# MATEMÁTICA DISCRETA I
# FAMAF - UNC

ALEJANDRO TIRABOSCHI

Año 2022
FAMAF - UNC

## AUTORES/COLABORADORES

- **Obra original:** coordinada y escrita por Alejandro Tiraboschi.
- **Colaboración:** Daniel Penazzi, colaborador de la sección "El criptosistema RSA" y autor principal del apéndice de grafos planares. Fernando Levstein colaborador en la sección "Máximo común divisor y mínimo común múltiplo".
- **Correcciones y sugerencias:** Pedro Pury, Romina Arroyo, Leandro Cagliero, Fredy Restrepo, Patricia Kysbye.

## LICENCIA

# ÍNDICE GENERAL

# ÍNDICE DE FIGURAS

# PREFACIO

Las siguientes notas se han utilizado para el dictado del curso "Matemática Discreta I" del primer año de la carrera de ciencias de la computación de FAMAF-UNC. Han sido las notas principales en el dictado del año 2019 y en algunos años anteriores (desde 1995). Las notas están basadas en diversas fuentes, principalmente en los libros "Discrete Mathematics" de N. Biggs y "Notas de Álgebra I" de E. Gentile, pero a lo largo de los años ha habido numerosas modificaciones y agregados por parte de los diferentes docentes de la cátedra.

El objetivo de las notas es tratar de explicar de una manera simple conceptos aritméticos y algebraicos elementales, de tal forma que luego estos puedan ser utilizados como herramientas en la práctica profesional. En particular, uno de nuestros principales objetivos es el desarrollo de la madurez matemática y la habilidad para resolver problemas matemáticos relacionados con la artitmética, conteo y grafos. A nivel metodológico, el curso comienza con un enfoque formal pero intuitivo que se vuelve cada vez más riguroso a medida que aumenta el interés y las capacidades de abstracción de los alumnos.

Las notas se limitan casi exclusivamente al contenido dictado en el curso y las partes señaladas con (*) y los apéndices son optativos.

El primer capítulo introduce a los alumnos al formalismo de los números enteros como sistema axiomático. En la mitad final de este capítulo se estudia el concepto de definición recursiva y se demuestra y aplica el principio de inducción. En el segundo capítulo se estudian los principios de conteo y diversas técnicas relacionadas a los mismos. Diferentes aspectos de la aritmética elemental son estudiados en el tercer y cuarto capítulo. Como aplicación de lo aprendido en estos dos capítulos se explica el algoritmo RSA. Finalmente, los capítulos 5 y 6 estudian la teoría de grafos y árboles, temas clásicos de la matemática discreta.

Parte I

# NÚMEROS ENTEROS Y ARITMÉTICA

# 1

# NÚMEROS ENTEROS

## 1.1 ARITMÉTICA

Todo lector de este apunte conoce los *enteros*. En una etapa muy temprana de nuestras vidas conocemos los números enteros positivos o "números naturales"

$$1, 2, 3, 4, 5, \ldots$$

Más adelante introducimos el $0$ (cero), y los enteros negativos

$$-1, -2, -3, -4, -5, \ldots$$

En este curso no nos preocupamos demasiado por el significado lógico y filosófico de estos objetos, pero necesitamos saber las propiedades que se supone que tienen. Si todos parten de las mismas suposiciones entonces todos llegarán a los mismos resultados. Estos supuestos son los llamados axiomas.

El punto de vista adoptado en este apunte es el señalado antes. Aceptamos sin reparo que existe un conjunto de objetos llamados *enteros* conteniendo los enteros positivos y los negativos, y el cero, familiares en nuestra temprana educación y experiencia. El conjunto de enteros se denotará por el símbolo especial $\mathbb{Z}$. Las propiedades de $\mathbb{Z}$ serán dadas por una lista de axiomas, a partir de las cuales seremos capaces de deducir todos los resultados sobre números enteros que necesitaremos en las cuestiones subsiguientes. Empezaremos listando aquellos axiomas que tratan la suma y la multiplicación.

Adoptaremos las notaciones usuales $a + b$ para la suma de dos enteros $a$ y $b$, y $a \cdot b$ (frecuentemente $ab$ o también $a \times b$) para su producto. Pensamos en $+$ y $\cdot$ como *operaciones* que a un par de enteros $a$ y $b$ les hacen corresponder un entero $a + b$ y otro $a \cdot b$. El hecho de que $a \cdot b$ y $a + b$ son enteros, y no algún objeto extraño como elefantes, es nuestra primera suposición, el axioma **I1**.

En la siguiente lista de axiomas $a$, $b$, $c$ denotan enteros arbitrarios, y $0$ y $1$ denotan enteros especiales que cumplen las propiedades especificadas más abajo.

