_i$$

Usando esta interpretación, el teorema de Hall [159] es:

**Teorema 24.21** (Hall, versión original). *La familia finita de conjuntos:*

$$\mathcal{F} = \{\mathcal{S}_i : i \in \mathcal{I}\}$$

tiene un transversal si y solo si:

$$\left| \bigcup_{i \in \mathcal{H}} \mathcal{S}_i \right| \geq |\mathcal{H}| \text{ para todo } \mathcal{H} \subseteq \mathcal{I}$$

Una forma simple de expresar esto es decir que cualquier unión de  $k$  de los conjuntos debe tener al menos  $k$  miembros en total.

En realidad este es el teorema de Hall original, que también se conoce como “*Hall's Marriage Theorem*”, por la interpretación siguiente:  $\mathcal{I}$  es un conjunto de mujeres, mientras  $\mathcal{S}_i$  corresponde al conjunto de hombres con los cuales  $i \in \mathcal{I}$  estaría dispuesta a casarse. Entonces hay forma de conseguirle pareja a todas las mujeres si y solo si para cada conjunto de mujeres el conjunto de hombres con los que estarían dispuestas a casarse en total no es menor a ese conjunto de mujeres.

## 24.15. Grafos rotulados

En muchas aplicaciones los arcos tienen asociados “pesos” (costos), definimos entonces un *grafo rotulado* como un grafo  $G = (V, E)$  y una función  $p: E \rightarrow C$  (típicamente  $C$  es  $\mathbb{R}$ ), que asocia el rótulo (peso)  $p(e)$  al arco  $e$ .

Una situación similar se da con rótulos en los vértices (una función  $r: V \rightarrow C$ ). Esto va más allá de la identidad del vértice, pueden haber varios vértices con el mismo rótulo. Hay aplicaciones en las cuales están rotulados los arcos, los vértices, o ambos.

### 24.15.1. Árboles rotulados

El resultado siguiente, debido a Cayley [66], fue uno de los máximos triunfos de la combinatoria del siglo XIX.

**Teorema 24.22** (Cayley). *Hay  $n^{n-2}$  árboles con  $n$  vértices rotulados.*

*Demuestra*ón. Sea  $\mathcal{T}$  la clase de árboles con vértices rotulados. La clase de árboles rotulados con raíz corresponde a marcar uno de los vértices, o sea es  $\mathcal{T}^\bullet$ . Estos a su vez están conformados por el vértice raíz conectado a las raíces de una colección de árboles rotulados. Esto lleva a la ecuación simbólica:

$$\mathcal{T}^\bullet = \mathcal{Z} \star \text{MSET}(\mathcal{T}^\bullet)$$

Para la función generatriz exponencial correspondiente  $z\hat{T}'(z)$  el teorema 21.6 da:

$$z\hat{T}'(z) = ze^{z\hat{T}'(z)}$$

Aplicar la fórmula de inversión de Lagrange, teorema 17.8, da los coeficientes de  $z\hat{T}'(z)$ :

$$\begin{aligned} n \frac{t_n}{n!} &= \frac{1}{n} [u^{n-1}] e^{nu} \\ &= \frac{1}{n} \cdot \frac{n^{n-1}}{(n-1)!} \\ t_n &= n^{n-2} \end{aligned}$$

□

Acá lo derivamos de forma muy simple, las demostraciones tradicionales son complejas. Esta derivación es una clara demostración del poder del método simbólico (capítulo 21) en conjunto con herramientas analíticas como el teorema de inversión de Lagrange (teorema 17.8).

### 24.15.2. Costo mínimo para viajar entre vértices

En muchos casos interesa saber el costo (suma de los pesos de los arcos) para llegar a cada uno de los vértices de  $G$  partiendo desde el vértice  $v$ . Hay varios algoritmos para resolver este importante problema.

#### 24.15.2.1. Algoritmo de Dijkstra

Una solución, debida a Dijkstra [93], es aplicar una variante de búsqueda a lo ancho. Supongamos que tenemos establecido que el camino más corto de  $v$  a  $x$  tiene largo  $l[x]$ . Supongamos que tenemos un vecino  $y$ , para el que tenemos la estimación  $l[y]$ . La ruta más corta que tenemos de  $v$  a  $y$  pasando por  $x$  tiene costo  $l[x] + w(xy)$ , y si nuestra estimación previa  $l[y] > l[x] + w(xy)$ , debiéramos actualizar  $l[y]$ .

Informalmente, el algoritmo es el siguiente: Inicialmente sabemos que  $l[v] = 0$ . Podemos partir con  $l[p] = \infty$  para todos los demás vértices  $p$ , e ir actualizando los  $l[p]$  en búsqueda a lo ancho partiendo de  $v$  con nuestra mejor estimación hasta el momento del largo del camino de  $v$  a cada vértice.

Una manera de entenderlo es considerar el grafo como una colección de hilos de los largos de los arcos y los vértices nudos entre ellos, y ponemos esto sobre la mesa. Tomamos el nudo que representa el vértice inicial, y lo levantamos hasta que un primer nudo se separa de la mesa. Este nudo es el que está más cerca del inicial, y registramos su distancia desde este. Continuamos de la misma forma, cada vez que un nudo se despegue de la mesa es que hemos llegado a su distancia mínima del nudo inicial. En términos de trabajar con el grafo, significa mantener una colección de vértices a los cuales ya conocemos la distancia mínima (inicialmente solo el vértice inicial), y luego ir agregando aquel vértice no incluido aún en la colección que queda más cerca de alguno cuya distancia mínima ya es definitiva.

Una versión más formal es el algoritmo 24.6. Lo que hacemos acá es ir calculando distancias tentativas, y las dejamos definitivas una vez que esté claro que no cambiarán más. El ciclo externo

---

Algoritmo 24.6: Costos mínimos desde el vértice  $v$  (Dijkstra)

---

```

procedure Dijkstra( $G, v$ )
variables  $Q$ : Conjunto de vértices
 $Q \leftarrow V$ 
Marque todos los vértices  $x \in Q$  con  $l[x] = \infty$ 
 $l[v] \leftarrow 0$ 
while  $Q$  no vacío do
    Elija  $x \in Q$  con  $l[x]$  mínimo
    if  $l[x] = \infty$  then Los restantes no son alcanzables
        break
    end
     $Q \leftarrow Q \setminus \{x\}$ 
    foreach  $y$  vecino de  $x$  do
         $l[y] \leftarrow \min\{l[y], l[x] + w(xy)\}$ 
    end
end
```

---

se ejecuta para cada vértice, el ciclo interno considera cada arco una vez. El tiempo de ejecución de este algoritmo depende de la estructura de datos usada para representar el conjunto  $Q$ , siendo:

$$O(|E| \cdot \langle \text{disminuir clave en } Q \rangle + |V| \cdot \langle \text{extraer mínimo de } Q \rangle)$$

Si mantenemos los  $l[x]$  en un arreglo, disminuir la clave es simplemente dos accesos al arreglo, extraer el mínimo es recorrer el arreglo. Esto es:

$$O(|E| + |V|^2) = O(|V|^2)$$

Usando una estructura más sofisticada, como un *Fibonacci heap* [135], los costos amortizados son:

$$\begin{aligned} \langle \text{extraer mínimo de } Q \rangle &= O(\log|Q|) = O(\log|V|) \\ \langle \text{disminuir clave en } Q \rangle &= O(\log|Q|) = O(\log|V|) \end{aligned}$$

y el costo resulta ser:

$$O((|E| + |V|) \log|V|)$$

#### 24.15.2.2. Algoritmo de Bellman-Ford

Otro algoritmo que resuelve el mismo problema, pero que tiene la ventaja de poder manejar arcos con costo negativo (claro que no ciclos de costo negativo, en cuyo caso la distancia mínima no está bien definida), es el de Bellman-Ford [32] (algoritmo 24.7). Que este algoritmo es correcto se

---

Algoritmo 24.7: Costos mínimos desde el vértice  $v$  (Bellman-Ford)

---

```

procedure BellmanFord( $G, v$ )
     $l[v] \leftarrow 0$ 
    Marque todos los vértices  $x \in V \setminus \{v\}$  con  $l[x] = \infty$ 
    for  $i \leftarrow 1$  to  $|V| - 1$  do
        foreach  $xy \in E$  do
             $l[y] \leftarrow \min\{l[y], l[x] + w(xy)\}$ 
        end
    end
    if hay un arco  $xy$  con  $l[x] + w(xy) < l[y]$  then
        /* Hay un ciclo de costo negativo
    end
```

---

demuestra por inducción sobre las ejecuciones del ciclo **for** externo.

**Teorema 24.23.** *Después de  $k$  repeticiones del ciclo, si para un vértice  $u$  tenemos  $l[u] < \infty$  entonces es el largo de algún camino desde  $v$  a  $u$ . Si hay un camino de  $v$  a  $u$  de a lo más  $k$  arcos, entonces  $l[u]$  es a lo más el largo del camino más corto con a lo más  $k$  arcos de  $v$  a  $u$ .*

*Demostración.* Por inducción sobre el número de iteraciones.

**Base:** Cuando  $k = 0$ , antes de ejecutar el ciclo por primera vez. En esta situación  $l[v] = 0$  y para los demás  $l[u] = \infty$ , que corresponde a la situación descrita.

**Inducción:** Primero lo primero. Al ajustar  $l[y] \leftarrow \min\{l[y], l[x] + w(xy)\}$ , por inducción tenemos que  $l[x]$  es el largo de algún camino de  $v$  a  $x$ , y  $l[x] + w(xy)$  es entonces el largo del camino que va de  $v$  a  $y$  y luego pasa por el arco  $xy$  para llegar a  $y$ . También  $l[y]$  es el largo de algún camino de  $v$  a  $y$ , y al ajustar estamos depositando en  $l[y]$  el largo de algún camino de  $v$  a  $y$ .

Para lo segundo, consideremos el camino más corto de  $v$  a  $y$  con a lo más  $k$  arcos. Sea  $z$  el último vértice antes de  $y$  en este camino. Por inducción, después de  $k - 1$  iteraciones tenemos que  $l[z]$  es a lo más el largo de un camino con a lo más  $k - 1$  arcos desde  $v$  a  $z$ , y  $l[y]$  el largo de un camino de a lo más  $k - 1$  arcos desde  $v$  a  $y$ . Agregando el arco  $zy$  al camino de  $v$  a  $z$  tenemos un camino de  $k$  arcos, si resulta más corto que el que tiene a lo más  $k - 1$  arcos actualizamos  $l[y]$ . El resultado final, luego de considerar todos los arcos que llegan a  $y$ , es que tenemos el largo del camino más corto con a lo más  $k$  arcos.  $\square$

Para completar la demostración de que el algoritmo 24.7 es correcto, basta observar que luego de  $|V| - 1$  iteraciones hemos calculado los costos mínimos de los caminos de largo a lo más  $|V| - 1$ , que es el largo máximo posible de un camino en el grafo. Si aún pueden hacerse mejoras, es porque hay un ciclo de largo negativo.

El tiempo de ejecución de este algoritmo es  $O(|V| \cdot |E|)$ ). Esto es mayor que la complejidad del algoritmo de Dijkstra, pero como ya indicamos este algoritmo tiene la virtud de manejar arcos de largo negativo. Por lo demás, si en algún ciclo del **for** externo no hay cambios, ya no los habrá más y podemos terminar el algoritmo (básicamente hemos llegado al final del camino más largo), por lo

que esta complejidad es pesimista. Hay una mejora debida a Yen [366] que efectivamente disminuye a la mitad el número de pasadas requeridas.

Una variante de este algoritmo se usa en redes de computadores (por ejemplo, es parte del protocolo RIP [248]) para encontrar rutas óptimas, ya que los cómputos pueden distribuirse a los nodos: Cada nodo calcula los largos (y el primer paso del camino más corto) hacia todos los destinos en la red, recogiendo información de rutas y distancias óptimas estimadas desde sus vecinos, actualiza sus propias estimaciones de las mejores rutas y sus costos, y distribuye los resultados de vuelta a sus vecinos.

#### 24.15.2.3. Algoritmo de Floyd-Warshall

A diferencia de los anteriores, este algoritmo [130, 359] calcula los costos de los caminos mínimos entre todos los pares de vértices del grafo. Tomamos como los vértices del grafo los números  $\{1, 2, \dots, |V|\}$ , y actualizamos un arreglo  $l[i, j]$  de forma que después de la iteración  $k$  el valor del elemento  $l[i, j]$  es el costo del camino más corto entre los vértices  $i$  y  $j$  que visita únicamente algunos de los vértices  $\{1, 2, \dots, k\}$  entremedio. Llamemos  $l^{(k)}[i, j]$  a este valor. Claramente  $l^{(0)}[i, j] = w(i, j)$ , el costo de ir directamente de  $i$  a  $j$ , ya que no podemos pasar por ningún vértice intermedio. Para calcular el valor de  $l^{(k+1)}[i, j]$ , consideramos que el camino más corto que pasa a lo más por  $k + 1$  tiene dos posibilidades: Nunca pasa por  $k + 1$ , solo llega hasta  $k$ , el costo es  $l^{(k)}[i, j]$  en tal caso; o pasa por  $k + 1$ , lo que significa que de  $i$  va a  $k + 1$  y luego de  $k + 1$  va a  $j$ , en ambos casos pasando a lo más por  $\{1, 2, \dots, k\}$ , con costo  $l^{(k)}[i, k + 1] + l^{(k)}[k + 1, j]$ . Calculamos:

$$l^{(k+1)}[i, j] = \min\{l^{(k)}[i, j], l^{(k)}[i, k + 1] + l^{(k)}[k + 1, j]\}$$

Una vez alcanzado  $k = |V|$ , ya no hay restricciones sobre los vértices visitados en el camino y hemos calculado los costos mínimos. Posibles caminos de largo negativo no afectan al funcionamiento del algoritmo. Esto resulta en el algoritmo 24.8, donde anotamos simplemente  $l[i, j]$  para  $l^{(k)}[i, j]$ . Nótese que si no hay cambios entre dos iteraciones, ya no habrán más cambios y el algoritmo puede terminarse. No seguimos rigurosamente la descripción anterior, a veces usamos valores ya actualizados (en el fondo, de la iteración siguiente) de  $l^{(k)}[i, j]$ . Esto no afecta la correctitud, pero ahorra espacio (no requiere guardar dos juegos de valores de  $l^{(k)}[i, j]$ ) y hace que el algoritmo sea algo más rápido al adelantar pasos si se detiene cuando ya no hay cambios. Lo notable de este

---

Algoritmo 24.8: Costos mínimos entre todos los vértices (Floyd-Warshall)

---

```

procedure FloydWarshall( $G = (V, E)$ )
  for  $i \leftarrow 1$  to  $|V|$  do
    for  $j \leftarrow 1$  to  $|V|$  do
       $l[i, j] \leftarrow w(i, j)$ 
    end
  end
  for  $k \leftarrow 1$  to  $|V|$  do
    for  $i \leftarrow 1$  to  $|V|$  do
      for  $j \leftarrow 1$  to  $|V|$  do
         $l[i, j] \leftarrow \min\{l[i, j], l[i, k] + l[k, j]\}$ 
      end
    end
  end
end

```

---

algoritmo es que en un grafo con  $n$  vértices es que efectúa solo  $2n^3$  comparaciones, cuando pueden

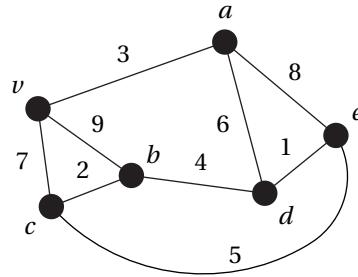


Figura 24.49 – Ejemplo de grafo para árbol recubridor mínimo

haber hasta  $n - 1$  arcos en cada camino, y debemos considerar  $n(n - 1)/2$  pares de vértices como inicio y fin.

### 24.15.3. Árbol recubridor mínimo

En muchas aplicaciones interesa encontrar el grafo de costo mínimo (el costo es simplemente la suma de los pesos de los arcos en el subgrafo) que conecta a un conjunto dado de vértices. Claramente tal grafo será un árbol recubridor, el *árbol recubridor mínimo* (*Minimal Spanning Tree* en inglés, abreviado *MST*). Veremos varios algoritmos para construirlo.

#### 24.15.3.1. Algoritmo de Prim

Una estrategia, debida a Prim [293] es agregar a un árbol parcial aquel arco que conecta a un vértice al árbol de forma que el costo sea mínimo.

Un poco más formalmente, eso sí abusando de la notación dando el nombre del grafo como su conjunto de vértices o arcos según corresponda: Inicialmente  $T$  es solo un vértice cualquiera del grafo. Sea  $T$  el árbol actual, elegimos el vértice  $v \in V \setminus T$  tal que el costo de llegar a él desde un vértice  $x \in T$  es mínimo. Agregamos el arco  $vx$  a  $T$ . Esto se repite hasta que no queden vértices sin cubrir.

Aplicando el algoritmo al grafo de la figura 24.49, paso a paso se obtienen los árboles de la figura 24.50.

**Teorema 24.24.** *El algoritmo de Prim obtiene un árbol recubridor mínimo.*

*Demostración.* Por contradicción. Sea  $w(G)$  el costo total de los arcos en el grafo  $G$ . Sea  $T$  el árbol recubridor construido por el algoritmo, con  $e_1, e_2, \dots, e_n$  los arcos en el orden en que los elige el algoritmo. Entonces:

$$w(T) = w(e_1) + w(e_2) + \dots + w(e_n)$$

Sea  $U$  un árbol recubridor mínimo de  $G$ , y supongamos que el árbol recubridor  $T$  que construye el algoritmo no es mínimo, vale decir  $w(U) < w(T)$ .

Sea  $e_k$  el primer arco en  $T$  (en el orden en que los elige el algoritmo) que no está en  $U$ . Eliminando  $e_k$  de  $T$ , por el teorema 24.9 (propiedad T5) obtenemos dos componentes conexos que son árboles. Habrá algún arco  $e^* \in U$  que conecta estos dos componentes conexos. Si  $w(e^*) < w(e_k)$  el algoritmo habría elegido  $e^*$  en vez de  $e_k$ , así que  $w(e^*) \geq w(e_k)$ .

Aplicando la misma idea al grafo obtenido al eliminar los arcos  $e_1$  a  $e_{k-1}$  (y los vértices que contienen) del grafo vemos que nuestro algoritmo siempre habría elegido un arco de costo no mayor que el incluido en  $U$ , con lo que  $w(T) \leq w(U)$  y  $T$  es un árbol recubridor mínimo.  $\square$

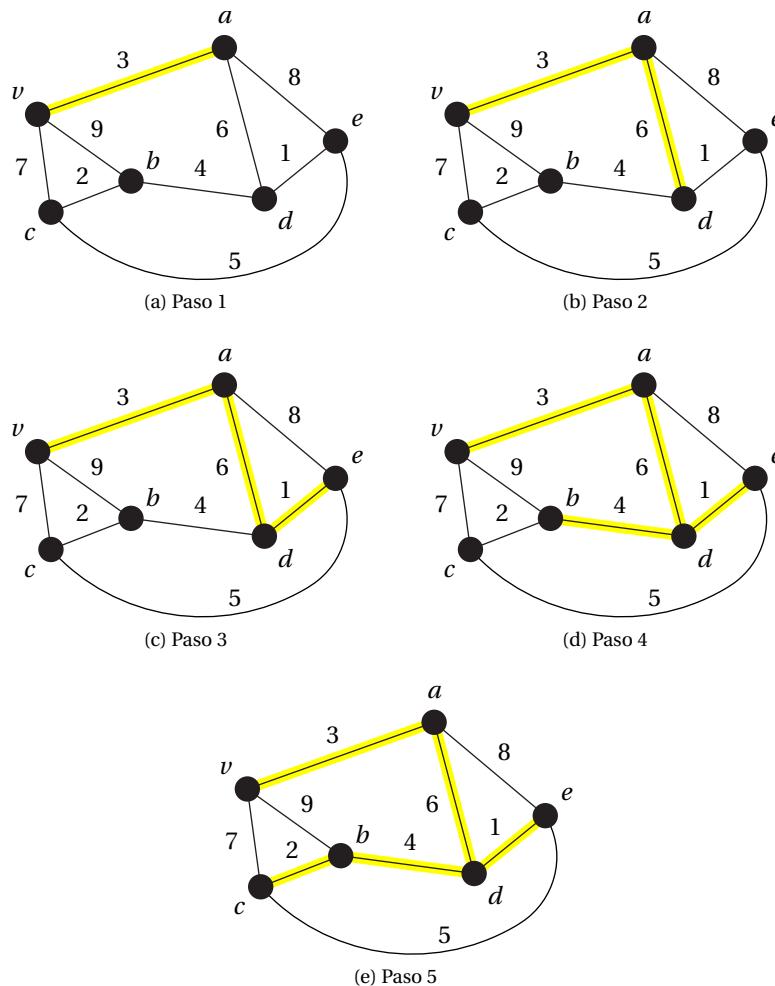


Figura 24.50 – El algoritmo de Prim aplicado al grafo de la figura 24.49

En este caso, la estrategia voraz de elegir “el mejor ahora” sin considerar consecuencias futuras tiene éxito.

La complejidad del algoritmo depende de cómo se almacena el grafo y los respectivos costos por arco. Con la representación obvia de matriz de adyacencia en la que  $a[i, j]$  es el costo del arco  $ij$  y se busca en la matriz es  $O(|V|^2)$ , almacenando el grafo en una lista de adyacencia y usando una estructura eficiente para ubicar el mínimo en cada paso esto se reduce a  $O(|E| + |V|\log|V|)$ .

### 24.15.3.2. Algoritmo de Kruskal

Otra idea, debida a Kruskal [225], es ordenar los arcos en orden de costo creciente, y agregar sucesivamente el siguiente arco que no forma un ciclo. Un ejemplo paso a paso para el grafo de la figura 24.49 se muestra en la figura 24.51.

Aplicando el algoritmo, vamos creando un bosque (una colección de árboles, en inglés “*forest*”) Inicialmente el bosque es cada vértice por sí solo, luego en cada paso conectamos dos árboles. Se van agregando arcos con el menor costo posible que no generen un ciclo. Como el grafo resultante

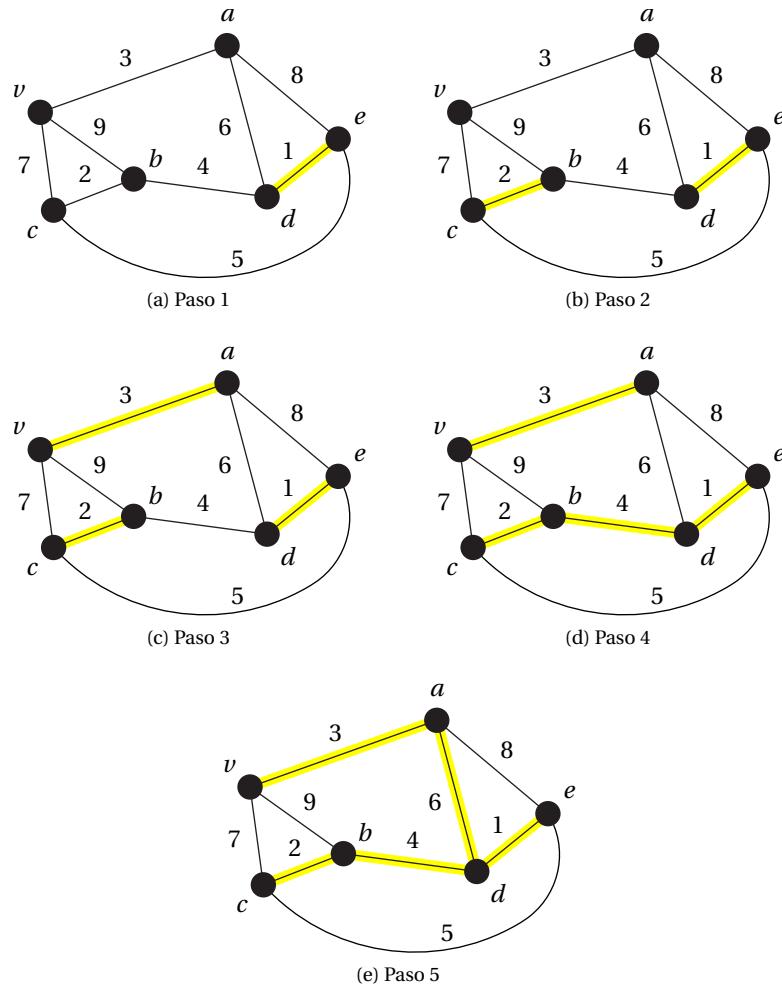


Figura 24.51 – El algoritmo de Kruskal aplicado al grafo de la figura 24.49

es conexo y no tiene ciclos, es un árbol recubridor del grafo. En adición, resulta un árbol recubridor mínimo, por un razonamiento similar al dado para el algoritmo de Prim. Nuevamente la estrategia voraz de tomar el mejor localmente tiene éxito.

Para construir un programa eficiente para el algoritmo de Kruskal bastan estructuras simples. Sabemos de la sección 19.7 que podemos ordenar los  $|E|$  arcos por orden de costo con  $O(|E| \log |E|)$  comparaciones. Luego consideramos cada arco por turno, y vemos si sus extremos están en árboles distintos del bosque que estamos construyendo.

Requerimos seguir la pista a los árboles, fundamentalmente mantener conjuntos de vértices en cada uno de ellos, determinar rápidamente en qué conjunto está cada vértice, y unir dos conjuntos. Una forma sencilla (y suficientemente eficiente para los propósitos presentes) es representar cada conjunto mediante una lista, en la cual cada elemento mantiene un puntero al primer elemento de la lista. Para ver en qué lista está un vértice dado basta hacer referencia al primer elemento de su lista, lo que toma tiempo constante. Esta operación se efectúa  $2|E|$  veces, para un total de  $O(|E|)$ . Crear las  $|V|$  listas que representan los vértices individuales toma  $O(|V|)$ . Para unir dos conjuntos se agregan

los elementos de la lista más corta a la más larga, ajustando los punteros correspondientes. El costo total en que incurre el algoritmo uniendo conjuntos hasta tener uno solo podemos calcularlo a través de contar cuántas veces en el peor caso el puntero al primer elemento de la lista debe ajustarse para un vértice  $v$  cualquiera. Esto ocurrirá solo si  $v$  pertenece a la lista menor en una unión, y cada vez que esto ocurra la lista a la que pertenece  $v$  al menos se duplica, con lo que esto podrá ocurrir a lo más  $\log_2 |V|$  veces. Como hay un total de  $|V|$  vértices, el costo total de las uniones será  $O(|V|\log|V|)$ . El costo total del algoritmo es entonces, dado que  $|E| = O(|V|^2)$ :

$$O(|E|\log|E|) + O(|E|) + O(|V|\log|V|) = O(|E|\log|V|)$$

#### 24.15.3.3. Árboles recubridores en redes de computadores

Las redes de área local actualmente en uso (ver algún texto del área, como Stallings [329, 344]) son redes de difusión, vale decir, lo que una de las estaciones transmite lo pueden recibir todas las demás conectadas al mismo medio físico. Suele ser de interés conectar entre sí redes de área local, lo que se hace a través de equipos denominados *bridges*, que se encargan de retransmitir solo el tráfico de interés en la otra rama. Por razones de confiabilidad interesa tener conexiones redundantes, vale decir, varios caminos entre redes. Pero esto introduce la posibilidad de crear ciclos, y por tanto tráfico que se retransmite indefinidamente. Un ejemplo se muestra en la figura 24.52. Esta situación puede

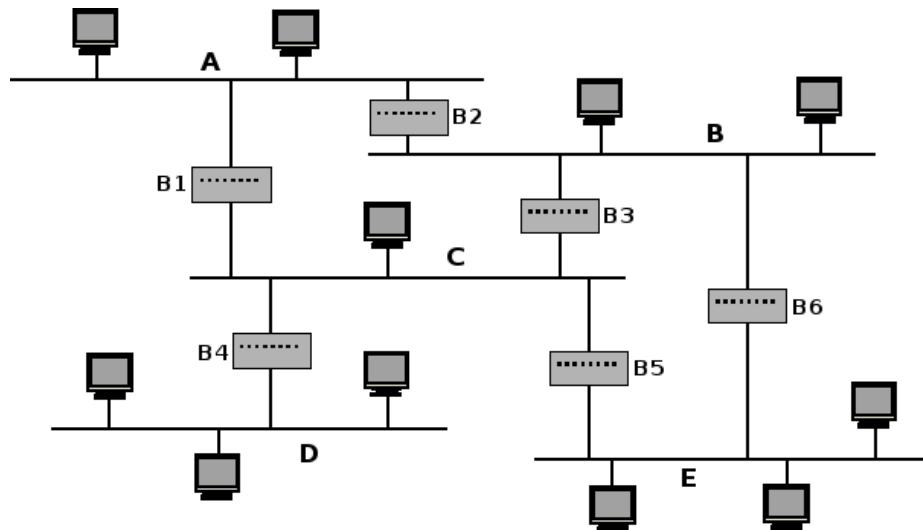


Figura 24.52 – Esquema de redes interconectadas por *bridges*

modelarse mediante un grafo, en el cual las redes son vértices y las conexiones entre redes son arcos. Para la red de la figura 24.52 resulta el grafo de la figura 24.53. En estos términos, lo que se busca es hallar un árbol recubridor del grafo (inhabilitando *bridges* que no participan en él). Para cumplir con redundancia y tolerancia a fallas (y evitar el siempre presente error humano) interesa que en caso de falla la red se reconfigure automáticamente. Los *bridges* originalmente contemplados (que conectan entre sí a dos redes) han sido desplazados por *switches*, que cumplen la misma función pero pueden conectar varias redes entre sí.

Para la tarea descrita se han estandarizado algoritmos (conocidos como STP, por *Spanning Tree Protocol* y RSTP, por *Rapid Spanning Tree Protocol*, definidos por IEEE [181]) mediante los cuales los equipos cooperan para configurar un árbol recubridor automáticamente. Perlman [279] describe cómo se hace. En resumen es que intercambian sus prioridades (fijadas por el administrador de

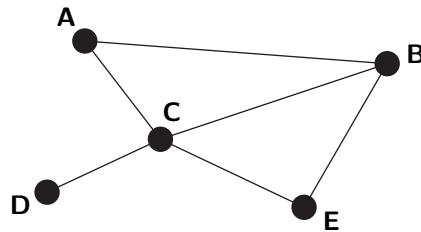


Figura 24.53 – La red de la figura 24.52 como grafo

la red) junto con sus identificadores (fijados de fábrica, únicos en el mundo). Aquel que tenga el mínimo par prioridad e identificador se elige de raíz, y todos los demás calculan sus distancias hacia la raíz a través de cada una de sus interfases. Se habilitan únicamente las interfases que dan el camino más corto hacia la raíz. Este proceso se repite periódicamente, de forma de reaccionar frente a fallas y reconfiguraciones.

## 25 Digrafos, redes, flujos

---

En muchas situaciones que podrían modelarse mediante grafos las conexiones no son bidireccionales. Por ejemplo, están las calles de una sola vía. En un proyecto hay actividades que deben efectuarse en orden, interesa representar estas dependencias y organizarlas de forma de completar el proyecto lo antes posible. Si queremos analizar el flujo a través de una red de tuberías o el flujo de bienes transportados hay una dirección definida. En esto suele interesar la capacidad de transporte de la red. Estas situaciones se modelan por grafos dirigidos rotulados. Generalmente se tratan solo en un capítulo de textos que se concentran en grafos, pero se puede argüir que la importancia práctica de los grafos dirigidos (digrafos, para abreviar) es similar a la de los grafos. Trataremos algunos algoritmos importantes del área con análisis somero de sus rendimientos.

### 25.1. Definiciones básicas

Nos interesa representar estructuras similares a grafos, solo que los arcos tienen una dirección definida. No está la simetría entre ambos extremos del arco como en grafos. Por ejemplo, si queremos representar las llamadas de funciones en un programa, interesa cuál de las dos es quien llama y cuál es llamada.

**Definición 25.1.** Un *digrafo* (o *grafo dirigido*) consta de un conjunto finito  $V$  de *vértices*, y un subconjunto  $A$  de  $V \times V$ , cuyos miembros se llaman *arcos*. Anotaremos  $D = (V, A)$  para el digrafo definido de esta forma.

Un texto reciente, que cubre desde temas elementales hasta áreas de investigación activa, es el de Bang-Jensen y Gutin [27].

Los digrafos se pueden representar gráficamente de forma similar a los grafos, solo que en este caso un arco es un par ordenado  $(x, y)$ , mientras en el grafo es un par no ordenado  $\{x, y\}$ . Si  $(x, y)$  es un arco, lo indicamos mediante una flecha de  $x$  a  $y$ , si hay un arco  $(x, x)$  lo indicamos mediante un ciclo, si hay arcos  $(x, y)$  e  $(y, x)$  los indicamos por dos flechas. Para simplificar notación, similar al caso de grafos usaremos  $uv$  para indicar el arco  $(u, v)$ . La figura 25.1 muestra ejemplos. Nuestras representaciones de grafos para uso computacional se aplican con cambios obvios a este caso. Igualmente, podemos aplicar los algoritmos de recorrido acá. Los algoritmos de Dijkstra, algoritmo 24.6, de Floyd-Warshall, algoritmo 24.8 (que en este caso es llamado simplemente algoritmo de Floyd) y de Bellman-Ford 24.7 son aplicables con modificaciones obvias.

Un digrafo es simplemente otra manera de representar una relación  $R$  entre elementos del *mismo* conjunto (un grafo bipartito, por otro lado, representa una relación entre elementos de conjuntos *disjuntos*). Las propiedades de las relaciones pueden fácilmente traducirse en propiedades del digrafo. Por ejemplo, si la relación es simétrica los arcos aparecen en pares (salvo los bucles),  $xy$  es un arco exactamente cuando lo es  $yx$ .

Las definiciones de camino, camino simple, circuito y ciclo en un grafo dirigido son análogas a las para grafos. Un *camino dirigido* en  $D = (V, A)$  es una secuencia de vértices  $v_1, v_2, \dots, v_k$  tal que

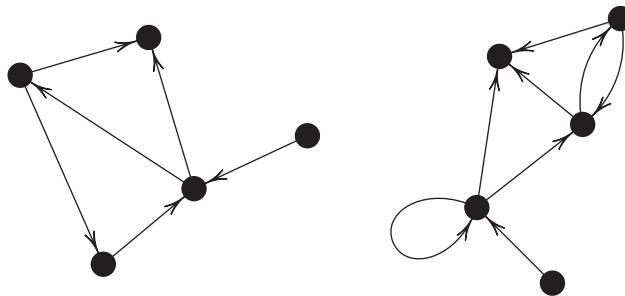


Figura 25.1 – Ejemplos de digrafos

$v_i v_{i+1} \in A$  para  $1 \leq i \leq k - 1$ , un *camino dirigido simple* es un camino dirigido en que todos los vértices son diferentes, un *ciclo dirigido* es un camino cuyo inicio y fin coinciden, mientras un *ciclo dirigido* es un camino dirigido en que todos los vértices son distintos, solo que el inicial y el final coinciden. Un caso particularmente importante lo ponen los *grafos dirigidos acíclicos* (abreviados comúnmente *DAG*, por la frase en inglés *Directed Acyclic Graph*), de alguna forma análogos a los árboles.

## 25.2. Orden topológico

Dado un digrafo  $G = (V, E)$ , un *orden topológico* (en inglés, *topological sort*) de los vértices de  $G$  es un ordenamiento de  $V$  tal que para cada arco  $uv \in E$  el vértice  $u$  aparece antes que  $v$ . Esto claramente solo puede existir si el digrafo es acíclico.

La aplicación típica es definir un orden para efectuar un conjunto de tareas que dependen entre sí. Por ejemplo, al vestirse uno debe ponerse los calcetines antes que los zapatos, pero no hay precedencia entre la camisa y los calcetines. La figura 25.2 ilustra las restricciones. Otras aplicaciones

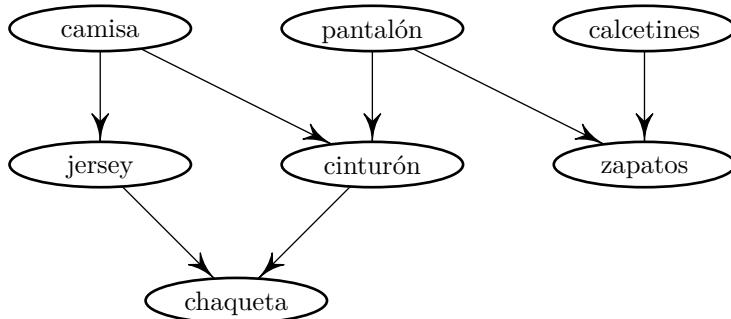


Figura 25.2 – Restricciones al vestirse

aparecen en compiladores, al reordenar instrucciones; al definir el orden en que se calculan las celdas en planillas de cálculo; y lo usa `make(1)` para organizar el orden en que se generan los archivos. Unix ofrece el comando `tsort(1)`, que toma líneas indicando dependencias y entrega un orden consistente con ellas. Aplicando este último a la tarea de vestirse, sugiere el orden calcetines, camisa, pantalón, jersey, zapatos, cinturón y finalmente chaqueta. Este orden no es único, se ve de la figura que podríamos haber comenzado por la camisa, o haber terminado con los zapatos.

Algoritmos para hallar un orden topológico se basan en que en un digrafo acíclico habrán vértices que no tienen arcos de entrada (respectivamente de salida). Kahn [192] publicó el algoritmo clásico 25.1. Se basa en la observación que en un digrafo acíclico deben haber vértices sin arcos

---

Algoritmo 25.1: Ordenamiento topológico de Kahn

---

```

 $L \leftarrow$  lista vacía
 $S \leftarrow$  conjunto de nodos sin arcos entrantes
while  $S \neq \emptyset$  do
    Extraiga un nodo  $n$  cualquiera de  $S$ 
    Agregue  $n$  al final de  $L$ 
    foreach nodo  $m$  con arco  $e = (n, m)$  do
        Elimine  $e$  del grafo
        if  $m$  no tiene más arcos entrantes then
            Inserte  $m$  en  $S$ 
        end
    end
end
if quedan arcos en el grafo then
    return error
    /* El digrafo tiene ciclos */
else
    return  $L$ 
end
```

---

entrantes, y que cualquiera de ellos puede tomar el primer lugar en el orden.

El algoritmo 25.2 es debido a Tarjan [345]. Es una aplicación de búsqueda en profundidad (ver

---

Algoritmo 25.2: Ordenamiento topológico de Tarjan

---

```

 $L \leftarrow$  lista vacía
 $S \leftarrow$  conjunto de todos los nodos sin arcos salientes

procedure visit( $n$ )
begin
    if el nodo  $n$  no ha sido visitado then
        Marque  $n$  como visitado
        foreach nodo  $m$  con  $(m, n) \in E$  do
            visit( $m$ )
        end
        Agregar  $n$  al final de  $L$ 
    end
end

foreach nodo  $n$  en  $S$  do
    visit( $n$ )
end
return  $L$ 
```

---

la sección 24.11.1). Notar que procesa los vértices desde el final hacia el comienzo (orden inverso al algoritmo de Kahn). Cuidado, el algoritmo 25.2 como está escrito falla si el digrafo tiene ciclos.

### 25.3. Redes y rutas críticas

Es común que se asocien costos o distancias a los arcos. Con esta idea en mente, llamaremos *red* a un digrafo  $D = (V, A)$  junto con una función  $w: A \rightarrow \mathbb{R}$ , que representa costos de algún tipo o capacidades, según la aplicación.

Una aplicación típica de redes son las *redes de actividades*. Suponiendo un gran proyecto, este se subdivide en actividades menores. Las actividades a su vez están relacionadas, en el sentido que algunas no pueden iniciarse antes que terminen otras. Al planificar un proyecto de este tipo se suele usar una red de actividades, con arcos representando actividades y los vértices representando “eventos”, donde un evento es el fin de una actividad. Es claro que tal digrafo es acíclico, ninguna actividad puede depender directa o indirectamente de sí misma. El peso de un arco es la duración de la actividad, y se busca organizar las actividades de forma de minimizar el tiempo total del proyecto. Técnicas basadas en esta idea son CPM (Critical Path Method) [199] y PERT (Project Management and Evaluation Technique) [247].

Consideremos un ejemplo concreto. El cuadro 25.1 da las duraciones de las actividades (en meses), y las dependencias entre ellas (qué actividades deben estar completas antes de comenzar la actividad indicada).

Act	Descripción	Requisitos	Dur
A	Diseño del producto		5
B	Análisis de mercado		1
C	Análisis de producción	A	2
D	Prototipo del producto	A	3
E	Diseño de folleto	A	2
F	Análisis de costos	C	3
G	Pruebas del producto	D	4
H	Entrenamiento ventas	B, E	2
I	Definición de precios	H	1
J	Reporte del proyecto	F, G, I	1

Cuadro 25.1 – Actividades y dependencias

El primer paso es construir la red de actividades, ver figura 25.3. Los arcos representan actividades, y los vértices sus inicios y finales. Es claro que resulta un digrafo sin ciclos. Para cada evento calcularemos  $E(v)$ , el instante más temprano en que ese evento puede tener lugar. Esto corresponde al momento más temprano en que todas las actividades previas a  $v$  han terminado. Iniciamos el proceso con  $E(1) = 0$ . Luego está claro que  $E(2) = 5$ , ya que la única actividad involucrada es  $A = (1, 2)$ . Ahora, como el evento 3 involucra a  $B = (1, 3)$ , pero también  $A = (1, 2)$  y  $E = (2, 3)$ ,  $E(3) = \max\{E(1) + 1, E(2) + 2\} = \max\{0 + 1, 5 + 2\} = 7$ . Continuando de esta forma, obtenemos los instantes de término dados en el cuadro 25.2, con lo que el plazo mínimo para completar el proyecto

$v:$	1	2	3	4	5	6	7	8
$E(v):$	0	5	7	7	8	9	12	13

Cuadro 25.2 – Términos más tempranos por actividad para la red de la figura 25.3

es de 13 meses.

Esto es básicamente usar el algoritmo de Dijkstra (ver sección 24.15.2.1), solo que estamos calculando el camino más *largo* a través de la red. Éste está perfectamente definido en este caso, ya que no hay ciclos. Basta un barrido a lo ancho, al no haber ciclos se obtiene el valor final directamente.

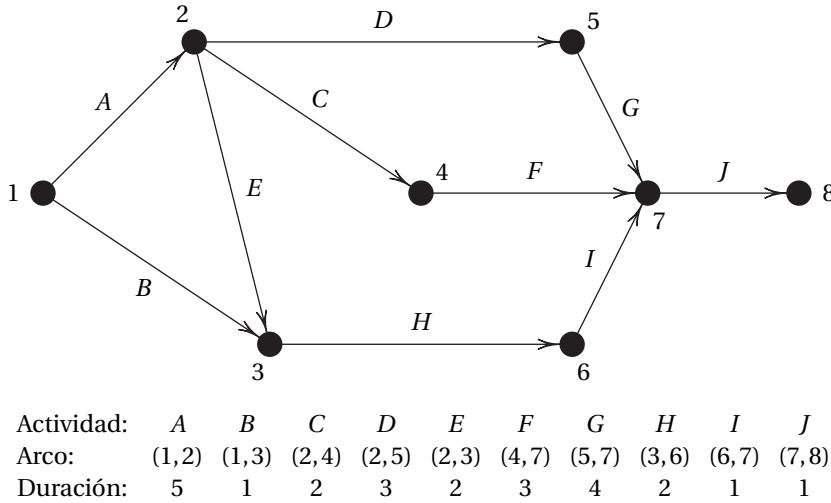


Figura 25.3 – Una red de actividades

En cada vértice visitado calculamos  $E(v)$  partiendo del evento inicial  $s$  (el comienzo del proyecto) mediante la regla:

$$E(s) = 0 \quad E(v) = \max_x \{E(x) + w(x, v)\}$$

donde el máximo es sobre los vértices  $x$  predecesores de  $v$ .

Esto es parte de la técnica que se conoce como *análisis de camino crítico*. El resto de la técnica continúa como sigue: Calculamos  $L(v)$ , el último instante en que puede ocurrir el evento  $v$  sin retrasar el proyecto completo de forma similar a como se calcularon los  $E(v)$ , pero comenzando del evento final  $t$  y trabajando en reversa:

$$L(t) = E(t) \quad L(v) = \min_x \{L(x) - w(v, x)\}$$

donde el mínimo es sobre los vértices  $x$  sucesores de  $v$ . Aplicando esto al ejemplo de la figura 25.3 da el cuadro 25.3.

$v:$	1	2	3	4	5	6	7	8
$L(v):$	0	5	9	9	8	11	12	13

Cuadro 25.3 – Inicio más tardío por actividad para la red 25.3

Podemos además calcular la *holgura* de cada actividad  $uv$ , que representa el máximo retraso que puede sufrir el comienzo de la actividad sin retrasar el fin del proyecto:

$$F(u, v) = L(v) - E(u) - w(u, v)$$

Las actividades sin holgura se dice que son *críticas*, cualquier retraso en éstas se traduce en un retraso del proyecto completo. Toda red de actividades tiene al menos un camino dirigido entre principio y fin formado únicamente por actividades críticas, tal camino se llama *ruta crítica*. Combinando los valores en los cuadros 25.2 y 25.3 obtenemos las holguras dadas en el cuadro 25.4. Son actividades críticas las que no tienen holgura, en nuestro caso  $A, D, G$  y  $J$ ; y se ve en la figura 25.3 que forman un camino a través del grafo.

El procedimiento es fundamentalmente un par de recorridos a lo ancho del digrafo. Como se discutió para este algoritmo en el caso de grafos en la sección 24.11.3, la complejidad es  $O(|V| + |E|)$ .

Actividad:	$A$	$B$	$C$	$D$	$E$	$F$	$G$	$H$	$I$	$J$
Arco:	(1, 2)	(1, 3)	(2, 4)	(2, 5)	(2, 3)	(4, 7)	(5, 7)	(3, 6)	(6, 7)	(7, 8)
Holgura:	0	8	2	0	2	2	0	2	2	0

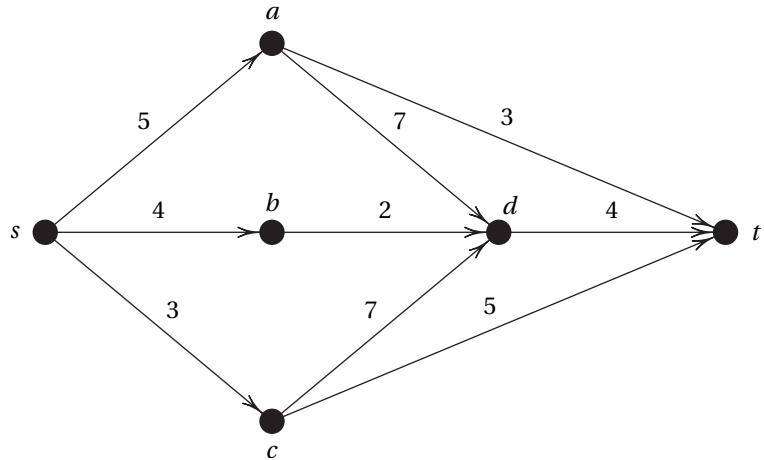
Cuadro 25.4 – Holguras para las actividades de la figura 25.3

## 25.4. Redes y flujos

En lo que sigue interpretaremos los arcos como “tuberías” por las que puede fluir alguna mercadería. Un ejemplo claro es el de circuitos eléctricos, con corrientes en los distintos conductores. Nótese que a diferencia de la aplicación anterior a redes de actividades acá un ciclo dirigido es perfectamente posible (aunque probablemente ineficiente). Los pesos numéricos representan la capacidad del arco. Además, habrá un vértice  $s$  con la propiedad que todos los arcos que contienen a  $s$  se alejan de él, y otro vértice  $t$  con la propiedad de que todos los arcos que lo contienen se dirigen a él. Al primero se le llama *fuente* (en inglés *source*), al segundo *sumidero* (en inglés *sink*). Si hubieran varias fuentes o varios sumideros, basta combinarlos en uno. En resumen, trataremos con redes que incluyen:

- (I) Un digrafo  $D = (V, A)$ .
- (II) Una función de capacidad  $c: A \rightarrow \mathbb{R}$ . Comúnmente haremos referencia a capacidades de enlaces inexistentes, usamos la convención que si  $xy \notin A$  entonces  $c(xy) = 0$ .
- (III) Una fuente  $s$  y un sumidero  $t$ .

La figura 25.4 muestra una red, con los arcos rotulados con sus capacidades. También describe un flujo en esta red.



$(x, y):$	$(s, a)$	$(s, b)$	$(s, c)$	$(a, d)$	$(b, d)$	$(c, d)$	$(a, t)$	$(c, t)$	$(d, t)$
$c(x, y):$	5	4	3	7	2	7	3	5	4
$f(x, y):$	3	2	3	1	2	1	2	2	4

Figura 25.4 – Una red, sus capacidades y un flujo en la red

Supongamos que algún material fluye por la red, y sea  $f(x, y)$  el flujo a lo largo del arco  $xy$ , de  $x$  a  $y$ . Si  $xy$  ni  $yx$  son arcos, por convención  $f(x, y) = 0$ . Insistiremos para todos los vértices, salvo

para la fuente y el sumidero, en que el flujo que entra al vértice debe ser el flujo que sale (no hay acumulación de material en los vértices).

**Definición 25.2.** Un *flujo* en una red es una función que asigna un número  $f(x, y)$  a cada arco  $xy$ , sujeto a las condiciones:

**Viabilidad:** El flujo en cada enlace es a lo más su capacidad,  $f(x, y) \leq c(x, y)$  para todo arco  $xy \in A$ .

**Simetría torcida:** En inglés *skew symmetry*, una convención de notación:  $f(y, x) = -f(x, y)$  para todo arco  $xy \in A$ .

**Conservación:** Para todo vértice  $y \in V$  que no sea la fuente ni el sumidero de la red requerimos que el flujo neto que entra en él sea cero:

$$\sum_{x \in V} f(x, y) = 0$$

El *valor* del flujo es el flujo total que entra a la red:

$$\text{val}(f) = \sum_{x \in V} f(s, x)$$

Exploraremos un poco las propiedades de la definición. La viabilidad indica únicamente que el flujo no puede exceder la capacidad del enlace. Simetría torcida es simplemente una conveniencia notacional (básicamente, si vamos “contra la corriente” contabilizamos el flujo como negativo). La conservación indica que el flujo neto que entra a un vértice es nulo, y por simetría el que sale también:

$$\sum_{y \in V} f(x, y) = \sum_{y \in V} -f(y, x) = -\sum_{y \in V} f(y, x) = 0$$

En el caso de circuitos eléctricos, la conservación es lo que se conoce como la ley de Kirchhoff. Si no hay arco  $xy$ , no puede haber flujo entre ellos, y  $f(x, y) = -f(y, x) = 0$ . Como no se permite acumulación en los vértices intermedios, está claro que el flujo que sale de  $s$  debiera ser el flujo que entra en  $t$ :

$$\text{val}(f) = \sum_{x \in V} f(x, t)$$

Esto lo demostraremos formalmente más adelante.

Un problema obvio es obtener el valor máximo del flujo en una red. Este problema nos ocupará de ahora en adelante.

Para conveniencia, definimos los flujos de entrada y salida de un vértice:

$$\text{inflow}(v) = \sum_{\substack{u \in V \\ f(u, v) > 0}} f(u, v)$$

$$\text{outflow}(u) = \sum_{\substack{v \in V \\ f(u, v) > 0}} f(u, v)$$

Algunos autores anotan  $v^-$  para lo que llamamos  $\text{inflow}(v)$ , y similarmente  $v^+$  para  $\text{outflow}(v)$ .

En estos términos, conservación se expresa simplemente como el flujo que entra a un vértice es igual al que sale si el vértice no es la fuente ni el sumidero:

$$\text{inflow}(v) = \text{outflow}(v)$$

Lo indicado en la figura 25.4 debe cumplir las condiciones para ser un flujo. La figura no da flujos “contracorriente”, estamos suponiendo implícitamente que por ejemplo  $f(d, b) = -f(b, d) = -2$ . Las condiciones de capacidad se cumplen, ya que por ejemplo  $f(c, d) = 1$  mientras  $c(c, d) = 7$ . También debemos verificar conservación, por ejemplo que para el vértice  $d$  la suma de los flujos se anula:

$$\begin{aligned} f(a, d) + f(b, d) + f(c, d) + f(t, d) &= 1 + 2 + 1 - 4 \\ &= 0 \end{aligned}$$

El valor de este flujo es la suma de los flujos que salen de la fuente, vale decir:

$$\begin{aligned} \text{val}(f) &= f(s, a) + f(s, b) + f(s, c) \\ &= 8 \end{aligned}$$

Resulta también, como esperábamos, que el flujo hacia el sumidero es igual al flujo que sale de la fuente:

$$f(a, t) + f(d, t) + f(c, t) = 8$$

No contabilizamos flujos entre  $s$  y los demás vértices (respectivamente entre los otros vértices y  $t$ ) ya que no hay conexiones directas entre ellos.

#### 25.4.1. Trabajando con flujos

Usaremos una convención de *suma implícita*, en que si mencionamos un conjunto de vértices como argumento a  $f$ , estamos considerando la suma de los flujos sobre ese conjunto, y similarmente para  $c$ . Por ejemplo, al anotar  $f(X, Y)$ , donde  $X$  e  $Y$  son conjuntos de vértices, entenderemos:

$$f(X, Y) = \sum_{\substack{x \in X \\ y \in Y}} f(x, y)$$

En estos términos, la condición de conservación se reduce a  $f(V, x) = 0$  para todo  $x \notin \{s, t\}$  (recuérdese que por convención  $s$  es la fuente y  $t$  el sumidero de la red). Además, omitiremos las llaves al restar conjuntos de un solo elemento. Así, en  $f(s, V - s) = f(s, V)$  la notación  $V - s$  significa el conjunto  $V \setminus \{s\}$ . Esto simplifica mucho las ecuaciones que involucran flujos. El lema siguiente recoge varias de las identidades más comunes. La demostración queda como ejercicio.

**Lema 25.1.** *Sea  $D = (V, A)$  una red, y sea  $f$  un flujo en  $D$ . Entonces:*

1. *Para todo  $X \subseteq V$ , se cumple  $f(X, X) = 0$ .*
2. *Para todo  $X, Y \subseteq V$  se cumple  $f(X, Y) = -f(Y, X)$ .*
3. *Para todo  $X, Y, Z \subseteq V$  siempre que  $X \cap Y = \emptyset$ , se cumplen:*

$$\begin{aligned} f(X \cup Y, Z) &= f(X, Z) + f(Y, Z) \\ f(Z, X \cup Y) &= f(Z, X) + f(Z, Y) \end{aligned}$$

Como un ejemplo de uso de la notación y del lema 25.1, demostraremos que  $\text{val}(f) = f(V, t)$ . Intuitivamente, lo que entra a la red por la fuente debe salir por el sumidero, ya que no se permiten

acumulaciones entremedio. Formalmente, dado que  $f(V, V) = 0$  podemos escribir:

$$\begin{aligned} f(V, t) &= f(V, V) - f(V, V - t) \\ &= -f(V, V - t) \\ &= f(V - t, V) \\ &= f(s, V) + f(V - s - t, V) \\ &= f(s, V) \\ &= \text{val}(f) \end{aligned}$$

En esto usamos el hecho:

$$\begin{aligned} f(V - s - t, V) &= \sum_{x \in V \setminus \{s, t\}} f(x, V) \\ &= - \sum_{x \in V \setminus \{s, t\}} f(V, x) \\ &= 0 \end{aligned}$$

que sigue de conservación, ya que cada término de la última suma se anula.