**I1)** $a + b$ y $a \cdot b$ pertenecen a $\mathbb{Z}$.

**I2)** *Conmutatividad.* $a + b = b + a; \qquad ab = ba.$

**I3)** *Asociatividad.* $(a + b) + c = a + (b + c); \qquad (a \cdot b) \cdot c = a \cdot (b \cdot c).$

**I4)** *Existencia de elemento neutro.* Existen números $0, 1 \in \mathbb{Z}$ con $0 \neq 1$ tal que $a + 0 = a; \qquad a \cdot 1 = a.$

**I5)** *Distributividad.* $a \cdot (b + c) = a \cdot b + a \cdot c.$

**I6)** *Existencia del inverso aditivo, también llamado opuesto.* Por cada $a$ en $\mathbb{Z}$ existe un único entero $-a$ en $\mathbb{Z}$ tal que $a + (-a) = 0.$

**I7)** *Cancelación.* Si $a \neq 0$ y $a \cdot b = a \cdot c$, entonces $b = c.$

Debido a la ley de asociatividad para la suma, axioma **I3**, $(a + b) + c$ es igual a $a + (b + c)$ y por lo tanto podemos eliminar los paréntesis sin ambigüedad. Es decir, denotamos

$$a + b + c := (a + b) + c = a + (b + c).$$

De forma análoga, usaremos la notación

$$abc = (ab)c = a(bc).$$

Debido a la ley de conmutatividad, axioma **I2**, es claro que del axioma **I4** se deduce que $0 + a = a + 0 = a$ y $1 \cdot a = a \cdot 1 = a$. Análogamente, por **I2** e **I6** obtenemos que $-a + a = a + (-a) = 0.$

Una propiedad que debemos mencionar es la siguiente: si $a, b, c \in \mathbb{Z}$ y $a = b$, entonces $a + c = b + c$ y $ac = bc$. Esto se debe a que la suma y el producto son operaciones que, como acabamos de decir, toman un par de enteros y devuelven otro entero. Si $a = b$, entonces el par $a, c$ es igual al par $b, c$ y por lo tanto devuelven la misma suma y el mismo producto. Esta propiedad no es un axioma, sino una mera aplicación de la lógica formal.

Todos los axiomas corresponden a propiedades familiares de los enteros que aprendemos en distintos niveles de nuestra educación matemática. De ellas pueden deducirse la mayoría de las reglas aritméticas comunes de los enteros como en el siguiente ejemplo.

*Ejemplo* 1.1.1. Demostremos que, para todo $n$ entero, el opuesto de $-n$ es $n$, es decir que

$$-(-n) = n.$$

*Demostración.* El axioma **I6** nos dice que $-(-n)$ es el único número que sumado a $-n$, da cero. Por lo tanto, para demostrar que $-(-n) = n$ basta ver que $(-n) + n = 0$. Esto se cumple puesto que

$$\begin{aligned} (-n) + n &= n + (-n) && \text{(axioma I2)} \\ &= 0 && \text{(axioma I6)} \end{aligned}$$

Por lo tanto $(-n) + n = 0$. □

Como ya dijimos, los números enteros vienen provistos con dos operaciones fundamentales, la suma y la multiplicación. A continuación definimos la resta o sustracción.

**Definición 1.1.2.** Si $a, b \in \mathbb{Z}$ definimos $a - b$ como la suma de $a$ más el opuesto de $b$, es decir que $a - b = a + (-b)$ por definición.

Ahora demostremos una propiedad básica de la resta.

*Ejemplo.* Demostremos que para dos enteros $m$ y $n$ cualesquiera

$$m - (-n) = m + n.$$

*Demostración.* Por la definición de sustracción, $m - (-n)$ es la suma $m + (-(-n))$, es decir

$$m - (-n) = m + (-(-n)).$$

Por el ejemplo 1.1.1 sabemos que $-(-n) = n$ y por lo tanto $m - (-n) = m + (-(-n)) = m + n$. □

Tanto formalismo, como el usado en las demostraciones realizadas en el ejemplo anterior, puede ser tedioso, pero nos permite comenzar a comprender la estructura de una demostración formal.

**Proposición 1.1.3.** *Supongamos que existen dos enteros $0$ y $0'$ ambos cumpliendo el axioma **I4**, esto es*

$$a + 0 = a, \qquad a + 0' = a$$

*para todo $a$ de $\mathbb{Z}$. Entonces $0 = 0'$.*

*Demostración.*

$$\begin{aligned} 0 &= 0 + 0' && \text{(axioma \textbf{I4} aplicado a } 0 \text{ y con } 0' \text{ como neutro)} \\ &= 0' + 0 && \text{(axioma \textbf{I2})} \\ &= 0' && \text{(axioma \textbf{I4} aplicado a } 0' \text{ y con } 0 \text{ como neutro).} \end{aligned}$$

□

El resultado anterior nos demuestra que hay un único elemento elemento que cumple el axioma **I4** en lo que respecta a la suma. A este elemento lo denotamos $0$ y lo denominamos el *elemento neutro de la suma*. Lo mismo podemos probar con el elemento neutro respecto al producto (ver ejercicio 3), es decir hay un único elemento, denotado $1$, que satisface el axioma **I4** en lo que se refiere al producto. A este elemento lo llamamos el *elemento neutro del producto*.