Las capacidades son los flujos máximos en la dirección indicada. Si hay tuberías de capacidades 5 de  $u$  a  $v$  y 3 de  $v$  a  $u$ , el máximo flujo de  $u$  a  $v$  es 5 y el máximo de  $v$  a  $u$  es 3. Esto se traduce en que al aplicar la notación a capacidades los términos negativos se omiten.

#### 25.4.2. Método de Ford-Fulkerson

Presentaremos ahora una manera de obtener el flujo de máximo valor en una red. No lo llamaremos “algoritmo”, ya que la estrategia general [133] puede implementarse de varias formas, con características diferentes. En el proceso introduciremos varias ideas importantes en muchos pro-

---

##### Algoritmo 25.3: El método de Ford-Fulkerson

---

```

Inicialice  $f$  en 0
while hay un camino aumentable  $p$  do
    Aumente el flujo  $f$  a lo largo de  $p$ 
end
```

---

blemas relacionados con flujos. Supondremos que las capacidades son enteras, de otra forma puede ser que los métodos planteados no terminen nunca (aunque converjan hacia la solución).

El método de Ford-Fulkerson es iterativo. Comenzamos con  $f(x, y) = 0$  para todo arco  $xy$ , con un valor inicial cero. En cada iteración aumentamos el valor del flujo a través de identificar un *camino aumentable* (*augmenting path* en inglés, un camino entre  $s$  y  $t$  que no está en su máxima capacidad) y aumentamos el flujo a lo largo de este camino. Continuamos hasta que no se pueda encontrar otro camino aumentable. Por el teorema *Max-Flow Min-Cut* (teorema 25.7, que demostraremos más adelante) al finalizar el valor del flujo es máximo. Si las capacidades están dadas por números enteros, los flujos también serán enteros. Los flujos no pueden crecer indefinidamente, los algoritmos terminan.

#### 25.4.3. Redes residuales

Dada una red y un flujo  $f$ , habrán arcos que admiten flujo adicional, y estos arcos con sus capacidades sin usar a su vez constituyen una red. Intuitivamente, esta nos dice cuáles son las posibles mejoras del flujo, así interesa analizar la relación entre esta red y la original.

Más formalmente, supongamos una red  $D = (V, A)$ , con capacidades  $c: A \rightarrow \mathbb{R}^+$ , fuente  $s$  y sumidero  $t$ . Sea  $f$  un flujo en  $D$ , y consideremos un par de vértices  $x$  e  $y$ . El flujo adicional que podemos enviar de  $x$  a  $y$  antes de sobrepasar la capacidad de ese enlace es la *capacidad residual* del enlace  $xy$ , que se anota  $c_f(x, y)$ . Por ejemplo, si  $c(x, y) = 10$  y  $f(x, y) = 7$ , podemos enviar un flujo adicional de 3 de  $x$  a  $y$  sin sobrepasar la capacidad de ese enlace, o podemos disminuir ese flujo en 7. O sea, para un enlace  $xy$  con flujo positivo  $f(x, y)$  tenemos una capacidad residual de  $c_f(x, y) = c(x, y) - f(x, y)$  de  $x$  a  $y$ , y una capacidad residual de  $c_f(y, x) = f(x, y)$  de  $y$  a  $x$ . De forma similar, para un enlace  $xy$  con flujo negativo  $f(x, y)$ , podemos aumentar el flujo de  $x$  a  $y$  disminuyendo el flujo de  $y$  a  $x$ , el máximo aumento posible es dejarlo en cero. La red residual  $D_f = (V, A_f)$  inducida por  $f$  es simplemente la red formada por los enlaces y sus capacidades residuales (capacidad libre con la corriente, flujo a través del enlace en contracorriente), o sea  $A_f = \{uv \in V \times V : c_f(u, v) > 0\}$ . En  $D_f$  todos los arcos pueden admitir flujos mayores a cero, los arcos de  $D_f$  son ya sea arcos de  $D$  o sus reversos.

Conviene definir la suma de flujos  $f_1$  y  $f_2$ :

$$(f_1 + f_2)(u, v) = f_1(u, v) + f_2(u, v)$$

Nótese que esto no siempre es un flujo, ya que no necesariamente cumple las restricciones de nuestra definición.

El siguiente lema relaciona flujos en  $D$  con flujos en  $D_f$ .

**Lema 25.2.** *Sea  $D = (V, A)$  una red con fuente  $s$  y sumidero  $t$ , y  $f$  un flujo en  $D$ . Sea  $D_f = (V, A_f)$  la red residual inducida por  $f$ , y  $f'$  un flujo en  $D_f$ . Entonces la suma  $f + f'$  es un flujo en  $D$ , con valor  $\text{val}(f + f') = \text{val}(f) + \text{val}(f')$ .*

*Demostración.* Primero, para verificar que es un flujo, debe cumplir las condiciones de la definición. Para simetría torcida tenemos:

$$\begin{aligned} (f + f')(x, y) &= f(x, y) + f'(x, y) \\ &= -f(y, x) - f'(y, x) \\ &= -(f + f')(y, x) \end{aligned}$$

Para las restricciones de capacidad, note que  $f'(x, y) \leq c_f(x, y)$  para todo  $x, y \in V$  (incluso cuando  $f'(x, y) < 0$ , o sea, el arco  $xy$  es contracorriente). Por tanto:

$$\begin{aligned} (f + f')(x, y) &= f(x, y) + f'(x, y) \\ &\leq f(x, y) + (c(x, y) - f(x, y)) \\ &= c(x, y) \end{aligned}$$

Para conservación, al ser  $f$  y  $f'$  flujos, con  $x \neq s, t$  es  $f(x, V) = f'(x, V) = 0$ , y  $(f + f')(x, V) = 0$ .

Finalmente:

$$\begin{aligned} \text{val}(f + f') &= (f + f')(s, V) \\ &= f(s, V) + f'(s, V) \\ &= \text{val}(f) + \text{val}(f') \end{aligned}$$

Como cumple con nuestra definición y nuestras convenciones, queda demostrado lo que perseguíamos.  $\square$

#### 25.4.4. Caminos aumentables

Dada una red  $D = (V, A)$  y un flujo  $f$ , un *camino aumentable* (en inglés *augmenting path*)  $p$  es un camino dirigido entre  $s$  y  $t$  en la red residual  $D_f$ . Por la definición de red residual, cada arco  $xy$  a lo largo de  $p$  admite flujo positivo de  $x$  a  $y$  sin violar la restricción de capacidad. Podemos aumentar el flujo a lo largo de  $p$  en:

$$c_f(p) = \min_{(x,y) \in p} \{c_f(x,y)\}$$

sin sobrepasar la capacidad de ningún enlace. A  $c_f(p)$  se le llama la *capacidad residual* de  $p$ . Hemos demostrado:

**Lema 25.3.** *Sea  $D = (V, A)$  una red, sea  $f$  un flujo en  $D$ , y sea  $p$  un camino aumentable en  $D_f$ . Defina la función  $f_p: V \times V \rightarrow \mathbb{R}$  mediante:*

$$f_p(u, v) = \begin{cases} c_f(p) & \text{si } xy \text{ está en } p \\ -c_f(p) & \text{si } yx \text{ está en } p \\ 0 & \text{caso contrario} \end{cases}$$

Entonces  $f_p$  es un flujo en  $D_f$  con valor  $\text{val}(f_p) = c_f(p) > 0$ .

De lo anterior tenemos:

**Corolario 25.4.** *Sea  $D = (V, A)$  una red,  $f$  un flujo en  $D$  y  $p$  un camino aumentable en  $D_f$ . Sea  $f_p$  como definido en el lema 25.3, y defina  $f': V \times V \rightarrow \mathbb{R}$  como  $f' = f + f_p$ . Entonces  $f'$  es un flujo en  $D$ , y su valor es:*

$$\text{val}(f') = \text{val}(f) + \text{val}(f_p) > \text{val}(f)$$

*Demuestra*ón. Inmediata por los lemas 25.2 y 25.3. □

Para clarificar estas ideas, véanse las figuras 25.5 y 25.6. La figura 25.5 muestra una red, la fi-

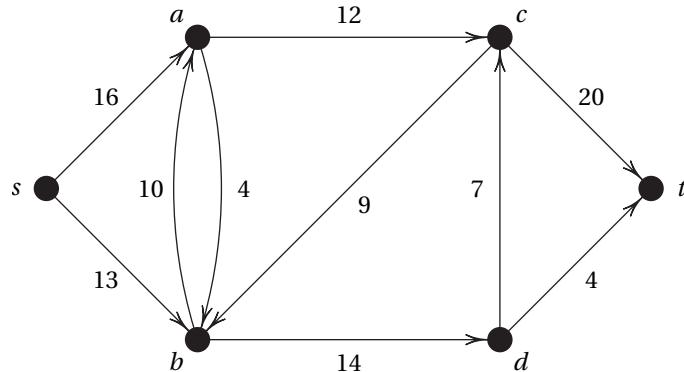


Figura 25.5 – Una red

gura 25.6a muestra un flujo en la red de la figura 25.5. La figura 25.6b muestra la red residual con ese flujo con un camino aumentable marcado. Hay otros caminos aumentables, como  $(s, a, b, c, t)$ . Nótese que en la red residual tenemos enlaces contracorriente cuyas capacidades son el flujo actual. Esto significa que podemos enviar hasta ese flujo contracorriente (disminuyendo el flujo actual) a través de ese enlace. Este camino aumentable tiene capacidad residual 4, y la figura 25.7 muestra el resultado de aumentar el flujo.

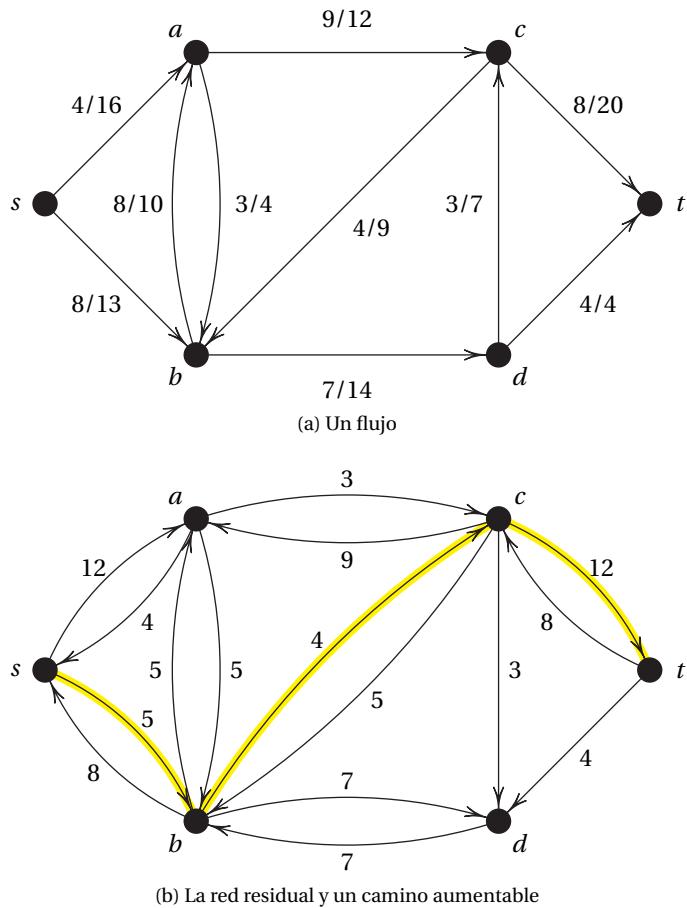


Figura 25.6 – Flujo y red residual en la red de la figura 25.5

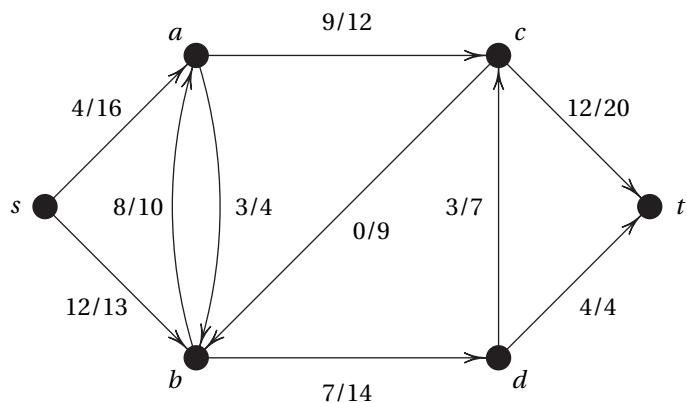


Figura 25.7 – El flujo aumentado según el camino aumentable de la figura 25.6b

### 25.4.5. Cortes

La idea del método de Ford-Fulkerson es hallar sucesivamente un camino aumentable y aumentar el flujo a lo largo de él. Cuando este proceso termina por no hallar un camino aumentable, tenemos un flujo de valor máximo. Al discutir estos métodos se restringen las capacidades a números naturales. De partida, capacidades negativas no tienen sentido, y resulta que si las capacidades son irracionales hay casos en que los algoritmos no terminan nunca (convergen hacia la solución, pero nunca la alcanzan).

La correctitud de estos métodos la garantiza el teorema Max-Flow Min-Cut, que es nuestro próximo objetivo. Primeramente consideraremos el concepto de un *corte* (en inglés *cut*) en una red. Un corte  $(S, T)$  corresponde simplemente a una partición de los vértices de la red en conjuntos  $S$  y  $T = V \setminus S$  tal que  $s \in S$  y  $t \in T$ , véase por ejemplo la figura 25.8. Si  $f$  es un flujo, el *flujo neto* a través

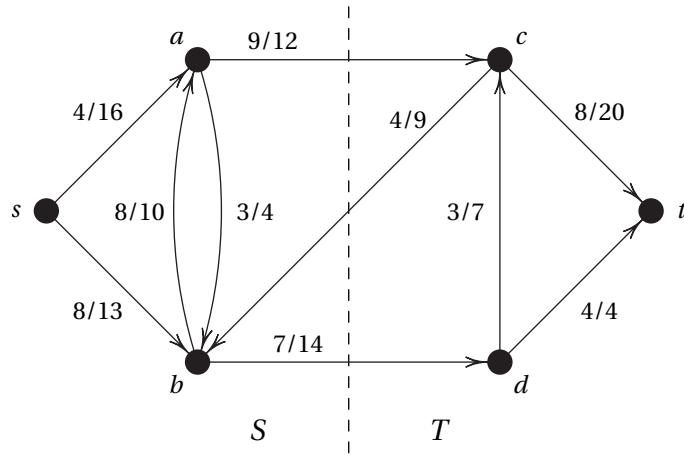


Figura 25.8 – Un corte en la red de la figura 25.5 con el flujo de la figura 25.6a

del corte  $(S, T)$  se define como  $f(S, T)$ . En nuestro caso (figura 25.8) el flujo neto es  $9 - 4 + 7 = 12$ . La *capacidad* del corte  $(S, T)$  es  $c(S, T)$ , que en la misma figura correspondería a  $12 + 14 = 26$ . También se define un *corte mínimo* (en inglés *minimum cut*) como un corte de capacidad mínima. El flujo neto que cruza el corte incluye flujos de  $S$  a  $T$  (aportes positivos) y flujos de  $T$  a  $S$  (aportes negativos). Por otro lado, en las capacidades se incluyen solo las de arcos de  $S$  a  $T$ . El lema siguiente relaciona los flujos con las capacidades a través de cortes de la red.

**Lema 25.5.** *Sea  $f$  un flujo en la red  $D = (V, A)$  con fuente  $s$  y sumidero  $t$ , y sea  $(S, T)$  un corte de la red. Entonces el flujo neto a través del corte es el valor del flujo.*

*Demuestração.* Por conservación de flujo  $f(S - s, V) = 0$ , y aplicando el lema 25.1, tenemos:

$$\begin{aligned} f(S, T) &= f(S, V) - f(S, S) \\ &= f(S, V) \\ &= f(s, V) + f(S - s, V) \\ &= f(s, V) \\ &= \text{val}(f) \end{aligned}$$

□

Un resultado inmediato del lema 25.5 es el resultado que demostramos antes, que el flujo al sumidero es el valor del flujo en la red: Basta tomar el corte  $(V - t, \{t\})$  para ello.

Pero también podemos deducir:

**Corolario 25.6.** En una red  $D$  con un corte  $(S, T)$ , el valor de cualquier flujo está acotado por la capacidad del corte.

*Demostración.* Sea  $(S, T)$  un corte cualquiera de  $D$  y sea  $f$  un flujo. Por el lema 25.5 y las restricciones de capacidad:

$$\begin{aligned}\text{val}(f) &= f(S, T) \\ &= \sum_{x \in S} \sum_{y \in T} f(x, y) \\ &\leq \sum_{x \in S} \sum_{y \in T} c(x, y) \\ &= c(S, T)\end{aligned}$$

□

Una consecuencia inmediata del corolario 25.6 es que el valor de un flujo está acotado por la capacidad de un corte mínimo. El teorema siguiente nos dice que el flujo máximo en realidad es esta cota.

**Teorema 25.7** (Max-Flow Min-Cut). *Si  $f$  es un flujo en la red  $D = (V, A)$  con fuente  $s$  y sumidero  $t$ , entonces las siguientes son equivalentes:*

- (1)  $f$  es un flujo máximo en  $D$ .
- (2) La red residual  $D_f$  no contiene caminos aumentables.
- (3)  $\text{val}(f) = c(S, T)$  para algún corte  $(S, T)$  de  $D$ .

*Demostración.* Demostramos la equivalencia a través de un ciclo de implicancias.

(1)  $\Rightarrow$  (2): Por contradicción. Supongamos en contrario que  $f$  es máximo en  $D$ , pero que  $D_f$  tiene un camino aumentable  $p$ . Por el corolario 25.4 sabemos que  $f + f_p$  es un flujo, cuyo valor es mayor que  $\text{val}(f)$ , lo que contradice la suposición de que  $f$  es máximo.

(2)  $\Rightarrow$  (3): Supongamos que  $D_f$  no tiene camino aumentable, es decir, no hay camino dirigido de  $s$  a  $t$  en  $D_f$ . Definamos:

$$\begin{aligned}S &= \{x \in V : \text{hay un camino de } s \text{ a } x \text{ en } D_f\} \\ T &= V \setminus S\end{aligned}$$

Entonces  $(S, T)$  es un corte de  $D$ , ya que obviamente  $s \in S$  y  $t \notin S$  ya que no hay camino de  $s$  a  $t$  en  $D_f$  por suposición. Para cada par de vértices  $x \in S$  e  $y \in T$  tenemos  $f(x, y) = c(x, y)$ , dado que de lo contrario  $xy \in A_f$  y habría un camino  $s \rightsquigarrow x \rightarrow y$  y así  $y$  estaría en  $S$ . Por el lema 25.5 es:

$$\text{val}(f) = f(S, T) = c(S, T)$$

(3)  $\Rightarrow$  (1): Por el corolario 25.6,  $\text{val}(f) \leq c(S, T)$  para todo corte  $(S, T)$ . La condición  $\text{val}(f) = c(S, T)$  entonces asegura que el flujo es máximo. □

Este teorema sirve para demostrar la validez del método de Ford-Fulkerson: Si en una iteración no hay un camino aumentable, quiere decir que el flujo actual es máximo. Una manera razonable de buscar un camino aumentable es usar búsqueda a lo ancho en la red residual. A esta forma de implementar el método de Ford-Fulkerson se le conoce como el algoritmo de Edmonds-Karp [110]. Una discusión detallada del problema, incluyendo historia de los algoritmos, presenta Wilf [363, capítulo 3].

## 26 Permutaciones

---

Informalmente, una permutación es un reordenamiento de un conjunto de objetos. Las permutaciones aparecen, en forma más o menos prominente, en casi todos los ámbitos de las matemáticas. Al tratar con conjuntos finitos es común estar interesados en las distintas formas de ordenarlos, posiblemente simplemente para considerar equivalentes los distintos órdenes. En el análisis de muchos algoritmos, particularmente los de ordenamiento, son características de las permutaciones lo que determina su rendimiento.

### 26.1. Definiciones básicas

Al reordenar elementos de un conjunto estamos definiendo una biyección entre la posición original y la nueva. Nos interesa estudiar estas biyecciones.

**Definición 26.1.** Una *permutación* de un conjunto finito  $\mathcal{X}$  es una biyección de  $\mathcal{X}$  a  $\mathcal{X}$ .

Comúnmente usaremos  $\mathcal{X} = \{1, 2, \dots, n\}$  para concretar. Por ejemplo, una permutación típica de  $\{1, 2, \dots, 5\}$  es la función  $\alpha$  definida por la tabla:

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \alpha \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 4 & 5 & 1 & 3 \end{array}$$

Para abreviar, anotaremos una permutación dando el elemento al que va el de la posición indicada, o sea en este caso particular:

$$\alpha = (2 \ 4 \ 5 \ 1 \ 3)$$

Viene a ser simplemente la última línea en lo anterior.

Hay  $n!$  permutaciones de un conjunto de  $n$  elementos (para crear la permutación  $\pi$  el valor de  $\pi(1)$  puede elegirse de  $n$  maneras, una vez elegido este quedan solo  $n - 1$  opciones para  $\pi(2)$ , y así sucesivamente, y finalmente queda solo una opción para  $\pi(n)$ ).

Tomemos la anterior permutación  $\alpha$  y la permutación  $\beta = (3 \ 5 \ 1 \ 4 \ 2)$ . La composición  $\beta\alpha$  se obtiene de aplicar  $\alpha$ , luego  $\beta$ , y resulta:

$$\beta\alpha = (5 \ 4 \ 2 \ 3 \ 1)$$

En general, la composición no es commutativa, en nuestro caso:

$$\alpha\beta = (5 \ 3 \ 2 \ 1 \ 4)$$

y claramente  $\alpha\beta \neq \beta\alpha$ . Cuidado, la convención general al operar con permutaciones es que las operaciones se efectúan de izquierda a derecha, no de derecha a izquierda como correspondería dado que la operación es composición de funciones. O sea,  $\alpha\beta\gamma$  se interpreta como  $(\alpha\beta)\gamma$ . En todo caso, dado que esto es un grupo, la operación es asociativa.

**Teorema 26.1.** *Las permutaciones cumplen las siguientes:*

- (I) *Si  $\pi$  y  $\sigma$  son permutaciones de un conjunto de  $n$  elementos, lo es también  $\pi\sigma$ .*
- (II) *Para todas permutaciones  $\pi, \sigma, \tau$  de un conjunto, se cumple:*

$$(\pi\sigma)\tau = \pi(\sigma\tau)$$

- (III) *La función identidad, que llamaremos  $\iota$ , definida por  $\iota(r) = r$ , es una permutación, y tenemos para toda permutación  $\sigma$ :*

$$\iota\sigma = \sigma\iota = \sigma$$

- (IV) *Para toda permutación  $\pi$  de un conjunto dado hay una permutación inversa  $\pi^{-1}$  tal que:*

$$\pi\pi^{-1} = \pi^{-1}\pi = \iota$$

*Demostración.* La propiedad (I) sigue directamente de que la composición de biyecciones es una biyección, (II) es una propiedad básica de la composición de funciones, (III) es obvio, y (IV) es simplemente que toda biyección tiene una inversa.  $\square$

El teorema 26.1 equivale a decir que las permutaciones forman un grupo con la operación de composición. Al grupo de permutaciones de  $n$  elementos se le llama el *grupo simétrico de orden  $n$* , que se anota  $S_n$ . Note eso sí que el orden de  $S_n$  es  $n!$ , a diferencia de lo que parece indicar su nombre.

Es conveniente una notación compacta para permutaciones individuales. Consideremos nuevamente la permutación  $\alpha$ . Es  $\alpha(1) = 2$ ,  $\alpha(2) = 4$ ,  $\alpha(4) = 1$ . Esto forma un *ciclo*  $(1 \rightarrow 2 \rightarrow 4 \rightarrow 1)$  de largo 3. Similarmente, 3 y 5 forman un ciclo de largo 2, y podemos escribir  $\alpha$  en *notación de ciclos* como  $\alpha = (1\ 2\ 4)(3\ 5)$ .

Toda permutación  $\pi$  se puede escribir en notación de ciclos mediante el siguiente algoritmo:

- Comience con algún símbolo (digamos 1), y trace el efecto de  $\pi$  sobre él y sus sucesores hasta que nuevamente encontramos 1, así tenemos un ciclo.
- Tome un símbolo cualquiera que no haya sido considerado aún, y construya el ciclo que lo contiene de la misma forma.
- Continúe de la misma forma hasta haber dado cuenta de todos los símbolos.

Podemos elegir cualquiera de los elementos de cada ciclo como primero – por ejemplo,  $(7\ 8\ 2\ 1\ 3)$  es lo mismo que  $(1\ 3\ 7\ 8\ 2)$ . Por otro lado, podemos reordenar los ciclos – por ejemplo,  $(1\ 2\ 4)(3\ 5)$  y  $(3\ 5)(1\ 2\ 4)$  corresponden a la misma permutación, ya que al operar los ciclos en esta representación sobre elementos diferentes los ciclos conmutan. Lo importante son el número de ciclos, sus largos, y la disposición de sus elementos. Se adopta la convención de comenzar cada ciclo con su mínimo elemento, y luego ordenar los ciclos en orden de elemento mínimo.

Para ver que la representación es única, debemos mostrar una biyección entre permutaciones y ciclos. Si anotamos los ciclos siempre con el máximo elemento al comienzo, y listamos los ciclos en orden de máximo elemento creciente, tomamos una permutación cualquiera podemos interpretarla como escrita en notación de ciclos: Los comienzos de cada ciclo son los máximos hasta ese punto. Esto constituye una biyección, y toda permutación puede escribirse en ciclos de una única forma.

Por ejemplo, para la permutación  $\beta$  dada anteriormente, la notación de ciclos es  $\beta = (1\ 3)(2\ 5)(4)$ . Acá 4 forma un ciclo “degenerado” por sí mismo, ya que  $\beta(4) = 4$ . Simplemente omitiremos estos ciclos de largo 1, ya que corresponden a símbolos que no son afectados por la permutación. En todo

caso, es mejor no omitirlos hasta que uno se haya familiarizado con la notación. Puede considerarse la notación de ciclos como el producto de las permutaciones con esos ciclos (los demás elementos permanecen fijos). O sea, en nuestro caso:

$$\beta = (1\ 3)(2\ 4)(5) \cdot (1\ 2\ 5)(3\ 4)$$

Esto es consistente con la convención de omitir ciclos de largo uno.

**Ejemplo 26.1.** Se tienen cartas numeradas 1 a 12, que se reparten en filas como muestra la figura 26.1a. Luego se toman las cartas por filas y se distribuyen en columnas, quedando como lo muestra

1    2    3	1    4    7
4    5    6	10    2    5
7    8    9	8    11    3
10    11    12	6    9    12
(a) Original	(b) Columnas

Figura 26.1 – Ordenamiento de cartas

la figura 26.1b. ¿Cuántas veces hay que repetir esta operación hasta obtener nuevamente el orden original?

Sea  $\pi$  la permutación que corresponde a esta operación, lo que buscamos es el orden de  $\pi$  en  $S_{12}$ . Esta manera de verlo nos dice que el problema tiene solución, cosa que no es obvia: Perfectamente podría ocurrir que saliendo de la configuración inicial ya no haya manera de volver a ella. En notación de ciclos tenemos  $\pi = (1)(2\ 4\ 10\ 6\ 5)(3\ 7\ 8\ 11\ 9)(12)$ . Las cartas 1 y 12 no cambian de posición, las demás forman dos ciclos de largo 5. Al repetir esta operación 5 veces todas las cartas quedan en sus posiciones originales.

**Ejemplo 26.2.** En la Prisión de Dunwich hay 100 prisioneros. En su aburrimiento al alcaide se le ocurre un jueguito: Toma 100 cajas, las rotula con los números de los prisioneros y en cada una coloca un número de prisionero al azar. Luego ofrece a los prisioneros lo siguiente: Cada uno puede elegir 50 de las cajas, si alguno no encuentra su número los llevará a todos a un paseo a las colinas de Vermont.

Si se considera que cada prisionero abre 50 cajas al azar, es claro que hallará su número la mitad de las veces, y por tanto la probabilidad que todos encuentren los suyos es  $2^{-100}$ , verdaderamente microscópico.

Sin embargo, hay un algoritmo que asegura una razonable probabilidad de evitar una suerte horrorosa: Cada cual abre la caja con su número, luego la caja con el número que halló en la primera, y así sucesivamente hasta agotar las 50 o hallar el suyo. Lo que está haciendo cada prisionero es trazar un ciclo de la permutación, interesa entonces saber cuántas permutaciones de 100 elementos tienen ciclos de largo mayor a 50. Como son 100 prisioneros, una permutación puede tener a lo más un ciclo de los largos de interés, por lo que contar el número de permutaciones con estos ciclos es simplemente contar el número total de tales ciclos en permutaciones de 100 elementos. Si consideramos un ciclo de  $r$  elementos, estos podemos elegirlos de  $\binom{100}{r}$  maneras entre los 100, y podemos ordenarlos de  $(r - 1)!$  formas en un ciclo. Los  $100 - r$  elementos restantes se pueden organizar de  $(100 - r)!$  maneras, con lo que el número de permutaciones con un ciclo de largo  $r$  son:

$$\binom{100}{r} (r - 1)! (100 - r)! = \frac{100!}{r}$$

Vale decir, exactamente 1 en  $r$  permutaciones tienen un ciclo de largo  $r$  cuando  $r > 50$ . Nos interesa entonces la proporción:

$$\sum_{51 \leq r \leq 100} \frac{1}{r} = H_{100} - H_{50} \approx 0,6882$$

Tienen un poco más de 31% de probabilidades de salvarse.

Si un ciclo se compone consigo mismo, el primer elemento del ciclo termina en el tercer lugar, y así sucesivamente. Para que el primer elemento de un ciclo de largo  $k$  vuelva a su posición original debe elevarse a la potencia  $k$ . Para que todos los elementos de una permutación de tipo  $[1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}]$  vuelvan por primera vez a sus posiciones originales (lo que determina el orden de la permutación) deben volver a sus posiciones originales todos los elementos de todos los ciclos. Esto es el mínimo común múltiplo de los largos de los ciclos. No importa cuántos ciclos de cada largo hay, solo si de los largos respectivos hay o no ciclos.

**Definición 26.2.** Una permutación  $\tau$  que es su propio inverso se llama *involución*.

Las involuciones son aquellas permutaciones que solo tienen ciclos de largo 1 y 2, quedan representadas por  $\text{MSET}(\text{CYC}_{\leq 2}(\mathcal{Z}))$ . Como la función generatriz exponencial de un ciclo de largo  $r$  es simplemente  $z^r/r$ , la función generatriz exponencial  $\hat{I}(z)$  para el número de involuciones de  $n$  elementos es:

$$\hat{I}(z) = \exp(z + z^2/2) \quad (26.1)$$

Prácticamente indoloro.

Un desarreglo (ver sección 22.10 y también el capítulo 15) es simplemente una permutación que no tiene ciclos de largo uno. La expresión simbólica correspondiente es  $\text{MSET}(\text{CYC}_{\geq 2}(\mathcal{Z}))$ , que podemos expresar  $\text{MSET}(\text{CYC}(\mathcal{Z}) - \text{CYC}_{=1}(\mathcal{Z}))$ , la función generatriz exponencial que resulta es:

$$\hat{D}(z) = \exp(-\ln(1-z) - z) = \frac{e^{-z}}{1-z}$$

De acá nuevamente obtenemos el número de desarreglos de  $n$  elementos como  $D_n = n! \exp|_n(-1)$ .

En el ejemplo de la prisión de Dunwich buscábamos el número de permutaciones con ciclos de largo mayor a 50. Este tipo de problemas puede atacarse marcando las subestructuras de interés. Usamos la clase  $\mathcal{U}$  para marcar, con un único elemento  $v$  de tamaño uno, y usamos la letra  $u$  en funciones generatrices. Si queremos saber cuántos ciclos de largo  $r$  hay en total en permutaciones de  $n$  elementos, consideraremos:

$$\text{MSET}(\text{CYC}_{\neq r}(\mathcal{Z}) + \mathcal{U} \times \text{CYC}_{=r}(\mathcal{Z}))$$

Abusando de la notación, escribimos:

$$\text{MSET}(\text{CYC}_{\neq r}(\mathcal{Z}) + u \text{CYC}_{=r}(\mathcal{Z})) = \text{MSET}(\text{CYC}(\mathcal{Z}) + (u-1) \text{CYC}_{=r}(\mathcal{Z}))$$

Tenemos directamente:

$$C_r(z, u) = \exp\left(-\ln(1-z) + (u-1) \frac{z^r}{r}\right) = \frac{e^{(u-1)z^r/r}}{1-z}$$

El número de ciclos de largo  $r$  es el exponente de  $u$ , que podemos extraer derivando y haciendo  $u = 1$ , lo que da la función generatriz exponencial para el número total de ciclos de largo  $r$  en permutaciones de  $n$  elementos:

$$C_r(z) = \frac{\partial}{\partial u} C_r(z, u) \Big|_{u=1} = \frac{z^r}{r} \frac{1}{1-z}$$

De acá podemos obtener el número promedio de ciclos de largo  $r$  en las permutaciones de  $n$  elementos, al haber  $n!$  permutaciones y ser una función generatriz exponencial es directamente el coeficiente de  $z^n$ :

$$[z^n] \frac{z^r}{r} \frac{1}{1-z} = \frac{1}{r}$$

Esto ya lo habíamos obtenido en el ejemplo, y al discutir desarreglos en el capítulo 15 vimos que para  $r = 1$  es 1, pero esta técnica es mucho más general.

A cada permutación  $\pi$  en  $S_n$  corresponde una partición de los  $n$  elementos en los elementos de sus ciclos. Al número de ciclos de cada largo de la permutación le llamaremos su *tipo*. O sea, si  $\pi$  tiene  $\alpha_i$  ciclos de largo  $i$  ( $1 \leq i \leq n$ ), el tipo de  $\pi$  lo anotamos  $[1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}]$ . Generalmente omitiremos los factores con  $\alpha_i = 0$  (largos para los cuales no hay ciclos).

**Definición 26.3.** Si hay una permutación  $\sigma$  tal que  $\sigma\alpha\sigma^{-1} = \beta$  se dice que  $\beta$  es *conjugada* de  $\alpha$ .

El teorema siguiente es básico en la teoría algebraica de permutaciones.

**Teorema 26.2.** Dos permutaciones  $\alpha$  y  $\beta$  son conjugadas si y solo si tienen el mismo tipo.

*Demostración.* Demostramos implicancias en ambas direcciones.

Si  $\alpha$  y  $\beta$  son permutaciones conjugadas, hay  $\sigma$  tal que podemos escribir  $\sigma\alpha\sigma^{-1} = \beta$ . Tomemos un ciclo  $(x_1, x_2, \dots, x_r)$  de  $\alpha$ , vale decir,  $\alpha(x_1) = x_2, \alpha(x_2) = x_3, \dots, \alpha(x_{r-1}) = x_r, \alpha(x_r) = x_1$ . Definamos  $y_i = \sigma(x_i)$  para  $1 \leq i \leq r$ . Tenemos, tomando los índices módulo  $r$ :

$$\beta(y_i) = \sigma\alpha\sigma^{-1}(\sigma(x_i)) = \sigma\alpha(x_i) = \sigma(x_{i+1}) = y_{i+1}$$

Esto es una biyección entre el ciclo de  $\alpha$  que contiene a  $x_1$  y el ciclo de  $\beta$  que contiene a  $y_1$ , y habrán biyecciones similares entre los demás ciclos de  $\alpha$  y  $\beta$ , que así tienen el mismo tipo.

Por otro lado, supongamos que  $\alpha$  y  $\beta$  tienen el mismo tipo. Como tienen el mismo número de ciclos de cada uno de los largos, podemos construir una biyección entre ciclos del mismo largo de  $\alpha$  y  $\beta$ , digamos  $(x_1, x_2, \dots, x_r)$  en  $\alpha$  corresponde a  $(y_1, y_2, \dots, y_r)$  en  $\beta$ . Definiendo  $\sigma(x_i) = y_i$  para este ciclo, y de forma similar para los demás ciclos, tenemos  $\sigma\alpha\sigma^{-1} = \beta$  ya que (considerando los índices módulo el largo del ciclo) tenemos:

$$\sigma\alpha\sigma^{-1}(y_i) = \sigma\alpha(x_i) = \sigma(x_{i+1}) = y_{i+1} = \beta(y_i)$$

□

Una manera fundamental de clasificar permutaciones viene de considerarlas como composición de *transposiciones*, que son permutaciones que solo intercambian dos elementos.

Una permutación es una transposición si es del tipo  $[1^{n-2} 2^1]$  (tiene  $n - 2$  ciclos de largo 1 y un ciclo de largo 2). Ahora bien, el ciclo  $(x_1 x_2 \dots x_r)$ , transforma  $(x_1 x_2 \dots x_r)$  en  $(x_2 x_3 \dots x_r x_1)$ , y este mismo efecto se logra intercambiando  $x_1$  con  $x_2$ , luego  $x_2$  (que ahora está en la posición  $x_1$ ) con  $x_3$ , y así sucesivamente. Así podemos escribir  $(x_1 x_2 \dots x_r) = (x_1 x_r) \dots (x_1 x_3)(x_1 x_2)$ . Como toda permutación se puede descomponer en ciclos, toda permutación puede expresarse en términos de transposiciones. Por ejemplo, aplicando la idea indicada arriba a cada uno de los ciclos:

$$(1 \ 3 \ 6)(2 \ 4 \ 5 \ 7) = (1 \ 6)(1 \ 3)(2 \ 7)(2 \ 5)(2 \ 4)$$

Las transposiciones se pueden traslapar, un elemento puede moverse más de una vez. Esta representación no es única, además de reordenar las transposiciones podemos usar un conjunto completamente diferente de estas, como:

$$(1 \ 3 \ 6)(2 \ 4 \ 5 \ 7) = (1 \ 5)(3 \ 5)(3 \ 6)(5 \ 7)(1 \ 4)(2 \ 7)(1 \ 2)$$

Sin embargo, hay una característica común entre estas descomposiciones. Sea  $c(\pi)$  al número total de ciclos de  $\pi$ . Si  $\pi$  es de tipo  $[1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}]$ , entonces  $c(\pi) = \alpha_1 + \alpha_2 + \dots + \alpha_n$ . Si combinamos  $\pi$  con una transposición  $\tau$ , dando  $\tau\pi$ , interesa determinar la relación entre  $c(\pi)$  y  $c(\tau\pi)$ . Si  $\tau$  intercambia  $a$  con  $b$ , tenemos  $\tau(a) = b$ ,  $\tau(b) = a$  y  $\tau(k) = k$  si  $k \neq a, b$ . Cuando  $a$  y  $b$  están en el mismo ciclo de  $\pi$ , podemos escribir:

$$\pi = (ax\dots yb\dots z) \text{ y otros ciclos}$$

Veamos  $\tau\pi$ . Como  $\tau$  intercambia  $a$  con  $b$ , los ciclos de  $\pi$  que no los incluyen no cambian. Sean  $\pi(a) = x$ ,  $\pi(y) = b$ ,  $\pi(z) = a$ ; con lo que  $\tau\pi(a) = \tau(x) = x$  y  $\tau\pi(y) = \tau(b) = a$ . De la misma forma  $\tau\pi(b) = \pi(b), \dots, \tau\pi(z) = \tau(a) = b$ . Se corta el ciclo y resulta:

$$\tau\pi = (ax\dots y)(b\dots z) \text{ y los otros ciclos}$$

con lo que  $c(\tau\pi) = c(\pi) + 1$ . Por otro lado, si  $a$  y  $b$  pertenecen a ciclos distintos, o sea podemos escribir:

$$\pi = (ax\dots y)(b\dots z) \text{ y otros ciclos}$$

vemos que  $\tau\pi(y) = \tau(a) = b$  y  $\tau\pi(z) = \tau(b) = a$ , los ciclos se funden:

$$\tau\pi = (ax\dots yb\dots z) \text{ y los otros ciclos}$$

con lo que  $c(\tau\pi) = c(\pi) - 1$ . En resumen, seguir una permutación por una transposición cambia el número de ciclos en 1, y tenemos:

**Teorema 26.3.** *Supóngase que la permutación  $\pi$  de  $S_n$  puede escribirse como la composición de  $r$  transposiciones y también como la composición de  $r'$  transposiciones. Entonces  $r$  y  $r'$  son ambos pares o ambos impares.*

*Demostración.* Sea  $\pi = \tau_r \tau_{r-1} \dots \tau_1$ , con  $\tau_i$  ( $1 \leq i \leq r$ ) una transposición. Como  $\tau_1$  es un ciclo de largo 2 y  $n - 2$  ciclos de largo 1, es  $c(\tau_1) = 1 + (n - 2) = n - 1$ . Combinando  $\tau_1$  con  $\tau_2, \tau_3, \dots, \tau_r$  finalmente se obtiene  $\pi$ . En cada paso  $c$  aumenta o disminuye en 1. Sea  $g$  el número de veces que aumenta y  $h$  el número de veces que disminuye. El número final de ciclos será  $c(\pi) = (n - 1) + g - h$ . Pero tenemos  $g + h = r - 1$ , con lo que:

$$\begin{aligned} r &= 1 + g + h \\ &= 1 + g + (n - 1 + g - c(\pi)) \\ &= n - c(\pi) + 2g \end{aligned}$$

De la misma forma, para cualquier otra manera de expresar  $\pi$  como producto de  $r'$  transposiciones hay un entero  $g'$  tal que  $r' = n - c(\pi) + 2g'$ , y  $r - r' = 2(g - g')$ , que es par.  $\square$

En vista del teorema 26.3 podemos clasificar las permutaciones en *pares* o *impares* dependiendo del número de transposiciones que las conforman. Definimos el *signo* de la permutación  $\rho$ , escrito  $\operatorname{sgn} \rho$ , como  $+1$  si  $\rho$  es par, y  $-1$  si es impar:

$$\operatorname{sgn} \rho = (-1)^r$$

donde  $\rho$  es la composición de  $r$  transposiciones. En particular,  $\operatorname{sgn} \iota = (-1)^0 = +1$ . Claramente, si  $\rho$  se puede descomponer en  $r$  transposiciones y  $\sigma$  se puede descomponer en  $s$  transposiciones, entonces  $\rho\sigma$  se puede descomponer en  $r + s$  transposiciones:

$$\begin{aligned} \operatorname{sgn}(\rho\sigma) &= (-1)^{r+s} \\ &= (-1)^r \cdot (-1)^s \\ &= \operatorname{sgn} \rho \cdot \operatorname{sgn} \sigma \end{aligned}$$

Como  $\rho\rho^{-1} = \iota$ , resulta  $\operatorname{sgn} \rho = \operatorname{sgn} \rho^{-1}$ .

Recordando nuestra técnica para escribir un ciclo de largo  $k$  como  $k-1$  transposiciones, tenemos un algoritmo simple para determinar el signo de una permutación: Descompóngala en ciclos, la paridad de la permutación es simplemente la del número de ciclos de largo par.

**Teorema 26.4.** *Para todo entero  $n \geq 2$  exactamente la mitad de las permutaciones de  $S_n$  son pares y la otra mitad impares.*

*Demostración.* Sea  $\pi_1, \pi_2, \dots, \pi_k$  la lista de permutaciones pares en  $S_n$ . Esta lista no es vacía, ya que  $\iota$  es par.

Sea  $\tau$  una transposición cualquiera en  $S_n$ , por ejemplo  $\tau = (1\ 2)$ . Entonces  $\tau\pi_1, \tau\pi_2, \dots, \tau\pi_k$  son todas distintas, ya que si  $\tau\pi_i = \tau\pi_j$  por asociatividad e inverso en el grupo:

$$\pi_i = (\tau^{-1}\tau)\pi_i = \tau^{-1}(\tau\pi_i) = \tau^{-1}(\tau\pi_j) = (\tau^{-1}\tau)\pi_j = \pi_j$$

Aún más, todas estas permutaciones son impares, ya que:

$$\operatorname{sgn}(\tau\pi_i) = \operatorname{sgn} \tau \cdot \operatorname{sgn} \pi_i = (-1) \cdot (+1) = -1$$

Finalmente, toda permutación impar  $\rho$  es de una de las  $\tau\pi_i$  ( $1 \leq i \leq k$ ), ya que:

$$\operatorname{sgn}(\tau^{-1}\rho) = \operatorname{sgn} \tau^{-1} \cdot \operatorname{sgn} \rho = (-1) \cdot (-1) = +1$$

con lo que  $\tau^{-1}\rho$  es par, y debe ser  $\pi_i$  para algún  $i$  en el rango  $1 \leq i \leq k$ , y así  $\rho = \tau\pi_i$ . Con esto tenemos una biyección entre las permutaciones pares e impares.  $\square$

El conjunto de permutaciones pares es un subgrupo de  $S_n$  ( $S_n$  es finito, y este subconjunto es cerrado respecto de la composición), se le llama el *grupo alternante* y se anota  $A_n$ .

Esto tiene aplicación en muchas áreas, por ejemplo en “matemáticas recreativas”.

**Ejemplo 26.3.** Ocho bloques marcados 1 a 8 se disponen en un marco cuadrado como se indica en la figura 26.2a. Una movida legal corresponde a deslizar un bloque al espacio vacío. Determine si es

1	2	3
4	5	6
7	8	

(a) Inicial

8	5	2
7	4	1
6	3	

(b) Final

Figura 26.2 – ¿Puede hacerse?

possible lograr la configuración de 26.2b.

Si anotamos  $\square$  para el espacio, la configuración inicial es 1 2 3 4 5 6 7 8  $\square$ , y la final solicitada es 8 5 2 7 4 1 6 3  $\square$ . Claramente toda movida legal es una transposición. Como el espacio solo puede moverse en vertical u horizontal, para regresar a su posición original debe hacer un número par de movidas en cada dirección, y el número total de movidas es par. Luego la permutación que lleva de la configuración inicial a otra configuración posible bajo las reglas en la que  $\square$  está nuevamente en la esquina inferior derecha está conformada por un número par de transposiciones, o sea es par. La permutación entre la configuración final solicitada y la inicial es  $(1\ 8\ 3\ 2\ 5\ 4\ 7\ 6)(\square)$ ; el ciclo de largo 8 que aparece acá es impar, por lo que esto no puede hacerse.

Nótese que esto sirve para demostrar lo que *no* puede hacerse, no significa que todas las permutaciones pares puedan lograrse con estas restricciones.

Es simple contabilizar las permutaciones de un tipo particular. Supongamos, por ejemplo, que nos interesa saber cuántos elementos de  $S_{14}$  tienen tipo  $[2^2 3^2 4^1]$ . Esto corresponde a poner los símbolos  $1, 2, \dots, 14$  en el patrón:

$$(.) (.) (\dots) (\dots) (\dots)$$

y hay  $14!$  formas de distribuir los 14 símbolos en las 14 posiciones. Sin embargo, muchas de estas dan la misma permutación. Considerando cada ciclo, podemos elegir el primer elemento de él y el resto quedará determinado por la permutación. Así hay 2 maneras de obtener cada 2-ciclo, 3 maneras de obtener cada 3-ciclo, y 4 maneras de obtener cada 4-ciclo. El ordenamiento interno de cada ciclo se puede llevar a cabo de  $2^2 \cdot 3^2 \cdot 4$  formas en este caso. En general, si el tipo es  $[1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}]$ , habrán  $1^{\alpha_1} \cdot 2^{\alpha_2} \dots n^{\alpha_n}$  ordenamientos internos equivalentes. Por otro lado, el orden de los ciclos del mismo largo es arbitrario, por lo que el número de reordenamientos en el caso general será  $\alpha_1! \alpha_2! \dots \alpha_n!$ , y el número de permutaciones de tipo  $[1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}]$  es:

$$\frac{n!}{1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n} \alpha_1! \alpha_2! \dots \alpha_n!}$$

Esto se ve seductoramente similar a un término multinomial, pero debe recordarse que acá la condición es:

$$\sum_k k\alpha_k = n$$

## 27 Teoría de colores de Pólya

---

Los problemas combinatorios que hemos enfrentado hasta acá han sido relativamente sencillos. Sólo al considerar la construcción ciclo de objetos no rotulados (capítulo 21) tuvimos que considerar simetrías de los objetos bajo estudio. El teorema de enumeración de Pólya (abreviado *PET*, por *Pólya Enumeration Theorem*) en realidad fue publicado en 1927 por John Howard Redfield, en 1937 George Pólya lo redescubrió independientemente y lo popularizó aplicándolo a muchos problemas de conteo, en particular de compuestos químicos [288, 291].

### 27.1. Grupos de permutaciones

Desarrollaremos la teoría para la situación simple en la cual solo contamos colores. Una derivación más intuitiva (que puede ser útil para motivar el desarrollo presente) ofrece Tucker [355].

**Definición 27.1.** Sea  $G$  un conjunto de permutaciones del conjunto finito  $\mathcal{X}$ . Si  $G$  es un grupo (con la composición de permutaciones) decimos que  $G$  es un grupo de permutaciones de  $\mathcal{X}$ .

Si tomamos  $\mathcal{X} = \{1, 2, \dots, n\}$ , entonces un grupo de permutaciones es simplemente un subgrupo de  $S_n$ . El cuadro 27.1 lista todos los subgrupos de  $S_3$ . El grupo alternante  $A_3$  aparece como  $H_5$  en el

$$\begin{array}{lll} H_1 = \{\iota\} & H_2 = \{\iota, (1\ 2)\} & H_3 = \{\iota, (1\ 3)\} \\ H_4 = \{\iota, (2\ 3)\} & H_5 = \{\iota, (1\ 2\ 3), (1\ 3\ 2)\} & H_6 = S_3 \end{array}$$

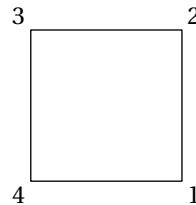
Cuadro 27.1 – Los subgrupos de  $S_3$

cuadro. Para ver si un subconjunto de un grupo finito es un subgrupo, basta verificar si es cerrado por lo demostrado anteriormente para grupos.

Otros ejemplos se obtienen como grupos de simetría de objetos geométricos. Por ejemplo, si rotulamos los vértices de un cuadrado en orden contrario a las manecillas del reloj (ver la figura 27.1), cada simetría induce una permutación del conjunto  $\{1, 2, 3, 4\}$ , y obtenemos las simetrías indicadas. Estas 8 permutaciones forman el llamado *grupo diedral de orden 8*,  $D_8$ . En general, las simetrías de un  $n$ -ágono regular forman un grupo de  $2n$  elementos, el *grupo diedral de orden  $2n$*  que se anota  $D_{2n}$ . Debe tenerse cuidado: Esta es la notación que se usa en álgebra, en geometría este mismo grupo se anota  $D_n$ . Si solo se consideran las rotaciones de un polígono regular de  $n$  lados, tenemos el grupo cíclico de orden  $n$ , anotado  $C_n$ , isomorfo a  $\mathbb{Z}_n$  con la suma.

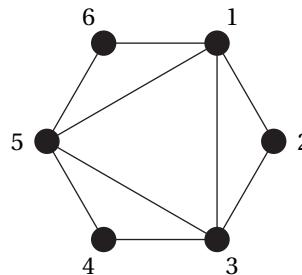
Una situación similar se produce cuando estudiamos grafos en vez de figuras geométricas, en donde las “simetrías” son permutaciones de los vértices que transforman arcos en arcos. A una permutación de este tipo se le llama *automorfismo* del grafo (viene a ser un isomorfismo del grafo consigo mismo).

Un ejemplo de grafo es la figura 27.2, interesa saber cuántos automorfismos tiene. Primero observamos que los vértices del grafo caen naturalmente en dos grupos: Los vértices  $\{1, 3, 5\}$  son de grado



Identidad	(1)(2)(3)(4)
Rotación en $\pi/2$	(1 2 3 4)
Rotación en $\pi$	(1 3)(2 4)
Rotación en $3\pi/2$	(1 4 3 2)
Reflexión en diagonal 1 3	(2 4)
Reflexión en diagonal 2 4	(1 3)
Reflexión en bisector perpendicular de 1 2	(1 2)(3 4)
Reflexión en bisector perpendicular de 1 4	(1 4)(2 3)

Figura 27.1 – Un cuadrado y sus simetrías



$\iota$	se extiende a $\iota$
$(1 \ 3 \ 5)$	se extiende a $(1 \ 3 \ 5)(2 \ 4 \ 6)$
$(1 \ 5 \ 3)$	se extiende a $(1 \ 5 \ 3)(2 \ 6 \ 4)$

$(1 \ 3) \text{ se extiende a } (1 \ 3)(4 \ 6)$

$(1 \ 5) \text{ se extiende a } (1 \ 5)(2 \ 4)$

$(3 \ 5) \text{ se extiende a } (3 \ 5)(2 \ 6)$

Figura 27.2 – Un grafo de seis vértices y sus automorfismos

4, mientras  $\{2, 4, 6\}$  son de grado 2. Ningún automorfismo puede transformar un vértice del primer grupo en uno del segundo. Por otro lado, está claro que podemos tomar *cualquier* permutación de  $\{1, 2, 3\}$  y extenderla a un automorfismo del grafo. Por ejemplo, si  $(1 \ 3 \ 5)$  es parte de un automorfismo  $\alpha$ , entonces  $\alpha$  tiene que transformar 2 en 4, ya que 2 es el único vértice adyacente a 1 y 3, y 4 es el único vértice adyacente a sus imágenes 3 y 5. De la misma forma,  $\alpha$  lleva 4 en 6 y 6 en 2, por lo que  $\alpha = (1 \ 3 \ 5)(2 \ 4 \ 6)$ . En forma análoga, cada una de las seis permutaciones de  $\{1, 2, 3\}$  puede extenderse de forma única a un automorfismo del grafo, como muestra la misma figura 27.2. Hay exactamente seis automorfismos, que son las permutaciones listadas arriba.

## 27.2. Órbitas y estabilizadores

Sea  $G$  un grupo de permutaciones de un conjunto  $\mathcal{X}$ . Veremos que la estructura del grupo lleva naturalmente a una partición de  $\mathcal{X}$ . Definamos la relación  $\sim$  sobre  $\mathcal{X}$  mediante  $x \sim y$  siempre que para algún  $\gamma \in G$  tenemos  $\gamma(x) = y$ . Verificamos que  $\sim$  es una relación de equivalencia de la forma usual:

**Reflexiva:** Como  $\iota$  es parte de todo grupo, y  $\iota(x) = x$  para todo  $x \in \mathcal{X}$ , tenemos  $x \sim x$ .

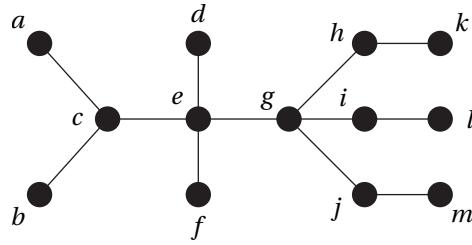
**Simétrica:** Supongamos  $x \sim y$ , o sea  $\gamma(x) = y$  para algún  $\gamma \in G$ . Como  $G$  es un grupo,  $\gamma^{-1} \in G$ , y como  $\gamma^{-1}(y) = x$ , tenemos  $y \sim x$ .

**Transitiva:** Si  $x \sim y$  y  $y \sim z$  debe ser  $\gamma_1(x) = y$  y  $\gamma_2(y) = z$  para  $\gamma_1, \gamma_2 \in G$ , y como  $G$  es un grupo,  $\gamma_2\gamma_1 \in G$ , con lo que  $\gamma_2\gamma_1(x) = z$  y  $x \sim z$ .

Como  $\sim$  es relación de equivalencia, define una partición de  $\mathcal{X}$ ;  $x$  e  $y$  pertenecen a la misma clase si y solo si hay una permutación en  $G$  que transforma  $x$  en  $y$ . A las clases de equivalencia se les conoce como las *órbitas* de  $G$  en  $\mathcal{X}$ . La *órbita de  $x$*  es la clase que contiene a  $x$ :

$$Gx = \{y \in \mathcal{X} : y = \gamma(x) \text{ para algún } \gamma \in G\}$$

Intuitivamente, la órbita  $Gx$  son los elementos de  $\mathcal{X}$  que no se distinguen de  $x$  bajo operaciones de  $G$ . En el caso de la figura 27.2 los conjuntos de vértices  $\{1, 3, 5\}$  y  $\{2, 4, 6\}$  son órbitas del grupo. El grafo de la figura 27.3 tiene un grupo más complejo. Acá los automorfismos se obtienen combinando



$$\begin{array}{lll} \iota & \iota & \iota \\ (a\ b) & (d\ f) & (h\ i)(k\ l) \\ & & (h\ j)(k\ m) \\ & & (i\ j)(l\ m) \\ & & (h\ i\ j)(k\ l\ m) \\ & & (h\ j\ i)(k\ m\ l) \end{array}$$

Figura 27.3 – Un ejemplo de grafo y los generadores de su grupo de automorfismos

las permutaciones de la figura 27.3. Hay un total de  $2 \cdot 2 \cdot 6 = 24$  permutaciones en este grupo. Son órbitas  $\{a, b\}$ ,  $\{c\}$ ,  $\{d, f\}$ ,  $\{e\}$ ,  $\{g\}$ ,  $\{h, i, j\}$ ,  $\{k, l, m\}$ , y se ve que “son parecidos” los elementos de cada una de ellas, en que las operaciones del grupo los intercambian.

Las órbitas presentan un par de problemas numéricos obvios: ¿Cuántas órbitas hay? ¿Qué tamaños tienen?

Si  $G$  es un grupo de permutaciones, llamaremos  $G(x \rightarrow y)$  al conjunto de permutaciones que llevan  $x$  a  $y$ , o sea:

$$G(x \rightarrow y) = \{\gamma \in G : g(x) = y\}$$

En particular,  $G(x \rightarrow x)$  es el conjunto de permutaciones que tienen a  $x$  como punto fijo. Este conjunto se llama el *estabilizador* de  $x$ , y se anota  $G_x$ . Si  $\gamma_1$  y  $\gamma_2$  están en  $G_x$ :

$$\gamma_2\gamma_1(x) = \gamma_2(x) = x$$

por lo que  $\gamma_2\gamma_1 \in G_x$ , y  $G_x$  es un subgrupo de  $G$ . También tenemos:

**Teorema 27.1.** *Sea  $G$  un grupo de permutaciones, y sea  $\gamma \in G(x \rightarrow y)$ . Entonces:*

$$G(x \rightarrow y) = \gamma G_x$$

*el coset izquierdo de  $G_x$  respecto a  $\gamma$ .*

*Demostración.* Demostraremos que todo elemento de  $\gamma G_x$  pertenece a  $G(x \rightarrow y)$  y viceversa, con lo que ambos conjuntos son iguales.

Si  $\alpha$  pertenece a  $\gamma G_x$ , es  $\alpha = \gamma\beta$  para algún  $\beta \in G_x$ . O sea,  $\alpha(x) = \gamma\beta(x) = \gamma(x) = y$ , con lo que  $\alpha$  pertenece a  $G(x \rightarrow y)$ . Por el otro lado, si  $\pi \in G(x \rightarrow y)$ , entonces  $\gamma^{-1}\pi(x) = \gamma^{-1}(y) = x$ , de manera que  $\gamma^{-1}\pi = \delta$ , donde  $\delta \in G_x$ , y así  $\pi = \gamma\delta \in \gamma G_x$ . Ambos conjuntos son iguales.  $\square$

De forma muy similar al teorema 27.1 se demuestra lo siguiente:

**Teorema 27.2.** *Sea  $G$  un grupo de permutaciones de  $\mathcal{X}$ , y sea  $\gamma \in G(x \rightarrow y)$ . Entonces:*

$$G(x \rightarrow y) = G_y\gamma$$

*el coset derecho de  $G_y$  respecto a  $\gamma$ .*

*Demostración.* Si  $\alpha$  pertenece a  $G_y\gamma$ , es  $\alpha = \beta\gamma$  para algún  $\beta \in G_y$ , vale decir  $\alpha(y) = \beta\gamma(y) = \beta(x) = y$  o sea  $\beta \in G(x \rightarrow y)$ . Al revés, supongamos  $\pi \in G(x \rightarrow y)$ , y consideremos  $\pi\gamma^{-1}(y) = \pi(x) = y$  y por tanto  $\pi\gamma^{-1} \in G_y$ , o  $\pi \in G_y\gamma$ , y sigue el resultado.  $\square$

De los anteriores teoremas obtenemos:

**Corolario 27.3.** *Sea  $G$  un grupo de permutaciones de  $\mathcal{X}$ , sea  $x \in \mathcal{X}$  un elemento cualquiera, e  $y$  un elemento en la órbita de  $x$ . Entonces  $|G_x| = |G_y|$ .*

*Demostración.* Inmediato, ya que el tamaño de un coset es el orden del subgrupo (lo demostramos para el teorema de Lagrange); y por los teoremas 27.1 y 27.2 tenemos  $|G_y| = |G(x \rightarrow y)| = |G_x|$ .  $\square$

**Teorema 27.4.** *Sea  $G$  un grupo de permutaciones de  $\mathcal{X}$ , y sea  $x$  un elemento de  $\mathcal{X}$ . Entonces:*

$$|Gx| \cdot |G_x| = |G|$$

*Demostración.* Usamos la idea de contar por filas y columnas. Para un elemento  $x \in \mathcal{X}$  el conjunto de pares  $S_x = \{(\gamma, y) : \gamma(x) = y\}$  puede describirse mediante una tabla como la del cuadro 27.2. Dado

	...	$y$	...	
⋮				
$\gamma$		✓ si $\gamma(x) = y$		$r_\gamma(S_x)$
⋮				
		$c_y(S_x)$		

Cuadro 27.2 – Pares  $(\gamma, y)$  para demostración del teorema 27.4

que  $\gamma$  es una permutación, hay un único  $y$  tal que  $\gamma(x) = y$  para cada  $\gamma$ , con lo que  $r_\gamma(S_x) = 1$ . El total por columna  $c_y(S_x)$  es el número de permutaciones  $\gamma$  tales que  $\gamma(x) = y$ , vale decir  $|G(x \rightarrow y)|$ . Si  $y$  está en la órbita  $Gx$ , por el teorema 27.1 y el hecho que el coset de un subgrupo tiene el tamaño del

subgrupo, tenemos  $|G(x \rightarrow y)| = |G_x|$ . Por otro lado, si  $y$  no está en la órbita  $Gx$ ,  $|G(x \rightarrow y)| = 0$ . Las dos formas de contar los elementos de  $S_x$  dan:

$$\sum_{y \in \mathcal{X}} c_y(S_x) = \sum_{\gamma \in G} r_\gamma(S_x)$$

Al lado izquierdo hay  $|Gx|$  términos que valen  $|G_x|$  cada uno, los demás valen 0; al lado derecho hay  $|G|$  términos que valen 1 cada uno. Así tenemos el resultado prometido.  $\square$

Este teorema permite calcular el tamaño de un grupo si se conoce el tamaño de una órbita y el estabilizador respectivo. Consideremos por ejemplo el grupo  $T$  de rotaciones en el espacio de un tetraedro, ver la figura 27.4. Las rotaciones alrededor del eje marcado son las que mantienen

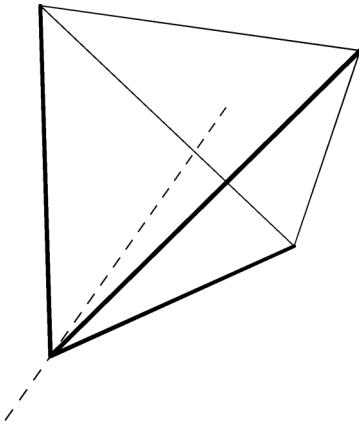


Figura 27.4 – Rotaciones de un tetraedro

fijo el vértice 1, y hay 3 de estas,  $|T_d| = 3$ . Por otro lado, girando el tetraedro en el espacio se puede colocar en la posición 1 cualquiera de los 4 vértices, y tenemos  $|Td| = 4$ . En consecuencia, el grupo de rotaciones en el espacio de un tetraedro es de orden  $|T| = |T_d| \cdot |Td| = 3 \cdot 4 = 12$ . Resulta que  $T$  no es más que el grupo alternante  $A_4$ .

Otro ejemplo lo da el icosaedro truncado, la forma básica de la pelota de fútbol tradicional, ver la figura 27.5. Este es el sólido arquimediano limitado por 12 hexágonos y 20 pentágonos (un total de

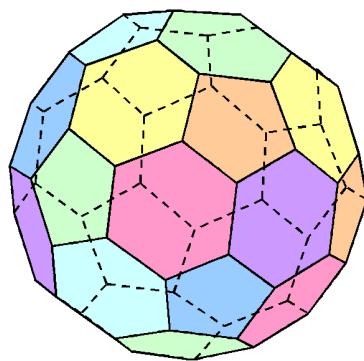


Figura 27.5 – Icosaedro truncado

32 caras), 90 aristas y 60 vértices. Si consideramos rotaciones en el espacio de este sólido, como en

cada vértice confluyen un pentágono y dos hexágonos la única simetría que mantiene fijo un vértice es  $\iota$ . Vía rotaciones podemos hacer coincidir ese vértice con cualquiera, por lo que tenemos que  $|G| = |G_x| \cdot |Gx| = 1 \cdot 60 = 60$ . Obtener el orden de este grupo manipulando el sólido sería mucho más complicado.

### 27.3. Número de órbitas

Vamos ahora a contar el número de órbitas de un grupo  $G$  de permutaciones de  $\mathcal{X}$ . Cada órbita es un subconjunto de elementos indistinguibles bajo las operaciones de  $G$ , y el número de órbitas dice cuántos tipos de elementos distinguibles hay.

Supóngase que se quieren fabricar tarjetas de identidad cuadradas, divididas en nueve cuadrados de los cuales se perforan dos. Véase la figura 27.6 para algunos ejemplos. Las primeras dos no se

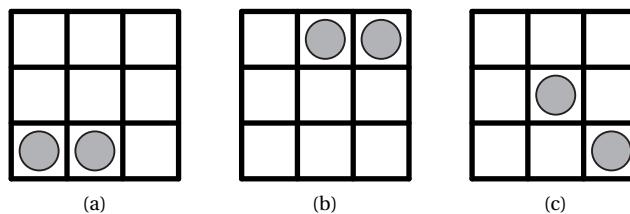


Figura 27.6 – Ejemplos de tarjetas de identidad

pueden distinguir, ya que se obtiene la de la figura 27.6b rotando la de 27.6a; en cambio, la de 27.6c claramente es diferente de las otras, independiente de si se gira o se da vuelta.

El grupo que está actuando acá es el grupo  $D_8$  de ocho simetrías de un cuadrado, pero interesa el efecto que tiene sobre las  $\binom{9}{2} = 36$  configuraciones de dos agujeros en un cuadrado de  $3 \times 3$ , no solo su acción sobre los cuatro vértices. El número de órbitas es el número de tarjetas distinguibles. Hacer esto por la vía de dibujar las 36 configuraciones, y analizar lo que ocurre con cada una de ellas con las 8 simetrías es bastante trabajo. Por suerte hay maneras mejores.

Dado un elemento  $\gamma$  del grupo de permutaciones  $G$  definimos:

$$F(\gamma) = \{x \in \mathcal{X} : \gamma(x) = x\}$$

Vale decir,  $F(\gamma)$  es el número de puntos fijos de  $\gamma$ . Nuestro teorema siguiente relaciona esto con el número de órbitas. Este resultado se conoce bajo el nombre de Burnside, de Cauchy-Frobenius y de Pólya. Burnside lo popularizó en su libro [59], atribuyéndolo a Frobenius, aunque el resultado lo conocía Cauchy antes. Por esta enredada historia a veces se le llama “el lema que no es de Burnside”.

**Teorema 27.5** (Lema de Burnside). *El número de órbitas de  $G$  sobre  $\mathcal{X}$  está dado por:*

$$\frac{1}{|G|} \sum_{\gamma \in G} |F(\gamma)|$$

*Demostración.* Nuevamente, contar por filas y columnas. Sea:

$$E = \{(\gamma, x) : \gamma(x) = x\}$$

Entonces el total por fila  $r_\gamma(E)$  es el número de  $x$  fijados por  $\gamma$ , o sea  $|F(\gamma)|$ . El total por columna  $c_x(E)$  es el número de  $\gamma$  que tienen  $x$  como punto fijo,  $|G_x|$ . Contabilizando  $E$  de ambas formas da:

$$\sum_{\gamma \in G} |F(\gamma)| = \sum_{x \in \mathcal{X}} |G_x|$$

Supongamos que hay  $t$  órbitas, y elijamos  $z \in \mathcal{X}$ . Por el teorema 27.2, si  $x$  pertenece a la órbita  $Gz$  entonces  $|G_x| = |G_z|$ . Cada órbita contribuye al lado derecho  $|Gz|$  términos, todos  $|G_z|$ ; la contribución total de la órbita es  $|Gz| \cdot |G_z| = |G|$  por el teorema 27.4, lo que lleva a:

$$\sum_{\gamma \in G} |F(\gamma)| = t \cdot |G|$$

que es equivalente a lo que queríamos demostrar.  $\square$

Ahora podemos resolver nuestro problema de tarjetas de identidad. Necesitamos calcular el número de configuraciones fijas bajo cada una de las ocho permutaciones. Por ejemplo, cuando  $\gamma$  es la rotación en  $\pi$ , hay cuatro configuraciones fijas (ver la figura 27.7). No hay configuraciones fijas bajo rotaciones de  $\pi/2$  ni de  $3\pi/2$ . Podemos de la misma forma enumerar las configuraciones fijas bajo

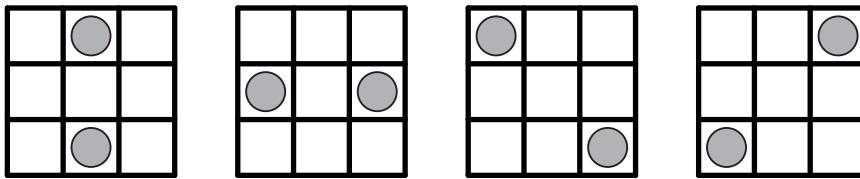


Figura 27.7 – Configuraciones fijas bajo rotación en  $\pi$

una reflexión en la vertical, ver la figura 27.8. Para la reflexión en la horizontal por simetría también tenemos seis configuraciones fijas. Al enumerar las configuraciones fijas bajo una reflexión en la

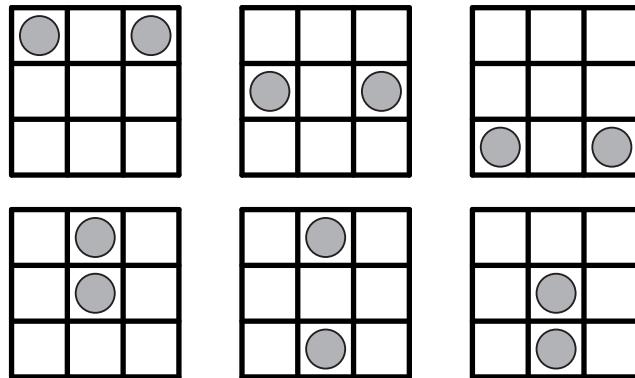


Figura 27.8 – Configuraciones fijas bajo reflexión en la vertical

diagonal de la esquina inferior izquierda a la superior derecha también resultan seis configuraciones (figura 27.9), y obtenemos otras seis para la reflexión en la otra diagonal. El cuadro 27.3 resume los valores anteriores. Con estos valores tenemos el lema de Burnside que el número de órbitas es:

$$\frac{1}{8} (36 + 0 + 4 + 0 + 6 + 6 + 6 + 6) = 8$$

En este caso es sencillo listar las ocho configuraciones por prueba y error, máxime sabiendo que son ocho (ver la figura 27.10), pero el resultado es aplicable en forma mucho más general.

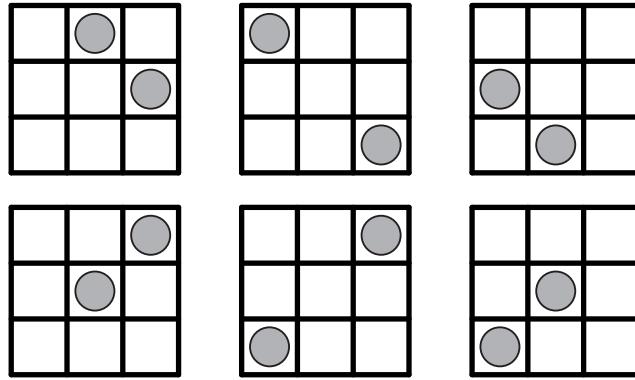


Figura 27.9 – Configuraciones fijas bajo reflexión en la diagonal de izquierda inferior a derecha superior

Operación	Fijos
Identidad	36
Rotación en $\pi/2$	0
Rotación en $\pi$	4
Rotación en $3\pi/2$	0
Reflexión en diagonal 1 3	6
Reflexión en diagonal 2 4	6
Reflexión en perpendicular a 1 2	6
Reflexión en perpendicular a 1 4	6

Cuadro 27.3 – Número de configuraciones de tarjetas respetadas por cada simetría del cuadrado

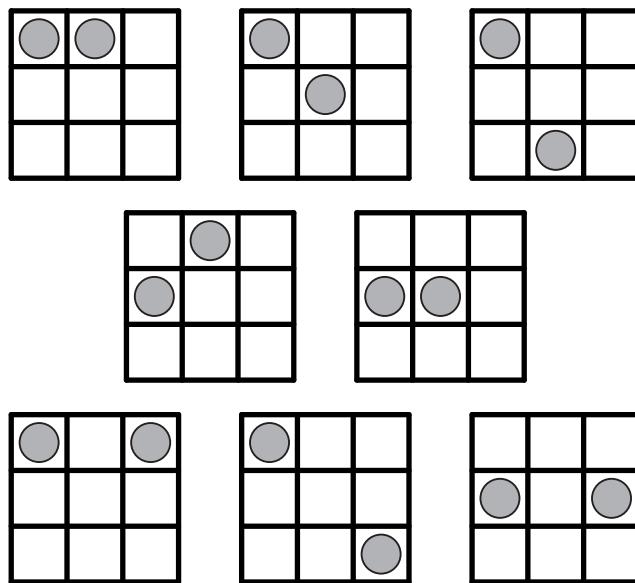


Figura 27.10 – Las ocho tarjetas distinguibles

## 27.4. Índice de ciclos

Definimos el tipo de una permutación como  $[1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}]$  si tiene  $\alpha_k$  ciclos de largo  $k$  para  $1 \leq k \leq n$ . Una expresión afín asociada a la permutación  $\gamma$  es:

$$\zeta_\gamma(x_1, x_2, \dots, x_n) = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$$

Para un grupo  $G$  de permutaciones definimos el *índice de ciclos*:

$$\zeta_G(x_1, x_2, \dots, x_n) = \frac{1}{|G|} \sum_{\gamma \in G} \zeta_\gamma(x_1, x_2, \dots, x_n)$$

Esto es esencialmente una función generatriz en la que  $x_l$  marca los ciclos de largo  $l$ . Esta función tiene muchos usos, algunos los veremos más adelante.

Interesa calcular el índice de ciclos para diversos grupos de manera de tenerlos a mano más adelante. Consideremos primero los grupos  $C_n$ , que sabemos isomorfos con  $\mathbb{Z}_n$  y la suma. Si consideramos  $a \in \mathbb{Z}_n$ , su orden determina el largo de los ciclos, y el número de ciclos es simplemente  $n/\text{ord}(a)$ . El orden es el mínimo  $b > 0$  tal que  $a \cdot b \equiv 0 \pmod{n}$ . Si  $\gcd(a, n) = 1$ , es  $b = n$  y hay  $\phi(n)$  de tales  $a$  que dan  $n/n = 1$  ciclo de largo  $n$ . En general, si  $\gcd(a, n) = c$ , las posibilidades de  $a$  esencialmente diferentes se restringen a  $n/c$  elementos, y de estos dan orden  $n/c$  exactamente los que tienen  $\gcd(a, n/c) = 1$ . Expresarlo de esta forma es incómodo, llamemos  $d = n/c$ . Entonces para  $d | n$  hay  $\phi(d)$  elementos de orden  $d$ , los cuales forman  $n/d$  ciclos de largo  $d$ :

$$\zeta_{C_n}(x_1, \dots, x_n) = \frac{1}{n} \sum_{d|n} \phi(d) x_d^{n/d}$$

Veamos ahora el caso  $D_{2n}$ . A las simetrías anteriores se añaden  $n$  reflexiones. Si  $n$  es par, hay  $n/2$  reflexiones a través de vértices opuestos, son 2 ciclos de largo 1 y  $n - 2$  ciclos de largo 2 que aportan  $nx_1^2 x_2^{(n-2)/2}/2$ ; y  $n/2$  reflexiones a través de lados opuestos, son  $n/2$  ciclos de largo 2 que aportan  $nx_2^{n/2}/2$ . Si  $n$  es impar, hay  $n$  reflexiones a través de un vértice y el lado opuesto, o sea un ciclo de largo 1 y  $(n-1)/2$  ciclos de largo 2, que aportan  $nx_1 x_2^{(n-1)/2}$ . En resumen, como en el índice de ciclos aparecen divididos por el orden del grupo, que se duplica a  $2n$  entre  $C_n$  y  $D_{2n}$ :

$$\zeta_{D_{2n}} = \frac{1}{2} \zeta_{C_n}(x_1, \dots, x_n) + \begin{cases} \frac{1}{4} (x_1^2 x_2^{(n-2)/2} + x_2^{n/2}) & \text{si } n \text{ es par} \\ \frac{1}{2} x_1 x_2^{(n-1)/2} & \text{si } n \text{ es impar} \end{cases}$$

Así tenemos por ejemplo para el cuadrado:

$$\begin{aligned} \zeta_{C_4}(x_1, x_2, x_3, x_4) &= \frac{1}{4} \sum_{d|4} \phi(d) x_d^{4/d} \\ &= \frac{1}{4} (x_1^4 + x_2^2 + 2x_4) \\ \zeta_{D_8}(x_1, x_2, x_3, x_4) &= \frac{1}{2} \zeta_{C_4}(x_1, x_2, x_3, x_4) + \frac{1}{4} (x_1^2 x_2 + x_2^2) \\ &= \frac{1}{8} (x_1^4 + 2x_1^2 x_2 + 3x_2^2 + 2x_4) \end{aligned}$$

## 27.5. Número de colores distinguibles

Supongamos un grupo  $G$  de permutaciones de un conjunto  $\mathcal{X}$  de  $n$  elementos, y a cada elemento se le puede asignar uno de  $r$  colores. Si el conjunto de colores es  $\mathcal{K}$ , un *colorido* es una función

$\omega: \mathcal{X} \rightarrow \mathcal{K}$ . El número total de colores es  $r^n$ , a este conjunto le llamaremos  $\Omega$ . Ahora bien, cada permutación  $g$  en  $G$  induce una permutación  $\hat{g}$  de  $\Omega$ : Para  $\omega$  definimos  $\hat{g}(\omega)$  como el color en el cual el color asignado a  $x$  es el que  $\omega$  asigna a  $g(x)$ , vale decir:

$$(\hat{g}(\omega))(x) = \omega g^{-1}(x)$$

La inversa aparece porque al aplicar la permutación al color estamos asignando a  $x$  el color que tiene su predecesor vía  $g$ . La figura 27.11 muestra un ejemplo. La función que lleva  $g$  a  $\hat{g}$  es una

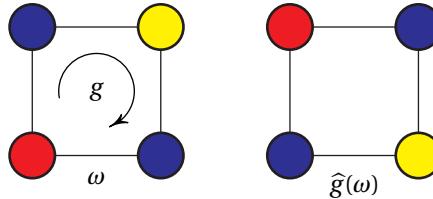


Figura 27.11 – Efecto de la permutación  $\hat{g}$  sobre un color  $\omega$

representación del grupo  $G$  en un grupo  $\hat{G}$  de permutaciones de  $\Omega$ . Dos colores son indistinguibles si uno puede transformarse en el otro mediante una permutación  $\hat{g}$ ; vale decir, si ambas pertenecen a la misma órbita de  $\hat{G}$  en  $\Omega$ . El número de colores distinguibles (*inequivalentes*) entonces es el número de órbitas de  $\hat{G}$ . Antes de aplicar nuestro teorema para el número de órbitas debemos relacionar  $G$  y  $\hat{G}$ . Supongamos que para dos permutaciones  $g_1$  y  $g_2$  tenemos  $\hat{g}_1 = \hat{g}_2$ , de forma que

$$(\hat{g}_1(\omega))(x) = (\hat{g}_2(\omega))(x)$$

y en consecuencia para todo  $\omega \in \Omega$  y todo  $x \in \mathcal{X}$  debe ser

$$\omega(g_1^{-1}(x)) = \omega(g_2^{-1}(x))$$

Como esto es válido para todo  $\omega$ , en particular vale para el color que asigna el color especificado a  $g_1^{-1}(x)$  y otro color a todos los demás miembros de  $\mathcal{X}$ . En este caso particular la ecuación dice que  $g_1^{-1}(x) = g_2^{-1}(x)$ , con lo que  $g_1 = g_2$ , y el grupo de permutaciones  $G$  de  $\mathcal{X}$  y el grupo de permutaciones  $\hat{G}$  de los colores  $\Omega$  son isomorfos.

Otra manera de entender esta situación es considerar un color que le asigna un color diferente a cada elemento de  $\mathcal{X}$ . Una permutación de ese color no es más que una permutación de nuevos “nombres” de los elementos de  $\mathcal{X}$ , con lo que está claro que ambos grupos de permutaciones están muy relacionados.

**Teorema 27.6.** Si  $G$  es un grupo de permutaciones de  $\mathcal{X}$ , y  $\zeta_G(x_1, \dots, x_n)$  es su índice de ciclos, el número de colores inequivalentes de  $\mathcal{X}$  con  $r$  colores es  $\zeta_G(r, \dots, r)$ , donde un color de  $\mathcal{X}$  es una función  $\omega: \mathcal{X} \rightarrow \mathcal{K}$ .

*Demostración.* Interesa el número de órbitas del grupo  $G$  operando sobre colores. Hemos demostrado que la representación  $g \rightarrow \hat{g}$  es una biyección, de forma que  $|G| = |\hat{G}|$ . Además, por el teorema de Burnside el número de órbitas de  $\hat{G}$  en  $\Omega$  es

$$\frac{1}{|\hat{G}|} \sum_{\hat{g} \in \hat{G}} |F(\hat{g})| = \frac{1}{|G|} \sum_{g \in G} |F(\hat{g})|$$

donde  $F(\hat{g})$  es el conjunto de colores fijados por  $\hat{g}$ . Supongamos ahora que  $\omega$  es un color fijo por  $\hat{g}$ , de forma que  $\hat{g}(\omega) = \omega$ , y sea  $(x \ y \ z \ \dots)$  un ciclo cualquiera de  $g$ . Tenemos:

$$\omega(x) = \omega(g(y)) = (\hat{g}(\omega))(y) = \omega(y)$$

de forma que  $\omega$  asigna el mismo color a  $x$  e  $y$ . Aplicando el mismo razonamiento, este es el color asignado a todo el ciclo. Esto ocurre con cada uno de los ciclos de  $g$ . Si  $g$  tiene  $k$  ciclos en total, el número de colores posibles es  $r^k$ , ya que podemos asignar independientemente cualquiera de los  $r$  colores a cada uno de los  $k$  ciclos. De esta forma, si  $g$  tiene  $\alpha_i$  ciclos de largo  $i$  para  $(1 \leq i \leq n)$ , tenemos  $\alpha_1 + \alpha_2 + \dots + \alpha_n = k$  y

$$|F(\hat{g})| = r^k = r^{\alpha_1 + \alpha_2 + \dots + \alpha_n} = \zeta_g(r, r, \dots, r)$$

y el resultado sigue de sumar esto.  $\square$

**Ejemplo 27.1.** Una tribu de hippies artesanos fabrica pulseras formadas alternadamente por tres arcos y tres cuentas, y tienen arcos y cuentas de cinco colores. Para efectos de simetría pueden considerarse las pulseras como triángulos equiláteros en los cuales se colorean los vértices y las aristas. Por razones que solo ellos entienden las pulseras deben siempre usar tres colores. Interesa saber cuántas pulseras diferentes pueden crear.

Esta es una aplicación típica del principio de inclusión y exclusión (capítulo 15), el teorema 27.6 da el número de colores con *a lo más* el número de colores dado, pero nos interesan los colores con *exactamente* tres colores.

Operación	Nº	Término
Identidad	1	$x_1^6$
Rotaciones (en $2\pi/3$ y $4\pi/3$ )	2	$x_3^2$
Reflexiones en cada eje	3	$x_1^2 x_2^2$

Cuadro 27.4 – Elementos del grupo para pulseras

El cuadro 27.4 da los elementos del grupo relevante. Este grupo es de orden 6, así que su índice de ciclos es:

$$\zeta_G(x_1, x_2, x_3, x_4, x_5, x_6) = \frac{1}{6} (x_1^6 + 3x_1^2 x_2^2 + 2x_3^2)$$

Luego aplicamos nuestra receta del principio de inclusión y exclusión.

1. El universo  $\Omega$  es el conjunto de colores con 5 colores. Un coloro tiene la propiedad  $i$  si el color  $i$  no está presente, e interesa el número de los que tienen exactamente 2 propiedades (están presentes los otros 3 colores).
2. Acá  $N(\supseteq S)$  es el número de colores que no consideran los colores en  $S$ , vale decir son colores tomando a lo más  $5 - |S|$  colores. Por el teorema 27.6:

$$N(\supseteq S) = \zeta_G(5 - |S|, 5 - |S|)$$

3. Como los  $r$  colores a excluir se eligen de entre los 5, y en el número de posibilidades solo influye el número de colores restantes con los que se colorean:

$$N_r = \binom{5}{r} \zeta_G(5 - r, 5 - r)$$

En este caso tenemos:

$$N_0 = \binom{5}{0} \zeta_G(5, 5, 5, 5, 5, 5) = 2925$$

$$N_1 = \binom{5}{1} \zeta_G(4, 4, 4, 4, 4, 4) = 4080$$

$$N_2 = \binom{5}{2} \zeta_G(3, 3, 3, 3, 3, 3) = 1650$$

$$N_3 = \binom{5}{3} \zeta_G(2, 2, 2, 2, 2, 2) = 200$$

$$N_4 = \binom{5}{2} \zeta_G(1, 1, 1, 1, 1, 1) = 5$$

$$N_5 = \binom{5}{5} \zeta_G(0, 0, 0, 0, 0, 0) = 0$$

La función generatriz es

$$N(z) = 5z^4 + 200z^3 + 1650z^2 + 4080z + 2925$$

4. Nos interesa  $e_2$ , que se obtiene de la función generatriz de los  $e_t$ , que es  $E(z) = N(z - 1)$ :

$$E(z) = 5z^4 + 180z^3 + 1080z^2 + 1360z + 300$$

Se pueden formar 1080 brazaletes de tres colores.

Pero podemos hacer algo más. Si hay  $r$  colores, podemos definir variables  $z_i$  para  $1 \leq i \leq r$  representando los distintos colores. Entonces la función generatriz de los números de nodos de cada color que se pueden asignar a un ciclo de largo  $k$  es simplemente:

$$z_1^k + z_2^k + \cdots + z_r^k$$

ya que serían  $k$  nodos, todos del mismo color. Si hay  $\alpha_k$  ciclos de largo  $k$ , entonces corresponde el factor:

$$(z_1^k + z_2^k + \cdots + z_r^k)^{\alpha_k}$$

La anterior discusión demuestra el siguiente resultado.

**Teorema 27.7** (Enumeración de Pólya). *Sea  $G$  un grupo de permutaciones de  $\mathcal{X}$ , y  $\zeta_G(x_1, \dots, x_n)$  su índice de ciclos. La función generatriz del número de colores inequivalentes de  $\mathcal{X}$  en que hay  $n_i$  nodos de color  $i$  para  $1 \leq i \leq r$ , llamémosle  $u_{n_1, n_2, \dots, n_r}$ , es:*

$$\begin{aligned} U(z_1, z_2, \dots, z_r) &= \sum_{n_1, n_2, \dots, n_r} u_{n_1, n_2, \dots, n_r} z_1^{n_1} z_2^{n_2} \cdots z_r^{n_r} \\ &= \zeta_G(z_1 + z_2 + \cdots + z_r, z_1^2 + z_2^2 + \cdots + z_r^2, \dots, z_1^n + z_2^n + \cdots + z_r^n) \end{aligned}$$

Volviendo a nuestro ejemplo de las tarjetas de identidad, el grupo subyacente es  $D_8$ , las operaciones y sus tipos (operando sobre los nueve cuadraditos) se resumen en el cuadro 27.5. El índice de ciclos del grupo que interesa es:

$$\zeta_t(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9) = \frac{1}{8} (x_1^9 + 2x_1x_4^2 + x_1x_2^4 + 4x_1^3x_2^3)$$

Operación	Nº	Término
Identidad	1	$x_1^9$
Giro en $\pi/2, 3\pi/2$	2	$x_1 x_4^2$
Giro en $\pi$	1	$x_1 x_2^4$
Reflexión horizontal, vertical	2	$x_1^3 x_2^3$
Reflexión diagonal	2	$x_1^3 x_2^3$

Cuadro 27.5 – Las operaciones sobre tarjetas y sus tipos

El número total de tarjetas distinguibles con dos colores (agujero o no) en cada cuadradito es:

$$\zeta_t(2, 2, 2, 2, 2, 2, 2, 2) = 102$$

Para obtener el número de tarjetas con dos agujeros calculamos:

$$[z^2] \zeta_t(1+z, 1+z^2, 1+z^3, 1+z^4, 1+z^5, 1+z^6, 1+z^7, 1+z^8, 1+z^9) = 8$$

Esto ya lo habíamos calculado antes, aunque de forma más trabajosa. Queda de ejercicio calcular el número de collares diferentes que se pueden crear de 16 cuentas con 3 negras de la misma forma.

La teoría de enumeración de Pólya fue desarrollada en parte para aplicación a la química. Algunos ejemplos de fórmulas químicas se dan en la figura 27.12. Este tipo de compuestos, derivados del

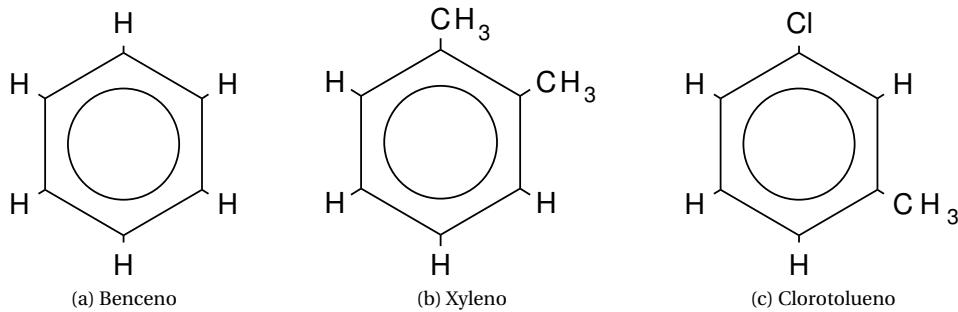


Figura 27.12 – Algunos compuestos aromáticos

benceno (figura 27.12a) son hexágonos que pueden girar en el espacio. Hay muchas posibilidades de grupos de átomos que pueden reemplazar los hidrógenos (H), como es radicales metilo ( $\text{CH}_3$ ) o átomos de cloro (Cl). Una pregunta obvia entonces es cuántos compuestos distintos pueden crearse con un conjunto de radicales, o cuántos son posibles con un número particular de cada uno de un conjunto de radicales dados. Por ejemplo, hay tres isómeros del xileno (un anillo de benceno en el cual dos de los hidrógenos se substituyen por metilos), como muestra la figura 27.13.

El grupo de simetría relevante es  $D_{12}$ , cuyo índice de ciclos podemos calcular como antes:

$$\begin{aligned} \zeta_{C_6}(x_1, x_2, x_3, x_4, x_5, x_6) &= \frac{1}{6} \sum_{d|6} \phi(d) x_d^{6/d} \\ &= \frac{1}{6} (x_1^6 + x_2^3 + 2x_3^2 + 2x_6) \\ \zeta_{D_{12}}(x_1, x_2, x_3, x_4, x_5, x_6) &= \frac{1}{2} \zeta_{C_6}(x_1, x_2, x_3, x_4, x_5, x_6) + \frac{1}{4} (x_1^2 x_2^2 + x_2^3) \\ &= \frac{1}{12} (x_1^6 + 3x_1^2 x_2^2 + 4x_2^3 + 2x_3^2 + 2x_6) \end{aligned}$$

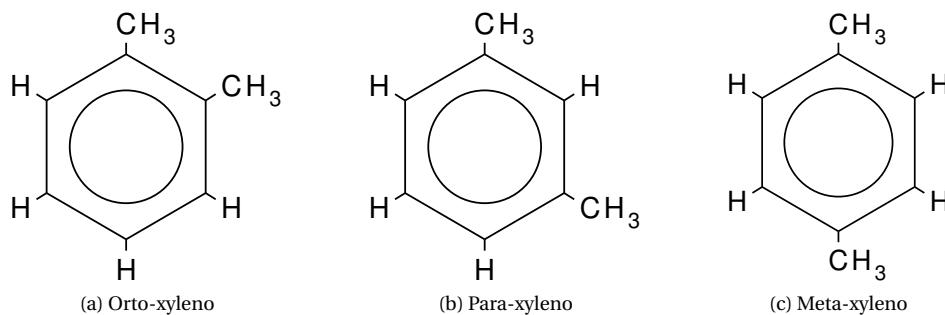


Figura 27.13 – Los tres isómeros del xileno

Hecho el trabajo duro, determinar cuántos compuestos pueden crearse con radicales hidrógeno (H) y metilo ( $\text{CH}_3$ ) es fácil: Es colorear los vértices con dos colores, lo que da:

$$\zeta_{D_{12}}(2, 2, 2, 2, 2, 2) = \frac{1}{12} (2^6 + 3 \cdot 2^2 \cdot 2^2 + 4 \cdot 2^3 + 2 \cdot 2) \\ = 13$$

Para comprobar cuántos isómeros del xileno hay, consideraremos coloreo de los vértices del hexágono con dos colores (hidrógenos y metilos), y de los últimos hay exactamente dos. Si consideramos que  $z$  marca metilo, la función generatriz que corresponde a un ciclo de largo  $l$  es simplemente  $1 + z^l$  (hay 1 forma de tener 0 metilos en él, lo que aporta  $1 \cdot z^0$ , y 1 forma de tener  $l$  metilo, lo que aporta  $1 \cdot z^l$ ), y al substituir  $x_l = 1 + z^l$  obtenemos:

$$\zeta_{D_{12}}(1+z, 1+z^2, 1+z^3, 1+z^4, 1+z^5, 1+z^6) = z^6 + z^5 + 3z^4 + 3z^3 + 3z^2 + z + 1$$

Esto confirma que hay tres isómeros en su coeficiente de  $z^2$ .

Si interesa determinar cuántos compuestos distintos tienen 2 radicales cloro ( $\text{Cl}$ ), 2 metilos ( $\text{CH}_3$ ) y 2 hidrógenos ( $\text{H}$ ), usamos las variables  $u$ ,  $v$  y  $w$  para estas tres opciones, y el valor buscado es simplemente:

$$\left[ u^2 v^2 w^2 \right] \zeta_{\mathbb{D}_6}(u+v+w, u^2+v^2+w^2, \dots, u^6+v^6+w^6) = 11$$

Por otro lado, un átomo de carbono puede unirse con cuatro otros átomos, dispuestos en los vértices de un tetraedro. Las operaciones de simetría de un tetraedro en el espacio (solo rotaciones, no reflexiones) son giros alrededor de un eje que pasa por un vértice y el centroide de la cara opuesta (ver la figura 27.14a) y giros alrededor de un eje que pasa por el punto medio de una arista y el punto medio de la arista opuesta (ver la figura 27.14b). Las simetrías son de los tipos dados en el

Operación	Ciclos	Tipo	Nº	Término
Identidad	(1)(2)(3)(4)	[1 <sup>4</sup> ]	1	$x_1^4$
Giro en vértice 4 en 1/3	(1 2 3)(4)	[1 3 <sup>1</sup> ]	4	$x_1^3 x_3$
Giro en vértice 4 en 2/3	(1 3 2)(4)	[1 3 <sup>1</sup> ]	4	$x_1^3 x_3$
Giro en arista 1 2 en 1/2	(1 2)(3 4)	[2 <sup>2</sup> ]	3	$x_2^2$

#### Cuadro 27.6 – Rotaciones de un tetraedro

cuadro 27.6 (resulta que esto no es más que el grupo alternante  $A_4$ ), y en consecuencia el índice de

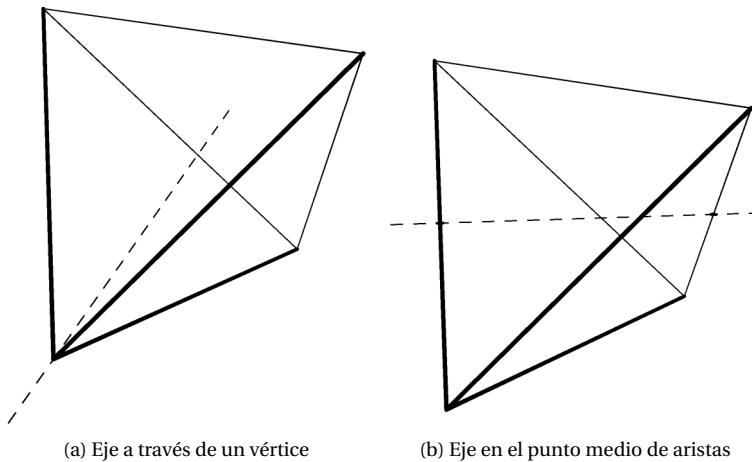


Figura 27.14 – Operaciones de simetría (rotaciones) de un tetraedro

ciclos del grupo es

$$\zeta_{A_4}(x_1, x_2, x_3, x_4) = \frac{1}{12}(x_1^4 + 8x_1x_3 + 3x_2^2)$$

Así, para dos radicales diferentes hay  $\zeta_{A_4}(2,2,2,2) = 5$  compuestos posibles, y para cuatro radicales hay  $\zeta_{A_4}(4,4,4,4) = 36$ . Si hay dos tipos de radicales, la función generatriz es:

$$\zeta_{A_4}(u+v, u^2+v^2, u^3+v^3, u^4+v^4) = u^4 + u^3v + u^2v^2 + uv^3 + v^4$$

Vale decir, hay un solo compuesto de cada una de las cinco composiciones posibles.

Considere árboles binarios completos de altura 2, como en la figura 27.15, que se consideran

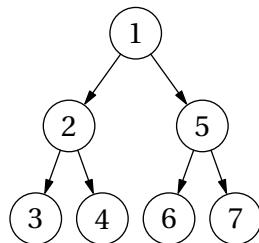


Figura 27.15 – Un árbol binario completo

iguales al intercambiar izquierda y derecha (como 3 con 4; pero también 2 con 5, que lleva consigo intercambiar 3 con 6 y 4 con 7). Interesa determinar cuántos árboles hay con 3 nodos azules, si los nodos se pintan de azul, rojo y amarillo.

Antes de entrar en el tema, es útil obtener información sobre el grupo. Para determinar el orden del grupo, tomamos algún elemento y analizamos su órbita y estabilizador. Tomando 3, su órbita es  $G_3 = \{3, 4, 6, 7\}$ , mientras su estabilizador es  $G_3 = \{i, (6\ 7)\}$ , con lo que  $|G| = |G_3| \cdot |G_3| = 4 \cdot 2 = 8$ . Los elementos del grupo los da el cuadro 27.7, el índice de ciclos del grupo resulta ser:

$$\zeta_G(x_1, x_2, x_3, x_4, x_5, x_6, x_7) = \frac{1}{8} (x_1^7 + 2x_1^5 x_2 + x_1^3 x_2^2 + 2x_1 x_2^3 + x_1 x_2 x_4)$$

Operación	Término
Identidad	$x_1^7$
(3 4)	$x_1^5 x_2$
(6 7)	$x_1^5 x_2$
(3 4)(6 7)	$x_1^3 x_2^2$
(2 5)(3 6)(4 7)	$x_1 x_2^3$
(2 5)(3 7)(4 6)	$x_1 x_2^3$
(2 5)(3 6 4 7)	$x_1 x_2 x_4$
(2 5)(3 7 4 6)	$x_1 x_2 x_4$

Cuadro 27.7 – El grupo de operaciones del árbol

La manera más simple de obtener el resultado buscado es reconocer que la función generatriz para el número de maneras de formar órbitas de  $l$  nodos donde  $u$  marca el número de nodos azules es simplemente  $2 + u^l$  (dos formas de ningún azul, vale decir solo rojos o solo amarillos; y una forma de  $l$  azules), y para aplicar el teorema de Pólya interesa:

$$\begin{aligned} [u^3] \zeta_G(2 + u, 2 + u^2, 2 + u^3, 2 + u^4, 2 + u^5, 2 + u^6, 2 + u^7) \\ = [u^3](u^7 + 6u^6 + 25u^5 + 68u^4 + 120u^3 + 146u^2 + 105u + 42) \\ = 120 \end{aligned}$$

Obtener esto por prueba y error sería impensable. Nuevamente agradecemos el apoyo algebraico de [maxima](#) [251].

Un dado es un cubo, cuyas caras están numeradas de 1 a 6. Interesa saber de cuántas maneras distintas se pueden distribuir los seis números sobre las caras. En este caso, interesan las simetrías rotacionales del cubo en el espacio (las reflexiones corresponden a operaciones imposibles con un sólido). Primeramente calculamos el orden del grupo que nos interesa, que resulta ser el grupo de rotaciones en el espacio de un octaedro y se denomina  $\mathbb{O}$ . Sabemos que  $|\mathbb{O}| = |\mathbb{O}_x| \cdot |\mathbb{O}_x|$ . Si fijamos una de las caras del cubo, hay 4 operaciones que la mantienen fija (rotaciones alrededor del centroide de esa cara en múltiplos de  $\pi/2$ ), y esta cara puede ocupar cualquiera de las 6 posiciones. Luego  $|\mathbb{O}| = 4 \cdot 6 = 24$ . Las operaciones y sus tipos las resume el cuadro 27.8. El índice de ciclos del grupo  $\mathbb{O}$

Operación	Nº	Término
Identidad	1	$x_1^6$
Giro alrededor de centro de una cara en $\pi/2$	3	$x_1^2 x_4$
Giro alrededor de centro de una cara en $\pi$	3	$x_1^2 x_2^2$
Giro alrededor de centro de una cara en $3\pi/2$	3	$x_1^2 x_4$
Giro alrededor del punto medio de una arista en $\pi$	6	$x_2^3$
Giro alrededor de un vértice en $2\pi/3$	4	$x_3^2$
Giro alrededor de un vértice en $4\pi/3$	4	$x_3^2$

Cuadro 27.8 – Operaciones de simetría rotacional de caras de un cubo

es

$$\zeta_{\mathbb{O}}(x_1, x_2, x_3, x_4, x_5, x_6) = \frac{1}{24} (x_1^6 + 6x_1^2 x_4 + 3x_1^2 x_2^2 + 6x_2^3 + 8x_3^2)$$

Como interesa saber de cuántas maneras se pueden distribuir los 6 números sobre las 6 caras:

$$[z_1 z_2 z_3 z_4 z_5 z_6] \zeta_{\mathbb{O}}(z_1 + \dots + z_6, z_1^2 + \dots + z_6^2, z_1^3 + \dots + z_6^3, z_1^4 + \dots + z_6^4, z_1^5 + \dots + z_6^5, z_1^6 + \dots + z_6^6)$$

Siquiera encontrar el término que interesa en esta expresión ya es toda una tarea. Pero si observamos que la única forma de obtener términos en los que los  $z_i$  entran en la primera potencia vienen de aquellos términos en que solo participa  $x_1$ , nuestro problema se reduce a calcular:

$$[z_1 z_2 z_3 z_4 z_5 z_6] \frac{1}{24} (z_1 + z_2 + z_3 + z_4 + z_5 + z_6)^6 = \frac{1}{24} \begin{pmatrix} 6 \\ 1 1 1 1 1 1 \end{pmatrix} = 30$$

Si nos interesa contar el número de maneras de numerar las caras del dado respetando la restricción que caras opuestas sumen 7, la situación relevante es considerar las tres caras numeradas 1, 2 y 3. Estas caras serán adyacentes, y por tanto la situación es la que indica la figura 27.16, que

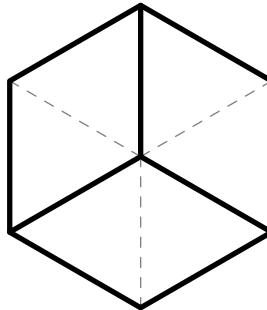


Figura 27.16 – Un cubo visto desde un vértice

muestra las tres caras vistas desde un vértice. Está claro que la simetría es  $C_3$ , un triángulo equilátero rotando en el plano (consideraremos los vértices del triángulo como las caras a ser numeradas). Para este grupo el índice de ciclos es:

$$\zeta_{C_3}(x_1, x_2, x_3) = \frac{1}{3} (x_1^3 + 2x_3)$$

Nos interesa colorear con tres colores, y que cada uno aparezca exactamente una vez, por Pólya:

$$[z_1 z_2 z_3] \zeta_{C_3}(z_1 + z_2 + z_3, z_1^2 + z_2^2 + z_3^2, z_1^3 + z_2^3 + z_3^3)$$

El único término en que entran los  $z_i$  en la primera potencia es el término de la identidad, y en él nos interesa cada uno en la primera potencia:

$$\begin{aligned} [z_1 z_2 z_3] \zeta_{C_3}(z_1 + z_2 + z_3, z_1^2 + z_2^2 + z_3^2, z_1^3 + z_2^3 + z_3^3) &= \frac{1}{3} [z_1 z_2 z_3] (z_1 + z_2 + z_3)^3 \\ &= \frac{1}{3} \begin{pmatrix} 3 \\ 1 1 1 \end{pmatrix} \\ &= 2 \end{aligned}$$

Hay dos maneras diferentes de numerar las caras de un cubo con los números uno a seis tal que caras opuestas sumen siete.



## 28 Introducción al análisis complejo

---

Nahin [263] narra la larga y variada historia de los números complejos. En forma similar al análisis con los reales se puede desarrollar análisis en el ámbito complejo. Muchos resultados son simples de obtener para los complejos, y algunos fenómenos misteriosos en el análisis real se explican al observar desde esta óptica. La teoría tiene su propio encanto.

Algunas de nuestras maniobras son en extremo engorrosas usando solo las técnicas del análisis real. Daremos acá los resultados más importantes del análisis complejo, que ayuda enormemente al simplificar integrales definidas y sumas. Entrega además herramientas útiles para construir aproximaciones asintóticas a muchos valores de interés. Textos introductorios más completos son por ejemplo los de Ash y Novinger [22], Beck, Marchesi, Pixton y Sabalka [30], Cain [61] y Chen [72]. Una visión detallada y bastante completa dan Stein y Shakarchi [337].

### 28.1. Aritmética

Sean  $w = u + iv$  y  $z = x + iy$  complejos (con la *unidad imaginaria*  $i = \sqrt{-1}$  y  $u, v, x, y \in \mathbb{R}$ ). La *parte real* de  $z$  es  $\Re z = x$ , la *parte imaginaria* de  $z$  es  $\Im z = y$ . La suma y multiplicación se calculan como polinomios en  $\mathbb{R}$  en la variable  $i$ , para luego considerar  $i^2 = -1$ . Vale decir:

$$\begin{aligned} w + z &= (u + x) + i(v + y) \\ w \cdot z &= (ux - vy) + i(vx + uy) \end{aligned}$$

Con estas operaciones los números complejos son un campo, que anotamos  $\mathbb{C}$ .

Podemos identificar los complejos con parte imaginaria 0 con los reales, y representar el complejo  $z = x + iy$  por el punto  $(x, y)$  del plano  $\mathbb{R}^2$ . A esta forma de representarlos se le llama *forma rectangular* o *forma cartesiana*. Llamamos *eje real* al eje  $X$  y *eje imaginario* al eje  $Y$ . La suma de complejos es simplemente la suma de los vectores correspondientes. Vea la figura 28.1a.