**Proposición 1.1.4** (Regla de los signos). *Veamos que si* $a, b \in \mathbb{Z}$ *entonces*

$$(-a)(-b) = ab, \qquad a(-b) = (-a)b = -(ab).$$

*Demostración.* Veremos que $a(-b) = -(ab)$. Los otros casos se dejan como ejercicio para el lector.

Una forma de demostrar este caso es observando que $-(ab)$ es el inverso aditivo de $ab$ y comprobando que $a(-b)$ es también inverso aditivo de $ab$. Luego, por unicidad del inverso aditivo, de deduce que $a(-b) = -(ab)$.

$$\begin{aligned} ab + a(-b) &= a(b-b) && \text{axioma } \mathbf{I5} \\ &= a \cdot 0 && \text{axioma } \mathbf{I4} \\ &= 0 && \text{ejercicio } 4. \end{aligned}$$

Es decir $a(-b)$ es el inverso aditivo de $ab$, luego por la unicidad del inverso aditivo axioma **I6**, $a(-b) = -(ab)$. □

Algunos resultados similares pueden encontrarse en los siguientes ejercicios. Como aún no tenemos todos los axiomas correspondientes a los enteros, los resultados no son particularmente interesantes, pero lo que importa es recordar que pueden ser probados sobre la base única de los axiomas.

§ *Ejercicios*

1) Demostrar la regla $(a+b)c = ac + bc$, explicando cada paso.

2) Como siempre $x^2$ denota $x \cdot x$. Demostrar que dados dos enteros $a$ y $b$ tal que $a + b \neq 0$, entonces existe un único $c$ tal que $(a+b)c = a^2 - b^2$.

3) Probar que hay un único elemento neutro del producto.

4) La siguiente es una demostración de la fórmula $0x = 0$ usando solo los axiomas planteados antes. Escribir la demostración completa, explicando que axioma es usado en cada paso.

$$\begin{aligned} 0x &= (0+0)x && \text{(axioma .....)} \\ &= 0x + 0x. && \text{(axioma .....)} \end{aligned}$$

Luego $0x = 0x + 0x$. Sumando $-0x$ a ambos miembros de la igualdad, obtenemos

$$\begin{aligned} 0x + (-0x) &= 0x + 0x + (-0x) && \text{(usando lógica formal)} \\ 0 &= 0x + 0 && \text{(axioma ..... dos veces)} \\ 0 &= 0x. && \text{(axioma .....)} \end{aligned}$$

## 1.2 ORDENANDO LOS ENTEROS

El orden natural de los enteros es tan importante como sus propiedades aritméticas. Desde el comienzo aprendemos los números en el orden $1, 2, 3, 4, 5$, y el hecho de que 4 es "mayor" que 3 se convierte en algo de importancia práctica para nosotros. Expresamos esta idea formalmente diciendo que existe una relación que indicamos "$<$" ($a < b$ se lee: $a$ es menor que $b$ o también $b$ es mayor que $a$).

Solo cuatro axiomas se necesitan para especificar las propiedades básicas del símbolo $<$ , y ellos son listados en lo que sigue. La numeración de los axiomas se continúa de la sección 1.1. Como antes, $a$, $b$ y $c$ denotan enteros arbitrarios.

**I8)** *Ley de tricotomía.* Vale una y sólo una de las relaciones siguientes:

$$a < b, \qquad a = b, \qquad b < a.$$

**I9)** *Ley transitiva.* Si $a < b$ y $b < c$, entonces $a < c$.

**I10)** *Compatibilidad de la suma con el orden.* Si $a < b$, entonces $a + c < b + c$.

**I11)** *Compatibilidad del producto con el orden.* Si $a < b$ y $0 < c$, entonces $ac < bc$.

Esta claro que podemos definir los otros símbolos de orden $>$, $\leqslant$ y $\geqslant$, en términos de los símbolos $<$ e $=$. Diremos que $m > n$ si $n < m$, diremos que $m \leqslant n$ si $m < n$ o $m = n$. Finalmente, diremos que $m \geqslant n$ si $m > n$ o $m = n$. Es importante notar que el axioma **I11** tiene una versión valedera para estos nuevos símbolos.

*a)* **($>$)** Si $a > b$ y $c > 0$, entonces $ac > bc$.

*b)* **($\leqslant$)** Si $a \leqslant b$ y $0 \leqslant c$, entonces $ac \leqslant bc$.