Como alternativa a dar las coordenadas del vector, podemos describirlo mediante su largo y el ángulo que forma con el eje  $X$ . Para  $z = x + iy$  el *valor absoluto* (también *módulo*)  $r = |z|$  se define como:

$$|z| = \sqrt{x^2 + y^2} \tag{28.1}$$

Un *argumento* de  $z$ , anotado  $\arg z$ , es un número real  $\phi$  tal que

$$x = r \cos \phi \quad y = r \sin \phi \tag{28.2}$$

Nótese que todo número complejo tiene infinitos argumentos. En el caso excepcional  $z = 0$  el módulo es 0 y cualquier ángulo sirve de argumento. En caso  $z \neq 0$  vemos que si  $\phi$  es un argumento de  $z$ , también lo es  $\phi + 2\pi k$ , para todo  $k \in \mathbb{Z}$ . La representación del número complejo como módulo y argumento se conoce como *representación polar*. El *valor principal* del argumento se anota  $\operatorname{Arg} z$ ,

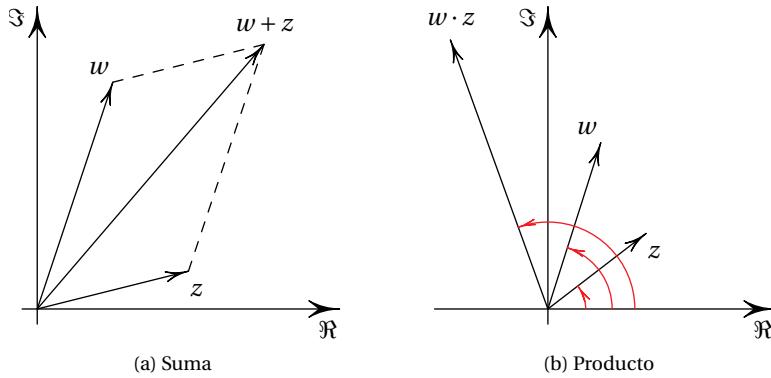


Figura 28.1 – Operaciones entre complejos

es el ángulo restringido al rango  $-\pi < \phi \leq \pi$ . A veces resulta útil restringir el ángulo a otro rango, usaremos  $\arg_\alpha z$  para el ángulo en el rango  $\alpha \leq \arg_\alpha z < \alpha + 2\pi$ .

La representación polar da una bonita interpretación de la multiplicación. Sean números complejos  $z_1 = x_1 + iy_1$  y  $z_2 = x_2 + iy_2$ , respectivamente con módulos  $r_1$  y  $r_2$  y argumentos  $\phi_1$  y  $\phi_2$ . Entonces:

$$\begin{aligned} (x_1 + iy_1) \cdot (x_2 + iy_2) &= (r_1 \cos \phi_1 + ir_1 \sin \phi_1) \cdot (r_2 \cos \phi_2 + ir_2 \sin \phi_2) \\ &= r_1 r_2 ((\cos \phi_1 \cos \phi_2 - \sin \phi_1 \sin \phi_2) + i(\sin \phi_1 \cos \phi_2 + \cos \phi_1 \sin \phi_2)) \\ &= r_1 r_2 (\cos(\phi_1 + \phi_2) + i \sin(\phi_1 + \phi_2)) \end{aligned}$$

Vea la figura 28.1b para un ejemplo.

Deberemos manipular expresiones de la forma  $\cos \phi + i \sin \phi$  con bastante frecuencia, rindiéndonos a la flojera (con la excusa de ahorrar papel, tinta, etc.) escribimos:

$$\exp(i\phi) = e^{i\phi} = \cos \phi + i \sin \phi \quad (28.3)$$

Por ahora (28.3) es simplemente una abreviatura cómoda, más adelante demostraremos que es consistente con la función exponencial del cálculo real. También es común la notación:

$$\text{cis } \phi = \cos \phi + i \sin \phi$$

El siguiente lema recoge algunas propiedades salientes, alentamos al lector interesado demostrarlas.

**Lema 28.1.** Para cualquier  $\phi, \phi_1, \phi_2 \in \mathbb{R}$  y todo  $k \in \mathbb{Z}$ :

- (I)  $|e^{i\phi}| = 1$
- (II)  $e^{i\phi_1} e^{i\phi_2} = e^{i(\phi_1 + \phi_2)}$
- (III)  $1/e^{i\phi} = e^{-i\phi}$
- (IV)  $e^{i(\phi + 2k\pi)} = e^{i\phi}$

Con esta notación, el número complejo de módulo  $r$  y argumento  $\phi$  puede escribirse:

$$x + iy = r e^{i\phi} \quad (28.4)$$

El cuadrado del valor absoluto de  $z$  tiene la bonita propiedad:

$$|z|^2 = x^2 + y^2 = (x + iy) \cdot (x - iy) \quad (28.5)$$

Esto hace útil la operación de *conjugado*:

$$\overline{x + iy} = x - iy \quad (28.6)$$

En el plano cartesiano corresponde a reflejar el vector en el eje  $X$ . Tenemos algunas propiedades, que nuevamente animamos a demostrar.

**Lema 28.2.** *Para todo  $z, z_1, z_2 \in \mathbb{C}$ , y para todo  $\phi \in \mathbb{R}$ :*

- (I)  $\overline{z_1 \pm z_2} = \overline{z_1} \pm \overline{z_2}$
- (II)  $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$
- (III)  $\overline{z_1/z_2} = \overline{z_1}/\overline{z_2}$
- (IV)  $\overline{\overline{z}} = z$
- (V)  $|\overline{z}| = |z|$
- (VI)  $|z|^2 = z\overline{z}$
- (VII)  $\Re z = \frac{1}{2}(z + \overline{z}) \quad \Im z = \frac{1}{2i}(z - \overline{z})$
- (VIII)  $\overline{e^{i\phi}} = e^{-i\phi}$

La parte (VI) del lema 28.2 da una fórmula limpia para el recíproco de un complejo no cero:

$$\frac{1}{z} = \frac{\overline{z}}{|z|^2} \quad (28.7)$$

## 28.2. Un poquito de topología del plano

Al considerar funciones en  $\mathbb{R}$  la situación es bastante simple, basta hablar de intervalos. Incluso en  $\mathbb{R}^n$  el tratamiento puede seguir esencialmente variable a variable y restringirse a intervalos adecuados. En  $\mathbb{C}$  esto no es satisfactorio, áreas del plano pueden tener relaciones mucho más complicadas entre sí que los simples intervalos. Las definiciones siguientes serán usadas con mucha frecuencia en lo que sigue, es importante familiarizarse con ellas.

Requeriremos alguna terminología para tratar con subconjuntos de  $\mathbb{C}$ . Si  $w, z \in \mathbb{C}$ , entonces  $|z - w|$  es la distancia en el plano entre esos puntos. Si fijamos un número complejo  $a$  y un real positivo  $r$ , el conjunto  $|z - a| = r$  es la circunferencia de radio  $r$  alrededor de  $a$ . Al interior del círculo se le llama el *disco abierto* de radio  $r$  alrededor de  $a$ , que anotaremos  $D_r(a)$ . Más precisamente,  $D_r(a) = \{z \in \mathbb{C} : |z - a| < r\}$ . Nótese que esto no incluye la circunferencia.

**Definición 28.1.** Sea  $E$  un subconjunto cualquiera de  $\mathbb{C}$ .

- (I) Un punto  $a$  es un *punto interior* de  $E$  si hay algún disco abierto  $D_r(a)$  que está completamente en  $E$
- (II) Un punto  $b$  es un *punto frontera* de  $E$  si todo disco abierto  $D_r(b)$  contiene un punto de  $E$  y un punto que no pertenece a  $E$ .

- (III) Un punto  $c$  es un *punto de acumulación* de  $E$  si todo disco abierto  $D_r(c)$  contiene un punto de  $E$  diferente de  $c$
- (IV) Un punto  $d$  es un *punto aislado* de  $E$  si pertenece a  $E$  y algún disco abierto  $D_r(d)$  no contiene ningún punto de  $E$  excepto  $d$

En lo anterior  $a$  pertenece a  $E$ , pero  $b$  y  $c$  no necesariamente pertenecen a  $E$ . Desde un punto interior podemos movernos un poco en cualquier dirección sin salir de  $E$ , de un punto frontera moviéndonos un poco quedamos dentro de  $E$ , pero otros movimientos arbitrariamente pequeños nos dejan al exterior. Como el nombre indica, un punto aislado está desconectado del resto del conjunto, hay un entorno de él que no contiene otros puntos del conjunto.

**Definición 28.2.** Un conjunto es *abierto* si todos sus puntos son internos, y es *cerrado* si incluye todos sus puntos frontera.

Como ejemplos, para  $r > 0$  y  $z_0 \in \mathbb{C}$  los conjuntos  $\{z \in \mathbb{C}: |z - z_0| < r\}$ ,  $\{z \in \mathbb{C}: |z - z_0| > r\}$  y  $\{x + iy \in \mathbb{C}: -1 < x < 1\}$  son abiertos. El conjunto  $\{x + iy \in \mathbb{C}: -1 \leq x \leq 1 \wedge -5 \leq y \leq 5\}$  es cerrado. Los conjuntos  $\emptyset$  y  $\mathbb{C}$  son abiertos, pero también son cerrados (no tienen puntos frontera, con lo que vacuamente incluyen sus fronteras). El conjunto  $\{x + iy: 0 \leq x \leq 1 \wedge 0 < y < 1\}$  no es abierto ni cerrado.

**Definición 28.3.** La *frontera* de  $E$ , anotada  $\partial E$ , es el conjunto de los puntos frontera de  $E$ . La *clausura* de  $E$ , anotada  $\bar{E}$ , es el conjunto  $E$  junto con su frontera.

Para el disco abierto  $D_r(z_0) = \{z \in \mathbb{C}: |z - z_0| < r\}$  la frontera es  $\partial D_r(z_0) = \{z \in \mathbb{C}: |z - z_0| = r\}$ , y su clausura es  $\overline{D_r(z_0)} = \{z \in \mathbb{C}: |z - z_0| \leq r\}$ . Un tema un tanto sutil en los complejos es la idea de *conectividad*. Intuitivamente, un conjunto es conexo si es “una sola pieza”. En los reales un conjunto es conexo exactamente si es un único intervalo, lo que no tiene mucho interés. En un plano hay gran variedad de conjuntos conexos, y se requiere una definición precisa.

**Definición 28.4.** Dos conjuntos  $X, Y \subseteq \mathbb{C}$  se dicen *separados* si hay conjuntos abiertos  $A$  y  $B$  disjuntos tales que  $X \subseteq A$  y  $Y \subseteq B$ . El conjunto  $D \subseteq \mathbb{C}$  es *conexo* si es imposible hallar conjuntos abiertos disjuntos tales que  $D$  es su unión. Una *región* es un conjunto conexo abierto.

Por ejemplo, los intervalos  $[0, 1]$  y  $(1, 2]$  en el eje real están separados (hay infinitas posibilidades para  $X$  e  $Y$  de la definición, por ejemplo  $X = D_1(0)$  e  $Y = D_1(2)$ ).

Un tipo de conjunto conexo que usaremos con frecuencia es la curva.

**Definición 28.5.** Un *camino* o *curva* en  $\mathbb{C}$  es la imagen de una función continua  $\gamma: [a, b] \rightarrow \mathbb{C}$ , donde  $[a, b]$  es un intervalo cerrado en  $\mathbb{R}$ . Acá la continuidad se refiere a que  $t \mapsto x(t) + iy(t)$ , y que tanto  $x$  como  $y$  son continuas. La curva se dice *suave* si ambas componentes son diferenciables.

Decimos que la curva está *parametrizada* por  $\gamma$ , y en un abuso común de la notación usaremos  $\gamma$  para referirnos a la curva. La curva se dice *cerrada* si  $\gamma(a) = \gamma(b)$ , y es una *curva simple cerrada* si  $\gamma(a) = \gamma(b)$  y  $\gamma(s) = \gamma(t)$  solo si  $s = t$ ,  $s = a$  y  $t = b$ , o  $s = b$  y  $t = a$ . Vale decir, la curva no se intersecta a sí misma, solo coinciden los puntos inicial y final.

Lo siguiente es intuitivamente obvio, pero requiere ahondar bastante para demostrarse:

**Teorema 28.3.** *Toda curva en  $\mathbb{C}$  es conexa.*

Es claro que  $\gamma: [0, 1] \rightarrow \mathbb{C}$  con  $\gamma(t) = z_0 + t(z_1 - z_0)$  define un segmento de una recta en  $\mathbb{C}$  que va de  $z_0$  a  $z_1$ . Al segmento de la recta  $z_0z_1$  así parametrizada la anotaremos  $[z_0, z_1]$ . Podemos definir una curva formada por los segmentos  $z_0z_1, z_1z_2, \dots, z_{n-1}z_n$ , que anotaremos  $[z_0, z_1, \dots, z_n]$ . A tales curvas las llamaremos *poligonales*. La parametrización quedará a cargo del amable lector. Un teorema intuitivamente obvio, pero cuya demostración tiene sus sutilezas, es el siguiente:

**Teorema 28.4.** Si  $D$  es un subconjunto de  $\mathbb{C}$  tal que cualquier par de puntos en  $D$  pueden conectarse mediante una curva en  $D$  entonces  $D$  es conexo. Por el otro lado, si  $D$  es un subconjunto abierto conexo de  $\mathbb{C}$  entonces cualquier par de puntos de  $D$  pueden conectarse mediante una curva en  $D$ , incluso es posible conectarlos mediante una curva poligonal.

Un teorema central, bastante difícil de demostrar en su generalidad (ver Jordan [188, páginas 587-594] para la demostración original) es el siguiente:

**Teorema 28.5 (Jordan).** Sea  $\gamma$  una curva suave simple cerrada. Entonces el complemento de  $\gamma$  consiste exactamente de dos componentes conexos. Uno de estos componentes es acotado (el interior de  $\gamma$ ), el otro no es acotado (el exterior de  $\gamma$ ).

Por este teorema comúnmente se les llama *curvas de Jordan* a las curvas simples cerradas.

### 28.3. Límites y derivadas

Si  $z$  es una variable compleja, y  $f(z)$  alguna función de la misma, el límite se define igual que en los reales. Decimos que

$$\lim_{z \rightarrow z_0} f(z) = \omega$$

si para todo  $\epsilon > 0$  existe  $\delta > 0$  tal que:

$$0 < |z - z_0| < \delta \implies |f(z) - \omega| < \epsilon \quad (28.8)$$

Formalmente es idéntica a la definición para los reales, pero debe tenerse presente que acá  $|z - z_0| < \delta$  representa un círculo alrededor de  $z_0$ . Esto suele describirse diciendo que el límite debe ser el mismo, independiente del camino que siga  $z = x + iy$  para acercarse a  $z_0 = x_0 + iy_0$ . Definimos que  $f(z)$  es *continua* en  $z_0$  si

$$\lim_{z \rightarrow z_0} f(z) = f(z_0)$$

Si  $f$  es continua en todos los puntos en que está definida decimos simplemente que es continua. Si  $z = x + iy$ ,  $z_0 = x_0 + iy_0$  y  $f(z) = u(x, y) + iv(x, y)$  (como por ejemplo  $f(z) = z^2 = x^2 - y^2 + 2xyi$ ), es fácil ver que  $f(z)$  es continua si y solo si lo son  $u(x, y)$  y  $v(x, y)$ .

**Lema 28.6.** Si  $\lim_{z \rightarrow z_0} f(z)$  y  $\lim_{z \rightarrow z_0} g(z)$  existen, tenemos las siguientes propiedades de los límites:

$$(I) \quad \lim_{z \rightarrow z_0} cf(z) = c \lim_{z \rightarrow z_0} f(z)$$

$$(II) \quad \lim_{z \rightarrow z_0} (f(z) + g(z)) = \lim_{z \rightarrow z_0} f(z) + \lim_{z \rightarrow z_0} g(z)$$

$$(III) \quad \lim_{z \rightarrow z_0} (f(z) \cdot g(z)) = \lim_{z \rightarrow z_0} f(z) \cdot \lim_{z \rightarrow z_0} g(z)$$

(IV) Siempre que  $\lim_{z \rightarrow z_0} g(z) \neq 0$  es:

$$\lim_{z \rightarrow z_0} \frac{f(z)}{g(z)} = \frac{\lim_{z \rightarrow z_0} f(z)}{\lim_{z \rightarrow z_0} g(z)}$$

La demostración es simple, y quedará de ejercicio. De acá es inmediato que la suma, diferencia, producto y cociente de funciones continuas son continuas (siempre que no tengamos un denominador cero, claro está).

Dada una función compleja  $f(z)$  definimos su *derivada* en  $z = z_0$  como el siguiente límite, si existe:

$$f'(z_0) = \lim_{h \rightarrow 0} \frac{f(z_0 + h) - f(z_0)}{h} \quad (28.9)$$

Una notación alternativa común es:

$$\frac{df}{dz} = f'(z)$$

La condición que el límite sea el mismo, independiente del camino seguido por  $h$  para aproximarse a cero, hace que para  $f(x + iy) = u(x, y) + i\nu(x, y)$  con  $\Delta x$  y  $\Delta y$  reales deba ser:

$$\begin{aligned} \lim_{\Delta x \rightarrow 0} \frac{f(z_0 + \Delta x) - f(z_0)}{\Delta x} &= \lim_{\Delta y \rightarrow 0} \frac{f(z_0 + i\Delta y) - f(z_0)}{i\Delta y} \\ \frac{\partial u}{\partial x} + i \frac{\partial v}{\partial x} &= -i \frac{\partial u}{\partial y} + \frac{\partial v}{\partial y} \end{aligned} \quad (28.10)$$

Las expresiones (28.10) expresan la derivada compleja en términos de las coordenadas.

Igualando partes reales y complejas, resultan las *ecuaciones de Cauchy-Riemann*:

$$\begin{aligned} \frac{\partial u}{\partial x} &= \frac{\partial v}{\partial y} \\ \frac{\partial u}{\partial y} &= -\frac{\partial v}{\partial x} \end{aligned} \quad (28.11)$$

Esto ya demuestra que hay condiciones fuertes para que una función tenga derivada en un punto. Resulta que las ecuaciones (28.11) junto con continuidad de las derivadas son condiciones necesarias y suficientes para que  $f(x + iy) = u(x, y) + i\nu(x, y)$  tenga derivada en  $z_0 = x_0 + iy_0$ .

Si la función  $f$  tiene derivada en  $z_0$ , se dice que es *diferenciable* en  $z_0$ . A una función diferenciable en todo punto en una región abierta se le llama *holomorfa* (mucha literatura erróneamente se refiere a ellas como *funciones analíticas*, un concepto relacionado). Una función holomorfa sobre todo  $\mathbb{C}$  se llama *entera*.

Las siguientes propiedades de la derivada se demuestran básicamente cambiando  $x$  por  $z$  en las demostraciones respectivas para los reales:

**Lema 28.7.** *Sean  $f$  y  $g$  diferenciables en  $z \in \mathbb{C}$ , sea  $c \in \mathbb{C}$ , sea  $n \in \mathbb{Z}$ , y sea  $h$  diferenciable en  $g(z)$ . Entonces:*

$$(I) \ (cf(z))' = cf'(z)$$

$$(II) \ (f(z) + g(z))' = f'(z) + g'(z)$$

$$(III) \ (f(z) \cdot g(z))' = f'(z) \cdot g(z) + f(z) \cdot g'(z)$$

$$(IV) \ Siempre que g(z) \neq 0 \ es \ (f(z)/g(z))' = (f'(z) \cdot g(z) - f(z) \cdot g'(z))/g^2(z)$$

$$(V) \ (z^n)' = nz^{n-1}$$

$$(VI) \ (h(g(z)))' = h'(g(z)) \cdot g'(z)$$

Un último resultado se refiere a funciones inversas.

**Lema 28.8.** Sean  $G$  y  $H$  conjuntos abiertos en  $\mathbb{C}$ ,  $f: G \rightarrow H$  una biyección con inversa  $g: H \rightarrow G$ , y sea  $z_0 \in H$ . Si  $f$  es diferenciable en  $g(z_0)$  con  $f'(g(z_0)) \neq 0$ , y  $g$  es continua en  $z_0$ , entonces  $g$  es diferenciable en  $z_0$ , y:

$$g'(z_0) = \frac{1}{f'(g(z_0))}$$

*Demostración.* Por definición:

$$g'(z_0) = \lim_{z \rightarrow z_0} \frac{g(z) - g(z_0)}{z - z_0} = \lim_{z \rightarrow z_0} \frac{g(z) - g(z_0)}{f(g(z)) - f(g(z_0))} = \lim_{z \rightarrow z_0} \frac{1}{\frac{f(g(z)) - f(g(z_0))}{g(z) - g(z_0)}}$$

Dado que  $g$  es continua en  $z_0$ ,  $g(z) \rightarrow g(z_0)$  cuando  $z \rightarrow z_0$ , lo que da:

$$g'(z_0) = \lim_{w \rightarrow g(z_0)} \frac{1}{\frac{f(w) - f(g(z_0))}{w - g(z_0)}}$$

El denominador es continuo y diferente de cero, por el lema 28.6 tenemos lo prometido.  $\square$

Un resultado importante es:

**Teorema 28.9.** Si  $f'(z) = 0$  para todo  $z$  en una región  $D$ , entonces  $f(z)$  es constante en  $D$ .

Elegimos un punto fijo  $z_0 \in D$ , y conectaremos un punto arbitrario  $z \in D$  con  $z_0$  mediante una poligonal, y demostraremos que  $f$  es constante sobre esa poligonal. Como  $z$  es arbitrario,  $f$  es constante en  $D$ .

*Demostración.* Sean  $z_0, z \in D$ . Por el teorema 28.4 hay una poligonal  $[z_0, z_1, \dots, z]$  en  $D$  que los conecta. Sea  $f(z) = u + iv$ , si  $f'(z) = 0$  de las ecuaciones de Cauchy-Riemann es:

$$\frac{\partial u}{\partial x} = \frac{\partial u}{\partial y} = \frac{\partial v}{\partial x} = \frac{\partial v}{\partial y} = 0$$

Considerando uno de los tramos, digamos  $[z_k, z_{k+1}]$  vemos que esta recta queda descrita por una parametrización de la forma  $z_k + (t - t_k)(z_{k+1} - z_k)/(t_{k+1} - t_k) = \alpha t + \beta$ . Resulta que la derivada de  $f$  respecto a  $t$  a lo largo de  $[z_k, z_{k+1}]$  se anula:

$$\frac{f(\alpha(t+h) + \beta) - f(\alpha t + \beta)}{h} = \frac{\partial u}{\partial x} \frac{dx}{dt} + i \frac{\partial v}{\partial x} \frac{dy}{dt} = 0$$

Acá usamos la fórmula (28.10) para la derivada compleja. Podemos aplicar el teorema del valor medio para funciones reales (componente a componente) a  $f$  como función de  $t$ . Como la derivada se anula, esto nos dice que no hay cambios:

$$f(z_{k+1}) - f(z_k) = 0$$

Esto es lo que queríamos demostrar.  $\square$

## 28.4. Funciones elementales

Es claro que los polinomios son funciones enteras, y si se restringen a argumentos reales son simplemente las funciones conocidas. Un poquito más delicado es el caso de funciones racionales, como:

$$\frac{z^3 - 3z + 2}{z^2 + 1}$$

Esta función es holomorfa salvo en los puntos  $z = \pm i$ , donde el denominador se anula. Como función real es continua y tiene derivada en todas partes.

Veamos la función exponencial. Parece razonable extender la propiedad básica  $e^{x_1} \cdot e^{x_2} = e^{x_1+x_2}$  a argumentos complejos, lo que para  $x, y \in \mathbb{R}$  da:

$$e^{x+iy} = e^x \cdot e^{iy}$$

Esto, con la convención (28.3), resulta en:

**Definición 28.6.** Para  $x, y \in \mathbb{R}$  definimos:

$$e^{x+iy} = e^x(\cos y + i \sin y) \quad (28.12)$$

Escribiendo:

$$e^z = u(x, y) + i v(x, y)$$

vemos que se satisfacen las ecuaciones de Cauchy-Riemann (28.11) y que las derivadas son continuas para todo  $z \in \mathbb{C}$ . Esta función es entera. Vemos también que:

$$\frac{d}{dz} e^z = \frac{\partial u}{\partial x} + i \frac{\partial v}{\partial x} = e^x \cos y + i e^x \sin y = e^z \quad (28.13)$$

Ya vimos que  $e^{iy_1} \cdot e^{iy_2} = e^{i(y_1+y_2)}$ , y  $e^{x_1} \cdot e^{x_2} = e^{x_1+x_2}$ , que en conjunto hacen que  $e^{z_1} \cdot e^{z_2} = e^{z_1+z_2}$ , como buscábamos. Notamos que:

$$|e^z| = |e^x| \cdot |\cos y + i \sin y| = |e^x| \cdot (\cos^2 y + \sin^2 y)^{1/2} = e^x \quad (28.14)$$

Como  $e^x$  nunca se anula para  $x \in \mathbb{R}$ , y  $\cos y$  y  $\sin y$  no se anulan juntas,  $e^z \neq 0$  para todo  $z \in \mathbb{C}$ .

En nuestra lista siguen las funciones trigonométricas. La convención (28.3) para  $\pm\phi$  da:

$$e^{i\phi} = \cos \phi + i \sin \phi \quad e^{-i\phi} = \cos \phi - i \sin \phi$$

De este sistema de ecuaciones:

$$\cos \phi = \frac{e^{i\phi} + e^{-i\phi}}{2} \quad \sin \phi = \frac{e^{i\phi} - e^{-i\phi}}{2i}$$

lo que sugiere definir:

$$\cos z = \frac{e^{iz} + e^{-iz}}{2} \quad (28.15)$$

$$\sin z = \frac{e^{iz} - e^{-iz}}{2i} \quad (28.16)$$

Es claro que estas funciones son enteras, y cumplen las identidades trigonométricas conocidas para los reales. Cuidado, estas funciones no son acotadas en  $\mathbb{C}$ . El lector escéptico podrá entretenérse demostrando algunas identidades, como  $\cos^2 z + \sin^2 z = 1$  o las fórmulas para sumas de ángulos.

De las relaciones (28.15) y (28.16) vemos que para las funciones hiperbólicas:

$$\cosh z = \frac{e^z + e^{-z}}{2} = \cos iz \quad (28.17)$$

$$\sinh z = \frac{e^z - e^{-z}}{2} = -i \sin iz \quad (28.18)$$

Estas funciones también son enteras. Podemos definir las demás funciones trigonométricas e hiperbólicas usando las mismas definiciones que para los reales.

## 28.5. Logaritmos y potencias

Entre los reales, el logaritmo es simplemente el inverso de la exponencial. Esto está perfectamente bien definido en ese caso. Entre los complejos, sin embargo, la exponencial es una función periódica (el período es  $2\pi i$ ). Como hay infinitas soluciones a la ecuación  $e^z = w$  siempre que  $w \neq 0$ , no podemos esperar definir una función análoga, deberemos dar algunos rodeos. En particular, para  $x \in \mathbb{R}$  con  $x > 0$  realmente es  $\log x = \ln x + 2k\pi i$ , ya que debemos considerar los posibles argumentos. Acá  $\ln x$  es el familiar logaritmo natural de los reales. En los reales simplemente dejamos de lado la componente imaginaria.

Para  $z \neq 0$  definimos:

$$\log z = \ln|z| + i \arg z \quad (28.19)$$

Con esto tenemos el caso emblemático:

$$\log(-1) = \ln 1 + i \arg(-1) = (2k+1)\pi i$$

Esto cumple el familiar:

$$e^{\log z} = e^{\ln|z| + i \arg z} = e^{\ln|z|} \cdot e^{i \arg z} = z$$

Pero aparece una complicación. Con el ya tradicional  $z = x + iy$  tenemos:

$$\log(e^z) = \ln e^x + i \arg e^z = x + (y + 2k\pi)i = z + 2k\pi i$$

Acá  $k$  es un entero cualquiera. De la misma manera, para un entero cualquiera  $k$ :

$$\begin{aligned} \log(wz) &= \ln(|w| \cdot |z|) + i \arg(wz) = \ln|w| + i \arg w + \ln|z| + i \arg z + 2k\pi i \\ &= \log w + \log z + 2k\pi i \end{aligned}$$

Definimos la *rama principal* del logaritmo mediante:

$$\text{Log } z = \ln|z| + i \text{Arg } z \quad (28.20)$$

Si  $z = x$ , un real positivo, es:

$$\text{Log } x = \ln x + i \text{Arg } x = \ln x$$

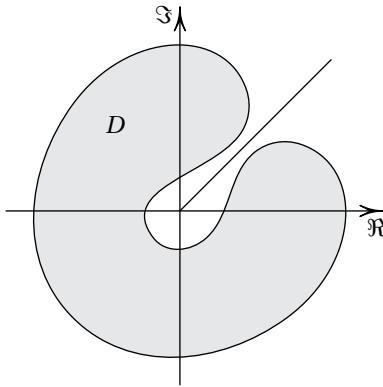
Vemos que la nueva función es una extensión del logaritmo real. La definición del argumento principal con este rango, en vez del mucho más natural  $0 \leq \phi < 2\pi$ , es precisamente para asegurar esta coincidencia sin estar equilibrándonos en el borde del abismo a lo largo de la línea real.

La función Log es holomorfa en muchas partes. No está definida para  $z = 0$ , y tiene un corte en la línea real negativa. Sea  $z_0 = x_0 + iy_0$  tal que  $\text{Log } z_0$  esté definido, y veamos su derivada:

$$\lim_{z \rightarrow z_0} \frac{\text{Log } z - \text{Log } z_0}{z - z_0} = \lim_{z \rightarrow z_0} \frac{\text{Log } z - \text{Log } z_0}{e^{\text{Log } z} - e^{\text{Log } z_0}}$$

Deberemos restringirnos a trabajar en una región que no incluya los puntos conflictivos mencionados. Con  $w = \text{Log } z$  y  $w_0 = \text{Log } z_0$ , notando que  $w \rightarrow w_0$  cuando  $z \rightarrow z_0$ , esto es:

$$\begin{aligned} \lim_{z \rightarrow z_0} \frac{\text{Log } z - \text{Log } z_0}{z - z_0} &= \lim_{w \rightarrow w_0} \frac{w - w_0}{e^w - e^{w_0}} = \frac{1}{e^{w_0}} \\ &= \frac{1}{z_0} \end{aligned}$$

Figura 28.2 – Dominio alternativo de  $\log z$ 

Nótese que la restricción del argumento es un tanto arbitraria, si nos interesa trabajar en la región  $D$  de la figura 28.2, podemos restringir el argumento al rango  $[\pi/4, 9\pi/4]$ .

Ahora estamos en condiciones de definir potencias arbitrarias de  $z$ . La definición obvia es:

$$z^c = e^{c \log z}$$

Hay muchos valores de  $\log z$ , con lo que pueden haber muchos valores de  $z^c$ . Al lector atento no le extrañará que se le llame el *valor principal* de  $z^c$  a  $e^{c \operatorname{Log} z}$ . En caso que  $c = n$ , un entero, la definición da:

$$\begin{aligned} z^n &= e^{n \log z} = e^{n(\operatorname{Log} z + 2k\pi i)} = e^{n \operatorname{Log} z} \cdot e^{2nk\pi i} \\ &= e^{n \operatorname{Log} z} \\ &= |z|^n \cdot e^{in \operatorname{Arg} z} \end{aligned}$$

Exactamente como debiera ser. El lector interesado verificará que si  $c$  es un racional, la fórmula da todos los valores esperados.

Esto introduce un nuevo problema. Tenemos una definición de potencias que aplicada a  $z = e$  puede dar infinitos valores para  $e^c$ . Hasta acá hemos asumido simplemente que para  $z = x + iy$  es:

$$e^z = \exp(z) = e^x (\cos y + i \sin y)$$

Equivalentemente,  $e^z$  se refiere al valor principal de esta expresión. Esta es la convención que adoptaremos, que por lo demás es universal.

## 28.6. Integrales

La integral en los reales es simplemente a lo largo de la línea real. Al integrar en los complejos hay muchos caminos distintos que podemos seguir. De todas formas, una definición natural para la integral de la función  $f$  a lo largo del camino suave  $\gamma: [a, b] \rightarrow \mathbb{C}$  es seguir la definición de la integral de Riemann en los reales. Imaginemos una subdivisión del rango  $[a, b]$  en  $n$  tramos  $[t_{k-1}, t_k]$ , donde  $1 \leq k \leq n$ . Vemos que al tramo  $[t_{k-1}, t_k]$  corresponde un arco  $[z_{k-1}, z_k]$  del camino  $\gamma$ , un punto  $t_k^*$  en el tramo  $[t_{k-1}, t_k]$  da un punto  $z_k^*$  en el arco correspondiente. Supongamos ahora dado  $\epsilon > 0$  cualquiera. Dada una partición  $P$  tal que se cumple para todo tramo que  $|z_k - z_{k-1}| < \epsilon$ , eligiendo puntos  $t_k^*$  en cada tramo calculamos la suma:

$$S(P) = \sum_{1 \leq k \leq n} f(z_k^*)(z_k - z_{k-1})$$

Si estas sumas tienden al valor  $L$  cuando  $\epsilon \rightarrow 0$ , llamamos a este límite el valor de la integral, y anotamos:

$$\int_{\gamma} f(z) dz = L$$

Podemos expresar la suma en términos de  $t$ :

$$\begin{aligned} S(p) &= \sum_{1 \leq k \leq n} f(\gamma(t_k^*)) (\gamma(t_k^*) - \gamma(t_{k-1}^*)) \\ &= \sum_{1 \leq k \leq n} f(\gamma(t_k^*)) (\gamma(t_k^*) - \gamma(t_{k-1}^*)) \\ &= \sum_{1 \leq k \leq n} f(\gamma(t_k^*)) \frac{\gamma(t_k^*) - \gamma(t_{k-1}^*)}{t_k^* - t_{k-1}^*} \cdot (t_k^* - t_{k-1}^*) \end{aligned}$$

Si  $\epsilon \rightarrow 0$ , vemos que esto tiende a:

$$\int_{\gamma} f(z) dz = \int_a^b f(\gamma(t)) \gamma'(t) dt \quad (28.21)$$

Esta misma fórmula indica que el valor de la integral es independiente de la parametrización de la curva.

Una cota que usaremos frecuentemente es la siguiente.

**Lema 28.10** (Cota para integrales complejas). *Supóngase que hay un número  $M$  tal que  $|f(z)| \leq M$  para todo  $z$  en la curva suave  $\gamma: [a, b] \rightarrow \mathbb{C}$ , y sea  $l_{\gamma}$  el largo de la curva  $\gamma$ . Entonces:*

$$\left| \int_{\gamma} f(z) dz \right| \leq M l_{\gamma} \quad (28.22)$$

*Demostración.* Usando la desigualdad triangular sobre la definición de la integral, vemos que:

$$\left| \int_{\gamma} f(z) dz \right| = \left| \int_a^b f(z) \gamma'(t) dt \right| \leq \int_a^b |f(z)| \cdot |\gamma'(t)| dt \leq M \int_a^b |\gamma'(t)| dt$$

Si describimos  $\gamma(t) = x(t) + iy(t)$  tenemos:

$$\int_a^b |\gamma'(t)| dt = \int_a^b \left( (x'(t))^2 + (y'(t))^2 \right)^{1/2} dt$$

que reconocemos como el largo  $l_{\gamma}$  de la curva. □

### 28.6.1. Integrales y antiderivadas

Supongamos nuevamente un camino suave  $\gamma$  entre  $a$  y  $b$ , una función  $g(z)$  diferenciable en  $\gamma$ , y consideremos  $t \in [a, b]$ . Veamos cuál es la derivada de  $g(\gamma(t))$ . Resulta ser exactamente como nos imaginamos. Primero, con  $g(x+iy) = u(x, y) + iv(x, y)$  y  $\gamma(t) = x(t) + iy(t)$ , es:

$$g(\gamma(t)) = u(x(t), y(t)) + iv(x(t), y(t))$$

Enseguida:

$$\frac{d}{dt} g(\gamma(t)) = \frac{\partial u}{\partial x} \frac{dx}{dt} + \frac{\partial u}{\partial y} \frac{dy}{dt} + i \left( \frac{\partial v}{\partial x} \frac{dx}{dt} + \frac{\partial v}{\partial y} \frac{dy}{dt} \right)$$

Usando las ecuaciones de Cauchy-Riemann:

$$\begin{aligned}\frac{d}{dt} g(\gamma(t)) &= \frac{\partial u}{\partial x} \frac{dx}{dt} - \frac{\partial v}{\partial x} \frac{dy}{dt} + i \left( \frac{\partial v}{\partial x} \frac{dx}{dt} + \frac{\partial u}{\partial x} \frac{dy}{dt} \right) \\ &= \left( \frac{\partial u}{\partial x} + i \frac{\partial v}{\partial x} \right) \cdot \left( \frac{dx}{dt} + i \frac{dy}{dt} \right) \\ &= g'(\gamma(t))\gamma'(t)\end{aligned}$$

Volvamos a las integrales ahora. Sea una región  $D$  y una función  $F: D \rightarrow \mathbb{C}$  tal que en  $D$  tenemos  $F'(z) = f(z)$ . Supongamos un camino suave  $\gamma: [a, b] \rightarrow D$ . Sabemos de arriba que:

$$\frac{d}{dt} F(\gamma(t)) = F'(\gamma(t))\gamma'(t) = f(\gamma(t))\gamma'(t)$$

Entonces:

$$\int_{\gamma} f(\zeta) d\zeta = \int_a^b f(\gamma(t))\gamma'(t) dt = \int_a^b \frac{d}{dt} F(\gamma(t)) dt = F(\gamma(b)) - F(\gamma(a)) \quad (28.23)$$

La última relación resulta del teorema fundamental del cálculo integral.

Muy agradable, la integral depende únicamente de los puntos inicial y final del camino. En particular, si el camino es cerrado, la integral es cero.

El recíproco ahora. Supongamos que la integral de la función continua  $f$  no depende del camino, vale decir podemos tomar un punto  $z_0 \in D$  y definir una función:

$$F(z) = \int_{\gamma_z} f(\zeta) d\zeta$$

donde el camino  $\gamma_z$  comienza en  $z_0$  y termina en  $z$ , sin salir de  $D$ . Sabemos que de existir tales caminos para cada elección de  $z$  la región  $D$  debe ser conexa. Evaluemos la derivada de  $F$ :

$$\lim_{h \rightarrow 0} \frac{F(z+h) - F(z)}{h} = \lim_{h \rightarrow 0} \frac{1}{h} \int_{\gamma_h} f(\zeta) d\zeta$$

Acá  $\gamma_h$  es un camino que comienza en  $z$  y termina en  $z+h$ . Vemos también que:

$$\begin{aligned}\int_{\gamma_h} d\zeta &= h \\ \int_{\gamma_h} f(z) d\zeta &= h f(z)\end{aligned}$$

Con esto:

$$\lim_{h \rightarrow 0} \frac{F(z+h) - F(z)}{h} - f(z) = \lim_{h \rightarrow 0} \frac{1}{h} \int_{\gamma_h} (f(\zeta) - f(z)) d\zeta$$

Ahora bien, como las integrales no dependen del camino podemos calcularla sobre la recta de  $z$  a  $z+h$ :

$$\left| \frac{1}{h} \int_{\gamma_h} (f(\zeta) - f(z)) d\zeta \right| \leq \left| \frac{1}{h} \right| \cdot |h| \cdot \max \{|f(\zeta) - f(z)| : \zeta \in [z, z+h]\}$$

Como  $f$  es continua, cuando  $h \rightarrow 0$  esto tiende a cero, y  $F'(z) = f(z)$ , como esperábamos.

En resumen:

**Teorema 28.11.** Sea  $D$  una región conexa, y sea  $f: D \rightarrow \mathbb{C}$  continua. Entonces  $f$  tiene antiderivada en  $D$  si y solo si la integral entre dos puntos de  $D$  es independiente del camino. El valor de la integral es la diferencia entre los valores de la antiderivada.

Pero también hemos demostrado:

**Teorema 28.12** (Morera). Sea  $f$  continua en  $D$  tal que para toda curva suave cerrada simple  $\gamma \subset D$ :

$$\int_{\gamma} f(z) dz = 0$$

Entonces  $f$  es holomorfa en  $D$ .

### 28.6.2. El teorema de Cauchy

Nos interesa evaluar integrales sobre caminos cerrados, en particular demostrar que tales integrales no dependen del detalle del camino. Para ello requeriremos algunas herramientas adicionales.

**Definición 28.7.** Sean  $\gamma_0$  y  $\gamma_1$  curvas cerradas en el conjunto abierto  $D \subseteq \mathbb{C}$ , parametrizadas por  $\gamma_0: [0, 1] \rightarrow D$  y  $\gamma_1: [0, 1] \rightarrow D$ , respectivamente. Decimos que  $\gamma_0$  es  $D$ -homotópica a  $\gamma_1$ , en símbolos  $\gamma_0 \sim_D \gamma_1$ , si hay una función continua  $h: [0, 1]^2 \rightarrow D$  tal que:

$$h(t, 0) = \gamma_0(t)$$

$$h(t, 1) = \gamma_1(t)$$

$$h(0, s) = h(1, s)$$

Si  $D$  es conexa y tal que toda curva cerrada simple es homotópica a un punto, se dice que  $D$  es *conexa simple*.

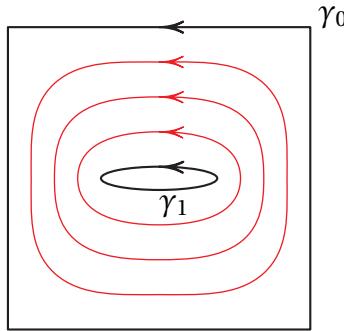


Figura 28.3 – Ejemplos de homotopía

La idea es que  $h(t, s)$  es una curva en  $D$ , la última condición asegura que sea siempre cerrada. Cambiando  $s$  cambia la curva, que va en forma continua de  $\gamma_0$  a  $\gamma_1$ . Nótese también que las curvas se recorren todas en dirección de  $t$  creciente, arbitrariamente definimos la dirección positiva como aquella en que el interior encerrado por la curva queda a su izquierda. Es simple ver que la homotopía es una relación de equivalencia entre curvas. Frecuentemente consideraremos un punto aislado como una “curva” de largo cero. Una región conexa simple no tiene “agujeros”.

Mucho de lo que viene a continuación se basa en el siguiente teorema. La demostración es de Beck, Marchesi, Pixton y Sabalka [30].

**Teorema 28.13** (Cauchy). *Sea  $D \subseteq \mathbb{C}$  una región abierta,  $f$  holomorfa en  $D$ , y  $\gamma_0 \sim_D \gamma_1$  vía una homotopía con segundas derivadas continuas y que coinciden para  $s = 0$  y  $s = 1$ . Entonces:*

$$\int_{\gamma_0} f(z) dz = \int_{\gamma_1} f(z) dz$$

La condición de suavidad de la homotopía puede relajarse bastante, pero la demostración se hace muy compleja. Para las aplicaciones de nuestro interés esta condición se cumple.

*Demostración.* Sea  $h(t, s)$  la homotopía de  $\gamma_0$  a  $\gamma_1$ , y definamos  $\gamma_s$  como la curva definida por  $h$  para  $s$ . Consideremos la función:

$$I(s) = \int_{\gamma_s} f(z) dz = \int_0^1 f(h(t, s)) \frac{\partial h}{\partial t} dt$$

Esta expresión resulta de (28.21). Demostraremos que  $I(s)$  es constante, con lo que se cumple lo prometido como  $I(0) = I(1)$ . Por la regla de Leibnitz:

$$\frac{d}{ds} I(s) = \frac{d}{ds} \int_0^1 f(h(t, s)) \frac{\partial h}{\partial t} dt = \int_0^1 \frac{\partial}{\partial s} \left( f(h(t, s)) \frac{\partial h}{\partial t} \right) dt$$

Usando el menú completo de propiedades de las derivadas parciales:

$$\begin{aligned} \frac{d}{ds} I(s) &= \int_0^1 \left( f'(h(t, s)) \frac{\partial h}{\partial s} \frac{\partial h}{\partial t} + f(h(t, s)) \frac{\partial^2 h}{\partial s \partial t} \right) dt \\ &= \int_0^1 \left( f'(h(t, s)) \frac{\partial h}{\partial t} \frac{\partial h}{\partial s} + f(h(t, s)) \frac{\partial^2 h}{\partial t \partial s} \right) dt \\ &= \int_0^1 \frac{\partial}{\partial t} \left( f(h(t, s)) \frac{\partial h}{\partial s} \right) dt \end{aligned}$$

Aplicando el teorema fundamental del cálculo integral por separado a las componentes real e imaginaria, y recordando la condición  $h(0, s) = h(1, s)$  y que las respectivas derivadas coinciden:

$$\frac{d}{ds} I(s) = f(h(1, s)) \frac{\partial h}{\partial s}(1, s) - f(h(0, s)) \frac{\partial h}{\partial s}(0, s) = 0$$

Si la derivada compleja es cero, lo son las derivadas parciales de las componentes real e imaginaria, y así la función es constante.  $\square$

Una consecuencia inmediata es que si  $D$  es una región conexa simple en la cual la función  $f$  es holomorfa entonces para todo camino suave cerrado  $\gamma \subset D$ :

$$\int_{\gamma} f(z) dz = 0$$

Esto porque en este caso cualquier curva  $\gamma \subset D$  es homotópica con un punto, y claramente la integral para un punto es cero. Por el teorema 28.11 en tales regiones la integral es independiente del camino y existe una antiderivada.

### 28.6.3. La fórmula integral de Cauchy

Tenemos el siguiente resultado notable:

**Teorema 28.14** (Fórmula integral de Cauchy). *Sea  $f$  holomorfa en la región  $D$  que contiene el camino cerrado simple  $\gamma$ , con la orientación habitual que el interior está a la izquierda, y suponga que  $z_0$  está al interior de  $\gamma$ . Entonces:*

$$f(z_0) = \frac{1}{2\pi i} \int_{\gamma} \frac{f(z)}{z - z_0} dz$$

*Demuestra.* Sea  $\epsilon > 0$  arbitrario. Sabemos que  $f$  es continua en  $z_0$ , por lo que existe  $\delta > 0$  tal que  $|f(z) - f(z_0)| < \epsilon$  siempre que  $|z - z_0| < \delta$ . Sea ahora  $r > 0$  tal que  $r < \delta$  y la circunferencia  $C_0 = \{z : |z - z_0| = r\}$  está dentro de  $\gamma$ . Entonces  $f(z)/(z - z_0)$  es holomorfa en la región entre  $\gamma$  y  $C_0$ , por lo que del teorema de Cauchy:

$$\int_{\gamma} \frac{f(z)}{z - z_0} dz = \int_{C_0} \frac{f(z)}{z - z_0} dz$$

La integral siguiente es fácil de evaluar si parametrizamos  $C_0$  como  $z_0 + re^{it}$ :

$$\int_{C_0} \frac{1}{z - z_0} dz = \int_0^{2\pi} \frac{1}{r} \cdot rie^{it} dt = 2\pi i$$

Con esto:

$$\int_{C_0} \frac{f(z)}{z - z_0} dz - 2\pi i f(z_0) = \int_{C_0} \frac{f(z)}{z - z_0} dz - \int_{C_0} \frac{f(z_0)}{z - z_0} dz = \int_{C_0} \frac{f(z) - f(z_0)}{z - z_0} dz$$

Sobre  $C_0$  tenemos:

$$\left| \frac{f(z) - f(z_0)}{z - z_0} \right| = \frac{|f(z) - f(z_0)|}{|z - z_0|} \leq \frac{\epsilon}{r}$$

De nuestra cota (28.22) para integrales:

$$\int_{C_0} \frac{f(z) - f(z_0)}{z - z_0} dz \leq \frac{\epsilon}{r} \cdot 2\pi r = 2\pi\epsilon$$

Pero  $\epsilon$  es un número positivo arbitrario, la integral debe ser cero.  $\square$

Esto es realmente notable: Si  $f$  es holomorfa al interior del camino cerrado simple  $\gamma$  y conocemos los valores de  $f$  sobre  $\gamma$ , los conocemos en todo su interior.

Incluso da una manera sencilla de evaluar ciertas integrales. Por ejemplo, evaluemos la integral:

$$\int_0^{\infty} \frac{1}{x^2 + 1} dx$$

Primero, el integrando es par, con lo que:

$$\int_0^{\infty} \frac{1}{x^2 + 1} dx = \frac{1}{2} \int_{-\infty}^{\infty} \frac{1}{x^2 + 1} dx$$

El integrando tiene problemas en  $\pm i$ , es holomorfo en  $\mathbb{C} \setminus \{-i, i\}$ . La curva  $\gamma$  de la figura 28.4 se descompone en un arco  $A$  de radio  $R$  y la línea  $L$  de  $-R$  a  $R$  a lo largo del eje  $X$ . Si hacemos tender  $R \rightarrow \infty$ , la integral sobre  $L$  es el resultado que nos interesa. Debemos evaluar la integral sobre el arco. Como nos interesa  $R \rightarrow \infty$ , perfectamente podemos concentrarnos en  $R > 1$ . Tenemos:

$$\left| \int_A \frac{1}{z^2 + 1} dz \right| \leq \int_A \frac{1}{|z^2 + 1|} dz \leq \int_A \frac{1}{|z|^2 - 1} dz = \frac{1}{R^2 - 1} \cdot \pi R$$

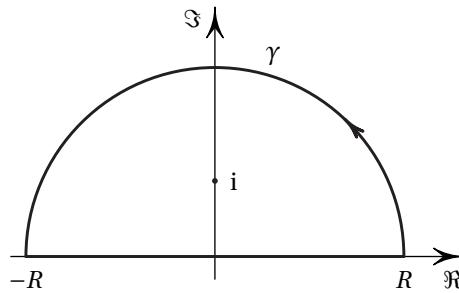


Figura 28.4 – Curva para integral ejemplo

Esto tiende a cero cuando  $R \rightarrow \infty$ , como esperábamos. Acá usamos:

$$|z|^2 = |(z^2 + 1) - 1| \leq |z^2 + 1| + 1$$

Por otro lado, por la fórmula de Cauchy podemos escribir para  $z_0 = i$ :

$$\int_{\gamma} \frac{1/(z+i)}{z-i} dz = 2\pi i \frac{1}{z+i} \Big|_{z=i} = \pi$$

y nuestra integral original es:

$$\int_0^{\infty} \frac{1}{x^2+1} dx = \frac{\pi}{2}$$

Esta integral es simple de evaluar en forma tradicional, pero esta técnica es aplicable en forma mucho más amplia.

**Teorema 28.15.** *Sea  $f$  holomorfa en la región  $D$ . Entonces  $f'$  es holomorfa en  $D$ .*

*Demostración.* Sea  $C$  una circunferencia centrada en  $z$  de radio  $r$  dentro de  $D$ , y  $z+h$  un punto dentro de  $C$ . Es rutina verificar que:

$$\frac{1}{h} \left( \frac{1}{\zeta-z-h} - \frac{1}{\zeta-z} \right) = \frac{1}{(\zeta-z)^2} + \frac{h}{(\zeta-z)^2(\zeta-z-h)}$$

Calculamos:

$$\begin{aligned} \frac{f(z+h)-f(z)}{h} &= \frac{1}{2\pi hi} \int_C \frac{f(\zeta)}{\zeta-z-h} d\zeta - \frac{1}{2\pi hi} \int_C \frac{f(\zeta)}{\zeta-z} d\zeta \\ &= \frac{1}{2\pi i} \int_C \frac{f(\zeta)}{(\zeta-z)^2} d\zeta + \frac{h}{2\pi i} \int_C \frac{f(\zeta)}{(\zeta-z)^2(\zeta-z-h)} d\zeta \end{aligned}$$

Si  $|h| < r/2$ , por la desigualdad triangular (teorema 1.2) para todo  $\zeta \in C$  es:

$$|\zeta-z-h| \geq |\zeta-z|-|h| > r - \frac{r}{2} = \frac{r}{2}$$

Por el otro lado,  $f$  es continua sobre  $C$ , por lo que hay  $M$  tal que  $|f(\zeta)| \leq M$  para  $\zeta \in C$ . De la estimación (28.22) tenemos:

$$\left| \frac{h}{2\pi i} \int_C \frac{f(\zeta)}{(\zeta-z)^2(\zeta-z-h)} d\zeta \right| \leq \frac{|h|}{2\pi} \frac{2M}{r^3} 2\pi r = \frac{2M|h|}{r^2}$$

Cuando  $h \rightarrow 0$  esto tiende a cero. Esto incluso da una fórmula explícita para  $f'(z)$ :

$$f'(z) = \frac{1}{2\pi i} \int_C \frac{f(\zeta)}{(\zeta - z)^2} d\zeta$$

□

Aplicando el mismo argumento, obtenemos  $f''(z)$ , con lo que  $f'$  es holomorfa. Continuando tenemos derivadas de todos los órdenes. Hemos demostrado:

**Teorema 28.16.** *Sea  $f$  holomorfa en la región  $D$ . Entonces para todo  $n \in \mathbb{N}$  la función  $f^{(n)}$  es holomorfa en  $D$ .*

Esto es notable, en los reales la existencia de la primera derivada nada dice de las derivadas superiores, acá la existencia de la primera derivada asegura que hay derivadas de todos los órdenes. Aún más:

**Teorema 28.17** (Fórmula integral de Cauchy generalizada). *Sea  $f$  holomorfa en la región  $D$ , y  $\gamma$  un camino cerrado simple al interior de  $D$ . Entonces:*

$$f^{(n)}(z) = \frac{n!}{2\pi i} \int_{\gamma} \frac{f(\zeta)}{(\zeta - z)^{n+1}} d\zeta \quad (28.24)$$

*Demostración.* Por el teorema 28.16 sabemos que  $f^{(n)}$  es holomorfa en  $D$ . La fórmula integral de Cauchy permite escribir:

$$f^{(n)}(z) = \frac{1}{2\pi i} \int_{\gamma} \frac{f^{(n)}(\zeta)}{\zeta - z} d\zeta$$

Integrando por partes  $n$  veces entrega lo prometido. □

Hay más consecuencias de interés.

**Teorema 28.18** (Liouville). *Si una función entera es acotada en valor absoluto, es constante.*

*Demostración.* Por hipótesis hay una constante  $M$  tal que  $|f(z)| \leq M$  para todo  $z \in \mathbb{C}$ . Demostramos por contradicción que  $f'(z) = 0$  en todo  $\mathbb{C}$ , con lo que por el teorema 28.9  $f$  es constante.

Supongamos que para algún  $z$  es  $f'(z) \neq 0$ . Elija  $R$  de manera que  $M/R < |f'(z)|$ . Sea  $C$  la circunferencia de radio  $R$  alrededor de  $z$ . Entonces:

$$\frac{M}{R} < |f'(z)| = \left| \frac{1}{2\pi i} \int_C \frac{f(\zeta)}{(\zeta - z)^2} d\zeta \right| \leq \frac{1}{2\pi} \frac{M}{R^2} 2\pi R = \frac{M}{R}$$

Esta contradicción muestra que tal  $z$  no existe. □

Del siguiente teorema Gauß en su disertación dio la primera demostración razonablemente satisfactoria. Pese a su nombre, poco tiene que ver con el álgebra actual y no es particularmente fundamental. Nuestra demostración se debe a Schep [313].

**Teorema 28.19** (Teorema fundamental del álgebra). *Todo polinomio no constante con coeficientes complejos tiene un cero complejo.*

*Demostración.* Por contradicción. Sea  $p(z)$  un polinomio no constante sin ceros complejos. En particular,  $p(0) \neq 0$ . Por el teorema integral de Cauchy:

$$\int_{|z|=r} \frac{dz}{zp(z)} = \frac{2\pi i}{p(0)}$$

Por otro lado:

$$\begin{aligned} \left| \int_{|z|=r} \frac{dz}{zp(z)} \right| &\leq 2\pi r \cdot \max_{|z|=r} \left| \frac{1}{zp(z)} \right| \\ &= \frac{2\pi}{\min_{|z|=r} |p(z)|} \end{aligned}$$

Cuando  $r \rightarrow \infty$ , esta última expresión tiende a 0, contradiciendo el valor anterior.  $\square$

La manera tradicional de expresar el teorema 28.19 es diciendo que todo polinomio no constante de coeficientes reales se puede factorizar en factores lineales o cuadráticos sin ceros reales, o que si tiene grado  $n$  tiene  $n$  ceros reales o complejos conjugados (contando multiplicidades).

## 28.7. Secuencias y series

Las definiciones de secuencias y series complejas son esencialmente las mismas que para los reales. Anotamos  $\langle a_n \rangle_{n \geq 0}$  para la secuencia de los  $a_n$  (formalmente, es una función  $a: \mathbb{N}_0 \rightarrow \mathbb{C}$ ). El número  $L$  se llama el *límite* de la secuencia si para cualquier  $\epsilon > 0$  que se elija hay un entero  $n_\epsilon$ , dependiente de  $\epsilon$ , tal que siempre que  $n \geq n_\epsilon$  es  $|L - a_n| < \epsilon$ . Esto lo anotamos  $\lim a_n = L$ . Es fácil ver que si  $a_n = u_n + iv_n$  y la secuencia  $\langle a_n \rangle_{n \geq 0}$  converge a  $L$ , tenemos  $\lim u_n = \Re L$  y  $\lim v_n = \Im L$ . Al revés, si las secuencias reales  $\langle u_n \rangle_{n \geq 0}$  y  $\langle v_n \rangle_{n \geq 0}$  convergen, converge la secuencia compleja  $\langle u_n + iv_n \rangle_{n \geq 0}$ . Se desprenden todas las familiares propiedades de los límites. Una condición necesaria y suficiente para la convergencia de la secuencia  $\langle a_n \rangle_{n \geq 0}$  es el *criterio de Cauchy*: Dado  $\epsilon > 0$  hay un entero  $n_\epsilon$  tal que  $|a_m - a_n| < \epsilon$  siempre que  $m, n \geq n_\epsilon$ .

Es obvio considerar secuencias de funciones en una región  $D$ . Para cada  $z \in D$  tenemos una secuencia ordinaria  $\langle f_n(z) \rangle_{n \geq 0}$ . Si estas secuencias convergen, la secuencia *converge punto a punto* a la función  $f(z) = \lim f_n(z)$ . Se dice que la secuencia de funciones converge *uniformemente* sobre el conjunto  $S$  si dado un  $\epsilon > 0$  hay un entero  $n_\epsilon$  tal que  $|f(z) - f_n(z)| < \epsilon$  para todo  $n \geq n_\epsilon$  y todo  $z \in S$ . El punto de la convergencia uniforme es que el mismo  $n_\epsilon$  sirve para todos los  $z \in S$ .

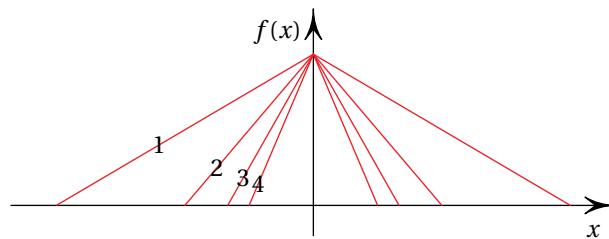


Figura 28.5 – Secuencia de funciones continuas con límite discontinuo

Note que una secuencia de funciones continuas puede converger a una función discontinua.

Considere por ejemplo la secuencia de funciones definidas para  $n \geq 1$  por:

$$f_n(x) = \begin{cases} 0 & x \leq -1/n \\ 1 + nx & -1/n < x \leq 0 \\ 1 - nx & 0 < x \leq 1/n \\ 0 & 1/n < x \end{cases} \quad (28.25)$$

La figura 28.5 grafica algunas de las funciones (28.25). Es claro que:

$$\lim_{n \rightarrow \infty} f_n(x) = \begin{cases} 0 & x \neq 0 \\ 1 & x = 0 \end{cases} \quad (28.26)$$

Este comportamiento es imposible si la convergencia es uniforme. Porque suponga que  $\langle f_n(z) \rangle_{n \geq 0}$  converge uniformemente a  $f$  en la región  $D$ , sea  $z_0 \in D$  y  $\epsilon > 0$ . Demostraremos que hay  $\delta$  tal que  $|f(z_0) - f(z)| < \epsilon$  siempre que  $|z_0 - z| < \delta$ . Elija  $n_\epsilon$  tal que  $|f_{n_\epsilon}(z) - f(z)| < \epsilon/3$ . Por convergencia uniforme también es  $|f_{n_\epsilon}(z_0) - f(z_0)| < \epsilon/3$ . Ahora elija  $\delta$  de forma que  $|f_{n_\epsilon}(z_0) - f_{n_\epsilon}(z)| < \epsilon/3$  siempre que  $|z_0 - z| < \delta$ . Esto es posible ya que  $f_{n_\epsilon}$  es continua. Si  $|z_0 - z| < \delta$  resulta para todo  $n > n_\epsilon$ :

$$\begin{aligned} |f(z_0) - f(z)| &= |f(z_0) - f_n(z_0) + f_n(z_0) - f_n(z) + f_n(z) - f(z)| \\ &\leq |f(z_0) - f_n(z_0)| + |f_n(z_0) - f_n(z)| + |f_n(z) - f(z)| \\ &< \frac{\epsilon}{3} + \frac{\epsilon}{3} + \frac{\epsilon}{3} \\ &= \epsilon \end{aligned}$$

En los reales hay secuencias de funciones diferenciables que convergen uniformemente a funciones que no son diferenciables. La función símbolo que no es diferenciable en 0 es  $|x|$ , interesa construir una secuencia de funciones que se parecen a las ramas del valor absoluto, “suavizando” la esquina por ejemplo con una parábola  $y = ax^2$  entre  $\pm 1/n$ . Las ramas serán rectas de pendiente  $\pm 1$ , digamos  $y = \pm x + b$ ; queremos que los valores y las derivadas coincidan en  $\pm 1/n$ :

$$f_n\left(\pm \frac{1}{n}\right) = \frac{1}{n} + b \quad f'_n\left(\pm \frac{1}{n}\right) = \pm 2a \frac{1}{n} = \pm 1$$

De acá:

$$a = \frac{n}{2} \quad b = -\frac{1}{2n}$$

Nuestra función es:

$$f_n(x) = \begin{cases} -x - 1/2n & -1 \leq x < 1/n \\ nx^2/2 & -1/n < x \leq 1/n \\ x - 1/2n & 1/n < x \leq 1 \end{cases}$$

Por la forma que la construimos,  $f_n$  es diferenciable en  $[-1, 1]$ . Difiere de  $|x|$  a lo más en  $1/2n$ , con lo que la convergencia es uniforme. Pero  $\lim f_n(x) = |x|$ , que no es diferenciable en  $x = 0$ .

Pero también:

**Teorema 28.20.** *Sea  $\gamma$  una curva suave, sobre la cual las funciones  $f_n$  son continuas y convergen uniformemente a  $f$ . Entonces:*

$$\lim_{n \rightarrow \infty} \int_{\gamma} f_n(z) dz = \int_{\gamma} f(z) dz \quad (28.27)$$

Este resultado tiene múltiples consecuencias, que veremos más adelante. La demostración es rutina:

*Demostración.* Podemos acotar:

$$\left| \int_{\gamma} f_n(z) dz - \int_{\gamma} f(z) dz \right| = \left| \int_{\gamma} (f_n(z) - f(z)) dz \right| \leq \max_{z \in \gamma} |f_n(z) - f(z)| \cdot l_{\gamma}$$

Por convergencia uniforme podemos hacer el primer factor de la cota tan pequeño como deseemos.  $\square$

Incluso más:

**Teorema 28.21.** *Sea una secuencia de funciones holomorfas  $\langle f_n(z) \rangle_{n \geq 0}$  que en  $D$  convergen uniformemente a  $f(z)$ . Entonces  $f$  es holomorfa en  $D$ .*

Nótese que el resultado no se cumple para reales.

*Demostración.* Sea  $\gamma \subset D$  una curva cerrada simple. Del teorema de Cauchy sabemos:

$$\int_{\gamma} f_n(z) dz = 0$$

Por convergencia uniforme:

$$\int_{\gamma} f(z) dz = 0$$

El teorema de Morera, teorema 28.12, nos dice que la función  $f$  es holomorfa en  $D$ .  $\square$

### 28.7.1. Series

Una serie es simplemente la secuencia  $\langle s_n \rangle_{n \geq 0}$  resultante de sumar los elementos de una secuencia  $\langle a_n \rangle_{n \geq 0}$ , vale decir,  $s_n = a_0 + a_1 + \dots + a_n$ . Si la serie converge, debe ser  $\lim a_n = 0$ . Para el límite de la serie anotamos según nuestra convención sobre sumas:

$$\sum_{n \geq 0} a_n$$

o el más familiar:

$$\sum_{n=0}^{\infty} a_n$$

Igual que en el caso de series en los reales, es útil distinguir series que *convergen en valor absoluto*, vale decir la secuencia:

$$\sum_{0 \leq k \leq n} |a_k|$$

converge. Es simple demostrar que si la serie converge en valor absoluto, converge la serie original; pero la convergencia de la serie original no asegura convergencia en valor absoluto. Por ejemplo, tenemos la serie harmónica alterna (el valor lo justificaremos más adelante):

$$\sum_{k \geq 1} \frac{(-1)^{k+1}}{k} = \ln 2 \tag{28.28}$$

pero la contraparte de valores absolutos es la serie harmónica, que no converge. Incluso más:

**Teorema 28.22** (Reordenamiento de Riemann). *Sea una serie real que converge pero no absolutamente. Entonces sus términos pueden reordenarse para dar cualquier suma, e incluso diverger a  $\pm\infty$  o no tener límite.*

*Demostración.* Si la serie converge, pero no absolutamente, tiene infinitos términos positivos cuya suma diverge y de la misma forma tiene infinitos términos negativos cuya suma diverge. Fijemos un valor  $L$  cualquiera; consideraremos el caso en que  $L \geq 0$ , el caso  $L < 0$  es similar. Ordenamos los términos como sigue:

- Elegimos términos positivos hasta que la suma sobrepase a  $L$ . Como la suma de los términos positivos diverge, esto puede hacerse.
- Elegimos luego términos negativos hasta que la suma sea menor a  $L$ . Nuevamente, como los términos negativos divergen esto puede hacerse.

Repitiendo este proceso obtenemos un ordenamiento de los términos de la serie que converge a  $L$ . La diferencia entre la suma y el valor elegido va disminuyendo, como la serie original converge sabemos que los términos de la serie reordenada disminuyen en valor absoluto.

Siendo suficientemente tacaños con los términos negativos (respectivamente positivos) logramos que diverja; tomando dos valores podemos hacer oscilar los valores de la suma alrededor de ellos.  $\square$

De tales series se dice que *convergen condicionalmente*. Un ejemplo de este fenómeno es escribir la serie harmónica alterna ([28.28](#)) como:

$$\sum_{k \geq 1} \left( \frac{1}{2k-1} - \frac{1}{2(2k-1)} - \frac{1}{4k} \right) = \sum_{k \geq 1} \left( \frac{1}{2(2k-1)} - \frac{1}{2 \cdot 2k} \right) = \frac{1}{2} \sum_{k \geq 1} \frac{(-1)^{k+1}}{k} = \frac{1}{2} \ln 2 \quad (28.29)$$

Este es un reordenamiento correcto, aparecen los recíprocos de todos los impares con signo positivo y los recíprocos de todos los pares con signo negativo. La mitad del valor original ([28.28](#)).

En forma análoga podemos considerar series de funciones:

$$\sum_{k \geq 0} f_k(z)$$

Tales series pueden converger para ciertos valores de  $z$  y no para otros. Un criterio útil de convergencia es el siguiente:

**Teorema 28.23** (Prueba  $M$  de Weierstraß). *Sea  $\langle M_k \rangle_{k \geq 0}$  una secuencia de números reales, que hay  $K$  tal que  $M_k \geq 0$  para todo  $k > K$ , y suponga que la secuencia*

$$\left\langle \sum_{0 \leq k \leq n} M_k \right\rangle_{n \geq 0}$$

*converge. Si para todo  $z \in D$  es  $|f_k(z)| \leq M_k$  para  $k \geq K$ , la serie*

$$\sum_{k \geq 0} f_k(z)$$

*converge uniformemente en valor absoluto en  $D$ .*

*Demostración.* Sea  $\epsilon > 0$  cualquiera, y elegimos  $N > K$  tal que:

$$\sum_{m \leq k \leq n} M_k < \epsilon$$

para todo  $m, n > N$  (esto resulta del criterio de Cauchy). Por la desigualdad triangular, teorema 1.2, es:

$$\left| \sum_{m \leq k \leq n} f_k(z) \right| \leq \sum_{m \leq k \leq n} |f_k(z)| \leq \sum_{m \leq k \leq n} M_k < \epsilon$$

La serie converge. Para convergencia uniforme, observe que para todo  $z \in D$  y  $n > m > N$ :

$$\left| \sum_{m \leq k \leq n} f_k(z) \right| = \left| \sum_{0 \leq k \leq n} f_k(z) - \sum_{0 \leq k \leq m-1} f_k(z) \right| < \epsilon$$

En consecuencia:

$$\lim_{n \rightarrow \infty} \left| \sum_{m \leq k \leq n} f_k(z) \right| = \left| \sum_{k \geq 0} f_k(z) - \sum_{0 \leq k \leq m-1} f_k(z) \right| \leq \epsilon$$

y la convergencia es uniforme y en valor absoluto.  $\square$

El caso más interesante es el de series de potencias:

$$s_n(z) = \sum_{0 \leq k \leq n} c_k (z - z_0)^k$$

Una serie de potencias podrá tener un límite para ciertos valores de  $z$  y no para otros. Claramente siempre tiene límite si  $z = z_0$ .

**Teorema 28.24** (Cauchy-Hadamard). *Sea la serie:*

$$\sum_{0 \leq k \leq n} c_k (z - z_0)^k$$

*Sea:*

$$\lambda = \limsup_{k \rightarrow \infty} \sqrt[k]{|c_k|} \quad (28.30)$$

*Sea  $R = \lambda^{-1}$ , donde diremos que  $R = \infty$  si  $\lambda = 0$  y que  $R = 0$  si  $\lambda = \infty$ . Entonces la serie converge uniformemente en valor absoluto para todo  $|z - z_0| < r < R$  y diverge para todo  $|z - z_0| > R$ .*

*Demostración.* Primero demostramos que la serie no converge para  $|z - z_0| > R$ . Sea  $L$  tal que:

$$\frac{1}{|z - z_0|} < L < \frac{1}{R} = \lambda$$

Hay un número infinito de  $c_k$  tales que  $\sqrt[k]{|c_k|} > L$ , ya que de lo contrario el límite superior sería menor a  $L$ . Para cada uno de ellos tenemos:

$$|c_k (z - z_0)^k| = \left( \sqrt[k]{|c_k|} \cdot |z - z_0| \right)^k > (L|z - z_0|)^k > 1$$

y la serie no puede converger.

Enseguida demostramos que converge uniformemente para todo  $|z - z_0| < r < R$ . Sea  $L$  tal que:

$$\lambda = \frac{1}{R} < L < \frac{1}{r}$$

Para  $k$  suficientemente grande es  $\sqrt[k]{|c_k|} < L$ , con lo que si  $|z - z_0| \leq r$ :

$$|c_k (z - z_0)^k| = \left( \sqrt[k]{|c_k|} \cdot |z - z_0| \right)^k < (L|z - z_0|)^k < (Lr)^k$$

La serie geométrica de los  $(Lr)^k$  converge, y la prueba de  $M$  da convergencia uniforme en valor absoluto.  $\square$

Nótese que hemos demostrado que toda serie de potencias converge uniformemente en valor absoluto en el disco abierto  $D_R(z_0)$ , su *región de convergencia*; a  $R$  se le llama el *radio de convergencia* de la serie.

Ya que estamos en eso, explicitemos lo que el teorema 28.20 dice para series de potencias. La función  $g$  que introduciremos nos vendrá bien más adelante.

**Corolario 28.25.** *Suponga una serie de potencias  $\sum_{k \geq 0} c_k(z - z_0)^k$  con radio de convergencia  $R$ , y una curva suave  $\gamma \subset D_R(z_0)$ , y sea  $g(z)$  continua sobre  $\gamma$ . Entonces:*

$$\int_{\gamma} g(z) \sum_{k \geq 0} c_k(z - z_0)^k dz = \sum_{k \geq 0} c_k \int_{\gamma} g(z)(z - z_0)^k dz$$

En particular, si  $\gamma$  es cerrada:

$$\int_{\gamma} \sum_{k \geq 0} c_k(z - z_0)^k dz = 0$$

*Demuestra*ón. Sea  $\epsilon > 0$ , y sea  $M$  el máximo de  $g$  sobre  $\gamma$ , y  $l_{\gamma}$  el largo de la curva. Entonces hay un entero  $N$  tal que para  $n > N$ :

$$\left| \sum_{k \geq n} c_k(z - z_0)^k \right| < \frac{\epsilon}{M l_{\gamma}}$$

de donde:

$$\left| \int_{\gamma} g(z) \sum_{k \geq n} c_k(z - z_0)^k dz \right| < M l_{\gamma} \frac{\epsilon}{M l_{\gamma}} = \epsilon$$

Con esto:

$$\left| \int_{\gamma} g(z) \sum_{k \geq n} c_k(z - z_0)^k dz - \sum_{0 \leq k \leq n-1} c_k \int_{\gamma} g(z)(z - z_0)^k dz \right| = \left| \int_{\gamma} g(z) \sum_{k \geq n} c_k(z - z_0)^k dz \right| < \epsilon$$

Esto es lo que prometimos.  $\square$

Si elegimos  $g(z) = 1$ , tenemos que podemos integrar término a término dentro del radio de convergencia, y la serie define una función holomorfa dentro de  $D_R(z_0)$ . Si analizamos los términos de la serie, tenemos el siguiente:

**Corolario 28.26.** *Sean  $c_k$  los coeficientes de una serie de potencias con radio de convergencia  $R$ . Entonces para  $r < R$ :*

$$\lim_{k \rightarrow \infty} |c_k|r^k = 0$$

mientras para  $r > R$ :

$$\lim_{k \rightarrow \infty} |c_k|r^k = \infty$$

Nótese que esto nada dice sobre la convergencia o divergencia en la frontera de la región de convergencia. La manoseada serie:

$$\sum_{k \geq 1} \frac{z^k}{k} \tag{28.31}$$

tiene radio de convergencia 1. Si partimos con:

$$\frac{1}{1-z} = \sum_{k \geq 0} z^k \quad (28.32)$$

cuyo radio de convergencia es 1, obtenemos que su integral (vale decir, (28.31)) tiene el mismo radio de convergencia. Dentro del radio de convergencia converge a  $\text{Log}(1-z)$ ; como converge para  $z = -1$ , por continuidad converge a  $\ln 2$  para  $z = -1$ . Diverge para  $z = 1$ , donde resulta la serie harmónica.

Una forma más sencilla de usar del corolario 28.26 es la siguiente:

**Corolario 28.27.** *Sean  $c_k$  los coeficientes de una serie de potencias, con  $c_k \neq 0$  para  $k$  suficientemente grande. Entonces su radio de convergencia es:*

$$R = \lim_{k \rightarrow \infty} \frac{|c_{k+1}|}{|c_k|} \quad (28.33)$$

Vimos (teorema 28.21) que si una secuencia de funciones holomorfas converge uniformemente en una región, su límite es holomorfo. Aplicando esto a series de potencias:

**Corolario 28.28.** *Suponga  $f(z) = \sum_{k \geq 0} c_k(z - z_0)^k$  tiene radio de convergencia positivo  $R$ . Entonces  $f$  es holomorfa en  $D_R(z_0)$ .*

Series de potencias con radio de convergencia infinito representan funciones enteras. Podemos derivar término a término:

**Teorema 28.29.** *Suponga  $f(z) = \sum_{k \geq 0} c_k(z - z_0)^k$  tiene radio de convergencia positivo  $R$ . En  $D_R(z_0)$  tenemos:*

$$f'(z) = \sum_{k \geq 0} k c_k (z - z_0)^{k-1}$$

*Demostración.* Sea  $z$  un punto dentro de la región de convergencia, y sea  $C$  una circunferencia orientada positivamente centrada en  $z$  al interior de la región de convergencia. Defina:

$$g(\zeta) = \frac{1}{2\pi i(\zeta - z)^2}$$

Aplicamos el corolario 28.25 para concluir:

$$\begin{aligned} \int_C g(\zeta) f(\zeta) d\zeta &= \sum_{k \geq 0} c_k \int_C g(\zeta) (\zeta - z_0)^k d\zeta \\ \frac{1}{2\pi i} \int_C \frac{f(\zeta)}{(\zeta - z)^2} d\zeta &= \sum_{k \geq 0} c_k \frac{1}{2\pi i} \int_C \frac{(\zeta - z_0)^k}{(\zeta - z)^2} d\zeta \end{aligned}$$

La fórmula integral de Cauchy, teorema 28.15, da:

$$f'(z) = \sum_{k \geq 0} k c_k (z - z_0)^{k-1}$$

La expansión es válida dentro de la región de convergencia original. □

## 28.8. Series de Taylor y Laurent

Veamos ahora cómo construir series para una función holomorfa dada.

### 28.8.1. Serie de Taylor

**Teorema 28.30** (Serie de Taylor). *Suponga  $f$  holomorfa en el disco abierto  $D_R(z_0)$ . Entonces:*

$$f(z) = \sum_{k \geq 0} \frac{f^{(k)}(z_0)}{k!} (z - z_0)^k \quad (28.34)$$

Esta serie converge en  $D_R(z_0)$ .

*Demuestra*o. Sea  $z \in D_R(z_0)$ , y sea  $C$  una circunferencia de radio  $r$  alrededor de  $z$  dentro del disco abierto. Entonces  $0 < r < R$ . Para  $\zeta \in C$  podemos escribir:

$$\frac{1}{\zeta - z} = \frac{1}{(\zeta - z_0) - (z - z_0)} = \frac{1}{\zeta - z_0} \cdot \frac{1}{1 - \frac{z - z_0}{\zeta - z_0}} = \sum_{k \geq 0} \frac{(z - z_0)^k}{(\zeta - z_0)^{k+1}}$$

Esto es válido ya que  $(z - z_0)/(\zeta - z_0) < 1$ , y la convergencia es uniforme. Podemos integrar:

$$\begin{aligned} \int_C \frac{f(\zeta)}{\zeta - z_0} d\zeta &= \sum_{k \geq 0} \left( \int_C \frac{f(\zeta)}{(\zeta - z_0)^{k+1}} d\zeta \right) (z - z_0)^k \\ f(z) &= \frac{1}{2\pi i} \int_C \frac{f(\zeta)}{\zeta - z} d\zeta = \sum_{k \geq 0} \left( \frac{1}{2\pi i} \int_C \frac{f(\zeta)}{(\zeta - z_0)^{k+1}} d\zeta \right) (z - z_0)^k \\ &= \sum_{k \geq 0} \frac{f^{(k)}(z_0)}{k!} (z - z_0)^k \end{aligned} \quad \square$$

A una función que puede representarse localmente (en un disco abierto centrado en  $z_0$ ) mediante una serie de potencias convergente se le llama *analítica* (en  $z_0$ ). Vemos que es muy similar al concepto de holomorfismo en los complejos, lo que explica que comúnmente se usen intercambiablemente.

Vale la pena tomar un poco de distancia y recapitular lo que hemos demostrado.

- Si la función  $f$  es derivable en una región  $D$  de  $\mathbb{C}$ , tiene derivadas de todos los órdenes en  $D$ . Igualmente tiene antiderivadas de todos los órdenes en  $D$ .
- La integral de  $f$  es independiente del camino al interior de la región simple  $D$ , y el valor de la integral es la diferencia de los valores de una antiderivada en los puntos inicial y final.
- El valor de la función en un punto interior de  $D$  queda determinado por los valores en la frontera de  $D$ .
- Podemos representar la función  $f$  mediante su serie de Taylor (28.34) sobre un disco abierto  $\{z : |z - z_0| < R\}$ .
- La serie de Taylor de  $f$  converge uniformemente en valor absoluto a  $f$  para  $\{z : |z - z_0| \leq r < R\}$ , donde el radio de convergencia  $R$  está dado por (28.30) o (28.33).
- Una serie de potencias puede derivarse e integrarse término a término, resultando series con el mismo radio de convergencia. Las series resultantes igualmente convergen uniformemente en valor absoluto.
- La serie de potencias para  $f$  es única (si tenemos dos series de potencias que representan la misma función centradas en el mismo punto, tienen los mismos coeficientes).

### 28.8.2. Singularidades

Requeriremos un poco de jerga adicional. Si la función  $f$  es tal que:

$$f(z_0) = 0$$

decimos que  $z_0$  es un *cero* de  $f$ . Si  $m \in \mathbb{N}$  es tal que:

$$\lim_{z \rightarrow z_0} \frac{f(z)}{(z - z_0)^{m-1}} = 0 \text{ y } \lim_{z \rightarrow z_0} \frac{f(z)}{(z - z_0)^m} \neq 0$$

decimos que es un *cero de multiplicidad m*. En el caso  $m = 1$  se habla de *cero simple*.

Veamos cómo extender la representación de funciones para abarcar puntos en los que dejan de ser holomorfas, *singularidades* en las que la función no está definida. Estamos interesados en *singularidades aisladas*, vale decir, hay un disco abierto perforado (en inglés, *punctured disk*)  $\{z \in \mathbb{C} : 0 < |z - z_0| < R\}$  sobre el que la función  $f$  es holomorfa. Tenemos los siguientes casos, que detallaremos en lo que sigue:

**Singularidad removable:** Si existe:

$$\lim_{z \rightarrow z_0} f(z)$$

la singularidad es removable. Basta definir  $f(z_0)$  como el límite del caso, y asunto resuelto. Véase el teorema 28.31.

**Polo:** Si hay  $m \in \mathbb{N}$  tal que la función  $g$  definida por:

$$g(z) = (z - z_0)^m f(z)$$

cumple

$$\lim_{z \rightarrow z_0} g(z) \neq 0$$

y  $g$  es holomorfa en un entorno de  $z_0$ , decimos que  $f$  tiene un *polo* de orden  $m$  en  $z_0$ . Si  $m = 1$ , también se le llama *polo simple*.

Es claro que si  $f$  tiene un cero de multiplicidad  $m$  en  $z_0$ , entonces  $1/f(z)$  tiene un polo de multiplicidad  $m$  en ese punto.

**Singularidad esencial:** Si  $f$  tiene una singularidad en  $z_0$  que no es removable ni es un polo, es una *singularidad esencial*.

Una definición que será útil más adelante es la siguiente:

**Definición 28.8.** A una función  $f$  que es holomorfa sobre una región  $D$  salvo polos se le llama *meromorfa*.

Nótese que al conocer todas las derivadas de una función en un punto cualquiera, podemos expandirla en serie de Taylor alrededor de ese punto, y esta serie converge en el disco abierto centrado en ese punto y que llega a la singularidad más cercana. De esta forma, podemos *extender analíticamente* la función a nuevas áreas del plano, salvo que las singularidades formen un conjunto denso en alguna curva cerrada.

Algunos resultados al respecto son los siguientes:

**Teorema 28.31** (De Riemann sobre singularidades removibles). *Suponga que  $f$  es holomorfa sobre el disco abierto perforado  $\{z : 0 < |z - z_0| < R\}$ , y que*

$$\lim_{z \rightarrow z_0} (z - z_0) f(z) = 0$$

*Entonces  $f$  tiene una singularidad removable en  $z_0$ .*

*Demuestra.* Sea  $z$  un punto en el disco perforado  $\{z : 0 < |z - z_0| < R\}$ , y sean  $r_1$  y  $r_2$  tales que  $0 < r_1 < |z| < r_2$ , y sean  $C_1$  y  $C_2$  circunferencias de radios  $r_1$  y  $r_2$  respectivamente centradas en  $z_0$ , orientadas ambas en sentido positivo. La función:

$$g(\zeta) = \begin{cases} f'(\zeta) & \zeta = z \\ \frac{f(\zeta) - f(z)}{\zeta - z} & \zeta \neq z \end{cases}$$

claramente es holomorfa en  $\{\zeta : |\zeta - z_0| < R\}$ . Por el teorema de Cauchy:

$$\int_{C_1} g(\zeta) d\zeta = \int_{C_2} g(\zeta) d\zeta$$

De la definición de  $g$  esto significa:

$$\int_{C_1} \frac{f(\zeta)}{\zeta - z} d\zeta - f(z) \int_{C_1} \frac{1}{\zeta - z} d\zeta = \int_{C_2} \frac{f(\zeta)}{\zeta - z} d\zeta - f(z) \int_{C_2} \frac{1}{\zeta - z} d\zeta$$

En la región  $\{\zeta : |\zeta - z_0| < |z - z_0|\}$  (que incluye la curva  $C_1$  y su interior, pero excluye  $z$ ) es holomorfa la función:

$$\frac{1}{\zeta - z}$$

y por lo tanto:

$$\int_{C_1} \frac{1}{\zeta - z} d\zeta = 0$$

Por el otro lado, la fórmula integral de Cauchy aplicada a la función  $1 = 1(z)$  da:

$$\int_{C_2} \frac{1}{\zeta - z} d\zeta = 2\pi i$$

Por hipótesis, dado  $\epsilon > 0$  hay  $\delta > 0$  tal que si  $0 < |\zeta - z_0| < \delta$  entonces  $|(\zeta - z_0)f(\zeta)| < \epsilon$ . Sin perder generalidad podemos suponer:

$$\delta < \frac{1}{2} |z - z_0|$$

Si elegimos  $r_1 = \delta$ , por (28.22):

$$\left| \int_{C_1} \frac{f(\zeta)}{\zeta - z} d\zeta \right| \leq \left| \int_{C_1} \frac{(\zeta - z_0)f(\zeta)}{(\zeta - z_0)(\zeta - z)} d\zeta \right| \leq \frac{\epsilon}{\delta(|z - z_0| - \delta)} \cdot 2\pi\delta \leq \frac{4\pi\epsilon}{|z - z_0|}$$

Como  $\epsilon$  es arbitrario, la integral se anula. Concluimos:

$$f(z) = \frac{1}{2\pi i} \int_{C_2} \frac{f(\zeta)}{\zeta - z} d\zeta$$

Esta definición vale sobre el disco perforado  $\{z : 0 < |z - z_0| < R\}$ , pero la integral define una función holomorfa en  $\{z : |z - z_0| < R\}$ , con lo que definiendo  $f(z_0)$  mediante:

$$f(z_0) = \frac{1}{2\pi i} \int_{C_2} \frac{f(\zeta)}{\zeta - z_0} d\zeta$$

la función  $f$  es holomorfa en  $\{z : |z - z_0| < R\}$ , como prometimos.  $\square$

La condición del teorema 28.31 se cumple si  $|f(z)|$  es acotada. Como una función holomorfa es continua, si la singularidad es removible basta definir:

$$f(z_0) = \lim_{z \rightarrow z_0} f(z)$$

Cerca de singularidades esenciales las funciones se comportan en forma descontrolada. El gran teorema de Picard [284] (para demostración ver textos de análisis complejo, como el de Conway [77]) muestra que en todo entorno de la singularidad la función toma todos los valores posibles, salvo posiblemente uno. El resultado siguiente es mucho más restringido, pero también más fácil de demostrar:

**Teorema 28.32** (Casorati-Weierstraß). *Sea  $f$  holomorfa en el disco perforado  $\{z : 0 < |z - z_0| < R\}$ , con una singularidad esencial en  $z_0$ . Entonces dado cualquier  $w \in \mathbb{C}$  y números reales arbitrarios  $\epsilon > 0$  y  $\delta > 0$  hay  $z$  en el disco perforado tal que*

$$0 < |z - z_0| < \delta \text{ y } |f(z) - w| < \epsilon$$

*Demostración.* Por contradicción. Suponga que hay  $w \in \mathbb{C}$ ,  $\epsilon > 0$  y  $\delta > 0$  tales que  $|f(z) - w| \geq \epsilon$  siempre que  $0 < |z - z_0| < \delta$ . Entonces la función

$$g(z) = \frac{1}{f(z) - w}$$

es holomorfa y acotada en el disco perforado  $\{z : 0 < |z - z_0| < \delta\}$ , con una singularidad removible en  $z_0$  (teorema 28.31). Definiendo  $g(z_0)$  apropiadamente,  $g(z)$  es holomorfa en  $\{z : |z - z_0| < \delta\}$ , y no es idénticamente cero en este disco. Note que:

$$f(z) = w + \frac{1}{g(z)}$$

con lo que si  $g(z_0) \neq 0$ ,  $f$  es derivable en  $z_0$ ; si  $g(z_0) = 0$  entonces  $f$  tiene un polo en  $z_0$ . Esto contradice la hipótesis de que  $f$  tiene una singularidad esencial en  $z_0$ .  $\square$

Un par de ejemplos servirán para clarificar el tema. La función  $e^{1/z}$  es holomorfa en todo  $\mathbb{C}$  salvo en  $z = 0$ , que es una singularidad aislada. Si nos restringimos al eje real, vemos que:

$$\lim_{x \rightarrow 0^+} e^{1/x} = \lim_{u \rightarrow \infty} e^u = \infty$$

y la singularidad no es removable. Por otro lado, para  $n \in \mathbb{N}$ :

$$\lim_{x \rightarrow 0^+} x^n e^{1/x} = \lim_{u \rightarrow \infty} \frac{e^u}{u^n} = \infty$$

y tampoco es un polo. En consecuencia, es una singularidad esencial.

Analicemos ahora la función:

$$f(z) = \frac{e^z - 1}{z(z - 1)}$$

Es claro que tiene singularidades aisladas en  $z = 0$  y  $z = 1$ . En  $z = 1$  tiene un polo simple, ya que:

$$g(z) = (z - 1)f(z) = \frac{e^z - 1}{z}$$

y  $g(1) = e - 1 \neq 0$ . La singularidad en  $z = 0$  es removable, ya que por la regla de l'Hôpital:

$$\lim_{z \rightarrow 0} \frac{e^z - 1}{z(z-1)} = \lim_{z \rightarrow 0} \frac{e^z}{2z-1} = -1$$

Podemos analizar lo que ocurre en  $\infty$  considerando  $f(1/z)$ , que tiene una singularidad aislada en 0. Según el comportamiento, diremos que  $f$  tiene una singularidad removable, un polo o una singularidad esencial en  $\infty$ . Primeramente, el límite:

$$\lim_{|z| \rightarrow \infty} \frac{e^z - 1}{z(z-1)}$$

no existe, ya que:

$$\lim_{x \rightarrow \infty} \frac{e^x - 1}{x(x-1)} = \infty \quad \lim_{x \rightarrow -\infty} \frac{e^x - 1}{x(x-1)} = 0$$

O sea, la singularidad no es removable. Enseguida, para  $n \in \mathbb{N}$  cualquiera, no existe el límite:

$$\lim_{|z| \rightarrow \infty} \frac{e^z - 1}{z^{n+1}(z-1)}$$

porque:

$$\lim_{x \rightarrow \infty} \frac{e^x - 1}{x^{n+1}(x-1)} = \infty \quad \lim_{x \rightarrow -\infty} \frac{e^x - 1}{x^{n+1}(x-1)} = 0$$

Por tanto, al no ser removable ni un polo, es una singularidad esencial.

Es simple demostrar que si  $\lim_{|z| \rightarrow \infty} |f(z)| = \infty$ , entonces  $f$  es entera si y solo si es un polinomio. O sea, una función entera que no es un polinomio tiene una singularidad esencial en  $\infty$ . Supongamos que  $f$  tiene un polo de orden  $m$  en  $\infty$ . Restando un polinomio  $p$  de  $f$ , de ser necesario, podemos arreglar que  $f(z) - p(z)$  tenga un cero de orden  $m$  en 0. Claramente  $p$  tiene grado a lo más  $m$ . La función:

$$g(z) = \frac{f(z) - p(z)}{z^m}$$

es entera y acotada, con lo que por el teorema de Liouville (teorema 28.18) es constante. Entonces  $f$  es un polinomio.

La función tangente se define como:

$$\tan z = \frac{\sin z}{\cos z}$$

Esta función tiene singularidades no removibles en los ceros de  $\cos z$ , que son  $(k + 1/2)\pi$  para  $k \in \mathbb{Z}$ . Por l'Hôpital vemos que:

$$\lim_{z \rightarrow (k + \frac{1}{2})\pi} \frac{\cos z}{z - (k + \frac{1}{2})\pi} = \lim_{z \rightarrow (k + \frac{1}{2})\pi} -\sin z = -1$$

Como los ceros de  $\cos z$  son simples, las singularidades mencionadas son polos simples. La singularidad en  $\infty$  no es aislada, ya que todo entorno de  $z = 0$  de  $\tan 1/z$  contiene infinitas singularidades (no hay  $R$  tal que  $\tan 1/z$  es holomorfa en  $\{z: R < |z| < \infty\}$ ).

### 28.8.3. Series de Laurent

Supongamos la función  $f$  holomorfa en el disco perforado  $\{z: 0 < |z - z_0| < R\}$ , con un polo de orden  $m$  en  $z_0$ . De la discusión precedente esto significa que la función siguiente es holomorfa en  $\{z: |z - z_0| < R\}$ :

$$g(z) = (z - z_0)^m f(z)$$

Como es holomorfa, tiene una serie de Taylor, lo que significa que podemos escribir:

$$f(z) = \sum_{k \geq 0} \frac{g^{(k)}(z_0)}{k!} (z - z_0)^{k-m} \quad (28.35)$$

A la expresión:

$$\frac{g(z_0)}{(z - z_0)^m} + \frac{g'(z_0)}{(z - z_0)^{m-1}} + \frac{g''(z_0)}{2!(z - z_0)^{m-2}} + \cdots + \frac{g^{(m-1)}(z_0)}{(m-1)!(z - z_0)} \quad (28.36)$$

se le llama la *parte principal* de la serie (28.35), que se anota  $\text{pp}(f; z_0)$ .

Nos interesa formalizar y extender lo anterior.

**Teorema 28.33.** *Sea  $f$  una función holomorfa en el disco perforado  $\{z: 0 < |z - z_0| < R\}$ , con una singularidad aislada en  $z_0$ . Entonces existen funciones únicas  $f_1$  y  $f_2$  tales que:*

- (a)  $f(z) = f_1(z) + f_2(z)$  en  $\{z: 0 < |z - z_0| < R\}$
- (b)  $f_1$  es holomorfa en  $\mathbb{C}$ , excepto posiblemente en  $z_0$
- (c)  $f_1(z) \rightarrow 0$  cuando  $|z| \rightarrow \infty$
- (d)  $f_2$  es holomorfa en  $\{z: |z - z_0| < R\}$

*Demostración.* Comenzamos como la demostración del teorema 28.31. Sea  $z$  un punto en el disco perforado  $\{z: 0 < |z - z_0| < R\}$ , y sean  $0 < r_1 < |z - z_0| < r_2 < R$ . Sean además  $C_1$  y  $C_2$  las circunferencias de radios  $r_1$  y  $r_2$  respectivamente alrededor de  $z_0$ . Obtenemos:

$$f(z) = \frac{1}{2\pi i} \int_{C_2} \frac{f(\zeta)}{\zeta - z} d\zeta - \frac{1}{2\pi i} \int_{C_1} \frac{f(\zeta)}{\zeta - z} d\zeta$$

Defina entonces:

$$f_1(z) = -\frac{1}{2\pi i} \int_{C_1} \frac{f(\zeta)}{\zeta - z} d\zeta \quad f_2(z) = \frac{1}{2\pi i} \int_{C_2} \frac{f(\zeta)}{\zeta - z} d\zeta$$

La parte (a) es inmediata. Para la parte (d), la función  $f_2$  definida por la integral es holomorfa en el disco  $\{z: |z - z_0| < r_2\}$  (como en el teorema 28.31). Para (b), la función  $f_2$  es holomorfa en el anillo  $\{z: r_1 < |z - z_0| < r_2\}$ . Como  $f$  y  $f_2$  no dependen de  $r_1$ , tampoco depende de  $r_1$  la función  $f_1(z) = f(z) - f_2(z)$ . Tampoco depende de  $r_2$  la función  $f_2$ , por un razonamiento similar. Se ve que:

$$\lim_{|z| \rightarrow \infty} \int_{C_1} \frac{f(\zeta)}{\zeta - z} d\zeta = 0$$

que es la parte (c). Para demostrar que  $f_1$  y  $f_2$  son únicas, suponga funciones  $g_1$  y  $g_2$  con las mismas propiedades en el disco perforado  $\{z: 0 < |z - z_0| < R\}$ , con lo que allí:

$$f_1(z) - g_1(z) = g_2(z) - f_2(z)$$

Defina:

$$F(z) = \begin{cases} g_2(z) - f_2(z) & |z - z_0| < R \\ g_1(z) - f_1(z) & |z - z_0| \geq R \end{cases}$$

Entonces  $F$  es entera. Pero por la parte (c)  $F(z) \rightarrow 0$  cuando  $|z| \rightarrow \infty$ , con lo que  $F$  es acotada. Por el teorema de Liouville,  $F(z)$  es constante, igual al límite mencionado antes; con lo que  $F(z) = 0$  para todo  $z \in \mathbb{C}$ , y las funciones coinciden.  $\square$

Estamos en condiciones de completar nuestro ejemplo inicial.

**Teorema 28.34** (Serie de Laurent). *Sea  $f$  holomorfa en el disco perforado  $\{z : 0 < |z - z_0| < R\}$ , con una singularidad aislada en  $z_0$ . Sea  $C$  una circunferencia de radio  $r$ , donde  $0 < r < R$ , y para cada  $n \in \mathbb{Z}$  sea*

$$a_n = \frac{1}{2\pi i} \int_C \frac{f(z)}{(z - z_0)^{n+1}} dz \quad (28.37)$$

Entonces la serie

$$f(z) = \sum_n a_n (z - z_0)^n \quad (28.38)$$

converge en el disco perforado  $\{z : 0 < |z - z_0| < R\}$ . Más aún, la convergencia es uniforme en todo anillo  $\{z : r_1 < |z - z_0| < r_2\}$ , donde  $0 < r_1 < r_2 < R$ .

Nótese que la convergencia uniforme de la serie en el anillo  $\{z : r_1 < |z - z_0| < r_2\}$  significa que para todo  $\epsilon > 0$  existe  $N_0 = N_0(\epsilon, r_1, r_2)$ , independiente de  $z$ , tal que si  $N_1 \geq N_0$  y  $N_2 \geq N_0$ :

$$\left| f(z) - \sum_{-N_1 \leq n \leq N_2} a_n (z - z_0)^n \right| < \epsilon$$

A la serie (28.38) se la llama la *serie de Laurent* de  $f$  alrededor de  $z_0$ .

*Demostración.* El primer paso es demostrar que la serie (28.38) converge uniformemente a  $f(z)$  sobre la circunferencia  $C$  centrada en  $z_0$  de radio  $r$ , donde  $0 < r < R$ , y los coeficientes están dados por (28.37). Suponga  $n \in \mathbb{Z}$  dado y fijo. Para cualquier  $\epsilon > 0$  podemos elegir  $N_1$  y  $N_2$  suficientemente grandes para que  $-N_1 \leq n \leq N_2$  y tal que para todo  $z \in C$ :

$$\left| f(z) - \sum_{-N_1 \leq k \leq N_2} a_k (z - z_0)^k \right| < \epsilon$$

Por la cota (28.22) es:

$$\left| \frac{1}{2\pi i} \int_C \left( f(z) - \sum_{-N_1 \leq k \leq N_2} a_k (z - z_0)^k \right) \frac{1}{(z - z_0)^n} dz \right| < \frac{\epsilon}{r^n}$$

Como:

$$\frac{1}{2\pi i} \int_C (z - z_0)^k dz = [k = -1]$$

resulta:

$$\frac{1}{2\pi i} \int_C \left( \sum_{-N_1 \leq k \leq N_2} a_k (z - z_0)^k \right) \frac{1}{(z - z_0)^{n+1}} dz = a_n$$

Esto permite simplificar:

$$\left| \frac{1}{2\pi i} \int_C \frac{f(z)}{(z - z_0)^{n+1}} dz - a_n \right| < \frac{\epsilon}{r^n}$$

Como  $\epsilon$  es arbitrario, resulta (28.37).

Queda por demostrar que la representación (28.38) vale en el disco perforado  $\{z: 0 < |z - z_0| < R\}$ , y que la convergencia es uniforme en todo anillo  $\{z: r_1 < |z - z_0| < r_2\}$  con  $0 < r_1 < r_2 < R$ . Suponga  $r_1 < r < r_2$ . Por el teorema 28.33 podemos escribir  $f(z) = f_1(z) + f_2(z)$  donde  $f_1$  y  $f_2$  son únicas y cumplen las condiciones (a) a (d). Como  $f_2$  es holomorfa en el disco  $\{z: |z - z_0| < R\}$ , su serie de Taylor:

$$f_2(z) = \sum_{n \geq 0} A_n (z - z_0)^n$$

converge en el disco  $\{z: |z - z_0| < R\}$ , uniformemente en el disco  $\{z: |z - z_0| < r_2\}$ . Para estudiar  $f_1$ , efectuamos el cambio de variables:

$$w = \frac{1}{z - z_0} \quad z = z_0 + \frac{1}{w}$$

La función:

$$f_1(z) = f_1\left(\frac{1}{w} + z_0\right)$$

es entera en  $w$ , con lo que la serie de Taylor:

$$f_1\left(\frac{1}{w} + z_0\right) = \sum_{m \geq 1} B_m w^m$$

converge en  $\mathbb{C}$ , uniformemente en el disco cerrado  $\{w: |w| \leq 1/r_1\}$ . El coeficiente  $B_0$  se anula. Es el valor de  $f_1$  en  $w = 0$ , vale decir  $z = \infty$ ; y por la parte (c) del teorema 28.33 esto se anula. Combinando las series para  $f_1$  en términos de  $z - z_0$  y para  $f_2$  resulta lo prometido.  $\square$

El tipo de singularidad aislada es sencillo de ver de los coeficientes de la serie de Laurent (28.38):

**Corolario 28.35.** *Sea  $f$  holomorfa en el disco perforado  $\{z: 0 < |z - z_0| < R\}$ , y serie de Laurent dada por (28.38) con coeficientes  $a_n$  como en (28.37). Entonces:*

- (a) *La función  $f$  es diferenciable en  $z_0$  o tiene una singularidad removable si y solo si  $a_n = 0$  para todo  $n < 0$*
- (b) *La función  $f$  tiene un polo si y solo si un número finito pero no nulo de coeficientes  $a_n$  con  $n$  negativo son diferentes de cero*
- (c) *La función  $f$  tiene una singularidad esencial si y solo si un número infinito de coeficientes  $a_n$  con  $n$  negativo son diferentes de cero*

*Demostración.* Para la parte (a), sabemos que si  $f$  tiene una singularidad removable en  $z_0$ , podemos hacerla holomorfa definiendo  $f(z_0)$  adecuadamente. Y la función holomorfa tiene serie de Taylor, vale decir, sin términos de índice negativo.

Para la parte (b), si solo un número finito de coeficientes de índice negativo no se anulan, habrá  $m > 0$  tal que  $a_{-m} \neq 0$  pero  $a_n = 0$  para todo  $n < -m$ . En tal caso:

$$f(z) = \sum_{n \geq -m} a_n (z - z_0)^n$$

de forma que:

$$g(z) = (z - z_0)^m f(z)$$

es holomorfa en un entorno de  $z_0$ , y  $g(z_0) = a_{-m} \neq 0$ , y  $f$  tiene un polo de orden  $m$  en  $z_0$ .

La parte (c) resulta por no ser (a) ni (b).  $\square$

Como la serie de Laurent es única, podemos usar técnicas alternativas a la fórmula (28.37) para obtener los coeficientes. Por ejemplo, de la sustitución  $w = 1/z$  en la serie para  $e^w$  tenemos directamente:

$$e^{1/z} = \sum_{n \geq 0} \frac{1}{n! z^n}$$

Nuevamente concluimos que la singularidad en  $z = 0$  de esta función es esencial.

#### 28.8.4. Residuos

Al calcular la integral sobre una curva cerrada simple que encierra una región en la que el integrando no es holomorfo, el resultado no siempre es cero. Primeramente tenemos:

**Lema 28.36.** *Sea  $f$  una función holomorfa en la región conexa simple  $D$ , excepto una singularidad aislada en  $z_0$ , y sea:*

$$f_1(z) = \sum_{n \leq -1} a_n (z - z_0)^n$$

*la parte principal de la serie de Laurent de  $f$  en  $z_0$ . Sea también  $\gamma \subset D$  una curva cerrada simple suave que se sigue en la dirección positiva, que no pasa por  $z_0$ . Entonces:*

$$\frac{1}{2\pi i} \int_{\gamma} f(\zeta) d\zeta = \begin{cases} a_{-1} & \text{si } z_0 \text{ está en el interior de } \gamma \\ 0 & \text{si } z_0 \text{ está en el exterior de } \gamma \end{cases}$$

*Demostración.* Si  $z_0$  está al exterior de  $\gamma$ , vemos que  $\gamma$  es holomorfa a un punto en  $D$ , y la integral es cero.

En caso que  $z_0$  esté al interior de  $\gamma$ , la integral no es más que el coeficiente  $a_{-1}$  de la serie de Laurent según (28.37).  $\square$

Al coeficiente  $a_{-1}$  se le llama el *residuo* de  $f$  en  $z_0$ , y se anota  $a_{-1} = \text{res}(f, z_0)$ .

Con esto podemos demostrar una forma simple del teorema de residuos de Cauchy.

**Teorema 28.37** (De residuos de Cauchy). *Sea  $f$  holomorfa, salvo singularidades aisladas  $z_1, \dots, z_n$ , en la región simple conexa  $D$ , y  $\gamma \subset D$  una curva cerrada simple trazada en dirección positiva. Entonces:*

$$\int_{\gamma} f(z) dz = \sum_{\substack{1 \leq k \leq n \\ z_k \text{ interior a } \gamma}} \text{res}(f, z_k) \quad (28.39)$$

*Demostración.* Sea  $f_k(z)$  la parte principal de  $f(z)$  en  $z_k$ . Por el teorema 28.33 sabemos que  $f_k$  es holomorfa excepto en  $z_k$ , por lo que la función:

$$g(z) = f(z) - \sum_{1 \leq k \leq n} f_k(z)$$

es holomorfa en  $D$ . Aplicando el lema 28.36 resulta:

$$\int_{\gamma} f(z) dz = \int_{\gamma} g(z) dz + \sum_{1 \leq k \leq n} \int_{\gamma} f_k(z) dz = 0 + \sum_{\substack{1 \leq k \leq n \\ z_k \text{ interior a } \gamma}} \text{res}(f_k, z_k) = \sum_{\substack{1 \leq k \leq n \\ z_k \text{ interior a } \gamma}} \text{res}(f, z_k) \quad \square$$

Para que esto resulte útil, requerimos formas de calcular el residuo de  $f$  en una singularidad  $z_0$ . Si la singularidad es removable,  $f$  tiene una serie de Taylor alrededor de  $z_0$ , y el residuo es cero. Enseguida, si  $z_0$  es un polo simple de  $f$ , entonces tiene serie de Laurent:

$$f(z) = \frac{a_{-1}}{z - z_0} + g(z)$$

La función  $g(z)$  está representada por una serie de Taylor, con lo que es holomorfa en un disco centrado en  $z_0$ , y  $\lim_{z \rightarrow z_0} (z - z_0)g(z) = 0$ . O sea:

$$a_{-1} = \lim_{z \rightarrow z_0} (z - z_0)f(z)$$

Una forma alternativa útil es la siguiente: Suponga que  $f(z) = g(z)/h(z)$ , donde  $g$  y  $h$  son holomorfas,  $g(z_0) \neq 0$  y  $h$  tiene un cero simple en  $z_0$ . Entonces, como  $h(z_0) = 0$ :

$$\lim_{z \rightarrow z_0} (z - z_0) \frac{g(z)}{h(z)} = \frac{\lim_{z \rightarrow z_0} g(z)}{\lim_{z \rightarrow z_0} \frac{h(z) - h(z_0)}{z - z_0}} = \frac{g(z_0)}{h'(z_0)}$$

Si  $z_0$  es un polo de orden  $m$  de  $f$ , tenemos:

$$f(z) = \frac{a_{-m}}{(z - z_0)^m} + \frac{a_{-m+1}}{(z - z_0)^{m-1}} + \cdots + \frac{a_{-1}}{z - z_0} + g(z)$$

Entonces es holomorfa:

$$(z - z_0)^m f(z) = a_{-m} + a_{-m+1}(z - z_0) + \cdots + a_{-1}(z - z_0)^{m-1} + (z - z_0)^m g(z)$$

Derivando  $m - 1$  veces:

$$\frac{d^{m-1}}{dz^{m-1}} ((z - z_0)^m f(z)) = a_{-1}(m - 1)! + \frac{d^{m-1}}{dz^{m-1}} ((z - z_0)^m g(z))$$

Como  $g$  es holomorfa, el segundo término tiende a 0 cuando  $z \rightarrow z_0$ :

$$a_{-1} = \frac{1}{(m - 1)!} \lim_{z \rightarrow z_0} \frac{d^{m-1}}{dz^{m-1}} ((z - z_0)^m f(z))$$

Un resultado que requeriremos más adelante es el siguiente. Para  $0 < \alpha < 1$  tenemos la integral real:

$$\int_{-\infty}^{\infty} \frac{e^{\alpha x}}{1 + e^x} dx = \frac{\pi}{\sin \pi \alpha} \quad (28.40)$$

Usamos como contorno el rectángulo con vértices en  $-R, R, R + 2\pi i, -R + 2\pi i$ , luego haremos tender  $R \rightarrow \infty$ . El numerador del integrando es una función entera, el denominador tiene un único cero simple en  $z = \pi i$  dentro de la curva:

$$\text{res}\left(\frac{e^{\alpha z}}{1 + e^z}, \pi i\right) = \frac{e^{\alpha \pi i}}{e^{\pi i}} = -e^{\alpha \pi i}$$

Veamos las integrales sobre los lados del rectángulo. Sea  $I_R$  la integral que nos interesa, a lo largo del eje real desde  $-R$  a  $R$ ; y similarmente  $I$  la integral de interés. La integral a lo largo del lado superior del rectángulo (recordar que estamos integrando de derecha a izquierda) es:

$$-e^{2\pi i \alpha} I_R$$

Finalmente, para el lado derecho  $V_R = \{R + it : 0 \leq t \leq 2\pi\}$  resulta:

$$\left| \int_{V_R} \frac{e^{\alpha z}}{1 + e^z} dz \right| \leq \int_0^{2\pi} \left| \frac{e^{\alpha(R+it)}}{1 + e^{R+it}} dt \right| \leq \int_0^{2\pi} e^{R(\alpha-1)t} \cdot |e^{(\alpha-1)it}| dt \leq Ce^{R(\alpha-1)}$$

Como  $\alpha < 1$ , esto tiende a 0 al tender  $R$  a infinito. El lado izquierdo es casi lo mismo. Por el teorema de residuos:

$$\begin{aligned} I - e^{2\alpha\pi i} I &= -2\pi i e^{\alpha\pi i} \\ I &= -2\pi i \frac{e^{\alpha\pi i}}{1 - e^{2\alpha\pi i}} = \frac{2\pi i}{e^{\alpha\pi i} - e^{-\alpha\pi i}} = \frac{\pi}{\sin \alpha\pi} \end{aligned}$$

### 28.8.5. Principio del argumento

Aplicado adecuadamente, el teorema de residuos de Cauchy (teorema 28.37) permite calcular el número de ceros y de polos de funciones meromorfas.