*c)* **($\geqslant$)** Si $a \geqslant b$ y $c \geqslant 0$, entonces $ac \geqslant bc$.

Usando las definiciones de $\geqslant$, $<$, $>$ y el axioma **I11** original es muy sencillo demostrar estas variantes. Por otro lado,

**Proposición 1.2.1.** *Sean* $a, b, c \in \mathbb{Z}$.

*a) Si* $c < 0$, *entonces* $0 < -c$.

*b) Si* $a < b$ *y* $c < 0$, *entonces* $ac > bc$.

*Demostración (*).*

*a)* Sumando $-c$ a ambos miembros de la desigualdad $c < 0$, obtenemos $c + (-c) < 0 + (-c)$ (compatibilidad de la suma con la relación de orden).

Por los axiomas de inverso aditivo y elemento neutro, la expresión se reduce a $0 < -c$.

*b)* Como $a < b$, si sumamos a ambos miembros de la desigualdad $-a - b$, por la compatibilidad de la suma con $<$, obtenemos $a - a - b < b - a - b$ y por la aplicación reiterada de los axiomas de inverso aditivo y elemento neutro obtenemos $-b < -a$. Por a) sabemos que $0 < -c$, por lo tanto, por **I11**, $(-b)(-c) < (-a)(-c)$. Aplicando la regla de los signos obtenemos $bc < ac$ y por lo tanto $ac > bc$.

□

Ya hemos usado (en axiomas **I4** e **I7**) el símbolo $\neq$ que denota "*no* es igual a " o bien "es distinto a". En general, cuando tachamos un símbolo, estamos indicando la negación de la relación que define. Por ejemplo, $a \not< b$ denota "$a$ *no* es menor que $b$".

*Observación.* Demostremos que $a \not< b$ es equivalente a $a \geqslant b$: por la ley de tricotomía axioma **I8** tenemos que solo vale una y solo una de las siguientes afirmaciones

$$a < b, \qquad a = b, \qquad b < a.$$

Como $a \not< b$, entonces vale una de las dos afirmaciones siguientes, $a = b$ o $b < a$, es decir vale que $a \geqslant b$. De forma análoga se prueba que $a \leqslant b$ si y sólo si $a > b$, $a \not> b$ si y sólo si $a \leqslant b$ y $a \ngeqslant b$ si y sólo si $a < b$.

*Ejemplo* 1.2.2. Demostremos las siguiente propiedades de $\leqslant$. Sean $a$, $b$ y $c$ enteros arbitrarios, entonces

**O1)** *Reflexividad.* $a \leqslant a$.

**O2)** *Antisimetría.* Si $a \leqslant b$ y $b \leqslant a$, entonces $a = b$.

**O3)** *Transitividad.* Si $a \leqslant b$ y $b \leqslant c$, entonces $a \leqslant c$.

*Demostración.*

(**O1**) Como $a = a$, tenemos entonces que $a \leqslant a$ (por definición de $\leqslant$).

(**O2**) Como $a \leqslant b$, tenemos que $a < b$ o bien $a = b$ (por tricotomía no pueden valer ambas). Si ocurriera que $a < b$, por la observación anterior, tendríamos que $a \ngeqslant b$, es decir $b \nleqslant a$, lo cual es absurdo pues una de nuestras hipótesis es, justamente, lo contrario: $b \leqslant a$. Es decir, la única posibilidad que queda es que $a = b$.

(**O3**) Como $a \leqslant b$, entonces $a < b$ o bien $a = b$. Como $b \leqslant c$, entonces $b < c$ o bien $b = c$. Para hacer la demostración, debemos pensar en todas las posibles combinaciones de estas afirmaciones:

- $a < b$ y $b < c$. Es este caso, por **I9**, $a < c$. Luego $a \leqslant c$.
- $a < b$ y $b = c$. Luego $a < c$ y eso implica que $a \leqslant c$.
- $a = b$ y $b < c$. Luego $a < c$ y eso implica que $a \leqslant c$.
- $a = b$ y $b = c$. Es claro entonces que $a = c$, lo cual implica que $a \leqslant c$.

□

Una relación que satisfaga las tres propiedades anteriores (reflexividad, antisimetría y transitividad) es llamada *una relación de orden*. Observar que $<$ *no* es una relación de orden, en el sentido de la definición anterior.