**Lema 28.38.** *Sea  $f$  holomorfa en un entorno de  $z_0$ , donde tiene un cero de multiplicidad  $m$ . Entonces la función  $f'(z)/f(z)$  es holomorfa en un entorno perforado de  $z_0$ , con un polo simple en  $z_0$  con residuo  $m$ .*

**Lema 28.39.** *Sea  $f$  holomorfa en un entorno de  $z_0$ , donde tiene un polo de multiplicidad  $m$ . Entonces la función  $f'(z)/f(z)$  es holomorfa en un entorno perforado de  $z_0$ , con un polo simple en  $z_0$  con residuo  $-m$ .*

*Demostración del lema 28.38.* Podemos escribir  $f(z) = (z - z_0)^m g(z)$ , con  $g$  holomorfa en un entorno de  $z_0$  y  $g(z_0) \neq 0$ . Entonces:

$$\frac{f'(z)}{f(z)} = \frac{m(z - z_0)^{m-1}g(z) + (z - z_0)^m g'(z)}{(z - z_0)^m g(z)} = \frac{m}{z - z_0} + \frac{g'(z)}{g(z)}$$

El segundo término es holomorfo en el entorno de  $z_0$  y tenemos lo prometido.  $\square$

*Demostración del lema 28.39.* Podemos escribir  $f(z) = (z - z_0)^{-m} g(z)$ , con  $g$  holomorfa en un entorno de  $z_0$  y  $g(z_0) \neq 0$ . Entonces:

$$\frac{f'(z)}{f(z)} = \frac{-m(z - z_0)^{-m-1}g(z) + (z - z_0)^{-m}g'(z)}{(z - z_0)^{-m}g(z)} = \frac{-m}{z - z_0} + \frac{g'(z)}{g(z)}$$

El segundo término es holomorfo en el entorno de  $z_0$  y tenemos lo prometido.  $\square$

Uniendo los lemas 28.38 y 28.39 resulta:

**Teorema 28.40** (Principio del argumento). *Sea  $f$  meromorfa en la región  $D$ , y  $\gamma \subset D$  una curva cerrada simple trazada en dirección positiva, y tal que no hayan ceros ni polos de  $f$  sobre  $\gamma$ . Sea  $N$  el número de ceros de  $f$  al interior de  $\gamma$ , contados con sus multiplicidades; y análogamente  $P$  el número de polos de  $f$  al interior de  $\gamma$ , contados con sus multiplicidades. Entonces:*

$$\frac{1}{2\pi i} \int_{\gamma} \frac{f'(z)}{f(z)} dz = N - P \tag{28.41}$$

El nombre del teorema (28.40) viene de lo siguiente:

$$\int_{\gamma} \frac{f'(z)}{f(z)} dz$$

es la variación del logaritmo de  $f(z)$  al trazar  $\gamma$ , como  $\gamma$  es cerrada esto es únicamente la variación del argumento de  $f$  en unidades de  $2\pi i$ .

Para aplicación concreta del principio del argumento al contar ceros el resultado siguiente permite obviar el principio mismo, o al menos aplicarlo a una función más simple.

**Teorema 28.41** (Rouché). *Sean  $f$  y  $g$  holomorfas en  $D$ , y sea  $\gamma \subset D$  una curva conexa simple. Suponga además que  $|f(z)| > |g(z)|$  sobre  $\gamma$ . Entonces el número de ceros de  $f$  y  $f + g$  al interior de  $\gamma$  es el mismo.*

La demostración que daremos se debe a Chen [72].

*Demostración.* Para  $\tau \in [0, 1]$  defina:

$$N(\tau) = \int_{\gamma} \frac{f'(z) + \tau g'(z)}{f(z) + \tau g(z)} dz$$

Como en  $\gamma$  es  $|f(z)| > |g(z)|$ , esto asegura:

$$|f(z) + \tau g(z)| \geq |f(z)| - \tau |g(z)| \geq |f(z)| - |g(z)| > 0$$

de forma que  $f + \tau g$  no tiene ceros sobre  $\gamma$ , con lo que  $N(\tau)$  es continua. Siendo entero el valor, la única posibilidad es que  $N(\tau)$  sea constante. Pero  $N(0)$  es el número de ceros de  $f$  al interior de  $\gamma$ , y  $N(1)$  el número de ceros de  $f + g$ .  $\square$

## 28.9. Aplicaciones discretas

Para ir a nuestro tema, veremos algunas aplicaciones discretas del análisis complejo.

### 28.9.1. Sumas infinitas

Para mostrar la técnica general, veamos un par de ejemplos.

Consideremos la función:

$$f(z) = \frac{\pi \cot \pi z}{z^2}$$

Esta función tiene singularidades en  $z = k$  para todo  $k \in \mathbb{Z}$  (sin  $\pi z$  tiene ceros simples allí). En  $z = 0$  es un polo de orden 3, los demás son polos simples. En el origen:

$$\text{res}(f, 0) = \frac{1}{2!} \lim_{z \rightarrow 0} \frac{d^2}{dz^2} z^3 f(z) = -\frac{\pi^2}{3}$$

Para los demás polos:

$$\text{res}(f, k) = \frac{\pi \cos k\pi}{k^2 \pi \cos k\pi + 2k \sin k\pi} = \frac{1}{k^2}$$

Nuestra estrategia será hallar una curva que encierre todas las singularidades de interés de  $f$ , y sobre la cual sea sencillo calcular la integral (o demostrar que dicha integral tiende a cero). Elegir adecuadamente la curva es un arte, no hay recetas simples. Con eso tenemos la suma.

Una curva simple de manejar es  $\gamma_n$ , el cuadrado con esquinas en  $\pm(n + 1/2) \pm i(n + 1/2)$ . Es importante mantenerse alejado de los polos, ya que en ellos la función tiende a infinito y acotar la integral sobre un camino que pase cerca de un polo será complicado.

Otras alternativas populares son circunferencias centradas en el origen cuyo radio tiende a infinito, y también semicircunferencias (en el semiplano imaginario positivo o negativo) completadas con el eje  $x$ .

Consideremos la función  $\cot z$  para  $z = x + iy$ . Podemos expresar:

$$\cot z = \frac{\cos x \cosh y - i \sin x \sinh y}{\sin x \cosh y + i \cos x \sinh y} \quad (28.42)$$

En los lados verticales del cuadrado es  $\cos x = 0$ , con lo que  $\sin x = 1$  y (28.42) queda:

$$\begin{aligned} \cot z &= \frac{-i \sinh y}{\cosh y} = -i \tanh y \\ |\cot z| &= |\tanh y| \leq 1 \end{aligned} \quad (28.43)$$

Obtenemos la cota:

$$\left| \int_{\text{vertical}} f(z) dz \right| \leq \max(|f(z)|) \cdot (2n+1) \leq \frac{1}{(n+1/2)^2} \cdot (2n+1)$$

En los lados horizontales escribimos:

$$|\cot z|^2 = \frac{\cos^2 x \cosh^2 y + \sin^2 x \sinh^2 y}{\sin^2 x \cosh^2 y + \cos^2 x \sinh^2 y}$$

Por (28.42) podemos expresar:

$$\begin{aligned} |\cot z|^2 &= \frac{\cos^2 x \cosh^2 y + \sin^2 x \sinh^2 y}{\sin^2 x \cosh^2 y + \cos^2 x \sinh^2 y} \\ &= \frac{\cos^2 x \cosh^2 y + (1 - \cos^2 x)(\cosh^2 y - 1)}{(1 - \cos^2 x) \cosh^2 y + \cos^2 x (\cosh^2 y - 1)} \\ &= 1 + \frac{2 \cos^2 x - 1}{\cosh^2 y - \cos^2 x} \end{aligned}$$

Como cuando  $y \rightarrow \pm\infty$  también  $\cosh y \rightarrow \infty$ , para  $y$  suficientemente grande es:

$$|\cot z| \leq 2 \quad (28.44)$$

Con este entendido resulta la cota:

$$\left| \int_{\text{horizontal}} f(z) dz \right| \leq \max(|f(z)|) \cdot (2n+1) \leq \frac{2}{(n+1/2)^2} \cdot (2n+1)$$

Uniendo las anteriores tenemos la cota para la integral sobre  $\gamma_n$ :

$$\left| \int_{\gamma_n} f(z) dz \right| \leq 2 \cdot \frac{1}{(n+1/2)^2} \cdot (2n+1) + 2 \cdot \frac{2}{(n+1/2)^2} \cdot (2n+1) = \frac{24}{2n+1}$$

Esto tiende a cero cuando  $n \rightarrow \infty$ . Por lo tanto:

$$\begin{aligned} \lim_{n \rightarrow \infty} \int_{\gamma_n} f(z) dz &= 0 \\ \sum_{k \in \mathbb{Z}} \operatorname{res}(f, k\pi) &= 0 = -\frac{\pi^2}{3} + 2 \sum_{k \geq 1} \frac{1}{k^2} \end{aligned}$$

De acá:

$$\sum_{k \geq 1} \frac{1}{k^2} = \frac{\pi^2}{6} \quad (28.45)$$

Otra solución al problema de Basilea. El mismo método entrega valores para  $\zeta(2n)$  para todo  $n$ .

Consideremos ahora la función:

$$f(z) = \frac{\pi \csc \pi z}{z^2}$$

Nuevamente tenemos singularidades aisladas en  $z \in \mathbb{Z}$ . En el origen es un polo de orden tres:

$$\text{res}(f, 0) = \lim_{z \rightarrow 0} \frac{1}{2!} \frac{d^2}{dz^2} f(z) = \frac{\pi^2}{6}$$

Para los demás polos, que son todos simples:

$$\text{res}(f, k) = \frac{\pi}{\pi k^2 \cos k\pi + 2k \sin k\pi} = \frac{(-1)^k}{k^2}$$

Veamos  $\csc z$  para  $z = x + iy$  sobre el mismo cuadrado  $\gamma_n$ . Primero:

$$\csc z = \frac{1}{\sin x \cosh y + i \cos x \sinh y}$$

En los lados verticales, donde  $\cos x = 0$  y  $\sin x = 1$ :

$$|\csc z| = \frac{1}{\cosh y} \leq 1 \quad (28.46)$$

Para los horizontales interesa una cota superior para  $\cot z$ , que es lo mismo que una cota inferior para  $\sin z$ :

$$\begin{aligned} |\sin z|^2 &= |\sin^2 x \cosh^2 y + \cos^2 x \sinh^2 y| \\ &= |(1 - \cos^2 x)(1 + \sinh^2 y) + \cos^2 x \sinh^2 y| \\ &= |1 - \cos^2 x + \sinh^2 y| \end{aligned}$$

Para  $y \rightarrow \pm\infty$  tenemos  $\sinh^2 y \rightarrow \infty$ , por lo que para  $y$  suficientemente grande  $|\csc z| \leq 1$ . Similar a antes:

$$\left| \int_{\gamma_n} f(z) dz \right| \leq 2 \cdot \frac{1}{(n+1/2)^2} \cdot (2n+1) + 2 \cdot \frac{1}{(n+1/2)^2} \cdot (2n+1) = \frac{16}{2n+1}$$

Resulta:

$$\begin{aligned} \lim_{n \rightarrow \infty} \int_{\gamma_n} f(z) dz &= 0 \\ \sum_{k \in \mathbb{Z}} \text{res}(f, k\pi) &= 0 = -\frac{\pi^2}{6} + 2 \sum_{k \geq 1} \frac{(-1)^k}{k^2} \end{aligned}$$

De acá:

$$\sum_{k \geq 1} \frac{(-1)^k}{k^2} = \frac{\pi^2}{12} \quad (28.47)$$

Si se revisa el desarrollo, es claro que para cualquier función meromorfa  $g(z)$  par en  $\mathbb{R}$  y tal que:

$$\lim_{|z| \rightarrow \infty} zg(z) = 0$$

podemos aplicar las mismas técnicas para evaluar las sumas:

$$\sum_{k \geq 1} g(k) \quad \sum_{k \geq 1} (-1)^k g(k)$$

Podemos usar el mismo método para evaluar series. Por ejemplo, si nos interesa evaluar la siguiente serie para  $w \in \mathbb{C}$ :

$$\sum_{k \geq 1} \frac{w}{k^2 - w^2}$$

Si consideramos  $w$  como una constante, podemos aplicar la idea precedente con:

$$f(z) = \frac{\pi \cot \pi z}{z^2 - w^2}$$

Esta función tiene polos simples en  $z \in \mathbb{Z}$  y en  $z = \pm w$ . Igual que antes, en las últimas singularidades:

$$\text{res}(f, \pm w) = \lim_{z \rightarrow \pm w} \frac{\pi \cot \pi z}{z \pm w} = \pm \frac{\pi \cot(\pm \pi w)}{2w} = \frac{\pi \cot \pi w}{2w}$$

En  $z = k \in \mathbb{Z}$ :

$$\text{res}(f, k) = \lim_{z \rightarrow k} \frac{\pi \cos \pi z}{(z^2 - w^2) \pi \cos \pi z + 2z \sin \pi z} = \frac{1}{k^2 - w^2}$$

Igual que arriba, la integral sobre el cuadrado se anula:

$$\begin{aligned} \sum_{k \in \mathbb{Z}} \frac{1}{k^2 - w^2} + 2 \cdot \frac{\pi \cot(\pi w)}{2w} &= 0 \\ 2 \sum_{k \geq 1} \frac{1}{k^2 - w^2} - \frac{1}{w^2} + \frac{\pi \cot(\pi w)}{w} &= 0 \end{aligned}$$

$$\begin{aligned} \sum_{k \geq 1} \frac{1}{k^2 - w^2} &= \frac{1}{2w^2} - \frac{\pi \cot(\pi w)}{2w} \\ \sum_{k \geq 1} \frac{w}{k^2 - w^2} &= \frac{1}{2w} - \frac{\pi}{2} \cot \pi w \end{aligned}$$

### 28.9.2. Números de Fibonacci

Los números de Fibonacci quedan definidos por la recurrencia (ver sección 19.4):

$$F_{n+2} = F_{n+1} + F_n \quad F_0 = 0, F_1 = 1 \tag{28.48}$$

Sabemos que la función generatriz ordinaria es (28.49):

$$F(z) = \sum_{k \geq 0} F_k z^k = \frac{z}{1 - z - z^2} \tag{28.49}$$

Los ceros del denominador de (28.49) son  $(-1 \pm \sqrt{5})/2$ , siendo  $(-1 + \sqrt{5})/2$  el más cercano al origen. Esto determina el radio de convergencia de la serie. Recordamos las definiciones:

$$\tau = \frac{1 + \sqrt{5}}{2} \quad \phi = \frac{1 - \sqrt{5}}{2}$$

con lo que:

$$1 - z - z^2 = -(z + \tau)(z + \phi)$$

y también:

$$\tau\phi = -1 \tag{28.50}$$

Nuestro operador de extracción de coeficientes es:

$$[z^n] F(z) = \text{res}\left(\frac{F(z)}{z^{n+1}}, 0\right) = F_n$$

Las otras singularidades son polos simples:

$$\begin{aligned} \text{res}\left(\frac{F(z)}{z^{n+1}}, -\tau\right) &= -\lim_{z \rightarrow -\tau} \frac{1}{z^n(z + \phi)} = -\frac{1}{(-\tau)^n(-\tau + \phi)} = \frac{\phi^n}{\tau - \phi} \\ \text{res}\left(\frac{F(z)}{z^{n+1}}, -\phi\right) &= -\lim_{z \rightarrow -\phi} \frac{1}{z^n(z + \tau)} = -\frac{1}{(-\phi)^n(-\phi + \tau)} = -\frac{\tau^n}{\tau - \phi} \end{aligned}$$

Acá usamos la ecuación (28.50) para los recíprocos de  $\tau$  y  $\phi$ . Integremos sobre  $C_R$ , la circunferencia de radio  $R$  centrada en el origen, donde  $R > \tau$ . Por la desigualdad triangular, teorema 1.2:

$$|z|^2 - |z| - 1 \leq |z^2 + z - 1|$$

Para  $|z|$  suficientemente grande:

$$|z|^2 \left(1 - \frac{|z| + 1}{|z|^2}\right) \geq \frac{1}{2}|z|^2$$

Usando esto en la integral:

$$\left| \int_{C_R} \frac{z}{z^{n+1}(1 - z - z^2)} dz \right| \leq \frac{2}{R^{n+1}R^2} \cdot 2\pi R = \frac{4\pi}{R^{n+2}}$$

Esto tiende a cero al tender  $R$  a infinito:

$$F_n = \frac{1}{\tau - \phi} (\tau^n - \phi^n) = \frac{1}{\sqrt{5}} \left( \left(\frac{1 + \sqrt{5}}{2}\right)^n - \left(\frac{1 - \sqrt{5}}{2}\right)^n \right)$$

De nuevo la fórmula de Binet (19.24).

## 28.10. La función $\Gamma$

Tendremos ocasión de usar la función  $\Gamma$  (gamma mayúscula), interesa deducir sus propiedades elementales. No podemos hacerle justicia a este fascinante tema en este espacio, referimos al lector interesado al librito de Artin [20].

Para  $z$  complejo, se define:

$$\Gamma(z) = \int_0^\infty t^{z-1} e^{-t} dt \quad (28.51)$$

Para  $t > 0$  fijo el integrando de (28.51) es holomorfo en  $z$ , con lo que esto define una función holomorfa en el semiplano  $\Re z > 1$ . Integrando por partes:

$$\Gamma(z) = \int_0^\infty t^{z-1} e^{-t} dt = \frac{1}{z} \int_0^\infty e^{-t} dt^z = \frac{1}{z} t^z e^{-t} \Big|_0^\infty + \frac{1}{z} \int_0^\infty t^z e^{-t} dt = \frac{1}{z} \Gamma(z+1)$$

Tenemos así la *fórmula de reducción*:

$$\Gamma(z+1) = z \Gamma(z) \quad (28.52)$$

También tenemos  $\Gamma(1) = 1$ , lo que para  $n \in \mathbb{N}$  por la fórmula de reducción da:

$$\Gamma(n) = (n-1)! \quad (28.53)$$

Incidentalmente, como para  $z \in -\mathbb{N}_0$  resulta  $1/\Gamma(z) = 0$  es consistente nuestra convención (14.26) que  $1/n! = 0$  si  $n$  es un entero negativo.

Si  $\Re z > 1$ , tenemos el valor de (28.51). Fijemos entonces  $z$  con  $\Re z \leq 1$ , y sea  $n$  tal que  $\Re(z+n) > 0$ . En un entorno de  $z+n$  la función  $\Gamma$  es holomorfa, y por (28.52) tenemos:

$$\Gamma(z+n) = z^{\underline{n+1}} \Gamma(z)$$

Vale decir, si  $\Re z < 0$ , tiene sentido definir con  $n = \lceil -\Re z \rceil$ :

$$\Gamma(z) = \frac{\Gamma(z+n)}{z^{\underline{n+1}}} \quad (28.54)$$

Es claro que esto nos mete en problemas solo si  $z \in -\mathbb{N}_0$ . En el entorno de  $-n$ , para  $|w|$  chico, la función queda representada por:

$$\Gamma(-n+w) = \frac{\Gamma(1+w)}{(-n+w)^{\underline{n+1}}}$$

Como  $z^{\underline{n+1}}$  tiene un cero simple en  $-n$ , vemos que  $\Gamma(z)$  tiene polos simples en los enteros negativos. Es fácil calcular sus residuos:

$$\begin{aligned} \text{res}(\Gamma, 0) &= \lim_{z \rightarrow 0} z \frac{\Gamma(z+1)}{z} = 1 \\ \text{res}(\Gamma, -n) &= \lim_{z \rightarrow -n} (z+n) \frac{\Gamma(z+n+1)}{z^{\underline{n+1}}} = \frac{1}{(-n)^{\underline{n}}} = \frac{(-1)^n}{n!} \end{aligned} \quad (28.55)$$

La función  $\Gamma$  satisface muchas identidades notables. Por ejemplo, tenemos:

**Teorema 28.42** (Fórmula de reflexión de Euler). *Se cumple:*

$$\Gamma(z) \Gamma(1-z) = \frac{\pi}{\sin \pi z} \quad (28.56)$$

Seguimos la demostración de Stein y Shakarchi [337].

*Demostración.* Primeramente,  $\pi/\sin \pi z$  tiene polos en  $\mathbb{Z}$ . El residuo en  $n \in \mathbb{Z}$  es:

$$\text{res}\left(\frac{\pi}{\sin \pi z}, n\right) = \frac{\pi}{\pi \cos \pi n} = (-1)^n$$

La función  $\Gamma(1-z)$  tiene polos simples en  $z \in -\mathbb{N}$ , allí  $\Gamma(z)$  es holomorfa. Para  $n \in \mathbb{N}$ :

$$\text{res}(\Gamma(z)\Gamma(1-z), -n) = \text{res}(\Gamma(z), -n)\Gamma(n+1) = \frac{(-1)^n}{n!} n! = (-1)^{-n}$$

De la misma forma, para  $n \in \mathbb{N}_0$ :

$$\text{res}(\Gamma(z)\Gamma(1-z), n) = (-1)^n$$

O sea, los polos y residuos respectivos de ambas funciones coinciden.

Enseguida,  $\Gamma(z)\Gamma(1-z)$  y  $\pi/\sin \pi z$  son ambas periódicas, con período 1:

$$\Gamma(z+1)\Gamma(1-(z+1)) = z\Gamma(z) \cdot \frac{\Gamma(1-z)}{z} = \Gamma(z)\Gamma(1-z)$$

Finalmente, demostramos que ambas funciones coinciden en  $0 < s < 1$ . Podemos escribir:

$$\Gamma(1-s) = \int_0^\infty u^{-s} e^{-u} du = t \int_0^\infty e^{-vt} (vt)^{-s} dv$$

Acá usamos el cambio de variables  $u = vt$ . Luego:

$$\begin{aligned} \Gamma(s)\Gamma(1-s) &= \int_0^\infty e^{-t} t^{s-1} \Gamma(1-s) dt \\ &= \int_0^\infty e^{-t} t^{s-1} \left( t \int_0^\infty e^{-vt} (vt)^{-s} dv \right) dt \\ &= \int_0^\infty \int_0^\infty e^{-t(1+v)} v^{-s} dv dt \\ &= \int_0^\infty \frac{v^{-s}}{1+v} dv \end{aligned}$$

Con el cambio de variables  $v = e^t$  queda la integral que evaluamos en (28.40):

$$\int_{-\infty}^\infty \frac{e^{-st}}{1+e^t} dt = \frac{\pi}{\sin s\pi}$$

Uniendo todas las piezas, ambas funciones deben ser iguales.  $\square$

De acá resulta directamente el valor para argumento no entero más usado:

$$\begin{aligned} (\Gamma(1/2))^2 &= \Gamma(1/2)\Gamma(1-1/2) = \frac{\pi}{\sin \pi/2} = \pi \\ \Gamma(1/2) &= \sqrt{\pi} \end{aligned} \tag{28.57}$$

Íntimamente relacionada es la función B (beta mayúscula), definida para  $\Re x, \Re y > 0$ :

$$B(x, y) = \int_0^1 t^{x-1} (1-t)^{y-1} dt \tag{28.58}$$

Es claro que es simétrica:

$$B(x, y) = B(y, x) \tag{28.59}$$

También:

$$\Gamma(x)\Gamma(y) = \int_0^\infty e^{-u} u^{x-1} du \int_0^\infty e^{-v} v^{y-1} dv = \int_0^\infty \int_0^\infty e^{-u-v} u^{x-1} v^{y-1} du dv$$

El cambio de variables  $u = st$  y  $v = s(1-t)$  da:

$$\Gamma(x)\Gamma(y) = \int_0^\infty e^{-s} s^{x+y-1} ds \int_0^1 t^{x-1} (1-t)^{y-1} dt = \Gamma(x+y)B(x,y)$$

de donde resulta la identidad básica, que sirve para definir  $B(x,y)$ :

$$B(x,y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)} \quad (28.60)$$

Por la fórmula de reducción (28.54) tenemos de (14.22):

$$\binom{\alpha}{n} = \frac{\alpha^n}{n!} = \frac{\Gamma(\alpha+1)}{\Gamma(\alpha-n+1)n!}$$

Con (28.53) esto se parece a (14.24), que hace sentido adoptar como definición:

$$\binom{m+n}{m} = \frac{(m+n)!}{m! n!} = \frac{\Gamma(m+n+1)}{\Gamma(m+1)\Gamma(n+1)} \quad (28.61)$$



## 29 Estimaciones asintóticas

---

Es común requerir una estimación ajustada de alguna cantidad, como una suma o el valor aproximado del coeficiente de una serie horrible. Hay una variedad de técnicas disponibles para esta tarea, desde simples a complejas. Interesan estimaciones asintóticas que entreguen resultados numéricos precisos y simples para el número de estructuras combinatorias, generalmente en el ámbito de rendimiento de algoritmos con el objetivo de comparar alternativas o estimar los recursos requeridos para resolver un problema particular. Describiremos sólo algunos de los métodos más importantes. Resúmenes detallados de las principales técnicas ofrecen Odlyzko [272] y Flajolet y Sedgewick [126].

### 29.1. Estimar sumas

Primero una técnica simple, que ya habíamos visto (capítulo 18).

**Teorema 29.1.** *Sea  $f(x)$  una función continua y monótona. Entonces:*

$$\sum_{0 \leq k \leq n} f(k) \approx \int_0^n f(x) dx + \frac{f(0) + f(n)}{2}$$

*Demuestra*ón. Si  $f(x)$  es monótona creciente:

$$\begin{aligned} f(\lfloor x \rfloor) &\leq f(x) & \leq f(\lceil x \rceil) \\ \int_0^n f(\lfloor x \rfloor) dx &\leq \int_0^n f(x) dx \leq \int_0^n f(\lceil x \rceil) dx \\ \sum_{0 \leq k \leq n-1} f(k) &\leq \int_0^n f(x) dx \leq \sum_{0 \leq k \leq n-1} f(k+1) dx \\ \sum_{0 \leq k \leq n} f(k) - f(n) &\leq \int_0^n f(x) dx \leq \sum_{0 \leq k \leq n} f(k) - f(0) \end{aligned}$$

y directamente:

$$\int_0^n f(x) dx + f(0) \leq \sum_{0 \leq k \leq n} f(k) \leq \int_0^n f(x) dx + f(n)$$

Si  $f(x)$  es monótona decreciente, se intercambian  $f(0)$  y  $f(n)$  en este último resultado.  $\square$

Otras estimaciones simples resultan de acotar usando sumas conocidas. Si tenemos una suma finita de términos positivos, y la suma infinita correspondiente converge, tenemos una cota obvia. Suelen ser útiles como cotas la suma de secuencias geométricas (teorema 3.6):

$$\sum_{k \geq 0} a^k = \frac{1}{1-a} \tag{29.1}$$

$$\sum_{0 \leq k \leq n} a^k = \frac{1 - a^{n+1}}{1 - a} \tag{29.2}$$

También es común la suma de secuencias aritméticas:

$$\sum_{0 \leq k \leq n} k = \frac{n(n+1)}{2} \quad (29.3)$$

Ocasionalmente aparecen números harmónicos (sección 19.1):

$$\sum_{1 \leq k \leq n} \frac{1}{k} = H_n = \ln n + \gamma + O\left(\frac{1}{n}\right) \quad (29.4)$$

Una técnica simple es acotar parte de la suma. Por ejemplo, sabemos cómo derivar una fórmula para la suma de los primeros cubos, pero podemos obtener cotas sencillas mediante las siguientes observaciones:

$$\begin{aligned} \sum_{1 \leq k \leq n} k^3 &\leq \sum_{1 \leq k \leq n} n^3 \\ &= n^4 \\ \sum_{1 \leq k \leq n} k^3 &\geq \sum_{n/2 \leq k \leq n} k^3 \\ &\geq \sum_{n/2 \leq k \leq n} \left(\frac{n}{2}\right)^3 \\ &= \frac{n^4}{8} \end{aligned}$$

O sea:

$$\sum_{1 \leq k \leq n} k^3 = \Theta(n^4)$$

## 29.2. Estimar coeficientes

Hay diferentes técnicas aplicables en este caso, de diferentes grados de complejidad. Discutiremos algunos de aplicabilidad general, el lector interesado podrá hallar referencias a técnicas adicionales.

### 29.2.1. Cota trivial

Hay una cota bastante trivial, que resulta sorprendentemente ajustada en muchos casos. Típicamente el error cometido es de un factor de  $n^{1/2}$ . Si consideramos la secuencia  $\langle a_n \rangle_{n \geq 0}$ , donde en aplicaciones combinatorias los  $a_n$  no son negativos:

$$A(z) = \sum_{n \geq 0} a_n z^n \quad (29.5)$$

Es claro que para  $u$  positivo:

$$a_n u^n \leq A(u)$$

de donde tenemos la cota:

$$a_n \leq \min_{u \geq 0} \left( \frac{A(u)}{u^n} \right) \quad (29.6)$$

### 29.2.2. Singularidades dominantes

Sabemos (ver capítulo 28, particularmente el teorema 28.33) que una función meromorfa cerca de una singularidad queda representada por la suma de una función entera y una función holomorfa en un disco perforado centrado en la singularidad. Esta segunda función (básicamente la parte principal de la serie de Laurent de la función) domina la expansión en serie, o, lo que es lo mismo, pone la mayor parte de los coeficientes de la serie de potencias. Un ejemplo de esto ya lo vimos en la sección 19.7.1, donde vimos que el cero del denominador más cercano al origen da los términos dominantes. Considerando únicamente un polo simple  $z_0$  como singularidad más cercana al origen, estamos aproximando:

$$A(z) = \sum_{n \geq 0} a_n z^n$$

mediante:

$$A(z) \approx \text{res}(A, z_0) \frac{1}{z - z_0} = -\text{res}(A, z_0) \frac{1}{z_0(1 - z/z_0)}$$

lo que se traduce en:

$$a_n \approx -\text{res}(A, z_0) \frac{1}{z_0^{n+1}} \quad (29.7)$$

Incluir singularidades adicionales significa añadir términos similares para ellas. En detalle, tenemos:

**Teorema 29.2.** *Sea  $f$  meromorfa en la región  $D$  que contiene el origen. Sea  $R > 0$  el módulo de los polos de mínimo módulo, y sean  $z_0, \dots, z_s$  estos polos. Sea  $R' > R$  el módulo de los polos de siguiente módulo mayor, y sea  $\epsilon > 0$  dado. Entonces:*

$$[z^n] f(z) = [z^n] \left( \sum_{0 \leq k \leq s} \text{pp}(f; z_k) \right) + O \left( \left( \frac{1}{R'} + \epsilon \right)^n \right) \quad (29.8)$$

*Demuestra.* Basta demostrar que al restar las partes principales de  $f$  indicadas de  $f$  el resultado es una función que es holomorfa en el disco  $D_{R'}(0)$ , la cota para el error es esencialmente el corolario 28.27. Por el teorema 28.33, la función  $f(z) - \text{pp}(f; z_0)$  es holomorfa en  $z_0$ , y debemos demostrar que su parte principal en  $z_1$  es la misma que la de  $f$ :

$$\begin{aligned} \text{pp}(f - \text{pp}(f; z_0); z_1) &= \text{pp}(f; z_1) - \text{pp}(\text{pp}(f; z_0); z_1) \\ &= \text{pp}(f; z_1) \end{aligned}$$

ya que  $\text{pp}(f; z_0)$  es holomorfa en  $z_1$ . Podemos ir aplicando esto polo a polo hasta demostrar que restando las partes principales indicadas de  $f$  obtenemos una función holomorfa en el disco de radio  $R'$  indicado.  $\square$

Para un ejemplo, vimos (sección 22.10) que la función generatriz exponencial de los números de desarreglos está dada por:

$$\widehat{D}(z) = \frac{e^{-z}}{1 - z} \quad (29.9)$$

Esta función generatriz tiene un polo simple en  $z = 1$ , con residuo  $-e^{-1}$ . Obtenemos directamente la aproximación (15.13). Sabemos también que la función:

$$d(z) = \frac{e^{-z}}{1 - z} - \frac{e^{-1}}{1 - z} = \frac{e^{-z} - e^{-1}}{1 - z} \quad (29.10)$$

es entera (tiene una singularidad removible en  $z = 1$ ), sus coeficientes son el error que comete la aproximación. Como el radio de convergencia para una función entera es  $R = \infty$ , nuestra cota (29.8) es:

$$D_n = n!e^{-1} + O(n!e^n) \quad (29.11)$$

Otro caso es el número de resultados de competencias con empate (números de Bell ordenados). En la sección 22.11 llegamos a:

$$R(z) = \frac{1}{2 - e^z} \quad (29.12)$$

Esto tiene singularidades cuando  $e^z = 2$ , o sea en los puntos para  $k \in \mathbb{Z}$ :

$$\log 2 = \ln 2 + 2k\pi i \quad (29.13)$$

Domina la singularidad en  $\ln 2$ , podemos refinar el resultado incluyendo singularidades adicionales en orden de cercanía de 0 ( $\ln 2, \ln 2 \pm 2\pi i, \ln 2 \pm 4\pi i, \dots$ ). Si escribimos  $z = \log 2 + u$ :

$$R(z) = \frac{1}{2} \frac{1}{1 - e^u}$$

Las singularidades son todas polos simples, sus residuos son:

$$\text{res}\left(\frac{1}{2 - e^z}, \ln 2 + 2k\pi i\right) = \lim_{z \rightarrow \ln 2 + 2k\pi i} \frac{1}{-e^z} = -\frac{1}{2} \quad (29.14)$$

El polo más cercano al origen es  $\ln 2$ , los siguientes están en  $\ln 2 \pm 2\pi i$ , de módulo  $\sqrt{\ln 2 + 4\pi^2} = 6,32$ . En consecuencia, de (29.7):

$$R_n = \frac{n!}{2(\ln 2)^{n+1}} + O(n! \cdot 0,16^n) \quad (29.15)$$

El cuadro 29.1 muestra los primeros valores exactos y aproximados, la concordancia es extremada-

<b><i>n</i></b>	<b><i>R<sub>n</sub></i></b>	(29.15)
0	1	0,7213
1	1	1,0407
2	3	3,0028
3	13	12,9963
4	75	74,9987
5	541	541,0015

Cuadro 29.1 – Números de Bell ordenados

mente buena.

Para un ejemplo un poquito más complejo, tenemos los números de Bernoulli, con función generatriz exponencial (ver la sección 18.6):

$$B(z) = \frac{z}{e^z - 1} \quad (29.16)$$

Tanto  $z$  como  $e^z - 1$  son enteras,  $B(z)$  solo puede tener polos. En los polos  $e^z = 1$ , o sea son polos  $z = 2k\pi i$  para todo  $k \in \mathbb{Z}$ . En este caso tenemos dos polos a la misma distancia del origen, debemos considerar el aporte de ambos. Es fácil corroborar que los polos son simples, interesan:

$$\text{res}(B(z), 2k\pi i) = \lim_{z \rightarrow 2k\pi i} \frac{z}{e^z - 1} = 2k\pi i \quad (29.17)$$

Usando los polos  $\pm 2\pi i$  tenemos la aproximación:

$$\frac{B_n}{n!} = -\frac{2\pi i}{(2\pi i)^{n+1}} + \frac{2\pi i}{(-2\pi i)^{n+1}} + O\left(\left(\frac{1}{4\pi}\right)^n\right) \quad (29.18)$$

Vemos que para  $n$  impar los aportes se cancelan, esta técnica no entrega demasiada información en ese caso. Para  $n = 2k$  volvemos a obtener (18.37):

$$B_{2k} \sim \frac{-2(2k)!}{(2\pi i)^{2k}} = (-1)^{k+1} \frac{2(2k)!}{(4\pi^2)^k} \quad (29.19)$$

Los valores exactos y aproximados de  $B_{2k}$  se contrastan en el cuadro 29.2. La aproximación no es par-

<b><i>n</i></b>	<b><i>B<sub>n</sub></i></b>	<b>(29.19)</b>	
0	1	1,0000	-2,0000
2	1/6	1,1666	0,1013
4	-1/30	-0,0333	-0,0308
6	1/42	0,0238	0,0234
8	-1/30	-0,0333	-0,0332
10	5/56	0,0758	0,0757
12	-691/2730	-0,2531	-0,2531
14	7/6	1,1666	1,1666
16	-3617/510	-7,0922	-7,0920

Cuadro 29.2 – Números de Bernoulli pares

ticularmente buena en los índices bajos, se siente la influencia de los polos más lejanos. Igualmente la aproximación es muy buena.

Si sumamos los aportes de todos los polos, resulta de nuevo la fórmula para  $\zeta(2k)$ :

$$B_{2k} = (-1)^{k+1} \frac{2(2k)!}{(4\pi^2)^k} \zeta(2k) \quad (29.20)$$

Una aplicación instructiva de las técnicas presentadas dan Odlyzko y Wilf [273] al tratar el caso de fuentes no necesariamente de bloques (ver la sección 14.10).

### 29.2.3. Número de palabras sin $k$ símbolos repetidos

Vimos en la sección 21.2.2 que el número de palabras de largo  $n$  sobre un alfabeto de  $s$  símbolos que no contienen el patrón  $p$  de largo  $k$  tiene función generatriz ordinaria (21.9):

$$\frac{c_p(z)}{(1-sz)c_p(z)+z^k}$$

Acá  $c_p(z)$  es el polinomio de autocorrelación del patrón  $p$ . Obtener una estimación asintótica de este número sirve de ejemplo detallado de la aplicación de las herramientas discutidas. El caso general es tratado por Guibas y Odlyzko [155].

Para simplificar, trataremos únicamente el caso en que el patrón es un símbolo repetido  $k$  veces, en cuyo caso  $c_p(z) = 1 + z + \dots + z^{k-1}$ . En este caso la función generatriz se reduce a:

$$\frac{1-z^k}{1-sz+(s-1)z^{k+1}} \quad (29.21)$$

Nos interesa el cero más cercano al origen del denominador de (29.21) para  $k$  dado. Sólo tiene sentido el caso  $k > 1$ . Llamemos:

$$h(z) = 1 - sz + (s-1)z^{k+1} \quad (29.22)$$

Claramente  $h(1) = 0$  con  $h'(1) = k(s-1) - 1 > 0$ , y  $h(1/s) = (s-1)s^{-k-1} > 0$  es pequeño. Podemos acotar:

$$h((s-1)^{-1}) = 1 - s(s-1)^{-1} + (s-1)^{-k} \leq 1 - s + 1 = 2 - s$$

Hay un cero entre  $s^{-1}$  y  $(s-1)^{-1}$ . Debemos asegurarnos que sea único. Para ello aplicamos el teorema de Rouché (28.41).

Consideremos el caso  $s > 2$ . Tomemos las funciones:

$$f(z) = -sz$$

$$g(z) = 1 + (s-1)z^{k+1}$$

Sobre la circunferencia  $|z| = r$  tenemos las cotas:

$$|f(z)| = sr$$

$$|g(z)| = 1 + (s-1)r^{k+1}$$

Nos interesa demostrar que:

$$sr > 1 + (s-1)r^{k+1}$$

$$0 > 1 - sr + (s-1)r^{k+1} = h(r)$$

Como interesan  $k \geq 2$  y  $s \geq 2$ , tenemos:

$$h(0) = 1$$

$$h(1) = 0$$

$$h'(1) = -s + (k+1)(s-1) = k(s-1) - 1 > 0$$

En consecuencia, hay  $0 < r^* < 1$  tal que  $h(r) < 0$ , o, lo que es lo mismo,  $|f(z)| > |g(z)|$  sobre la circunferencia  $|z| = r^*$ . Por el teorema de Rouché,  $f(z)$  y  $f(z) + g(z) = h(z)$  tienen el mismo número de ceros al interior de la circunferencia, uno solo. Como  $h(z)$  es un polinomio de coeficientes reales, sus ceros son reales o vienen en pares complejos. El cero que nos interesa es simple y real. Si lo llamamos  $\rho$ , por el teorema de Bender (29.3):

$$P_n \sim \frac{1 - \rho^k}{h'(\rho)} \cdot \rho^n = \frac{1 - \rho^k}{(s-1)(k+1)\rho^k - s} \cdot \rho^n \quad (29.23)$$

Tenemos cotas para  $\rho$ , para obtener una mejor aproximación del cero aplicamos una iteración del método de Newton (para detalles, ver textos de análisis numérico, como Acton [2, capítulo 2] o Ralston y Rabinowitz [296, capítulo 8]) partiendo con la aproximación  $1/s$ . Resulta que la expresión final es mucho más sencilla si partimos con:

$$h_r(u) = u^{k+1}h(1/u) = u^{k+1} - su^k + s - 1$$

Los ceros de  $h_r(u)$  son recíprocos de los ceros de  $h(z)$ . Tenemos:

$$(\rho^*)^{-1} \approx s - \frac{h_r(s)}{h'_r(s)} = s - \frac{s-1}{s^k}$$

Para el peor caso posible,  $s = k = 2$ , esto da la aproximación  $\rho^* \approx 0,571$ , cuando el valor correcto es  $\rho = 1/\tau = 0,618$ .

### 29.2.4. Singularidades algebraicas

Supongamos ahora que la singularidad  $z_0$  de  $f$  más cercana al origen es algebraica (un punto de ramificación), vale decir hay  $\alpha \in \mathbb{C}$  con  $\alpha \notin \mathbb{N}$  tal que la función  $g$  definida por lo siguiente es holomorfa en un entorno de  $z_0$ :

$$f(z) = (z_0 - z)^\alpha g(z)$$

El desarrollo de la sección anterior hace sospechar que en tal caso la serie:

$$f(z) = (z_0 - z)^\alpha \sum_{k \geq 0} g_k (z_0 - z)^k = \sum_{k \geq 0} g_k (z_0 - z)^{k+\alpha}$$

es clave.

Seguimos básicamente el desarrollo de Knuth y Wilf [222]. Sin pérdida de generalidad, podemos suponer que  $z_0 = 1$  (basta considerar  $f(zz_0)$  en caso contrario), y que hay una única singularidad de interés. Primero un par de resultados auxiliares, de interés independiente.

**Teorema 29.3** (Bender). *Sean  $A(z) = \sum a_k z^k$  y  $B(z) = \sum b_k z^k$  series de potencias con radios de convergencia  $\alpha > \beta \geq 0$ , respectivamente. Suponga que:*

$$\lim_{n \rightarrow \infty} \frac{b_{n-1}}{b_n} = b$$

*Si  $A(b) \neq 0$ , y  $A(z)B(z) = \sum c_n z^n$ , entonces  $c_n \sim A(b)b_n$ .*

La demostración sigue la de Bender [33].

*Demostración.* Basta demostrar que  $c_n/b_n \sim A(b)$ . Sabemos que:

$$c_n = \sum_{0 \leq k \leq n} a_k b_{n-k}$$

Con esto:

$$\begin{aligned} \left| A(b) - \frac{c_n}{b_n} \right| &= \left| A(b) - \sum_{0 \leq k \leq n} a_k \frac{b_{n-k}}{b_n} \right| \\ &= \left| \sum_{k > n} a_k b^k - \sum_{0 \leq k \leq n} a_k \left( b^k - \frac{b_{n-k}}{b_n} \right) \right| \\ &\leq \left| \sum_{k > n} a_k b^k \right| + \left| \sum_{0 \leq k \leq n} a_k \left( b^k - \frac{b_{n-k}}{b_n} \right) \right| \end{aligned}$$

El primer término es la cola de una serie convergente, tiende a cero al crecer  $n$ . Para el segundo término, dividiendo la suma en  $n/2$ :

$$\begin{aligned} \left| \sum_{0 \leq k \leq n} a_k \left( b^k - \frac{b_{n-k}}{b_n} \right) \right| &\leq \left| \sum_{0 \leq k < n/2} a_k \left( b^k - \frac{b_{n-k}}{b_n} \right) \right| + \sum_{n/2 \leq k \leq n} |a_k b^k| \cdot \left| \frac{b_{n-k}}{b_n b^k} \right| \\ &\leq \left| \sum_{0 \leq k < n/2} a_k \left( b^k - \frac{b_{n-k}}{b_n} \right) \right| + \max_{n/2 \leq k \leq n} \left| \frac{b_{n-k}}{b_n b^k} \right| \cdot \sum_{n/2 \leq k \leq n} |a_k b^k| \end{aligned}$$

El primer término tiende a cero, ya que  $b_{n-k}/b_n \sim b^k$ ; la suma del segundo término está acotada por la cola de una serie convergente. Para el factor:

$$\max_{n/2 \leq k \leq n} \left| \frac{b_{n-k}}{b_n b^k} \right| = \max_{n/2 \leq k \leq n} \left| \frac{b_{n-k} b^{n-k}}{b_n b^n} \right| = \max_{0 \leq k < n/2} \left| \frac{b_k b^k}{b_n b^n} \right|$$

Como la serie  $\sum b_k b^k$  converge, esto está acotado. □

Una aplicación simple del teorema de Bender es obtener una expansión asintótica para los números de Motzkin [261] (ver la discusión detallada de Donaghey y Shapiro [99]). Dedujimos (29.24) en la sección 22.4:

$$M(z) = \frac{1-z-\sqrt{1-2z-3z^2}}{2z^2} \quad (29.24)$$

Es claro que para  $n \geq 2$ :

$$\begin{aligned} M_n &= [z^n] \frac{1-z-\sqrt{1-2z-3z^2}}{2z^2} \\ &= -\frac{1}{2} [z^{n+2}] (1+z)^{1/2} (1-3z)^{1/2} \end{aligned}$$

Vemos que el radio de convergencia de esto último es  $1/3$ , igual que el segundo factor; el primer factor tiene radio de convergencia 1. Por el teorema de Bender:

$$\begin{aligned} M_n &\sim -\frac{1}{2} (1+1/3)^{1/2} [z^{n+2}] (1-3z)^{1/2} \\ &= -\frac{\sqrt{3}}{3} \binom{1/2}{n+2} (-3)^{n+2} \\ &= \frac{3\sqrt{3}}{8(n+2)} \binom{2n+2}{n+1} \left(\frac{3}{4}\right)^n \end{aligned} \quad (29.25)$$

El cuadro 29.3 contrasta los valores exactos con la aproximación (29.25). No es particularmente

<b><i>n</i></b>	<b><i>R<sub>n</sub></i></b>	<b>(29.25)</b>
0	1	—
1	1	—
2	2	1,827
3	4	3,836
4	9	8,631
5	21	20,346
6	51	49,593
7	127	123,981
8	323	316,153
9	835	819,123
10	2188	2150,198

Cuadro 29.3 – Números de Motzkin

bueno, pero invertimos muy poco esfuerzo en ella.

Un ejercicio simple de la función  $\Gamma$  y la fórmula de Stirling da:

**Lema 29.4.** *Para  $\beta$  fijo cuando  $n \rightarrow \infty$ :*

$$[z^n] (1-z)^\beta \begin{cases} \sim n^{-\beta-1}/\Gamma(-\beta) & \text{si } \beta \notin \mathbb{N} \\ \rightarrow 0 & \text{si } \beta \in \mathbb{N} \end{cases}$$

*Demostración.* Para el caso  $\beta \in \mathbb{N}$ , por el teorema del binomio sabemos que si  $n > \beta$  el coeficiente es cero.

En caso que  $\beta \notin \mathbb{N}$ :

$$[z^n](1-z)^\beta = \binom{\beta}{n}(-1)^n = \frac{\beta n}{n!}(-1)^n = \frac{(-\beta)^n}{n!} = \frac{\Gamma(n-\beta)}{\Gamma(-\beta)n!}$$

El resultado sigue de la fórmula de Stirling (18.18):

$$\Gamma(n+1) = n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$$

Tenemos:

$$\begin{aligned} \frac{\Gamma(n-\beta)}{\Gamma(-\beta)n!} &\sim \frac{1}{\Gamma(-\beta)} \cdot \frac{(n-\beta-1)^{n-\beta-3/2}}{e^{n-\beta-2}} \cdot \frac{e^n}{n^{n+1/2}} \\ &= \frac{1}{\Gamma(-\beta)} \cdot \frac{n^{n-\beta-1/2} \cdot (1-(\beta+2)/n)^n \cdot (1-(\beta+2)/n)^{-\beta-3/2} \cdot e^{-\beta-2}}{n^{n+1/2}} \\ &\sim \frac{n^{-\beta-1}}{\Gamma(-\beta)} \end{aligned}$$

Acá usamos el límite clásico:

$$\lim_{n \rightarrow \infty} \left(1 + \frac{\alpha}{n}\right)^n = e^\alpha$$

□

Con estos:

**Lema 29.5.** Sea  $u(z) = (1-z)^\gamma v(z)$ , donde  $v(z)$  es holomorfa en algún disco  $|z| < 1 + \eta$  (acá  $\eta > 0$ ). Entonces:

$$[z^n] u(z) = O(n^{-\gamma-1})$$

*Demostración.* Aplicando el teorema de Bender, teorema 29.3, queda:

$$[z^n](1-z)^\gamma v(z) \sim v(1)[z^n](1-z)^\gamma$$

El lema 29.4 entrega el resultado prometido. □

Estamos en condiciones de demostrar:

**Teorema 29.6** (Lema de Darboux). Sea  $f$  holomorfa en un disco  $|z| < 1 + \eta$ , donde  $\eta > 0$ . Suponga que en un entorno de  $z = 1$  tiene una expansión

$$f(z) = \sum_{k \geq 0} f_k (1-z)^k$$

Entonces para todo  $\beta \in \mathbb{C}$  y todo  $m \in \mathbb{N}_0$ :

$$\begin{aligned} [z^n](1-z)^\beta f(z) &= [z^n] \sum_{k \geq 0} f_k (1-z)^{\beta+k} + O(n^{-m-\beta-2}) \\ &= \sum_{0 \leq k \leq m} f_k \binom{n-\beta-k-1}{n} + O(n^{-m-\beta-2}) \end{aligned}$$

*Demostración.* Tenemos:

$$(1-z)^\beta f(z) - \sum_{0 \leq k \leq m} f_k (1-z)^{\beta+k} = \sum_{k>m} f_k (1-z)^{\beta+k} \\ = (1-z)^{\beta+m+1} \tilde{f}(z)$$

Las regiones de holomorfismo de  $f$  y  $\tilde{f}$  son las mismas. El resultado sigue del lema 29.5.  $\square$

Obtengamos una expansión más precisa de los números de Motzkin. Tenemos para  $n \geq 2$ , vía el cambio de variables  $u = 3z$ :

$$M_n = -\frac{1}{2} [z^{n+2}] (1+z)^{1/2} (1-3z)^{1/2} \\ = -\frac{3^{n+2}}{2} [u^{n+2}] \left(\frac{4}{3}\right)^{1/2} \left(1 - \frac{1-u}{4}\right)^{1/2} \cdot (1-u)^{1/2} \\ = -3\sqrt{3} \cdot 3^n \cdot \sum_{k \geq 0} \binom{1/2}{k} (-4)^{-k} [u^{n+2}] (1-u)^{1/2}$$

Si expandimos para  $m = 0$  y no aproximamos los coeficientes binomiales resulta nuevamente (29.25). Extendamos a  $m = 1$ , approximando los coeficientes binomiales mediante el lema 29.4. Necesitamos:

$$\binom{1/2}{n+2} \sim \frac{(n+2)^{-3/2}}{\Gamma(-1/2)} = -\frac{(n+2)^{-3/2}}{2\sqrt{\pi}} \\ \binom{3/2}{n+2} \sim \frac{(n+2)^{-5/2}}{\Gamma(-3/2)} = \frac{3(n+2)^{-5/2}}{4\sqrt{\pi}}$$

porque:

$$\left(-\frac{1}{2}\right) \cdot \Gamma\left(-\frac{1}{2}\right) = \Gamma\left(\frac{1}{2}\right) = \sqrt{\pi} \\ \left(-\frac{3}{2}\right) \cdot \Gamma\left(-\frac{3}{2}\right) = \Gamma\left(-\frac{1}{2}\right)$$

y tenemos la estimación:

$$M_n = \frac{\sqrt{3} \cdot 3^n}{16\sqrt{\pi}} \cdot (8(n+2)^{-3/2} + 3(n+2)^{-5/2}) \quad (29.26)$$

La aproximación (29.26) no es tan buena como (29.25), pero hay que considerar que usamos una aproximación bastante cruda para los coeficientes binomiales a cambio de reemplazarlos por potencias. Igual la fórmula diseñada para índices muy grandes da excelentes resultados ya para  $n = 10$ .

### 29.2.5. Singularidades algebraico-logarítmicas

Una técnica que resuelve muchos de los casos de interés en combinatoria es la que presentan Flajolet y Odlyzko [128] (ver también el resumen más accesible de Flajolet y Sedgewick [126, sección VI.2]). Las demostraciones son bastante engorrosas, nos remitiremos a citar los resultados.

**Teorema 29.7.** *Sea  $\alpha \in \mathbb{C} \setminus \mathbb{Z}_{\leq 0}$ . Entonces:*

$$[z^n] (1-z)^{-\alpha} \sim \frac{n^{\alpha-1}}{\Gamma(\alpha)} \quad (29.27)$$

$n$	$R_n$	(29.26)
0	1	—
1	1	—
2	2	1,804
3	4	3,805
4	9	8,583
5	21	20,263
6	51	49,438
7	127	123,678
8	323	315,526
9	835	817,783
10	2188	2147,245

Cuadro 29.4 – Números de Motzkin nuevamente

Si  $\alpha$  es un entero negativo,  $(1-z)^{-\alpha}$  es un polinomio, y los coeficientes del caso eventualmente se anulan. La exposición de Flajolet y Sedgewick [126, teorema VI.1] da la expansión asintótica.

**Teorema 29.8.** *Sea  $\alpha \in \mathbb{C} \setminus \mathbb{Z}_{\leq 0}$ . Entonces:*

$$[z^n](1-z)^{-\alpha} \left( \frac{1}{z} \ln \frac{1}{1-z} \right)^\beta \sim \frac{n^{\alpha-1}}{\Gamma(\alpha)} \ln^\beta n \quad (29.28)$$

Se introduce un factor  $1/z$  en frente del logaritmo para obtener una serie en  $z$ , no altera la expansión cerca de  $z = 1$ . Nuevamente Flajolet y Sedgewick [126, teorema VI.2] dan la expansión asintótica completa para el caso en que  $\beta$  no es un natural, citan a Jungen [191] para completar ese caso.