A primera vista podría parecer que ya tenemos todas las propiedades que necesitamos de $\mathbb{Z}$, pero, sorprendentemente, aún falta un axioma de vital importancia. Supongamos que $X$ es un subconjunto de $\mathbb{Z}$; entonces diremos que el entero $b$ es una *cota inferior* de $X$ si

$$b \leqslant x \qquad \text{para todo } \ x \in X.$$

Algunos subconjuntos no tienen cotas inferiores: por ejemplo, el conjunto de los enteros negativos $-1, -2, -3, \ldots$, claramente no tiene cota inferior. Por otro lado, el conjunto $S$ denotado por los números resaltados en la Fig. 1 tiene muchas cotas inferiores. Una mirada rápida nos dice que $-9$ por ejemplo es una cota inferior, mientras que una inspección más minuciosa revela que $-7$ es la "mejor" cota inferior, pues en realidad pertenece a $S$. En general, una cota inferior de un conjunto $X$ que es a su vez es un elemento de $X$, es conocido como el *mínimo* de $X$.

$$-10, -9, -8, \mathbf{-7}, \mathbf{-6}, -5, -4, \mathbf{-3}, -2, -1, 0, \mathbf{1}, \mathbf{2}, \mathbf{3}, 4, 5, 6, 7, 8, 9, 10$$

Figura 1: El mínimo de $S$ es $-7$.

Nuestro último axioma para $\mathbb{Z}$ afirma algo que es (aparentemente) una propiedad obvia.

**I12)** Si $X$ es un subconjunto de $\mathbb{Z}$ que no es vacío y tiene una cota inferior, entonces $X$ tiene un mínimo.

El axioma **I12** es conocido como el *axioma de buena ordenación* o *axioma del buen orden* o *principio de buena ordenación*. Una buena forma de entender su significado es considerar $X$ un conjunto de enteros acotado inferiormente y un juego en el cual dos personas eligen alternativamente un elemento de $X$, sujetos a la regla de que cada número debe ser estrictamente menor que el anterior. El axioma nos dice que cuando los números son enteros, el juego terminará; además el final se producirá cuando uno de los jugadores tenga el buen sentido de elegir el mínimo. Esta propiedad aparentemente

obvia *no* se mantiene necesariamente cuando tratamos con números que no son enteros, pues X puede no tener un mínimo aunque tenga una cota inferior. Por ejemplo supongamos que X es el conjunto de fracciones $3/2, 4/3, 5/4, \ldots$ teniendo por forma general $(n+1)/n$, $n \geqslant 2$. Este conjunto tiene una cota inferior (1, por ejemplo) pero no tiene mínimo y por lo tanto los jugadores podrían seguir jugando para siempre, eligiendo fracciones más y más cercanas a 1.

El axioma del buen orden nos da una justificación firme para nuestro intuitivo dibujo de los enteros: un conjunto de puntos regularmente espaciados sobre una linea recta, que se extiende indefinidamente en ambas direcciones como en la Fig. 2. En particular dice que no podemos acercarnos más y más a un entero sin alcanzarlo, de forma que el dibujo de la Fig. 3 no es correcto.



Figura 2: El dibujo correcto de $\mathbb{Z}$.



Figura 3: El dibujo incorrecto de $\mathbb{Z}$.

El hecho de que haya espacios vacíos entre los enteros nos lleva a decir que el conjunto $\mathbb{Z}$ es *discreto* y es esta propiedad la que da origen al nombre "matemática discreta". En cálculo y análisis, los procesos de límite son de fundamental importancia, y es preciso usar aquellos sistemas numéricos que son *continuos*, en vez de los discretos.

El siguiente resultado es obvio, pero debe ser demostrado. Sin embargo, la demostración es bastante compleja y sólo se da por completitud.

**Proposición 1.2.3.** $1$ *es el menor entero mayor que* $0$.

*Demostración (*).* Primero debemos probar que $0 < 1$. Ahora bien, como $0 \neq 1$ (por axioma **I4**), por la ley de tricotomía (axioma **I8**), debe ocurrir que $0 < 1$ o $1 < 0$. Supongamos que $1 < 0$, luego por proposición 1.2.1, $1 \cdot 1 > 1 \cdot 0$. Como 1 es elemento neutro de la multiplicación, obtenemos $1 > 0$, que contradice nuestra suposición. Esta contradicción vino de suponer que $1 < 0$. Por lo tanto, $0 < 1$.

Probaremos ahora que no existe $a$ entero tal que $0 < a < 1$ y lo haremos por el absurdo: supongamos que existe $a \in \mathbb{Z}$ tal que $0 < a < 1$ y sea

$$X = \{a \in \mathbb{Z} : 0 < a < 1\}.$$

La suposición que hicimos implica que X es no vacío. Dado que todos los elementos de X son positivos, X es un subconjunto de $\mathbb{Z}$ acotado inferiormente (0 es cota inferior). Por el axioma del buen orden (axioma **I12**) resulta que X tiene un elemento mínimo, que llamaremos $a_0$, y cumple

$$0 < a_0 < 1.$$

Usamos ahora la compatibilidad del producto con la relación de orden (**I11**): por un lado multiplicamos por $a_0$ la desigualdad $0 < a_0$ y obtenemos $0 < a_0^2$, y por otro lado multiplicamos por $a_0$ la desigualdad $a_0 < 1$ y obtenemos $a_0^2 < a_0$. Es decir

$$0 < a_0^2 < a_0 < 1.$$

La desigualdad $0 < a_0^2 < 1$ dice que $a_0^2 \in X$ pero la desigualdad $a_0^2 < a_0$ dice que $a_0$ no es el mínimo elemento de X, lo cual es una contradicción pues dijimos que $a_0$ es el mínimo elemento de X. El absurdo vino de suponer que existe $a \in \mathbb{Z}$ tal que $0 < a < 1$. □