### 29.2.6. El método de Hayman

Las técnicas precedentes dan excelentes resultados cuando las funciones generatrices de interés tienen singularidades cerca del origen. Son totalmente inútiles si la función generatriz es entera. Nos interesaría, por ejemplo, obtener una expansión asintótica de  $n!$  vía considerar la serie para la exponencial. Para ello podemos razonar como sigue: De la fórmula generalizada de Cauchy, teorema 28.17, tenemos que para toda curva simple cerrada que incluya el origen:

$$\frac{1}{n!} = \frac{1}{2\pi i} \int_{\gamma} \frac{e^z}{z^{n+1}} dz$$

Si usamos la circunferencia de radio  $R$  centrada en el origen, tomando valores absolutos:

$$\begin{aligned} \frac{1}{n!} &\leq \frac{1}{2\pi} \max_{|z|=R} \left\{ \frac{|e^z|}{|z|^{n+1}} \right\} \cdot 2\pi R \\ &= \frac{e^R}{R^n} \end{aligned}$$

Pero el valor de  $R$  es arbitrario, podemos elegir aquel que minimice esta expresión, que resulta ser  $R = n$ , dando la cota:

$$\frac{1}{n!} \leq \left( \frac{e}{n} \right)^n$$

Nada mal, si se compara con la fórmula de Stirling (18.18).

Si queremos mayor precisión, debemos tratar la integral en forma más cuidadosa. Hayman [171] desarrolló maquinaria poderosa para esta situación. Seguimos la exposición de Wilf [364]. En una circunferencia alrededor del origen el módulo de una función con coeficientes reales no negativos tiene un máximo marcado en el eje real positivo, y es precisamente en ese caso que el método es más efectivo. Y este es el caso de las funciones generatrices de la combinatoria. El método en realidad es aplicable siempre, pero las técnicas basadas en singularidades son más sencillas de aplicar.

Sea  $f(z)$  holomorfa en el disco  $|z| < R$ , donde  $0 < R \leq \infty$ , y suponga que  $f(z)$  es *admissible* para el método. Las condiciones de admisibilidad son bastante complicadas, veremos algunas condiciones suficientes más adelante. En la práctica, que  $f(z)$  sea admissible significa simplemente que la técnica funciona.

Defina:

$$M(r) = \max_{|z|=r} \{|f(z)|\} \quad (29.29)$$

Una consecuencia de las condiciones de admisibilidad es que para  $r$  suficientemente grande:

$$M(r) = f(r) \quad (29.30)$$

Esto porque, como notamos arriba, el método apunta a funciones que toman el valor máximo en la dirección real positiva. Defina funciones auxiliares:

$$a(r) = r \frac{f'(r)}{f(r)} \quad (29.31)$$

$$b(r) = r a'(r) = r \frac{f'(r)}{f(r)} + r^2 \frac{f''(r)}{f(r)} - r^2 \left( \frac{f'(r)}{f(r)} \right)^2 \quad (29.32)$$

El resultado central es:

**Teorema 29.9** (Hayman). *Sea  $f(z) = \sum f_n z^n$  una función admissible. Sea  $r_n$  el cero positivo de  $a(r_n) = n$  para cada  $n \in \mathbb{N}$ , donde  $a(r)$  es la función (29.31). Entonces para  $n \rightarrow \infty$ :*

$$f_n \sim \frac{f(r_n)}{r_n^n \sqrt{2\pi b(r_n)}} \quad (29.33)$$

La receta misma es de aplicación directa, lo complicado es determinar si  $f(z)$  es admissible.

Continuemos con nuestro ejemplo  $e^z$ , aceptando por ahora que es admissible. Resultan:

$$a(r) = r \quad b(r) = r e^r$$

con lo que  $r_n = n$ . La estimación de Hayman (29.33) es:

$$\frac{1}{n!} \sim \frac{e^n}{n^n \sqrt{2\pi n}}$$

La fórmula de Stirling.

Veamos las condiciones de admisibilidad. En lo que sigue, las funciones  $a$  y  $b$  son las definidas por las ecuaciones (29.31) y (29.32), respectivamente. Sea  $f(z) = \sum_{n \geq 0} f_n z^n$  holomorfa en  $|z| < R$ , donde  $0 < R \leq \infty$ . Suponga que:

- (a) Existe  $R_0 < R$  tal que para  $R_0 < r < R$  es  $f(r) > 0$
- (b) Hay una función  $\delta(r)$ , definida para  $R_0 < r < R$ , tal que  $0 < \delta(r) < \pi$  en ese rango, y tal que cuando  $r \rightarrow R$ , uniformemente para  $|\theta| \leq \delta(r)$ , tenemos:

$$f(re^{i\theta}) \sim f(r)e^{i\theta a(r) - \frac{1}{2}\theta^2 b(r)}$$

(c) Uniformemente para  $\delta(r) \leq |\theta| \leq \pi$  tenemos cuando  $r \rightarrow R$ :

$$f(re^{i\theta}) = \frac{o(f(r))}{\sqrt{b(r)}}$$

Si esto se cumple,  $f$  es admisible y el teorema 29.9 da una estimación asintótica de los coeficientes.

Como puede verse, las condiciones son complejas de verificar. Hay teoremas que dan condiciones suficientes, mucho más sencillas de manejar. Para nuestra fortuna, corresponden a operaciones comunes con funciones generatrices.

- (A) Si  $f(z)$  es admisible, lo es  $e^{f(z)}$ .
- (B) Si  $f(z)$  y  $g(z)$  son admisibles para  $|z| < R$ , lo es  $f(z)g(z)$ .
- (C) Sea  $f(z)$  admisible en  $|z| < R$ . Sea  $p(z)$  un polinomio con coeficientes reales tal que  $p(R) > 0$  si  $R \neq \infty$ , o tal que el coeficiente de máximo grado es positivo si  $R = \infty$ . Entonces  $f(z)p(z)$  es admisible en  $|z| < R$ .
- (D) Sea  $p(z)$  un polinomio de coeficiente reales, y sea  $f(z)$  admisible en  $|z| < R$ . Si  $f(z) + p(z)$  es admisible, y el coeficiente de máximo grado de  $p$  es positivo, entonces  $p(f(z))$  es admisible.
- (E) Sea  $p(z)$  un polinomio no constante con coeficientes reales, y sea  $f(z) = e^{p(z)}$ . Si  $[z^n] e^{p(z)} > 0$  para todo  $n$  suficientemente grande, entonces  $f(z)$  es admisible en  $\mathbb{C}$ .

Como un ejemplo, tomemos las involuciones, con función generatriz exponencial (26.1):

$$e^{z+z^2/2}$$

Es claro que se cumplen las condiciones (E). Obtenemos:

$$a(r) = r + r^2 \quad b(r) = r + 2r^2$$

Tenemos una excelente aproximación para  $r_n$ :

$$\begin{aligned} r_n &= \sqrt{n+1/4} - 1/2 \\ &= \sqrt{n} \left(1 + \frac{1}{4n}\right)^n - \frac{1}{2} \\ &= \sqrt{n} \left(1 + \frac{1}{8n} - \frac{1}{128n^2} + \dots\right) - \frac{1}{2} \\ &= \sqrt{n} - \frac{1}{2} + \frac{1}{8n^{1/2}} - \frac{1}{128n^{3/2}} + \dots \end{aligned}$$

Una revisión de la fórmula (29.33) nos dice que requerimos estimaciones estilo  $\sim$  cuando  $n \rightarrow \infty$  de las cantidades  $f(r_n)$ ,  $b(r_n)$  y  $r_n^n$ . Por turno:

$$f(r_n) = e^{r_n + \frac{1}{2}r_n} = e^{\frac{1}{2}(r_n + n)} = e^{n/2} e^{r_n/2}$$

Pero:

$$e^{r_n/2} = \exp\left(\frac{\sqrt{n}}{2} - \frac{1}{4} + O(n^{-1/2})\right) \sim e^{\frac{1}{2}\sqrt{n} - \frac{1}{4}}$$

En la lista sigue  $b(r_n)$ :

$$b(r_n) = r_n + 2r_n^2 \sim 2(r_n^2 + r_n) = 2n$$

El último es el más complicado:

$$\begin{aligned} r_n^n &= \left( \sqrt{n} - \frac{1}{2} + \frac{1}{8\sqrt{n}} - \dots \right)^n \\ &= n^{n/2} \left( 1 - \frac{1}{2n^{1/2}} + \frac{1}{8n} - \dots \right)^n \end{aligned}$$

Esta situación debe tratarse con cuidado, a pesar de tender a 1 el paréntesis la potencia no necesariamente tiende a 1. La técnica general en estos casos es usar logaritmos para calcular la potencia:

$$\left( 1 - \frac{1}{2n^{1/2}} + \frac{1}{8n} - \dots \right)^n = \exp \left( n \ln \left( 1 - \frac{1}{2n^{1/2}} + \frac{1}{8n} - \dots \right) \right)$$

Luego expandimos el logaritmo en serie, hasta llegar a términos de orden  $o(n^{-1})$ . En nuestro caso:

$$\begin{aligned} \exp \left( n \ln \left( 1 - \frac{1}{2n^{1/2}} + \frac{1}{8n} - \dots \right) \right) &= \exp \left( n \left( \left( -\frac{1}{2n^{1/2}} + \frac{1}{8n} \right) - \frac{1}{2} \left( -\frac{1}{2n^{1/2}} + \frac{1}{8n} \right)^2 + O(n^{-3/2}) \right) \right) \\ &\sim \exp(-\sqrt{n}/2) \end{aligned}$$

con lo que:

$$r_n^n \sim n^{n/2} \exp(-\sqrt{n}/2)$$

Finalmente, uniendo las distintas piezas:

$$\frac{i_n}{n!} \sim \frac{e^{\frac{n}{2} + \sqrt{n} - \frac{1}{4}}}{2n^{n/2} \sqrt{\pi n}}$$

Mediante la fórmula de Stirling:

$$i_n \sim \frac{1}{\sqrt{2}} n^{n/2} \exp \left( -\frac{n}{2} + \sqrt{n} - \frac{1}{4} \right) \quad (29.34)$$

## Bibliografía

---

- [1] Niels Henrik Abel: *Beweis eines Ausdruckes, von welchem die Binomial-Formel ein einzelner Fall ist.* Journal für die reine und angewandte Mathematik, (1):159–160, 1826.
- [2] Forman S. Acton: *Numerical Methods that Work.* Mathematical Association of America, 1990.
- [3] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena: *PRIMES is in p.* Annals of Mathematics, 160(2):781–793, September 2004.
- [4] Alfred V. Aho, John E. Hopcroft, and Jeffrey D. Ullman: *The Design and Analysis of Computer Algorithms.* Addison-Wesley, 1974.
- [5] Martin Aigner: *A Course in Enumeration.* Number 238 in *Graduate Texts in Mathematics.* Springer, 2007.
- [6] Martin Aigner and Günter M. Ziegler: *Proofs from THE BOOK.* Springer, fifth edition, 2014.
- [7] Mohamad Akra and Louay Bazzi: *On the solution of linear recurrence equations.* Computational Optimization and Applications, 10(2):195–210, May 1998.
- [8] Michael Albert: *Basic counting principles.*  
<http://www.mathsolympiad.org.nz/wp-content/uploads/2009/01/counting.pdf>, January 2009.
- [9] W. R. Alford, Andrew Granville, and Carl Pommerance: *There are infinitely many Carmichael numbers.* Annals of Mathematics, 139(3):703–722, May 1994.
- [10] R. B. J. T. Allenby and Alan Slomson: *How to Count: An Introduction to Combinatorics.* CRC Press, second edition, 2011.
- [11] Ross Anderson and Serge Vaudenay: *Minding your P's and Q's.* In *Advances in Cryptology - ASIACRYPT'96, LNCS 1163*, pages 26–35. Springer, 1996.
- [12] Ross J. Anderson: *Security Engineering: A Guide to Building Dependable Distributed Systems.* John Wiley & Sons, second edition, 2008.
- [13] Désiré André: *Sur les Permutations Alternées.* Journal de Mathématiques Pures et Appliquées, 3<sup>e</sup> série, 7 :167–184, 1881.
- [14] Kenneth Appel and Wolfgang Haken: *Every planar map is four colorable. Part I: Discharging.* Illinois Journal of Mathematics, 21:429–490, 1977.
- [15] Kenneth Appel and Wolfgang Haken: *Every planar map is four colorable. Part II: Reducibility.* Illinois Journal of Mathematics, 21:491–567, 1977.

- [16] Krzysztof R. Apt: *Ten years of Hoare's logic: A survey – part I*. ACM Transactions on Programming Languages and Systems, 3(4):431–483, October 1981.
- [17] Krzysztof R. Apt: *Ten years of Hoare's logic: A survey – part II: Nondeterminism*. Theoretical Computer Science, 28(1-2):83–109, 1984.
- [18] Cecilia R. Aragon and Raimund G. Seidel: *Randomized search trees*. In *Thirtieth Annual Symposium on Foundations of Computer Science*, pages 540–545, October - November 1989.
- [19] Jörg Arndt: *Matters Computational: Ideas, Algorithms, Source Code*. Springer, 2011.
- [20] Emil Artin: *The Gamma Function*. Athena Series. Holt, Rinehart and Winston, 1964.
- [21] Robert B. Ash: *Basic Probability Theory*. Dover Publications, Inc., 2008.
- [22] Robert B. Ash and Phil Novinger: *Complex Variables*. Dover Publications, Inc., second edition, 2007.
- [23] Richard Askey: *Orthogonal Polynomials and Special Functions*, volume 21 of *CBMS-NSF Regional Conference Series in Applied Mathematics*. SIAM, 1975.
- [24] Daniel V. Bailey, Brian Baldwin, Lejla Batina, Daniel J. Bernstein, Peter Birkner, Joppe W. Bos, Gauthier van Damme, Giacomo de Meulenaer, Junfeng Fan, Tim Gueneysu, Frank Gurkaynak, Thorsten Kleinjung, Tanja Lange, Nele Mentens, Christof Paar, Francesco Regazzoni, Peter Schwabe, and Leif Uhsadel: *The Certicom challenges ECC2-X*. <http://cr.yp.to/papers.html#ecc2x>, September 2009.
- [25] Daniel V. Bailey, Lejla Batina, Daniel J. Bernstein, Peter Birkner, Joppe W. Bos, Hsieh Chung Chen, Chen Mou Cheng, Gauthier van Damme, Giacomo de Meulenaer, Luis Julian Dominguez Perez, Junfeng Fan, Tim Gueneysu, Frank Gurkaynak, Thorsten Kleinjung, Tanja Lange, Nele Mentens, Ruben Niederhagen, Christof Paar, Francesco Regazzoni, Peter Schwabe, Leif Uhsadel, Anthony Van Herrewege, and Bo Yin Yang: *Breaking ECC2K-130*. <http://cr.yp.to/papers.html#ecc2k130>, November 2009.
- [26] Cyril Banderier and Sylviane Schwer: *Why Delannoy numbers?* Journal of Statistical Planning and Inference, 135(1):40–54, November 2005.
- [27] Jørgen Bang-Jensen and Gregory Gutin: *Digraphs: Theory, Algorithms and Applications*. Springer, second edition, December 2009.
- [28] Edward J. Barbeau: *Mathematical Fallacies, Flaws, and Flimflam*. The Mathematical Association of America, 2000.
- [29] Christian Bauer, Alexander Frink, and Richard Kreckel: *Introduction to the GiNaC framework for symbolic computation within the C++ programming language*. Journal of Symbolic Computation, 33(1):1–12, January 2002.
- [30] Matthias Beck, Gerald Marchesi, Dennis Pixton, and Lucas Sabalka: *A first course in complex analysis*. <http://math.sfsu.edu/beck/complex.html>, 2012. Version 1.4.
- [31] Eric Temple Bell: *Exponential numbers*. The American Mathematical Monthly, 41:411–419, August 1934.
- [32] Richard Bellman: *On a routing problem*. Quarterly of Applied Mathematics, 16(1):87–90, 1958.

- [33] Edward A. Bender: *Asymptotic methods in enumeration*. SIAM Review, 16(4):485–515, October 1974.
- [34] Edward A. Bender and S. Gill Williamson: *Foundations of Combinatorics with Applications*. Dover Publications, Inc., 2006.
- [35] Arthur T. Benjamin and Jennifer J. Quinn: *Proofs that Really Count: The Art of Combinatorial Proof*. Dolciani Mathematical Expositions. The Mathematical Association of America, 2003.
- [36] Jon Louis Bentley: *Writing Efficient Programs*. Software Series. Prentice-Hall, 1982.
- [37] Jon Louis Bentley: *Programming Pearls*. Prentice Hall, second edition, 2000.
- [38] Jon Louis Bentley, Dorothea Haken, and James B. Saxe: *A general method for solving divide-and-conquer recurrences*. ACM SIGACT News, 12(3):36–44, Fall 1980.
- [39] Jon Louis Bentley and M. Douglas McIlroy: *Engineering a sort function*. Software: Practice and Experience, 23(11):1249–1265, November 1993.
- [40] Daniel J. Bernstein: *Research announcement: Faster factorization into coprimes*. <http://cr.yp.to/papers.html#dcba2>, November 2004.
- [41] Daniel J. Bernstein: *Factoring into coprimes in essentially linear time*. Journal of Algorithms, 54(1):1–30, January 2005.
- [42] Daniel J. Bernstein, Peter Birkner, Tanja Lange, and Christiane Peters: *ECM using Edwards curves*. Cryptology ePrint Archive, Report 2008/016, 2008.
- [43] Daniel J. Bernstein, Tanja Lange, and Peter Schwabe: *The security impact of a new cryptographic library*. In Alejandro Hevia and Gregory Neven (editors): *Progress in Cryptology – LATINCRYPT 2012*, volume 7533 of *Lecture Notes in Computer Science*, pages 159–176. Springer, October 2012.
- [44] Daniel M. Berry: *Academic legitimacy of the software engineering discipline*. Technical Report CMU/SEI-92-TR-34, Software Engineering Institute, November 1992.
- [45] J. Bertrand: *Mémoire sur le nombre des valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme*. Journal de l'Ecole Royale Polytechnique, 17:123–140, 1845.
- [46] W. A. Blankinship: *A new version of the Euclidean algorithm*. The American Mathematical Monthly, 70(7):742–745, September 1963.
- [47] Kenneth P. Bogart and Peter G. Doyle: *Non-sexist solution of the ménage problem*. The American Mathematical Monthly, 93(7):514–518, August - September 1986.
- [48] Alexander Bogomolny: *Sylvester's problem: A second look*. <http://www.cut-the-knot.org/blue/Sylvester2.shtml>, October 2012.
- [49] Dan Boneh: *Twenty years of attacks on the RSA cryptosystem*. Notices of the AMS, 46(2):203–213, February 1999.
- [50] Jorge Luis Borges: *La Biblioteca de Babel*. En *El Jardín de los Senderos que se Bifurcan*. Editorial Sur, 1941.
- [51] Alin Bostan, Frédéric Chyzak, Bruno Salvy, Grégoire Lecerf, and Éric Schost: *Differential equations for algebraic functions*. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, ISSAC '07, pages 25–32, New York, NY, USA, 2007. ACM.

- [52] Louis Brand: *A sequence defined by a difference equation*. American Mathematical Monthly, 62(7):489–492, September 1955.
- [53] Richard P. Brent: *An improved Monte Carlo factorization algorithm*. BIT Numerical Mathematics, 20(2):176–184, 1980.
- [54] Richard P. Brent and Paul Zimmermann: *Modern Computer Arithmetic*. Number 18 in *Cambridge Monographs on Computational and Applied Mathematics*. Cambridge University Press, November 2010.
- [55] Duane M. Broline: *Renumbering the faces of dice*. Mathematics Magazine, 52(5):312–315, November 1979.
- [56] Stephen I. Brown and Marion I. Walter: *The Art of Problem Posing*. Lawrence Erlbaum Associates, third edition, 2005.
- [57] Andrew M. Bruckner, Brian S. Thomson, and Judith B. Bruckner: *Mathematical Discovery*. ClassicalRealAnalysis.com, 2011.
- [58] A. di Bucchianico and D. Loeb: *A selected survey of umbral calculus*. The Electronic Journal of Combinatorics, DS3, 2000.
- [59] William Burnside: *Theory of Groups of Finite Order*. Cambridge University Press, 1897.
- [60] Cristian Cadar, Daniel Dunbar, and Dawson Engler: *KLEE: Unassisted and automatic generation of high-coverage tests for complex systems programs*. In *Proceedings of the 8th USENIX Symposium on Operating Systems Design and Implementation*, pages 209–224. USENIX, December 2008.
- [61] George Cain: *Complex Analysis*. Georgia Institute of Technology, 2001.  
<http://people.math.gatech.edu/~cain/winter99/complex.html>.
- [62] Cristian S. Calude, Elena Calude, and Solomon Marcus: *Proving and programming*. Technical Report 309, CDMTCS, University of Auckland, NZ, June 2007.
- [63] Robert Daniel Carmichael: *Note on a new number theory function*. Bulletin of the American Mathematical Society, 16(5):232–238, February 1910.
- [64] David A. Carte: *A review of the Diffie-Hellman algorithm and its use in secure Internet protocols*.  
[http://www.sans.org/reading\\_room/whitepapers/vpns/review-diffie-hellman-algorithm-secure-internet-protocols\\_751](http://www.sans.org/reading_room/whitepapers/vpns/review-diffie-hellman-algorithm-secure-internet-protocols_751), November 2001.
- [65] Augustin Louis Cauchy: *Cours d'Analyse de l'Ecole Royale Polytechnique, première partie, Analyse Algébrique*. Impr. Royale Debure frères, 1821.
- [66] Arthur Cayley: *A theorem on trees*. Quarterly Journal of Mathematics, 23:376–378, 1889.
- [67] Certicom: *Certicom ECC challenge*.  
<http://www.certicom.com/index.php/the-certicom-ecc-challenge>, 1997.
- [68] Gregory J. Chaitin: *Register allocation & spilling via graph coloring*. SIGPLAN Notices, 17:98–101, June 1982.
- [69] Pafnuty L. Chebyshev: *Mémoire sur les nombres premiers*. Mémoires de la Academie Scientifique de St. Pétersbourg, 7 :17–33, 1954.

- [70] William W. L. Chen: *First year calculus*.  
<http://rutherglen.science.mq.edu.au/wchen/lnfycfolder/lnfyc.html>, 2008.
- [71] William W. L. Chen: *Fundamentals of analysis*.  
<http://rutherglen.science.mq.edu.au/wchen/lnfafolder/lnfa.html>, 2008.
- [72] William W. L. Chen: *Introduction to complex analysis*.  
<http://rutherglen.science.mq.edu.au/wchen/lnicafolder/lnica.html>, 2008.
- [73] William W. L. Chen: *Miscelaneous topics in first year mathematics*.  
<http://rutherglen.science.mq.edu.au/~maths/notes/wchen/-lnmtfymfolder/lnmtfym.html>, 2008.
- [74] Barry A. Cipra: *How the Grinch stole mathematics*. Science, 245:595, August 1989.
- [75] Sir Arthur Ignatius Conan Doyle: *The Sign of the Four*. Spencer Blackett, February 1890.
- [76] Edwin H. Connell: *Elements of abstract and linear algebra*.  
<http://www.math.miami.edu/~ec/book>, March 2004.
- [77] John B. Conway: *Functions of One Complex Variable I*, volume 11 of *Graduate Texts in Mathematics*. Springer, second edition, 1978.
- [78] Stephen A. Cook: *The complexity of theorem proving procedures*. In *Proceedings of the Third Annual ACM Symposium on Theory of Computing*, pages 151–158, 1971.
- [79] James W. Cooley and John W. Tukey: *An algorithm for the machine calculation of complex Fourier series*. Mathematics of Computation, 19(90):297–301, April 1965.
- [80] Don Coppersmith, Matthew Franklin, Jacques Patarin, and Michael Reiter: *Low-exponent RSA with related messages*. In *Advances in Cryptology – EUROCRYPT’96*, pages 1–7, 1996.
- [81] *The Coq proof assistant*. <http://coq.inria.fr>, August 2012. Version 8.4.
- [82] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein: *Introduction to Algorithms*. MIT Press, third edition, 2009.
- [83] Romain Cosset: *Factorization with genus 2 curves*. Mathematics of Computation, 79(270):1191–1208, August 2010.
- [84] Pascal Cuoq, Florent Kirchner, Nikolai Kosmatov, Virgile Prevosto, Julien Signoles, and Boris Yakobowski: *Frama-C, A software analysis perspective*. In G. Eleftherakis, M. Hinckey, and M. Holcombe (editors): *International Conference on Software Engineering and Formal Methods*, volume 7504 of *LNCS*, pages 233–247. Springer, October 2012.
- [85] Matt Curtin: *Snake oil warning signs: Encryption software to avoid*.  
<http://www.interhack.net/people/cmcurtin/snake-oil-faq.html>, April 1998.
- [86] Larry W. Cusick: *How to write proofs*.  
<http://zimmer.csufresno.edu/~larryc/proofs/proofs.html>.
- [87] Richard A. De Millo, Richard J. Lipton, and Alan J. Perles: *Social processes and proofs of theorems and programs*. Communications of the ACM, 22(5):271–280, May 1979.
- [88] Jean Paul Delahaye: *The science behind Sudoku*. Scientific American, 294:80–87, June 2006.

- [89] Henri Delannoy: *Sur une Question de Probabilités traitée par d'Alembert*. Bulletin de la Société Mathématique de France, 23 :262–265, 1895.
- [90] L. Dewaghe: *Remarks on the Schoof-Elkies-Atkin algorithm*. Mathematics of Computation, 67(223):1247–1252, July 1998.
- [91] Reinhard Diestel: *Graph Theory*. Graduate Texts in Mathematics. Springer, fourth edition, 2010.
- [92] Edsger W. Dijkstra: *The cruelty of teaching computer science*. Communications of the ACM, 32(12):1397–1404, December 1989.
- [93] Edsger W. Dijkstra: *A note on two problems in connexion with graphs*. Numerische Mathematik, 1(1):269–271, 1959.
- [94] Edsger W. Dijkstra: *A Discipline of Programming*. Prentice Hall, 1976.
- [95] Dušan Djukić: *Arithmetic in extensions of  $\mathbb{Q}$* . [http://www.imomath.com/tekstkut/extensions\\_ddj.pdf](http://www.imomath.com/tekstkut/extensions_ddj.pdf), 2007.
- [96] Dušan Djukić: *Pell's equation*. [http://www.imomath.com/tekstkut/pelleqn\\_ddj.pdf](http://www.imomath.com/tekstkut/pelleqn_ddj.pdf), 2007.
- [97] G. Dobiński: *Summirung der Reihe  $\sum \frac{n^m}{n!}$  für  $m = 1, 2, 3, 4, 5, \dots$* . Grunert's Archiv, 61:333–336, 1877.
- [98] Vladimir A. Dobrushkin: *Methods in Algorithmic Analysis*. Chapman & Hall/CRC, 2010.
- [99] Robert Donaghey and Louis W. Shapiro: *Motzkin numbers*. Journal of Combinatorial Theory, Series A, 23(3):291–301, November 1977.
- [100] Jack Dongarra and Francis Sullivan: *Guest editor introduction to the top 10 algorithms*. Computing in Science and Engineering, 2(1):22–23, January/February 2000.
- [101] Leo Dorst, Daniel Fontijne, and Stephen Mann: *Geometric Algebra for Computer Science*. Morgan Kaufmann, 2007.
- [102] Michael Drmota and Wojciech Szpankowski: *A master theorem for discrete divide and conquer recurrences*. In *Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '11, pages 342–361. SIAM, 2011.
- [103] William Dunham: *Journey through Genius: The Great Theorems of Mathematics*. Penguin Books, 1990.
- [104] William Dunham: *The Mathematical Universe: An Alphabetical Journey Through the Great Proofs, Problems, and Personalities*. John Wiley & Sons, Inc., 1997.
- [105] William Dunham: *When Euler met l'Hôpital*. Mathematics Magazine, 82(1):16–25, February 2009.
- [106] Richard A. Dunlap: *The Golden Ratio and Fibonacci Numbers*. World Scientific Publishing Co., March 1998.
- [107] Ivo Düntsch and Günther Gediga: *Sets, Relations, Functions*, volume 1 of *Primers*. Methodos, 2000.

- [108] Glenn Durfee: *Cryptanalysis of RSA Using Algebraic and Lattice Methods*. PhD thesis, Department of Computer Science, Stanford University, June 2002.
- [109] Standard curves and curve generation.  
<http://www.ecc-brainpool.org/download/Domain-parameters.pdf>, October 2005.
- [110] Jack Edmonds and Richard M. Karp: *Theoretical improvements in algorithmic efficiency for network flow problems*. Journal of the ACM, 19(2):248–264, 1972.
- [111] Georgy P. Egorychev: *Integral Representation and the Computation of Combinatorial Sums*, volume 59 of *Translations of Mathematical Monographs*. American Mathematical Society, 1984.
- [112] Taher ElGamal: *A public key cryptosystem and a signature scheme based on discrete logarithms*. IEEE Transactions on Information Theory, IT-31(4):469–472, July 1985.
- [113] David Eppstein: *Nineteen proofs of Euler's formula:  $v - e + f = 2$* .  
<http://www.ics.uci.edu/~eppstein/junkyard/euler>, October 2005.
- [114] Paul Erdős: *Beweis eines Satzes von Tschebyschef*. Acta Scientiarum Mathematicarum Szegediensis, 5(3-4):194–198, 1930–1932.
- [115] Paul Erdős: *Über die Reihe  $\sum \frac{1}{p}$* . Mathematica, Zutphen B 7:1–2, 1938.
- [116] Paul Erdős, Adolf J. Hildebrand, Andrew Odlyzko, Paul Pudaite, and Bruce Reznick: *The asymptotic behavior of a family of sequences*. Pacific Journal of Mathematics, 126(2):227–241, 1987.
- [117] William Feller: *An Introduction to Probability Theory and its Applications*, volume 1. John Wiley & Sons, third edition, 1968.
- [118] William Feller: *An Introduction to Probability Theory and its Applications*, volume 2. John Wiley & Sons, second edition, 1971.
- [119] Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno: *Cryptography Engineering*. John Wiley & Sons, 2010.
- [120] Mark Finkelstein and Edward O. Thorp: *Nontransitive dice with equal means*. In Stewart N. Ethier and William R. Eadington (editors): *Optimal Play: Mathematical Studies of Games and Gambling*, pages 293–310. Institute for the Study of Gambling and Commercial Gaming, December 2007, ISBN 0-9796873-0-6.
- [121] Secure Hash Standard (SHS). Federal Information Processing Standards Publication 180-3, October 2008.  
[http://csrc.nist.gov/publications/fips/fips180-3/fips180-3\\_final.pdf](http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf).
- [122] Digital Signature Standard (DSS). Federal Information Processing Standards Publication 186, May 1994. <http://www.itl.nist.gov/fipspubs/fip186.htm>.
- [123] Digital Signature Standard, change no. 1. Federal Information Processing Standards Publication 186, December 1996. <http://www.itl.nist.gov/fipspubs/186chg-1.htm>.
- [124] Digital Signature Standard. Federal Information Processing Standards Publication 186, June 2009. [http://csrc.nist.gov/publications/fips/fips186-3/fips\\_186-3.pdf](http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf).
- [125] Digital Signature Standard. Federal Information Processing Standards Publication 186, July 2013. <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>.

- [126] Philipe Flajolet and Robert Sedgewick: *Analytic Combinatorics*. Cambridge University Press, 2009.
- [127] Philipe Flajolet and Michèle Soria: *The cycle construction*. SIAM Journal of Discrete Mathematics, 4(1):58–60, February 1991.
- [128] Phillippe Flajolet and Andrew M. Odlyzko: *Singularity analysis of generating functions*. SIAM Journal of Discrete Mathematics, 3(2):216–240, May 1990.
- [129] M. Fleury: *Deux Problèmes de Géométrie de Situation*. Journal de Mathematiques Élémentaires, 2:257–261, 1883.
- [130] Robert W. Floyd: *Algorithm 97: Shortest path*. Communications of the ACM, 5(6):345, June 1962.
- [131] Robert W. Floyd: *Assigning meaning to programs*. Proceedings of the American Mathematical Society Symposia on Applied Mathematics, 19:19–31, 1967.
- [132] Robert W. Floyd: *Non-deterministic algorithms*. Journal of the ACM, 14(4):636–644, October 1967.
- [133] Lester R. Ford Jr and Delbert R. Fulkerson: *Maximal flow through a network*. Canadian Journal of Mathematics, 8:399–404, 1956.
- [134] M. K. Franklin and M. K. Reiter: *A linear protocol failure for RSA with exponent three*. In *CRYPTO'95 Rump Session*, August 1995.
- [135] Michael Lawrence Fredman and Robert E. Tarjan: *Fibonacci heaps and their uses in improved network optimization algorithms*. Journal of the ACM, 34(3):596–615, July 1987.
- [136] Robert Frucht: *Herstellung von Graphen mit vorgegebener abstrakter Gruppe*. Compositio Mathematica, 6:239–250, 1939.
- [137] Martin Fürer: *Faster integer multiplication*. In *Proceedings of the ACM Symposium on the Theory of Computing*, volume 39, pages 57–66, 2007.
- [138] Joseph A. Gallian and David J. Rusin: *Cyclotomic polynomials and nonstandard dice*. Discrete Mathematics, 27(3):245–259, December 1979.
- [139] The GAP Group: *GAP – Groups, Algorithms, and Programming, Version 4.7.5*, 2014. <http://www.gap-system.org>.
- [140] Martin Gardner: *Mathematical games*. Scientific American, 238(2):19–32, February 1978.
- [141] Michael R. Garey and David S. Johnson: *Computers and Intractability: A Guide to the Theory of NP-completeness*. A Series of Books in the Mathematical Sciences. W. H. Freeman and Co., 1979.
- [142] GiNaC version 1.6.2. <http://www.ginac.de/Download.html>, November 2011.
- [143] Georges Gonthier: *Formal proof – the four color theorem*. Notices of the American Mathematical Society, 55(11):1382–1393, December 2008.
- [144] I. J. Good: *The number of orderings of  $n$  candidates when ties are permitted*. The Fibonacci Quarterly, 13(1):11–18, February 1975.

- [145] John Goodenough and Sue L. Gerhart: *Toward a theory of test data selection*. IEEE Transactions on Software Engineering, SE-1(2):156–173, June 1975.
- [146] John Gordon: *The Alice and Bob after dinner speech*.  
<http://downlode.org/Etext/alicebob.html>, April 1984. Given at the Zurich Seminar.
- [147] Mike Gordon and Hélène Collavizza: *Forward with Hoare*. In A. W. Roscoe, Cliff B. Jones, and Kenneth R. Wood (editors): *Reflections on the Work of C.A.R. Hoare*, History of Computing, pages 101–121. Springer London, 2010.
- [148] Ian P. Goulden and David M. Jackson: *Combinatorial Enumeration*. Dover Publications, Inc., 2004.
- [149] Xavier Gourdon and Pascal Sebah: *The Euler constant:  $\gamma$* .  
<http://numbers.computation.free.fr/Constants/Gamma/gamma.html>, February 2003.
- [150] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik: *Concrete Mathematics: A Foundation for Computer Science*. Addison-Wesley Professional, second edition, 1994.
- [151] Torbjörn Granlund *et al.*: *The GNU multiple precision arithmetic library, version 6.0.0*.  
<http://gmplib.org>, March 2014.
- [152] Daniel H. Greene and Donald E. Knuth: *Mathematics for the Analysis of Algorithms*. Modern Birkhäuser Classics. Birkhäuser, 2010.
- [153] David Gries: *The Science of Programming*. Springer, 1987.
- [154] Charles M. Grinstead and J. Laurie Snell: *Introduction to Probability*. American Mathematical Society, second edition, 1997.
- [155] Leonidas J. Guibas and Andrew M. Odlyzko: *String overlaps, pattern matching, and nontransitive games*. Journal of Combinatorial Theory, Series A, 30(2):183–208, March 1981.
- [156] Peter Gutmann: *Cryptographic Security Architecture: Design and Verification*. Springer, 2004.
- [157] Bruno Haible and Richard B. Kreckel: *CLN, a Class Library for Numbers*, October 2014.  
<http://www.ginac.de/CLN>, Version 1.3.4.
- [158] Seifollah L. Hakimi: *On realizability of a set of integers as degrees of the vertices of a linear graph*. Journal of the Society for Industrial and Applied Mathematics, 10(3):496–506, September 1962.
- [159] Phillip Hall: *On representatives of subsets*. Journal of the London Mathematical Society, 10(1):26–30, 1935.
- [160] William Rowan Hamilton: *On quaternions, or on a new system of imaginaries in algebra*. Philosophical Magazine, 25(3):489–495, 1844.
- [161] Richard Hammack: *The Book of Proof*, volume 1 of *Mathematics Textbook Series*. Virginia Commonwealth University Mathematics, second edition, 2013.
- [162] Richard W. Hamming: *Error detecting and correcting codes*. Bell System Technical Journal, 29(2):147–160, April 1950.
- [163] Richard W. Hamming: *The unreasonable effectiveness of mathematics*. The American Mathematical Monthly, 87(2):81–90, February 1980.

- [164] Darrel Hankerson, Alfred J. Menezes, and Scott Vanstone: *Guide to Elliptic Curve Cryptography*. Springer, 2004.
- [165] Helmut Hasse: *Zur Theorie der abstrakten elliptischen Funktionenkörper. I. Die Struktur der Gruppe der Divisorenklassen endlicher Ordnung*. Journal für Reine und Angewandte Mathematik, (175):55–62, 1936.
- [166] Helmut Hasse: *Zur Theorie der abstrakten elliptischen Funktionenkörper. II. Automorphismen und Meromorphismen. Das Additionstheorem*. Journal für Reine und Angewandte Mathematik, (175):69–88, 1936.
- [167] Helmut Hasse: *Zur Theorie der abstrakten elliptischen Funktionenkörper. III. Die Struktur des Meromorphismenringes. Die Riemannsche Vermutung*. Journal für Reine und Angewandte Mathematik, (175):193–208, 1936.
- [168] Heba Hathout: *The old hats problem*. Undergraduate Mathematics Journal, 4(1), 2003.
- [169] Heba Hathout: *The old hats problem revisited*. The College Mathematics Journal, 35(2):97–102, March 2004.
- [170] Václav Havel: *Poznámka o existenci konečných grafů*. Časopsis pro pěstování matematiky, 80(4):477–480, 1955.
- [171] Walter K. Hayman: *A generalization of Stirling's formula*. Journal für die reine und angewandte Mathematik, (196):67–95, January 1956.
- [172] Michael T. Heideman, Don H. Johnson, and C. Sidney Burrus: *Gauß and the history of the Fast Fourier Transform*. IEEE ASSP Magazine, 1(4):14–21, October 1984.
- [173] Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman: *Mining your Ps and Qs: Detection of widespread weak keys in network devices*. In *Proceedings of the 21st USENIX Security Symposium*, August 2012.
- [174] Carl Hierholzer: *Über die Möglichkeit, einen Linienzug ohne Wiederholung und ohne Unterbrechung zu umfahren*. Mathematische Annalen, 6(1):30–32, 1873.
- [175] C. A. R. Hoare: *Quicksort*. Computer Journal, 5(1):10–15, April 1962.
- [176] C. A. R. Hoare: *An axiomatic basis for computer programming*. Communications of the ACM, 12(10):576–580, 583, October 1969.
- [177] C. A. R. Hoare: *The emperor's old clothes*. Communications of the ACM, 24(2):75–83, February 1981. Turing award lecture.
- [178] John E. Hopcroft and Richard M. Karp: *An  $n^{5/2}$  algorithm for maximum matchings in bipartite graphs*. SIAM Journal on Computing, 2(4):225–231, 1973.
- [179] John E. Hopcroft, Rajeev Motwani, and Jeffrey D. Ullman: *Introduction to Automata Theory, Languages, and Computation*. Addison-Wesley, third edition, 2006.
- [180] Guillaume Marquis de l'Hôpital: *Analyse des Infiniment Petits pour l'Intelligence des Lignes Courbes*. Paris, France, 1696.
- [181] IEEE Standard for local and metropolitan area networks: Media access control (MAC) bridges. IEEE Std 802.1d-2004, 2004.

- [182] International Organization for Standardization: *Information technology – Programming languages – C++*. ISO/IEC 14882:2011, 2011.
- [183] Kenneth E. Iverson: *A Programming Language*. John Wiley & Sons, 1962.
- [184] Ray Jennings and Andrew Hartline: *Disjunction*. In Edward N. Zalta (editor): *The Stanford Encyclopedia of Philosophy*. Center for the Study of Language and Information, Stanford University, summer 2009 edition, 2013.
- [185] William S. Jevons: *The Principles of Science: A Treatise on Logic and Scientific Method*. Macmillan, 1874.
- [186] Arne T. Jonassen and Donald E. Knuth: *A trivial algorithm whose analysis isn't*. Journal of Computer and System Sciences, 16(3):301–322, June 1978.
- [187] Cliff B. Jones: *The early search for tractable ways of reasoning about programs*. IEEE Annals of the History of Computing, 25(2):26–49, April/June 2003.
- [188] Camille Jordan: *Cours d'analyse de l'École Polytechnique : Calcul intégral Équations différentielles*, tome 3. Gauthier-Villars, Paris, France, 1887.
- [189] David Joyner: *Adventures in group theory: Rubik's cube, Merlin's machine, and Other Mathematical Toys*. Johns Hopkins University Press, second edition, 2008.
- [190] Thomas W. Judson: *Abstract Algebra: Theory and Applications*. Virginia Commonwealth University Mathematics, 2014.
- [191] R. Jungen: *Sur les séries de Taylor n'ayant que des singularités algébriko-logarithmiques sur leur cercle de convergence*. Comentarii Mathematici Helvetici, 3 :266–306, 1931.
- [192] Arthur B. Kahn: *Topological sorting of large networks*. Communications of the ACM, 5(11):558–562, November 1962.
- [193] Dan Kalman: *Six ways to sum a series*. The College Mathematics Journal, 24(5):402–421, November 1993.
- [194] Irving Kaplansky: *Solution to the “problème des ménages”*. Bulletin of the American Mathematical Society, 49(10):784–785, October 1943.
- [195] Jovan Karamata: *Théorèmes sur la Sommabilité Exponentielle et d'autres Sommabilités Rattachant*. Mathematica (Cluj), 9 :164–178, 1935.
- [196] A. Karatsuba and Yu. Ofman: *Multiplication of many-digital numbers by automatic computers*. Proceedings of the USSR Academy of Sciences, 145:293–294, 1962.
- [197] Richard M. Karp: *Reducibility among combinatorial problems*. In R. E. Miller and J. W. Thatcher (editors): *Complexity of Computer Computations*, pages 85–103. Plenum Press, 1972.
- [198] Manuel Kauers and Peter Paule: *The Concrete Tetrahedron: Symbolic Sums, Recurrence Equations, Generating Functions, Asymptotic Estimates*. Texts and Monographs in Symbolic Computation. Springer, 2011.
- [199] James Kelley and Morgan Walker: *Critical-path planning and scheduling*. In *Proceedings of the Eastern Joint Computer Conference*, 1959.

- [200] Alfred B. Kempe: *A memoir on the theory of mathematical form*. Philosophical Transactions of the Royal Society of London, 177:1–70, 1886.
- [201] Brian W. Kernighan and Rob Pike: *The Practice of Programming*. Addison-Wesley Professional, 1999.
- [202] Brian W. Kernighan and Dennis M. Ritchie: *The C Programming Language*. Prentice Hall, second edition, 1988.
- [203] J. Kiefer: *Sequential minimax search for a maximum*. Proceedings of the American Mathematical Association, 4:502–506, 1953.
- [204] Gerwin Klein: *The L4.verified project*.  
<http://ertos.nicta.com.au/research/l4.verified>, 2011.
- [205] Gerwin Klein, June Andronick, Kevin Elphinstone, Gernot Heiser, David Cock, Philip Derrin, Dharmika Elkaduve, Kai Engelhardt, Rafal Kolanski, Michael Norrish, Thomas Sewell, Harvey Tuch, and Simon Winwood: *seL4: Formal verification of an operating-system kernel*. Communications of the ACM, 53(6):107–115, June 2010.
- [206] Israel Kleiner: *Rigor and proof in mathematics: A historical perspective*. Mathematics Magazine, 64(5):291–314, December 1991.
- [207] Israel Kleiner and Nitsa Movshovitz-Hadar: *The role of paradoxes in the evolution of mathematics*. The American Mathematical Monthly, 101:963–974, 1994.
- [208] Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen Lenstra, Emmanuel Thomé, Joppe Bos, Pierrick Gaudry, Alexander Kruppa, Peter Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev, and Paul Zimmermann: *Factorization of a 768-bit RSA modulus*. Cryptology ePrint Archive, Report 2010/006, 2010.
- [209] Donald E. Knuth: *Structured programming with go to statements*. Computing Surveys, 6(4):261–301, December 1974.
- [210] Donald E. Knuth: *Big Omicron and big Omega and big Theta*. ACM SIGACT News, 8(2):18–24, April 1976.
- [211] Donald E. Knuth: *Notes on the van Emde Boas construction of priority queues: An instructive use of recursion*. Cited by the author on his webpage,  
<http://www-cs-faculty.stanford.edu/~knuth/faq.html>, March 1977.
- [212] Donald E. Knuth: *The errors of TeX*. Software: Practice and Experience, 19(7):607–685, July 1989.
- [213] Donald E. Knuth: *Two notes on notation*. The American Mathematical Monthly, 99(5):403–422, May 1992.
- [214] Donald E. Knuth: *Johann Faulhaber and sums of powers*. Mathematics of Computation, 61(203):277–294, July 1993.
- [215] Donald E. Knuth: *Bracket notation for the ‘coefficient of’ operator*. In A. W. Roscoe (editor): *A Classical Mind, Essays in Honour of C. A. R. Hoare*, pages 247–258. Prentice Hall, 1994.
- [216] Donald E. Knuth: *Fundamental Algorithms*, volume 1 of *The Art of Computer Programming*. Addison-Wesley, third edition, 1997.

- [217] Donald E. Knuth: *Seminumerical Algorithms*, volume 2 of *The Art of Computer Programming*. Addison-Wesley, third edition, 1997.
- [218] Donald E. Knuth: *Sorting and Searching*, volume 3 of *The Art of Computer Programming*. Addison-Wesley, second edition, 1998.
- [219] Donald E. Knuth: *Combinatorial Algorithms, Part 1*, volume 4a of *The Art of Computer Programming*. Addison-Wesley, 2011.
- [220] Donald E. Knuth, Tracy L. Larrabee, and Paul M. Roberts: *Mathematical Writing*. Mathematical Association of America, 1989.
- [221] Donald E. Knuth and Arnold Schönhage: *The expected linearity of a simple equivalence algorithm*. Theoretical Computer Science, 6(3):281–315, 1978.
- [222] Donald E. Knuth and Herbert S. Wilf: *A short proof of Darboux's lemma*. Applied Mathematics Letters, 2(2):139–140, 1989.
- [223] Dénes König: *Theorie der endlichen und unendlichen Graphen*. Akademische Verlagsgesellschaft, Leipzig, 1936.
- [224] Alvin R. Korselt: *Problème Chinois*. L'Intermédiaire des Mathématiciens, 6:142–143, 1899.
- [225] Joseph B. Kruskal: *On the shortest spanning subtree of a graph and the traveling salesman problem*. Proceedings of the American Mathematical Society, 7(1):48–50, February 1956.
- [226] Thomas S. Kuhn: *The Structure of Scientific Revolutions*. The University of Chicago Press, second edition, 1970.
- [227] Jeffrey C. Lagarias: *Euler's constant: Euler's work and modern developments*. Bulletin of the American Mathematical Society, 50(4):527–628, October 2013.
- [228] Ivo Lah: *A new kind of numbers and its application in the actuarial mathematics*. Boletim do Instituto dos Actuarios Portugueses, 9:7–15, June 1954.
- [229] Michael Lambrou: *Mathematical induction: Notes for the teacher I*. Creative Mathematics and Informatics, 14:19–30, 2005.
- [230] Michael Lambrou: *Mathematical induction: Notes for the teacher II*. Creative Mathematics and Informatics, 15:117–132, 2006.
- [231] Gabriel Lamé: *Note sur la limite du nombre des divisions dans la recherche du plus grand commun diviseur entre deux nombres entiers*. Comptes Rendus de l'Académie des Sciences, 19:867–870, 1844.
- [232] Nate Lawson: *DSA requirements for random k value*.  
<http://rdist.root.org/2010/11/19/dsa-requirements-for-random-k-value>, November 2010.
- [233] Burt Leavenworth: *Review #19420*. Computing Reviews, 11:396–397, 1970.
- [234] Eric Lehman, F. Thomson Leighton, and Albert R. Meyer: *Mathematics for Computer Science*.  
<http://courses.csail.mit.edu/6.042/spring15/mcs.pdf>, May 2015.
- [235] Tom Leighton: *Notes on better master theorems for divide-and-conquer recurrences*.  
<http://citeseer.ist.psu.edu/252350.html>, 1996.

- [236] Franz Lemmermeyer: *Quadratische Zahlkörper Schnupperkurs.* <http://www.rzuser.uni-heidelberg.de/~hb3/publ/qzk.pdf>, 1999.
- [237] Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, and Christophe Wachter: *Ron was wrong, Whit is right.* Cryptology ePrint Archive, Report 2012/064, 2012.
- [238] Hendrik W. Lenstra, Jr.: *Factoring integers with elliptic curves.* The Annals of Mathematics, 126(3):649–673, November 1987.
- [239] Hendrik W. Lenstra, Jr.: *Solving the Pell equation.* Notices of the AMS, 49(2):182–192, February 2002.
- [240] C. L. Liu: *Introduction to Combinatorial Mathematics.* Computer Science Series. McGraw-Hill, 1968.
- [241] Ralph L. London: *Software reliability through proving programs correct.* In *Proceedings of the IEEE International Symposium on Fault Tolerant Computing*, pages 125–129, March 1971.
- [242] London underground railways. [http://upload.wikimedia.org/wikipedia/commons/9/90/Tube\\_map\\_1908-2.jpg](http://upload.wikimedia.org/wikipedia/commons/9/90/Tube_map_1908-2.jpg), 1908.
- [243] Elisha Scott Loomis: *The Pythagorean Proposition.* The National Council of Teachers of Mathematics, 1968.
- [244] Circuit diagram of a 3rd order low pass filter using passive components (2 resistors, 2 capacitors, 1 inductor). <http://commons.wikimedia.org/wiki/File:LowPass3poleCauer.png>, July 2006.
- [245] Édouard Lucas: *Théorie des nombres.* Gautier-Villars, Paris, France, 1891.
- [246] Ben Lynn: *The Wallis product.* <http://crypto.stanford.edu/pbc/notes/pi/wallis.html>.
- [247] D. G Malcolm, H. Rosenboom, J. C. E. Clark, and W. Fazar: *Applications of a technique for research and development program evaluation.* Operations Research, 7(5):646–669, 1959.
- [248] G. Malkin: *RIP version 2.* IETF RFC 4822, November 1998.
- [249] Conrado Martínez and Salvador Roura: *Randomized binary search trees.* Journal of the ACM, 45(2):288–323, March 1998.
- [250] Yoshio Matsuoka: *On a proof of Hermite's identity.* The American Mathematical Monthly, 71(10):1115, December 1964.
- [251] *Maxima, a computer algebra system.* <http://maxima.sourceforge.net>, December 2014. Version 5.35.1.
- [252] M. Douglas McIlroy: *A killer adversary for Quicksort.* Software: Practice and Experience, 29(4):341–344, April 1999.
- [253] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone: *Handbook of Applied Cryptography.* CRC Press, 1996.

- [254] Donatella Merlini, Renzo Sprugnoli, and Maria Cecilia Verri: *The method of coefficients*. The American Mathematical Monthly, 114(1):40–57, January 2007.
- [255] Gary L. Miller: *Riemann's hypothesis and tests for primality*. Journal of Computer and System Sciences, 13(3):300–317, December 1976.
- [256] Louis Melville Milne-Thomson: *The Calculus of Finite Differences*. Macmillan and Co., 1933.
- [257] Douglas W. Mitchell: *An analytic Riccati solution for two-target discrete-time control*. Journal of Economic Dynamics and Control, 24(4):615–622, April 2000.
- [258] Louis Monier: *Evaluation and comparison of two efficient probabilistic primality testing algorithms*. Theoretical Computer Science, 12(1):97–108, September 1980.
- [259] Pierre Renard de Montmort: *Essai d'analyse sur les jeux de hazard*. Jacque Quillau, Paris, France, 1708.
- [260] Leo Moser: *An Introduction to the Theory of Numbers*. The Trillia Group, 2004.
- [261] Theodore S. Motzkin: *Relation between hypersurface cross ratios, and a formula for partitions of a polygon, for permanent preponderance, and for non-associative products*. Bulletin of the American Mathematical Society, 54(4):352–360, April 1948.
- [262] David Musser: *Introspective sorting and selection algorithms*. Software: Practice and Experience, 27(8):983–993, August 1997.
- [263] Paul J. Nahin: *An Imaginary Tale: The Story of  $\sqrt{-1}$* . Princeton University Press, 2010.
- [264] Peter Naur: *Programming by action clusters*. BIT, 9(3):250–258, September 1969.
- [265] *Recommended elliptic curves for Federal Government use*.  
<http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf>, July 1999.
- [266] Ivan Niven: *A simple proof that  $\pi$  is irrational*. Bulletin of the American Mathematical Society, 53(6):509, June 1947.
- [267] Ivan Niven: *Formal power series*. The American Mathematical Monthly, 76(8):871–889, October 1969.
- [268] Milan Novaković: *Generating functions*. [http://www.imomath.com/tekstkut/genf\\_mn.pdf](http://www.imomath.com/tekstkut/genf_mn.pdf), 2007.
- [269] John O'Connor and Edmund F. Robertson: *Königsberg bridges*.  
<http://www-history.mcs.st-andrews.ac.uk/Extras/Konigsberg.html>, March 2000.
- [270] Andrew M. Odlyzko: *Periodic oscillations of coefficients of power series that satisfy functional equations*. Advances in Mathematics, 44(2):180–205, May 1982.
- [271] Andrew M. Odlyzko: *Enumeration of strings*. In A. Apostolico and Z. Galil (editors): *Combinatorial Algorithms on Words*, volume 12 of *NATO Advance Science Institute Series, Series F: Computer and System Sciences*, pages 205–228. Springer, 1985.
- [272] Andrew M. Odlyzko: *Asymptotic enumeration methods*. In R. L. Graham, M. Gröschel, and L. Lovász (editors): *Handbook of Combinatorics*, volume 2, pages 1063–1229. Elsevier, 1995.