§ *Ejercicios*

1) Sean $a, b \in \mathbb{Z}$ tal que $a, b \neq 0$. Probar que $ab \neq 0$. (Ayuda: considerar primero el caso $a > 0$ y $b > 0$).

2) Demostrar que $\geqslant$ es una relación de orden.

3) Demostrar que dados cualesquiera $a, b, c \in \mathbb{Z}$ vale que si $a < b$ y $0 \leqslant c$, entonces $ac \leqslant bc$.

4) Demostrar que si $a \leqslant b$ y $c \leqslant 0$, entonces $bc \leqslant ac$.

5) Demostrar que $0 \leqslant x^2$ para todo x en $\mathbb{Z}$.

6) Deducir de la proposición 1.2.3 que $n + 1$ es el menor entero mayor que $n$ para todo $n$ en $\mathbb{Z}$.

7) Demostrar que si un conjunto X tiene mínimo, este es único. Dicho más formalmente: demostrar que si existen $c, c' \in X$ tal que $c \leqslant x$ y $c' \leqslant x$ para todo $x \in X$, entonces $c = c'$.

8) En cada uno de los siguientes casos decir si el conjunto X tiene o no una cota inferior, y si la tiene, encontrar el mínimo.

   (1) $X = \{x \in \mathbb{Z} | x^2 \leqslant 16\}$.

   (2) $X = \{x \in \mathbb{Z} | x = 2y \text{ para algún } y \in \mathbb{Z}\}$.

   (3) $X = \{x \in \mathbb{Z} | x \leqslant 100\, x\}$.

9) Un subconjunto Y de Z se dice que tiene una *cota superior* c si $c \geqslant y$ para todo $y \in Y$. Una cota superior que además es un elemento de Y

es llamada el *máximo* de Y. Usar el axioma **I12** para demostrar que si Y es no vacío y tiene una cota superior, entonces tiene máximo. [Ayuda: aplicar el axioma al conjunto cuyos elementos son $-y$ ($y \in Y$).]

10) Los enteros $n$ que satisfacen $1 \leqslant n \leqslant 25$ están acomodados en forma arbitraria en un arreglo cuadrado de cinco filas y cinco columnas. Se selecciona el máximo de cada fila, y se denota $s$ al mínimo entre ellos. De manera similar, el mínimo de cada columna es seleccionado y $t$ denota al máximo entre ellos. Demostrar que $s \geqslant t$ y de un ejemplo en el cual $s \neq t$.

## 1.3 DEFINICIONES RECURSIVAS

Sea $\mathbb{N}$ el conjuntos de enteros positivos, esto es

$$\mathbb{N} = \{n \in \mathbb{Z} | n \geqslant 1\},$$

y denotemos $\mathbb{N}_0$ el conjunto $\mathbb{N} \cup \{0\}$, esto es

$$\mathbb{N}_0 = \{n \in \mathbb{Z} | n \geqslant 0\}.$$

$\mathbb{N}$ es llamado el conjunto de *números naturales*. Si $X$ es un subconjunto de $\mathbb{N}$ (o de $\mathbb{N}_0$) entonces automáticamente tiene una cota inferior, pues cada elemento $x$ de $X$ satisface $x \geqslant 1$ (o $x \geqslant 0$). Así, en este caso el axioma del buen orden toma la forma

*si $X$ es un subconjunto no vacío de $\mathbb{N}$ o $\mathbb{N}_0$ entonces $X$ tiene un mínimo.*

Esta la forma más usada en la práctica.

Nuestro primer uso del axioma del buen orden será para justificar un procedimiento muy usual. Frecuentemente encontramos una expresión de la forma $u_n$, donde $n$ indica cualquier entero positivo: por ejemplo, podríamos tener $u_n = 3n + 2$, o $u_n = (n + 1)(n + 2)(n + 3)$. En estos ejemplos $u_n$ es dado por una fórmula explícita y no existe dificultad en calcular $u_n$ cuando se nos da un valor específico para $n$. Sin embargo en muchos casos no conocemos una fórmula para $u_n$; es más, nuestro problema puede ser encontrarla. En estos casos pueden darnos ciertos valores de $u_n$ para enteros positivos $n$ pequeños, y una relación entre el $u_n$ general y algunos de los $u_r$ con $r < n$. Por ejemplo, supongamos nos es dado

$$u_1 = 1, \qquad u_2 = 2, \qquad u_n = u_{n-1} + u_{n-2}, \qquad n \geqslant 3.$$