- [273] Andrew M. Odlyzko and Herbert S. Wilf: *The editor's corner: n coins in a fountain*. The American Mathematical Monthly, 95(9):840–843, November 1988.
- [274] Frank W. J. Olver, Daniel W. Lozier, Ronald F. Boisvert, and Charles W. Clark: *NIST Digital Library of Mathematical Functions*. <http://dlmf.nist.gov>.
- [275] Øystein Ore: *Invitation to Number Theory*. Number 20 in *New Mathematical Library*. Mathematical Association of America, 1969.
- [276] Øystein Ore: *Graphs and their Uses*. Number 10 in *New Mathematical Library*. Mathematical Association of America, revised edition, 1990.
- [277] Ian Parberry: *Problems on Algorithms*. Prentice-Hall, 1994.
- [278] The PARI Group, Bordeaux: *PARI/GP, Version 2.7.1*, September 2014. Available from <http://pari.math.u-bordeaux.fr>.
- [279] Radia Perlman: *An algorithm for distributed computation of a spanningtree in an extended LAN*. SIGCOMM Computer Communications Review, 15:44–53, September 1985.
- [280] Julius Petersen: *Sur le Théorème de Tait*. L'Intermédiaire des Mathématiciens, 5:225–227, 1898.
- [281] W. W. Peterson and D. T. Brown: *Cyclic codes for error detection*. Proceedings of the IRE, 49(1):228–235, January 1961.
- [282] Marko Petkovšek and Tomaž Pisanski: *Combinatorial interpretation of unsigned Stirling and Lah numbers*. Technical Report 837, IMFM/TCS, University of Ljubljana, November 2002.
- [283] Marko Petkovšek, Herbert S. Wilf, and Doron Zeilberger: *A = B*. A K Peters/CRC Press, 1996.
- [284] Charles Émile Picard: *Sur une Propriété des Fonctions Entières*. Comptes Rendus hebdomadiers des séances de l'Académie des sciences, 88:1024–1027, 1879.
- [285] Charles C. Pinter: *A Book of Abstract Algebra*. Dover Publications, Inc., second edition, 2010.
- [286] J. M. Pollard: *Theorems of factorization and primality testing*. Proceedings of the Cambridge Philosophical Society, 76(3):521–528, 1974.
- [287] J. M. Pollard: *A Monte Carlo method for factorization*. BIT Numerical Mathematics, 15(3):331–334, September 1975.
- [288] George Pólya: *Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen*. Acta Mathematica, 68(1):145–254, Dezember 1937.
- [289] George Pólya: *How to Solve It*. Princeton University Press, 1945.
- [290] George Pólya: *On picture-writing*. The American Mathematical Monthly, 63(10):689–697, December 1956.
- [291] George Pólya and Ronald C. Read: *Combinatorial Enumeration of Groups, Graphs, and Chemical Compounds*. Springer, 1987.
- [292] Carl Pommerance: *A tale of two sieves*. Notices of the AMS, 43(12):1473–1485, December 1996.
- [293] Robert C. Prim: *Shortest connection networks and some generalizations*. Bell System Technical Journal, 36(6):1389–1401, November 1957.

- [294] Helmut Prodinger: *Knuth's old sum – a survey*. Bulletin of the EATCS, 54:232–245, October 1994.
- [295] Michael O. Rabin: *Probabilistic algorithm for testing primality*. Journal of Number Theory, 12(1):128–138, February 1980.
- [296] Anthony Ralston and Philip Rabinowitz: *A First Course in Numerical Analysis*. Dover Publications, Inc., second edition, 2012.
- [297] Srinivasa Ramanujan: *A proof of Bertrand's postulate*. Journal of the Indian Mathematical Society, 11:181–182, 1919.
- [298] Jorge L. Ramírez Alfonsín: *The Diophantine Frobenius Problem*. Oxford University Press, 2006.
- [299] Peter L. Renz: *Mathematical proof: What it is and what it ought to be*. The College Mathematics Journal, 12(2):83–103, March 1981.
- [300] Fred Richman: *Number Theory: An Introduction to Algebra*. Brooks/Cole Publishing Company, 1971.
- [301] John Riordan: *Combinatorial Identities*. John Wiley & Sons, 1968.
- [302] Ronald L. Rivest, Adi Shamir, and Leonard Adleman: *A method for obtaining digital signatures and public-key cryptosystems*. Communications of the ACM, 21(2):120–126, February 1978.
- [303] Ronald L. Rivest, Adi Shamir, and Leonard Adleman: *A method for obtaining digital signatures and public-key cryptosystems*. Communications of the ACM, 26(1):96–99, January 1983.
- [304] Neil Robertson, Daniel P. Sanders, Paul D. Seymour, and Robin Thomas: *The four color theorem*. Journal of Combinatorial Theory Series B, 70(1):2–44, May 1997.
- [305] Andrew M. Rockett: *Sums of the inverses of binomial coefficients*. Fibonacci Quarterly, 19(5):433–437, December 1981.
- [306] Kenneth Rogers: *The axioms for Euclidean domains*. The American Mathematical Monthly, 78(10):1127–1128, December 1971.
- [307] Steven M. Roman and Gian Carlo Rota: *The umbral calculus*. Advances in Mathematics, 27(2):95–188, February 1978.
- [308] Salvador Roura: *Improved master theorems for divide-and-conquer recurrences*. Journal of the ACM, 48(2):170–205, March 2001.
- [309] Imad Khaled Salah, Abdullah Darwish, and Saleh Oqeili: *Mathematical attacks on the RSA cryptosystem*. Journal of Computer Science, 2(8):665–671, August 2006.
- [310] Pierre Samuel: *About Euclidean rings*. Journal of Algebra, 19(2):282–301, October 1971.
- [311] Augustin P. Sarr, Philippe Elbaz-Vincent, and Jean-Claude Bajard: *A secure and efficient authenticated Diffie-Hellman protocol*. Cryptology ePrint Archive, Report 2009/408, 2009.
- [312] Marilyn vos Savant: *The Power of Logical Thinking: Easy Lessons in the Art of Reasoning... and Hard Facts About Its Absence in Our Lives*. St. Martin's Griffin, 1997.
- [313] Anton R. Schep: *A simple complex analysis and an advanced calculus proof of the fundamental theorem of algebra*. The American Mathematical Monthly, 116(1):67–68, January 2009.

- [314] Bruce Schneier: *Applied Cryptography*. John Wiley & Sons, 1996.
- [315] Arnold Schönhage und Volker Strassen: *Schnelle Multiplikation großer Zahlen*. Computing, 7(3-4):281–292, September 1971.
- [316] René Schoof: *Counting points on elliptic curves over finite fields*. Journal de Théorie des Nombres de Bordeaux, 7:219–254, 1995.
- [317] Ernst Schröder: *Vier kombinatorische Probleme*. Zeitschrift für Angewandte Mathematik und Physik, 15:361–376, 1870.
- [318] SEC1: *Elliptic curve cryptography, version 2.0*.  
<http://www.secg.org/download/aid-780/sec1-v2.pdf>, May 2009. Standards for Efficient Cryptography (SEC).
- [319] SEC2: *Recommended elliptic curve domain parameters, version 2.0*.  
<http://www.secg.org/download/aid-784/sec2-v2.pdf>, January 2010. Standards for Efficient Cryptography (SEC).
- [320] Robert Sedgewick and Philippe Flajolet: *An Introduction to the Analysis of Algorithms*. Addison-Wesley, second edition, 2013.
- [321] Raimund G. Seidel and Cecilia A. Aragon: *Randomized search trees*. Algorithmica, 16(4/5):464–497, October 1996.
- [322] Ravi Sethi and Jeffrey D. Ullman: *The generation of optimal code for arithmetic expressions*. Journal of the ACM, 17(4):715–728, October 1970.
- [323] Victor Shoup: *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, second edition, 2009.
- [324] Victor Shoup: *NTL: A library for doing number theory, version 6.2.1*.  
<http://www.shoup.net/ntl>, August 2014.
- [325] Abraham Sinkov: *Elementary Cryptanalysis: A Mathematical Approach*. Number 22 in *New Mathematical Library*. Mathematical Association of America, second edition, 2009.
- [326] Steven S. Skiena: *The Algorithm Design Manual*. Springer, second edition, 2008.
- [327] Neil J. A. Sloane: *Online Encyclopedia of Integer Sequences*. <http://oeis.org>.
- [328] A. D. Solov'ev: *A combinatorial identity and its application to the problem concerning the first occurrence of a rare event*. Theory of Probability and Its Applications, 11(2):276–282, 1966.
- [329] William Stallings: *Data and Computer Communications*. Prentice-Hall, ninth edition, 2010.
- [330] Richard P. Stanley: *Hipparchus, Plutarch, Schröder and Hough*. The American Mathematical Monthly, 104(4):344–350, April 1997.
- [331] Richard P. Stanley: *A survey of alternating permutations*. [arXiv:0912.4240](https://arxiv.org/abs/0912.4240), December 2009.
- [332] Richard P. Stanley: *Catalan addendum*. <http://www-math.mit.edu/~rstan/ec/catadd.pdf>, May 2013.
- [333] Richard P. Stanley: *Enumerative Combinatorics*, volume 1. Cambridge University Press, second edition, February 2012.

- [334] Richard P. Stanley: *Enumerative Combinatorics*, volume 2. Cambridge University Press, April 1999.
- [335] Karl Georg Christian von Staudt: *Geometrie der Lage*. Nürnberg, 1847.
- [336] Clifford L. Stein, Robert Drysdale, and Kenneth Bogart: *Discrete Mathematics for Computer Scientists*. Addison-Wesley, 2010.
- [337] Elias M. Stein and Rami Shakarchi: *Complex Analysis*, volume II of *Princeton Lectures in Analysis*. Princeton University Press, 2010.
- [338] Sherman K. Stein and Anthony Barcellos: *Calculus and Analytic Geometry*. McGraw-Hill, fifth edition, 1992.
- [339] William Stein: *Sage open-source mathematical software system*. <http://sagemath.org>, August 2014. Version 6.3.
- [340] Gilbert Strang: *Introduction to Linear Algebra*. Wellesley-Cambridge Press, fourth edition, February 2009.
- [341] Volker Strassen: *Gaussian elimination is not optimal*. Numerische Mathematik, 13(4):354–356, August 1969.
- [342] Bjarne Stroustrup: *The C++ Programming Language*. Addison-Wesley Longman, special edition, 2000.
- [343] E. R. Swart: *The philosophical implications of the four color problem*. The American Mathematical Monthly, 87(9):697–702, November 1980.
- [344] Andrew S. Tanenbaum and David J. Wetherall: *Computer Networks*. Prentice-Hall, fifth edition, 2010.
- [345] Robert Endre Tarjan: *Edge-disjoint spanning trees and depth-first search*. Acta Informatica, 6(2):171–185, June 1976.
- [346] Richard Taylor and Andrew Wiles: *Ring theoretic properties of certain Hecke algebras*. Annals of Mathematics, 141(3):553–572, May 1995.
- [347] Ron Taylor: *Introduction to Proof*, volume 4. Journal of Inquiry-Based Learning in Mathematics, September 2007.
- [348] Robin Thomas: *An update on the Four-Color Theorem*. Notices of the American Mathematical Society, 45(7):848–859, August 1998.
- [349] Brian S. Thomson, Andrew M. Bruckner, and Judith B. Bruckner: *Elementary Real Analysis*. ClassicalRealAnalysis.com, second edition, 2008.
- [350] William P. Thurston: *On proof and progress in mathematics*. Bulletin of the American Mathematical Society, 30(2):161–177, April 1994.
- [351] Jacques Touchard: *Sur un problème des permutations*. Dans *Comptes Rendus de L'Académie des Sciences*, tome 198, pages 631–633, 1934.
- [352] Sergei Treil: *Linear algebra done wrong*. <http://www.math.brown.edu/~treil/papers/LADW/LADW.html>, September 2014.

- [353] William F. Trench: *Introduction to Real Analysis*, volume 7 of *Books and Monographs*. Trinity University, free hyperlinked edition 2.04 edition, December 2013.
- [354] Clifford Truesdell: *The new Bernoulli edition*. Isis, 49(1):54–62, 1958.
- [355] Alan Tucker: *Pólya's enumeration formula by example*. Mathematics Magazine, 47(5):248–256, November 1974.
- [356] Chris Tuffley: *Induction*.  
<http://www.mathsolympiad.org.nz/wp-content/uploads/2009/03/induction.pdf>, March 2009.
- [357] Thomas Tymoczko: *Computers, proofs and mathematicians: A philosophical investigation of the four-color proof*. Mathematics Magazine, 53(3):131–138, May 1980.
- [358] Stephen Vajda: *Fibonacci and Lucas Numbers, and the Golden Section: Theory and Applications*. Ellis Horwood Limited, 1989. Reprinted 2008 by Dover Publications, Inc.
- [359] Stephen Warshall: *A theorem on boolean matrices*. Journal of the ACM, 9(1):11–12, January 1962.
- [360] Michael J. Wiener: *Cryptanalysis of short RSA secret exponents*. IEEE Transactions on Information Theory, 36(3):553–558, May 1990.
- [361] Eugene Wigner: *The unreasonable effectiveness of mathematics in the natural sciences*. Communications in Pure and Applied Mathematics, 13(1):1–14, February 1960.
- [362] Andrew Wiles: *Modular elliptic curves and Fermat's last theorem*. Annals of Mathematics, 141(3):443–551, May 1995.
- [363] Herbert S. Wilf: *Algorithms and Complexity*. A. K. Peters, Ltd, second edition, 2003.
- [364] Herbert S. Wilf: *Generatingfunctionology*. A. K. Peters, Ltd., third edition, 2006.
- [365] J. W. J. Williams: *Algorithm 232 - Heapsort*. Communications of the ACM, 7(6):347–348, June 1964.
- [366] Yin Y. Yen: *An algorithm for finding shortest routes from all nodes to a given destination in general networks*. Quarterly of Applied Mathematics, 27:526–530, 1970.
- [367] Elias Zakon: *Mathematical Analysis II*. The Trillia Group, 2009.
- [368] Derek A. Zave: *A series expansion involving the harmonic numbers*. Information Processing Letters, 5(3):75–77, August 1976.
- [369] Paul Zeitz: *The Art and Craft of Problem Solving*. John Wiley & Sons, second edition, 2007.

# Índice alfabético

---

## Símbolos

$\Delta$ , 12  
 $\Gamma$ , 520  
factorial, 521  
fórmula de reducción, 521, 523  
fórmula de reflexión, 521  
residuo, 521  
 $\Sigma$ , 12  
 $\not\in$  (no contiene), 4  
 $\delta$  (grado de un vértice), 388  
 $\epsilon$  (identidad para convolución de Dirichlet), 132  
 $\epsilon$  (secuencia vacía), 8  
 $\gamma$  (constante de Euler), véase Euler, constante de  
 $\in$  (pertenece), 4  
 $\lambda(m)$  (máximo orden módulo  $m$ ), 152  
 $B$ , 522  
 $\mu$ , véase Möbius, función de  
 $\ni$  (contiene), 4  
 $\notin$  (no pertenece), 4  
 $\phi$  de Euler, 115, 129, 136  
 $\sigma$  (suma de divisores), 131  
 $\tau$  (número de divisores), 131  
 $\tau$  (sección áurea), véase sección áurea  
 $\emptyset$  (conjunto vacío), 4  
 $\zeta$  de Riemann, véase Riemann, función  $\zeta$  de

## A

Abel, fórmula binomial de, 277  
árbol binario, 383  
acotado, 82  
Akra-Bazzi, teorema de, 311  
AKS, algoritmo, 177  
álgebra abstracta, 102, 153  
álgebra simbólica, 139, 207, 268, 335  
álgebra, teorema fundamental del, 497  
Algol (lenguaje de programación), 71

algoritmo  
Euclides, véase Euclides, algoritmo de  
potencia, 171, 176, 183, 184  
binario, 171  
primalidad, 176  
algoritmo de división, 89, 91, 105  
polinomios, 141  
algoritmo de factorización, 171  
 $p - 1$  de Pollard, 174  
criba, 175  
curva elíptica, 176  
Fermat, 171  
récord, 184  
rho de Pollard, 173  
algoritmo voraz, 420, 436, 437  
algoritmos aritméticos, 167  
análisis complejo, 207, 289, véase también  $\mathbb{C}$   
(números complejos), 481, 527  
análisis de algoritmos, 24, 168, 371, 373  
árbol binario de búsqueda, 377  
búsqueda binaria, 224  
dividir y conquistar, 310  
asintótica, 310  
máximo, 381  
ordenamiento  
inserción, 24, 373  
quicksort, 312  
análisis de camino crítico, 445  
actividad crítica, 445  
holgura, 445  
ruta crítica, 445  
anillo, 101, 108, 140, 153, 268  
automorfismo, 118, 276  
con unidad, 101  
comutativo, 101, 135  
cuadrático, 110, 111, 160  
conjugado, 111  
norma, 111

- B**
- Bachmann-Landau, notaciones de, **18, 29**
  - operaciones, **23**
  - relación con límites, **19**
  - Basilea, problema de, **9, 60, 97, 289, 518**
  - Bayes, regla de, **260**
  - $bc(1)$ , **89**
  - Bell, Eric Temple, **360**
  - Bell, números de, **348, 360, 368**
    - fórmula, véase Dobiński, ecuación de recurrencia, **348**
  - Bell, números de (ordenados), **367**
    - asintótica, **528**
    - recurrencia, **368**
  - Bellman-Ford, algoritmo de, **434, 441**
  - Bender, teorema de, **376, 531, 533**
  - Bentley, Jon, **73**
  - Berge, lema de, **428**
  - Berge, teorema de, **395**
  - Bernoulli, distribución de, **261**
  - Bernoulli, ensayo de, **261, 262**
  - Bernoulli, Jakob, **283**
  - Bernoulli, Johann, **36**
  - Bernoulli, Nicolaus, **246**
  - Bernoulli, números de, **228, 281, 287, 528**
    - asintótica, **290, 529**
    - cuadro, **282**
    - generatriz, **289**
    - linda fórmula, **288**
  - Bernoulli, polinomios de, **281, 287**
    - ceros, **291**
    - cuadro, **282**
    - generatriz, **289**
    - gráfica, **291**
    - integral, **281**
    - recurrencia, **281, 281**
  - Bertrand, Joseph Louis François, **36**
  - Bertrand, postulado de, **36**
  - Bertrand-Chebyshev, teorema de, véase Bertrand, postulado de
  - Bézout, Étienne, **91**
  - Bézout, identidad de, **91, 92, 94, 115, 126, 159, 220**
  - Binet, fórmula de, **297, 520**
  - binomio, teorema del, **162, 196, 532**
    - potencias factoriales, **296**
  - birthday paradox*, véase paradoja del cumpleaños
  - biyección, **85, 456**

- número, 195  
 Blankinship, W. A., 94  
*block fountain*, véase fuente  
 Borges, Jorge Luis, 36  
 Borges, teorema de, 36  
 Brahmagupta, 111, 128  
 Brounker, William, 111  
 buen orden, principio de, 82, 84  
 Bürmann, Hans Heinrich, 276  
 Burnside, lema de, 36, 468  
 Burnside, William, 36  
 búsqueda binaria, 73, 307, 309  
     historia, 73
- C**
- C (lenguaje de programación), 23, 75  
 C (números complejos), 108, 153, 320  
     argumento, 481  
     conjulado, 483  
     derivada, 486  
     exponencial, 321, 482, 488  
     extensión analítica, 506  
     forma cartesiana, 481  
     forma polar, 481  
     función entera, 486  
     función holomorfa, 486, 497, 521  
     función meromorfa, 506  
     funciones elementales, 487  
     funciones hiperbólicas, 488  
     funciones trigonométricas, 488  
     integral, 490  
     límite, 485  
     logaritmo, 489  
         rama principal, 489  
     módulo, 481  
     operaciones, 481  
     parte imaginaria, 481  
     parte real, 481  
     polo, 506  
     potencia, 490  
         rama principal, 490  
     recíproco, 483  
     región conexa simple, 493  
     residuo, 528  
     secuencia, 498  
         convergencia, 498  
         límite, 498  
     singularidad, 506  
     unidad imaginaria, 481  
     valor principal, 481
- C++ (lenguaje de programación), 89, 139, 167, 268  
 cálculo de diferencias finitas, 12, 13  
 cálculo integral, teorema fundamental del, 494  
 cálculo umbral, 364  
 cambio de monedas, 218  
 camino, véase topología  
 campo (álgebra), 81, 105, 115, 148, 153, 268, 481  
     característica, 153  
     extensión, 153, 159, 160  
         grado, 159  
         simple, 160  
     finito, 153, 181  
         estructura, 156  
     isomorfo, 153, 161  
     subcampo, 153  
         primo, 153, 156  
         propio, 153  
 Cantor, Georg, 63, 85, 87  
 Cantor, teorema de, 87  
 Cantor-Bernstein-Schröder, teorema de, 85  
 cardinalidad, 85  
 Carmichael, número de, 177  
 carta  
     pinta, 198  
     corazón (♥), 198  
     diamante (◊), 198  
     pica (♠), 198  
     trébol (♣), 198  
     valor, 198  
 Casorati-Weierstraß, teorema de, 508  
 Catalan, función generatriz  
     Catalan, función generatriz, 357  
 Catalan, números de, 224, 236, 334, 356, 357, 375  
     fórmula, 224, 356  
 Cauchy, Augustin-Louis, 36, 52  
 Cauchy, criterio de, 498  
 Cauchy, fórmula de (generalizada), 535  
 Cauchy, fórmula integral de, 495, 496, 497, 507  
 Cauchy, teorema de, 494  
 Cauchy, teorema de residuos de, 513  
 Cauchy, teorema integral de, 500  
 Cauchy-Hadamard, teorema de, 502  
 Cauchy-Riemann, ecuaciones de, 486, 488, 492  
 Cauchy-Schwarz, desigualdad de, 16  
 Cayley, fórmula de, 349  
 Cayley, función de, 277  
 Cayley, teorema de, 432

- cero, **506**  
 Chebychev, desigualdad de, **265**  
 Chebyshev, Pafnuty Lvovich, **36**  
 Chebyshev, teorema de, véase Bertrand, postulado de  
 ciclo, **330**
  - primitivo, **340**
  - simetría, **339**
 circuito eléctrico, **446**  
 Clairaut, teorema de, **385**  
 clases de equivalencia, **26**  
 clausura, véase topología  
 CLN, **89, 167**  
 cociente, **89**  
 cociente entero, **90**  
 código, **164**
  - corrección de errores, **164**
  - detección de errores, **164**
  - Hamming, **164**
  - Hamming, distancia de, **164**
  - palabra, **164**
  - polinomio generador, **165**
  - redundancia cíclica, **164**
 código abierto, **89**  
 coeficiente binomial, **151, 193, 197, 301, 377, 523**
  - asintótica, **532, 534**
 coeficiente multinomial, **198, 203**  
 combinatoria, **189, 256, 355**
  - biyecciones, **189**
  - combinación, **193, 256**
  - contar por filas y columnas, **189**
  - generatrices, **217**
  - juegos de poker, **203**
  - manos de poker, **198**
  - multiconjunto, **256**
  - objetos rotulados, **330**
  - permutación, **256**
  - regla de división, **201**
  - regla de la suma, **189, 200**
  - regla del producto, **190, 199, 200, 205**
  - secuencia, **256**
  - secuencias con repeticiones, **203, 204**
  - secuencias restringidas, **204**
  - sobrecontar, **202**
  - subconjuntos sin elementos consecutivos, **194**
  - técnicas básicas, **189**
 completitud, axioma de, **82**  
 Conan Doyle, Sir Arthur, **43**
- conectivas lógicas  
 tablas de verdad, **2**  
 conectividad, véase topología  
 congruencia, **99**
  - propiedades, **99, 100**
 conjetura, **64**  
 conjunto, **4, 330**
  - abierto, véase topología
  - cardinalidad, **6, 85**
  - cerrado, véase topología
  - complemento, **5**
  - conjunto potencia, **7**
  - denso, **83**
  - descripción por extensión, **4**
  - descripción por intención, **5**
  - diferencia simétrica, **5**
  - disjunto, **5**
  - familia, **430**
  - finito, **85**
  - función característica, **195**
  - igualdad, **5**
    - demostrar, **6**
  - infinito, **85**
  - intersección, **5**
  - numerable, **86**
  - operaciones, **5**
    - notación lógica, **5**
    - propiedades, **7**
  - particiones, **27**
  - producto cartesiano, **7**
  - rangos (notación), **7**
  - resta, **5**
  - subconjunto, **5, 355**
    - número, **195, 236**
  - superconjunto, **5**
  - unión, **5**
  - universo, **5**
  - vacío, **4**
 conjunto índice, véase índice  
 contradicción, **44**  
 contraejemplo, **64**  
 contrapositivo, **2, 38, 39**  
 convergencia uniforme, **289, 498**  
 converse, véase recíproco  
 convolución binomial, **239**  
 coprimos, véase relativamente primos  
 corolario, **36**  
 coset, **115, 466**  
 cota, **82**  
 inferior, **82**

- superior, 82
- CPM, véase *Critical Path Method*
- criptoanálisis, 181
- criptografía, 110, 181
- criptología, 89
- criptología
  - confidencialidad, 182
  - criptología, 181
    - Alice, 181, 182
    - autenticación, 182
    - Bob, 181, 182
    - Charlie, 181
    - clave, 182
    - clave de sesión, 182
    - clave privada, 182
    - clave pública, 182
    - consideraciones, 187
    - curvas elípticas, 187
    - distribuir claves, 182
    - Eve, 181
    - firma digital, 182
      - DSA, 185
      - DSS, 185
      - RSA, 185
    - función de cifrado, 182
    - función de descifrado, 182
    - función de *hash*, 182
    - integridad, 182
    - no repudiación, 182
    - nomenclatura, 182
    - RSA, 183
    - sistemas híbridos, 182
    - texto cifrado, 182
    - texto claro, 182
    - y seguridad, 181
  - Critical Path Method*, 444
  - cuadrado perfecto, 111
  - cuantificadores (lógica), 4
  - cuaterniones, 114
    - conjugado, 114
    - en computación gráfica, 114
    - norma, 114
    - recíproco, 114
  - cuatro colores, teorema de, 43, 413
  - cubo, 478
  - curva, véase topología
  - curva cerrada
    - homotópica, 493
  - curva elíptica, 108, 176
  - grupo, 110
  - curva simple cerrada, 484

**D**

  - dados
    - lanzamiento, 251, 252, 257, 259, 264
    - locos, véase Sicherman, dados de
    - no transitivos, 26
    - probabilidad, 251
  - Darboux, lema de, 533
  - Dedekind, Richard, 85
  - demostración, 35
    - argumento diagonal, 87, 88
    - ciclo de implicancias, 454
    - combinatoria, 193
    - contradicción, 43–48, 64, 65, 90, 96–98, 142, 146, 159, 436, 508
    - desigualdad, 46
    - existencia, 63
    - implicancia, 38
    - inducción, 41, 49, 68, 125, 130, 141, 147, 149, 150, 162, 168, 196, 197, 260, 268, 291, 369, 396, 398, 404, 425, 434
    - estructural, 61
    - fuerte, 56, 400, 406
    - multivariable, 54
    - por casos, 42
    - si y solo si, 40
  - derangement*, véase desarreglo
  - derivada logarítmica, 226, 227, 348
    - receta, 226
  - derivada parcial, notación, 380
  - desarreglo, 246, 366, 458, 459
    - asintótica, 527
    - expresión, 366
    - función generatriz, 366
    - número de, fórmula, 247
    - recurrencia, 366, 367
  - Descartes, René, 410
  - desigualdad de Cauchy-Schwarz, véase Cauchy-Schwarz, desigualdad de
  - desigualdad triangular, 17, 44, 112, 491, 496, 520
  - desviación estándar, 40, 265
  - diente de sierra, véase parte fraccional
  - diferencias finitas, 364
  - Diffie-Hellman, algoritmo de, 177, 182
  - digrafo, 390, 441
    - acíclico, 442
    - arco, 441
    - camino dirigido, 441

- ciclo dirigido, 442  
 circuito dirigido, 442  
 orden topológico, 442  
 representación, 441  
 vértice, 441  
 Dijkstra, algoritmo de, 432, 441, 444  
 Dijkstra, Edsger W., 71  
 Diofanto, 116  
 Dirichlet, anillo de, 339, 341  
 Dirichlet, convolución de, 132, 135  
 disco abierto, 483  
 discriminante, 108  
 dividir y conquistar, 307  
     recurrencia, 308  
 divisor, 89  
 Dobiński, ecuación de, 348  
 dominio de ideal principal, 156  
 dominio euclíadiano, 146, 159  
 dominio integral, 106, 110, 140, 268  
 dualidad (lógica), 2
- E**  
 ecuación diferencial, 230, 359, 367  
 Edmonds-Karp, algoritmo de, 454  
 equivalencia (lógica), 2  
 Erdős, Paul, 36, 97  
 error, 165  
     ráfaga, 165  
 espacio vectorial, 154, 156, 159, 160, 269  
     axiomas, 154  
     base, 155  
     componentes (de un vector), 155  
     dimensión, 155  
     escalar, 154  
     independencia lineal, 154, 159  
     operaciones, 154  
     vector, 154  
 Euclides, 35, 93, 97, 131  
 Euclides, algoritmo de, 93, 94  
     análisis, 168, 296, 297  
     extendido, 94  
 Euclides, Elementos, 93  
 Eudoxo de Cnido, 44  
 Euler, constante de, 284, 284  
 Euler, constante de (para una función), 280  
 Euler, fórmula de (exponencial complejo), 214, 289  
 Euler, fórmula de (grafos planares), 410, 412  
 Euler, fórmula para seno, 287, 290  
 Euler, Leonhard, 46, 88, 97, 111, 115, 131, 207, 284, 287, 289, 388, 400, 410  
 Euler, números de, 351  
 Euler, polinomio de, 4, 46  
 Euler, teorema de, 115, 151, 400  
 Euler, transformación de, 215  
 Euler-Maclaurin, fórmula de, 282, 283, 284, 525  
     convergencia, 290  
     resto, 292  
 Euler-Mascheroni, constante de, *véase* Euler, constante de
- F**  
 factor, 89  
 factorial, 267  
 Faulhaber, Johann, 283  
 Fermat, pequeño teorema de, 116, 174, 176, 177  
 Fermat, Pierre de, 36, 116, 173  
 Fermat, primo de, 184  
 Fermat, último teorema, 36, 116  
 FFT, *véase* Fourier, transformada rápida de  
 Fibonacci, búsqueda de, 299  
     análisis, 325  
 Fibonacci, Leonardo (Leonardo Pisani Bigollo), 55  
 Fibonacci, números de, 30, 55, 168, 296, 336, 355, 519  
     asintótica, 298  
     fórmula de Binet, 297  
     generatriz, 297  
     relación con coeficientes binomiales, 298  
 Fidias, 297  
*field*, *véase* campo (álgebra)  
 Fleury, algoritmo de, 401  
 Floyd, algoritmo de, 441  
 Floyd, algoritmo de (detección de ciclos), 173  
 Floyd, Robert W., 71  
 Floyd-Warshall, algoritmo de, 435, 441  
 Ford-Fulkerson, método de, 449, 454  
*fountain*, *véase* fuente  
 Fourier, Joseph, 46  
 Fourier, transformada rápida de, 308  
 Frama-C, 79  
 Frobenius, Ferdinand Georg, 36  
 Frobenius, número de, 221  
 Frobenius, problema de, 221  
 frontera, *véase* topología  
 Frucht, grafo de, 422  
 fuente, 234, 299

- generatriz, 234
  - recurrencia, 234
  - función, 30
    - analítica, 273
    - aritmética, 129, 135
    - función suma, 130
    - multiplicativa, 129, 130, 131, 133
    - biyectiva, 30
    - codominio, 30
    - composición, 31
    - dominio, 30
    - fibra, 31
    - generatriz, véase generatriz
    - identidad, 32
    - imagen, 30
    - imagen de un conjunto, 32
    - inversa, 31
    - inyectiva, 30
      - número, 195
    - número, 194
    - preimagen, 30
    - preimagen de un conjunto, 32
    - rango, 30, 31
    - recorrido, 30
    - sobreyectiva, 30
      - número, 360
      - unimodal, 299
      - uno a uno, 30
  - función generatriz
    - múltiples índices, 236
  - función piso, 14
    - identidades, 14
  - función techo, 14
    - identidades, 14
  - fundamental de la aritmética, teorema, 97
- G**
- Galois, Evariste, 159
  - GAP, 110, 167
  - Gauß, Carl Friedrich, 14, 35, 135, 308, 497
  - Gauß, identidad de, 135, 135, 136, 190, 341
  - GCD, véase máximo común divisor
  - Gelfond-Schneider, constante de, véase Hilbert, número de
  - generar código, 408, 420, 442
  - generatriz, 207, 318, 331, 336, 337, 352, 355, 358, 471, 478
    - aceite de serpiente, 236
    - bivariada, 236
    - combinatoria, 329
  - cumulativa, 371
  - exponencial, 221, 230, 231, 239, 298, 347, 351, 366–368, 432, 458
    - reglas, 225
  - multivariada, 353, 361–363, 379
  - números harmónicos, 293
  - ordinaria, 209, 221, 229, 233, 235, 242, 255, 267, 303
    - reglas, 221
  - Germain, Sophie, 182
  - GiNaC, 139, 268
  - GMP, 89, 167
  - grafo, 388
    - árbol, 402, 442
      - hoja, 403
      - propiedades, 403
      - recorrido, 409
      - vértice interno, 403
    - árbol con raíz, 405
      - altura, 405
      - ancestro, 405
      - descendiente, 405
      - hijo, 405
      - padre, 405
      - recorrer, 405
    - árbol ordenado, 406
    - árbol recubridor, 404, 410, 413, 439
    - árbol recubridor mínimo, 436
    - arco, 388
    - arcos adyacentes, 388
    - automorfismo, 463
    - bipartito, 422
      - camino alternante, 427
      - deficiencia, 428
      - índice cromático, 425
      - matching, 426
        - matching completo, 427
        - matching maximal, 428
      - bipartito completo, 423
      - bosque, 437
      - búsqueda en profundidad, 443
      - camino, 392
        - camino de Euler, 399
        - camino hamiltoniano, 399
        - ciclo, 392
        - ciclo hamiltoniano, 399
        - círculo de Euler, 399
      - colorear
        - arcos, 421
      - coloreo

- vértices, 417, 417  
 completo, 392  
 componente conexo, 398, 400, 413  
 conexo, 398, 404  
 cubo, 392  
 dirigido, véase digrafo, véase digrafo  
 eliminar y reponer, 399  
 estrella, 423  
 índice cromático, 422, 425  
 isomorfismo, 391, 463  
 matching, 426  
 número cromático, 418  
 orden, 388  
 planar, 410  
 recorrido, 413, 416  
     a lo ancho, 415  
     profundidad, 413  
 recorrido a lo ancho, 445  
 regular, 388  
 representación, 389  
     enlazada, 390  
     implícita, 390  
     lista de adyacencia, 390  
     matriz de adyacencia, 390  
 rotulado, 432  
     árbol, 432  
 rueda, 392  
 secuencia gráfica, 395  
 subgrafo, 388  
 vecindario, 388  
 vértice, 388  
     grado, 388  
 vértices adyacentes, 388  
 vértices vecinos, 388  
 Gries, David, 71  
 grupo, 35, 101, 153, 181, 327, 456  
     abeliano, 101, 102, 110, 117, 154  
     alternante, 461, 463, 467, 476  
     automorfismo, 118  
     cancelación, 103  
     cíclico, 105, 148, 149, 463, 471  
     diedral, 103, 463, 468, 471, 474  
     exponente, 148  
     generador, 103, 105  
     homomorfismo, 118, 122  
     isomorfismo, 118, 119  
     isomorfo, 157  
     mutualidad, 103  
     orden, 102, 115, 456  
     orden de un elemento, 104, 115  
 permutaciones, 463  
 estabilizador, 464, 465  
 órbita, 464  
 potencia, 104  
 simetrías, 102  
 simétrico, 456, 463  
 subgrupo, 106, 114, 122, 463  
 subgrupo generado, 115  
 trivial, 102
- H**
- Hall, teorema de, 427, 431  
 Hamming, distancia de, 164  
 Hamming, Richard, 164  
 Hathout, Heba, 246  
 Havel-Hakimi, teorema de, 396  
 Hayman, método de, 535  
     funciones admisibles, 537  
 Hayman, teorema de, 536  
 Hermite, identidad de, 15  
 Hierholzer, algoritmo de, 401  
 Hilbert, David, 35, 64  
 Hilbert, número de, 64  
 Hipasso de Metaponto, 44  
 Hoare, lógica de, 71  
 Hoare, Tony (Sir Charles Anthony Richard), 71, 72  
 Holmes, Sherlock, 43  
 homomorfismo, 117, 118  
 Hopcroft-Karp, algoritmo de, 430  
 l'Hôpital, Guillaume Marquis de, 36  
 l'Hôpital, regla de, 36, 221, 509
- I**
- icosaedro truncado, 467  
 ideal, 91  
 iff, véase si y solo si  
 implicancia (lógica), 2, 38  
 inclusión y exclusión, principio de, 189, 236, 241, 303, 473  
     ejemplo  
         cursos, 244  
         lanzar 10 dados, 246  
         números con ceros par, 245  
     fórmula central, 243  
     fórmula clásica, 243  
     generatrices, 242  
     número promedio de propiedades, 243  
     propiedades, 242  
     receta, 244

- varianza del número de propiedades, 244  
índice, 86  
inducción, 97  
  estructural, 374  
  principio de, 82  
ínfimo, axioma de, 83  
Internet, 182  
inventor, paradoja del, véase paradoja del inventor  
inverso, 38  
involución, 458  
  función generatriz, 458  
irreducible, 95  
isomorfismo, 117, 118  
Iverson, convención de, 9, 331, 340, 372, 382  
  operaciones, 10  
Iverson, Kenneth E., 9
- J**
- Jevons, W. S., 173  
Jordan, curva de, véase curva simple cerrada  
Jordan, teorema de, 485
- K**
- Kahn, algoritmo de, 443  
Karatsuba, algoritmo de, 307, 309  
Kirchhoff, leyes de, 447  
KLEE, 79  
Knuth, Donald E., 9, 11, 14, 18, 24, 71, 72, 237, 360, 362  
Königsberg, puentes de, 400  
König, Julius, 85  
Kraitchik, Maurice, 175  
Kronecker, Leopold, 161  
Kronecker, teorema de, 161  
Kruskal, algoritmo de, 437  
Kummer, Ernst, 97
- L**
- Lagrange, inversión de, 276, 333, 334, 349, 350, 359, 432  
Lagrange, Joseph-Louis, 114  
Lagrange, teorema de, 114, 115, 148, 156, 466  
Lagrange-Bürmann, inversión de, véase Lagrange, inversión de  
Lah, números de, 363  
  cuadro, 364  
  fórmula, 363  
  recurrencia, 363  
  y potencias, 364  
Lamé, Gabriel Léon Jean Baptiste, 93, 168  
Laplace, Pierre Simon de, 207  
Laurent, serie de, 511, 514, 527  
LCM, véase mínimo común múltiplo  
Leibnitz  
  regla de, 494  
Leibnitz, fórmula de, 295  
lema, 36, 39, 41  
Linux, 71  
Liouville, teorema de, 497, 509, 511  
logaritmo discreto, 183  
lógica  
  conectiva, 3  
  convención variables, 3  
  cuantificador, 4  
  identidad, 3  
  predicado, 3  
lógica de predicados, 3  
lógica matemática  
  conectivas, 2  
  notación, 1  
Lucas, Édouard, 55  
Lucas, números de, 55, 355
- M**
- Maclaurin, teorema de, 21, 23, 48, 215, 226, 247  
Lagrange, forma del resto, 247  
Maclaurin-Cauchy, teorema de, 279, 284  
make(1), 442  
Markov, desigualdad de, 264  
matriz, 317  
  diagonal, 318  
  diagonalizable, 318  
  invertible, 318  
  valor propio, 318, 327  
max-flow min-cut, teorema, 453, 454  
maxima, 89, 139, 227, 268, 478  
máximo, 381  
máximo común divisor, 91, 91, 125  
  algoritmo, véase Euclides, algoritmo de  
  algoritmo binario, 169  
  propiedades, 91, 125  
máximo comun divisor, 167  
media, 40  
  aritmética, 52  
  aritmética y geométrica, 52  
  geométrica, 52  
  harmónica, 53  
mensaje, 164, 165, 181

- Mersenne, Marin, 38  
 Mersenne, primo de, 38, 131  
 método axiomático, véase axioma  
 método simbólico, 329, 337, 353, 356–358, 361, 363, 368, 372, 432, 458, 463  
 clase, 329  
 desarreglos, 347  
 objetos no rotulados, 331  
 objetos rotulados, 343  
 operaciones adicionales, 350  
 producto cajonado, 350  
 teorema de transferencia  
     objetos no rotulados, 331  
     objetos rotulados, 343  
 Miller-Rabin, prueba de, 177, 184  
 mínimo común múltiplo, 93, 184  
     propiedades, 125  
 Möbius, August Ferdinand, 133  
 Möbius, función de, 133  
 Möbius, inversión de, 134, 137, 163, 339, 341  
 Möbius, transformación de, 327  
 módulo, 90  
 Moivre, Abraham de, 207  
 momentos  
     función generatriz de, 255  
 Montmort, Pierre R., 246  
 Monty Hall, dilema de, 258  
 Moser, Leo, 45  
 Motzkin, números de, 357  
     asintótica, 532, 534  
 multiconjunto, 8, 330  
     generatriz, 214  
     número, 193, 205, 334  
     subconjunto, 355  
 multigrafo, 389, 400, 410  
     rizo, 390  
 multinomio, teorema del, 197  
 múltiplo, 89
- N**
- $\mathbb{N}$  (números naturales), 4, 82  
 $\mathbb{N}_0$  (números naturales y cero), 4  
 Naur, Peter, 71  
 necesario, véase implicancia (lógica)  
 necesario y suficiente (lógica), véase si y solo si  
 Newton, Isaac, 45  
 Newton, método de, 530  
 Nim, juego de, 57
- notación asintótica, véase también Bachmann-Landau, notaciones de, 262  
 algoritmos, 23  
 NP-completo, problema, 392, 399, 420  
 NTL, 89, 167  
 numerabilidad, 85  
 número  
     algebraico, 37, 88  
     Carmichael, véase Carmichael, número de  
     irracional, 39, 63, 82, 88, 94, 112, 297  
          $\gamma$ , 284  
          $\pi$ , 48  
          $\sqrt{2}$ , 44, 83, 94, 95, 110  
         e, 46  
     perfecto, 131  
         impar, 132  
         par, 131  
     primo, 95  
     pseudoprimo, 177  
     racional, 38, 39  
     real, 81  
     trascendente, 63, 64, 88  
 número natural  
     combinación, 335  
     partición, 369  
 números harmónicos, 10, 283, 293, 383, 526  
     aproximación, 284, 315  
     generalizados, 383  
 números harmónicos generalizados, 294
- O**
- o exclusivo, 2  
 o inclusivo, 2  
 Odlyzko-Flajolet, método de, 534  
 OEIS, 355  
 operación, 33, 125  
     asociativa, 5, 33, 81, 132, 455  
     asociativa derecha, 33  
     asociativa izquierda, 33  
     binaria, 33  
     cerrada, 33  
     comutativa, 33, 81, 132  
     distributiva, 33, 81  
     elemento neutro, 33, 81, 102, 132, 176  
     inverso, 81, 102  
     máximo común divisor, 91  
     no asociativa, 33  
     notación infijo, 33  
     notación postfijo, 33

- notación prefijo, 33  
 polinomios, 139  
 precedencia, 33  
 unaria, 33  
 operador, 62  
 ordenamiento  
   cotas, 407  
   heapsort, 316  
   inserción, 23, 373  
   intercalación, 307, 309  
     análisis, 310  
   quicksort, 308, 312
- P**
- palabra, 136, 192  
 asintótica, 529  
 autocorrelación, 337  
 correlación, 337  
 número, 336  
 patrón, 336  
 primitiva, 136  
   número, 137  
   raíz, 136  
 tiempo de espera, 337, 338  
 paradoja del cumpleaños, 173  
   análisis aproximado, 173  
 paradoja del inventor, 60, 239  
 paréntesis balanceados, *véase* Catalan, números de  
 PARI/GP, 89, 110, 139, 268  
 paridad, bits de, 164  
 parte fraccional, 14  
   identidades, 14  
 parte principal, 510  
 Pascal, distribución de, 262  
 Pascal, identidad de, 195, 197  
 Pascal, triángulo de, 304  
 pavimentación, 58, 309  
 Pell, ecuación de, 111, 113  
   solución fundamental, 112  
   solución trivial, 111  
 Pell, John, 111  
 Pell, números de, 111  
 permutación, 455  
   alternante, 350  
   ciclos, 383  
   clasificación, 459  
   conjugada, 459  
   generatriz, 346  
   grupo, 456  
   impar, 460  
   índice de ciclos, 471  
   inversión, 373  
     número promedio, 374  
   involución, 458  
   máximos izquierda a derecha, 382  
   notación ciclo, 456  
   número, 455  
   orden, 458  
   par, 460  
   punto fijo, 246  
   signo, 460  
     determinar, 461  
   tipo, 459, 471  
     número, 462  
   transposición, 459  
 PERT, *véase* Project Management and Evaluation Technique  
 Petersen, grafo de, 391  
 Picard, Charles Émile, 508  
 Picard, teorema de, 508  
*pigeonhole principle*, *véase* principio del palomar  
 Pitágoras, 36, 44, 45, 53, 111  
 Pitágoras, teorema de, 36  
 Pochhammer, símbolo de, 12  
 Poisson, distribución de, 262  
 poliedro, 467  
   arquimedeano, 467  
   regular, 411, 467, 476, 478  
 polígono, 463, 467  
   regular, 103  
   triangulación, 357  
 polinomio, 139  
   algoritmo de división, 160  
   campo divisor, 161  
   campo finito, 165  
   cero, 139, 497  
   ceros repetidos, 146  
   coeficiente principal, 139, 232  
   coeficientes enteros, 88  
   congruencia, 159  
   constante, 139  
   criterio de cero racional, 93  
   cuadrático, 139  
   cúbico, 139  
   derivada formal, 140  
   factorización, 146  
   grado, 139  
   irreducible, 157

- número, 163
- lineal, 139
- mínimo (de un elemento), 156, 157
- mónico, 94, 139, 156
- número de ceros, 147
- simétrico, 232
  - elemental, 232
  - generatriz, 233
  - homogéneo completo, 232
  - suma de potencias, 232
- teorema fundamental de la aritmética, 146, 159
- universal, 156
- polo, 289
- Pólya, George, 68
- Pólya, teoría de enumeración de, 463, 475
- potencia
  - cálculo, 318
  - cálculo eficiente, 327
  - factorial, 364, 365, 521
    - derivada, 294
  - potencia factorial, 11
  - potencias, suma, 228, 283
- predicado (lógica), 3
- premature optimization*, 72
- Prim, algoritmo de, 436
- principio de inclusión y exclusión, véase inclusión y exclusión, principio de
- principio del argumento, 515
- principio del palomar, 18, 112
- probabilidad, 251
  - Bayes, regla de, véase Bayes, regla de
  - como frecuencia, 252
  - condicional, 258
  - diagrama de árbol, 257
  - distribución binomial, 261, 262
  - distribución binomial negativa, véase Pascal, distribución de
  - distribución de Bernoulli, véase Bernoulli, distribución de
  - distribución de Poisson, véase Poisson, distribución de
  - distribución discreta, 252
  - distribución geométrica, 261
  - distribución hipergeométrica, 262
  - distribución multivariada, 257
  - distribución uniforme, 263
  - evento, 252, 252
    - mutuamente excluyente, 253, 254
  - propiedades, 253
- función de distribución, 252
- función generatriz de, 254
- independencia, 260
- independientes e idénticamente distribuidas, 261
- modelo de urna, 256
- valor esperado, 264
  - linealidad, 264
- varianza, 265
- probabilidades
  - evento
    - independiente, 260
  - variable
    - independiente, 260
- problème des ménages*, 248
- problema de franqueo, véase Frobenius, problema de
- producto cartesiano, 330
- productoria, 8
  - vacía, 11
- programa
  - afirmaciones, 77
  - casos de prueba, 76, 79
  - correctitud, 71
  - correctitud parcial, 72, 73
  - correctitud total, 72, 73
  - ejecución simbólica, 79
  - estructuras de control, 78
  - exponenciar, 76
  - invariante de ciclo, 73, 78
  - optimización de código, 79
  - raíz cuadrada entera, 77
  - recursión, 78
  - subrutinas, 78
  - traza, 79
  - variables, 78
  - verificación formal, 71
  - comedia, 72
- Project Management and Evaluation Technique*, 444
- propiedad, 371
  - promedio, 371–374, 376, 378, 379, 381, 383
  - varianza, 380, 381, 383
- propiedad arquimediana, 83, 84
- proporción, propiedades, 46
- proporciones, teoría de, 44
- proposición, 1, 36, 41
- pseudoprímo, véase número pseudoprímo
- punto aislado, 484
- punto de acumulación, 484

punto frontera, 483  
 punto interior, 483

**Q**

$\mathbb{Q}$  (números racionales), 4, 82, 153  
 $\mathbb{Q}^+$  (números racionales positivos), 4  
 quicksort, véase ordenamiento  
     análisis, 313  
     mejor caso, 315  
     peor caso, 315

**R**

$\mathbb{R}$  (números reales), 4, 81, 110, 153  
 $\mathbb{R}$  (números reales), 81  
     axioma, 81  
 $\mathbb{R}^+$  (números reales positivos), 4  
 raíz primitiva, 149, 177, 178, 182, 183  
     número, 152  
 raíz primitiva de 1, 216  
 Ramanujan, Srinivasa, 36  
 razonamiento matemático, 35  
 recíproco, 38  
 recíproco (lógica), 2  
 recurrencia, 168, 229, 317, 357  
     desarreglo, 367  
     generatriz, 320  
     historia completa, 317  
     historia limitada, 317  
     lineal, 317  
         coeficientes constantes, 320  
         factor sumador, 318  
         homogénea, 317  
         primer orden, 318  
         solución, 318  
         solución particular, 318  
     orden, 317  
     receta, 210  
     Riccati, véase Riccati, recurrencia de  
         transformación de Möbius, 327  
 red, véase grafo, 444, véase digrafo  
     camino aumentable, 449, 451  
     corte, 453  
     flujo, 446, 447  
     flujo máximo, 447  
     fuente, 446  
     residual, 449  
     suma implícita, 448  
         sumidero, 446  
 red de actividades, 444  
 red de computadores, 439

*bridge*, 439  
 protocolo RIP, 435  
 protocolo RSTP, 439  
 protocolo STP, 439  
 refutación, 64  
     contradicción, 65  
 relación, 25, 195, 441  
     antisimétrica, 26  
         transpuesta, 28  
     bien fundada, 61  
     composición, 25  
     equivalencia, 26, 31, 85, 99, 115, 395, 464  
         clases, véase clases de equivalencia  
     irreflexiva, 26, 82  
     número, 195  
     orden, 28, 81, 85, 89  
         tricotomía, 81  
     orden total, 82  
     reflexiva, 26  
         transpuesta, 28  
     simétrica, 26  
         transpuesta, 28  
     total, 26  
         transpuesta, 28  
     transitiva, 26, 81  
         transpuesta, 28  
         transpuesta, 25  
 relación de equivalencia, 119  
 relativamente primos, 91, 123  
     a pares, 123

**S**

Sage, 89  
 Schönhage y Strassen, algoritmo de, 308  
 Schröder, números de, 358  
 Schwartz, teorema de, 385

- sección áurea, 297  
 búsqueda de, véase Fibonacci, búsqueda de  
 secuencia, 8, 330, 352  
 binaria, 372, 380  
 geométrica, 49  
 largo (notación), 8  
 primitiva, 339  
 raíz, 339  
 seL4, 71  
 serie  
   convergencia absoluta, 500  
   convergencia condicional, 501  
 serie de potencias, 207, 267, 273  
   binomio, 211  
   coeficientes, 287  
   convergencia, 268  
   coseno, 214  
   coseno hiperbólico, 214  
   decimar, 216, 245, 299  
   exponencial, 214, 247  
   extraer coeficiente, 215  
   geométrica, 211  
   logaritmo, 214, 538  
   potencia, 227  
   radio de convergencia, 209, 289, 502  
   seno, 214  
   seno hiperbólico, 214  
   series útiles, 211  
 serie formal, 267  
   composición, 271  
   convergencia, 352  
   derivada, 274  
   función implícita, 275  
   igualdad, 268  
   integral, 275  
   multivariada, 275  
   operaciones, 269  
   orden, 270  
   orden total, 275  
   principio de transferencia, 273  
   recíproco, 269  
   secuencia, 270  
     convergencia, 270, 271  
     unidad, 269  
 serie geométrica, 303  
   suma, 226  
 Sethi-Ullman, algoritmo de, 408  
 Sethi-Ullman, números de, 408  
 si y solo si (lógica), 2, 40  
 Sicherman, dados de, 208  
 sin pérdida de generalidad, 43  
 singularidad, 506  
   esencial, 506  
   polo, 506  
   removable, 289, 506  
 sistema criptográfico, 181  
 solo si (lógica), véase implicancia (lógica)  
 Sophie Germain, primo de, 182  
 ssi (si y solo si), véase si y solo si  
*stars and bars*, 193  
 Stirling, constante de, 285  
 Stirling, fórmula de, 285, 290, 376, 533, 535, 536, 538  
 Stirling, números de  
   primera especie, 361, 383  
   cuadro, 362  
   función generatriz, 362  
   recurrencia, 362  
 segunda especie, 360  
   cuadro, 361  
   función generatriz, 361  
   recurrencia, 360  
 tercera especie, véase Lah, números de y potencias, 364  
 Strassen, algoritmo de, 309  
 Strassen, multiplicación de, 308  
*string*, véase secuencia, véase palabra  
 subanillo, 102  
 subgrupo, 102  
   generado, 104  
 Sudoku, 420  
 suficiente (lógica), véase implicancia (lógica)  
 suma  
   aritmética, 526  
   cuadrados, 226  
   de potencias, 228, 283  
   geométrica, 49  
     infinita, 50  
     potencias, 283  
 suma por partes, 13  
 sumatoria, 8  
   índice, 9  
   vacía, 11  
 Sun Tzu, véase Sunzi  
 Sunzi, 124  
 supremo, axioma de, 82  
**T**  
 tabla de verdad (lógica), 2

Tales de Mileto, 35  
Tarjan, algoritmo de, 443  
Taylor, serie de, 505, 512, 514  
Taylor, teorema de, 21, 274  
teorema, 36  
teorema fundamental de la aritmética, 125, 129,  
    159  
teoría, 35  
teoría de números, 89, 181  
tetraedro, 467, 476  
topología, 483  
Touchard, fórmula de, 249  
triángulo  
    congruencia, 45  
    semejanza, 45  
`tsort(1)`, 442  
tupla, 7  
    largo, 8

**U**

Unix, 442  
UTF-8, 182

**V**

valor esperado, 371, 380  
Vandermonde, convolución de, 238  
variable aleatoria, 251, 252, 257  
    función de distribución, 251  
vector, 114, 317  
Venn, diagrama de, 5  
Vieta, fórmulas de, 147, 148

**W**

Wallis, producto de, 11, 286, 286  
Weierstraß, prueba  $M$  de, 501  
Wilf, Herbert S., 242  
Wilson, teorema de, 148

**Z**

$\mathbb{Z}$  (números enteros), 4, 89, 108