Para calcular los valores de $u_n$ para todo $n$ de $\mathbb{N}$ podemos proceder como sigue:

$$\begin{aligned} u_3 &= u_2 + u_1 = 2 + 1 = 3, \\ u_4 &= u_3 + u_2 = 3 + 2 = 5, \\ u_5 &= u_4 + u_3 = 5 + 3 = 8, \end{aligned}$$

y así siguiendo. Éste es un ejemplo de una *definición recursiva*. Es "obvio" que el método dará un valor único de $u_n$ para todo entero positivo $n$. Pero hablando estrictamente necesitamos el axioma del buen orden para justificar la conclusión a través de las siguientes líneas.

Supongamos que existe un entero positivo $n$ para el cual $u_n$ no está definido de manera única. Entonces por el axioma del buen orden existe un entero positivo mínimo $m$ con esta propiedad. Como $u_1$ y $u_2$ están explícitamente definidos, $m$ no es 1 o 2 y la ecuación $u_m = u_{m-1} + u_{m-2}$ es aplicable. Por la definición de $m$, $u_{m-1}$ y $u_{m-2}$ están definidos de manera única, y la ecuación nos da un valor único para $u_m$ , contrariamente a la hipótesis. La contradicción surge de suponer que no está bien definido para algún $n$, y por lo tanto esta suposición debe ser falsa.

El lector no debe desanimarse por el uso de argumentos tan retorcidos para establecer algo que es "obviamente" verdadero. En primer lugar, no debemos usar resultados ilegítimamente (sin demostrarlos), y en segundo lugar, el hecho de que el resultado sea "obvio" simplemente indica que estamos trabajando con la correcta representación mental de $\mathbb{N}$ y $\mathbb{Z}$. Una vez que hemos establecido esa representación sobre bases firmes podemos empezar a extendernos y obtener resultados que no sean tan "obvios".

El método de definición recursiva aparecerá bastante seguido en el resto del apunte. Existen otras formas de este procedimiento que se "esconden" por su notación. ¿Qué significan las siguientes expresiones?

$$\sum_{r=1}^{n} 2r-1, \qquad 1+3+5+\cdots+(2n-1).$$

Claramente no basta decir que uno significa lo mismo que el otro, porque cada uno contiene un misterioso símbolo, $\sum$ y $\cdots$, respectivamente. Lo que deberíamos decir es que cada uno de ellos es equivalente a la expresión $s_n$, dada por la siguiente definición recursiva:

$$s_1 = 1, \qquad s_n = s_{n-1} + (2n-1), \qquad n \geqslant 2.$$

Esto hace ver claro que ambos símbolos misteriosos son, en realidad, una forma de acortar una definición recursiva, y que por lo tanto son expresiones definidas para todo $n$ en $\mathbb{N}$.

Ideas similares pueden aplicarse a la definición de productos tal como $n!$ (que se lee $n$ *factorial*). Si decimos que

$$n! = 1 \cdot 2 \cdot 3 \cdots n,$$

el significado es bastante claro para cualquiera. Pero para precisar (y hacerlo claro para una computadora) debemos usar las definiciones recursivas.

**Definición 1.3.1.** Sea $n \in \mathbb{N}$ sean $a_i$ para $1 \leqslant i \leqslant n$, una secuencia de números (enteros, reales, etc.). Entonces $\sum_{i=1}^{n} a_i$ denota la función recursiva definida

$$\sum_{i=1}^{1} a_i = a_1, \qquad \sum_{i=1}^{n} a_i = \sum_{i=1}^{n-1} a_i + a_n \quad (n \geqslant 2).$$

En este caso decimos que $\sum_{i=1}^{n} a_i$ es la *sumatoria* de los $a_i$ de $i = 1$ a $n$. El símbolo $\prod_{i=1}^{n} a_i$ denota la función recursiva definida

$$\prod_{i=1}^{1} a_i = a_1, \qquad \prod_{i=1}^{n} a_i = \prod_{i=1}^{n-1} a_i \cdot a_n \quad (n \geqslant 2).$$

En este caso decimos que $\prod_{i=1}^{n} a_i$ es la *productoria* de los $a_i$ de $i = 1$ a $n$.

En el caso de $n!$ se puede o bien definir como $\prod_{i=1}^{n} i$, o bien como

$$1! = 1, \qquad n! = n \cdot (n-1)! \quad (n \geqslant 2).$$

Otro caso que debemos mencionar es el de la definición de "$n$-ésima potencia": sea $x$ un número, si $n \in \mathbb{N}$ definimos

$$x^1 = x, \qquad x^n = x \cdot x^{n-1} \quad (n \geqslant 2).$$

Por completitud, definimos $x^0 = 1$.

§ *Ejercicios*

1) En el caso siguiente calcule (donde sea posible) los valores de $u_1$, $u_2$, $u_3$ y $u_4$ dados por las ecuaciones. Si no puede calcular los valores explicar porque la definición no esta bien.

   *a)* $u_1 = 1, \quad u_2 = 1, \quad u_n = u_{n-1} + 2u_{n-2}, \quad n \geqslant 3.$

   *b)* $u_1 = 1, \quad u_n = u_{n-1} + 2u_{n-2}, \quad n \geqslant 2.$

   *c)* $u_1 = 0, \quad u_n = nu_{n-1}, \quad n \geqslant 2.$

2) Sea $u_n$ definido por las ecuaciones

   $$u_1 = 2, \qquad u_n = 2^{u_{n-1}}, \qquad n \geqslant 2.$$

   ¿Cuál es el primer valor de $n$ para el cual no se puede calcular $u_n$ usando una calculadora de bolsillo o de su celular?

3) Escribir fórmulas explícitas para las expresiones $u_n$ definidas por las siguientes ecuaciones.

   *a)* $u_1 = 1, \quad u_n = u_{n-1} + 3, \quad n \geqslant 2.$

   *b)* $u_1 = 1, \quad u_n = n^2 u_{n-1}, \quad n \geqslant 2.$

## 1.4 EL PRINCIPIO DE INDUCCIÓN

Supongamos que nos piden que demostremos el resultado

$$1+3+5+\cdots+(2n-1)=n^2.$$

En otras palabras, debemos demostrar que la expresión de la izquierda definida recursivamente es igual a la expresión definida explícitamente por la fórmula de la derecha, para todos los enteros positivos $n$. Podemos proceder como sigue.

La fórmula es ciertamente correcta cuando $n=1$ puesto que $1=1^2$. Supongamos que es correcta para un valor específico de $n$, digamos para $n=k$, de modo que

$$1+3+5+\cdots+(2k-1)=k^2.$$

Podemos usar esto para simplificar la expresión definida recursivamente a la izquierda cuando $n$ es igual a $k+1$,

$$\begin{aligned}1+3+5+\cdots+(2k+1) &= 1+3+5+\cdots+(2k-1)+(2k+1)\\ &= k^2+(2k+1)\\ &= (k+1)^2.\end{aligned}$$

Por lo tanto si el resultado es correcto cuando $n=k$, entonces lo es cuando $n=k+1$. Se comienza observando que si es correcto cuando $n=1$, debe ser por lo tanto correcto cuando $n=2$. Con el mismo argumento como es correcto cuando $n=2$ debe serlo cuando $n=3$. Continuando de esta forma veremos que es correcto para todos los enteros positivos $n$.

La esencia de este argumento es comúnmente llamada *principio de inducción*. Es una técnica poderosa, fácil de aplicar y la aplicaremos frecuentemente. Pero primero debemos examinar sus bases lógicas y para hacerlo necesitamos una formulación más general.

Supongamos que queremos demostrar que un resultado es verdadero para todo $n\in\mathbb{N}$. Con $S$ denotemos al subconjunto de $\mathbb{N}$ para el cual el resultado es correcto: por supuesto, nuestra intención es probar que $S$ es todo $\mathbb{N}$. El primer paso es probar que 1 pertenece a $S$, y luego demostraremos que si $k$ pertenece a $S$, también $k+1$. Entonces lo pensamos paso a paso, un procedimiento infinito, y concluimos que $S=\mathbb{N}$. Afortunadamente el pensarlo paso a paso no es esencial debido a que el principio de inducción es consecuencia de los axiomas que elegimos tan cuidadosamente para $\mathbb{Z}$ y $\mathbb{N}$. Más específicamente es consecuencia del axioma del buen orden.

Veremos ahora una versión muy utilizada del principio de inducción.

**Teorema 1.4.1** (Principio de inducción). *Sea* $P(n)$ *una propiedad para* $n \in \mathbb{N}$ *tal que:*

*a)* $P(1)$ *es verdadera.*

*b) Para todo* $k \in \mathbb{N}$, $P(k)$ *verdadera implica* $P(k+1)$ *verdadera.*

*Entonces* $P(n)$ *es verdadera para todo* $n \in \mathbb{N}$.

*Demostración.* Basta tomar

$$S = \{n \in \mathbb{N} | P(n) \text{ es verdadera}\}.$$

Entonces $S$ es un subconjunto de $\mathbb{N}$ y las condiciones *a)* y *b)* nos dicen que 1) $1 \in S$ y 2) si $k \in S$ entonces $k+1 \in S$.

Si la conclusión es falsa, tenemos que $S \neq \mathbb{N}$ y entonces el conjunto complementario $S^c$ definido por

$$S^c = \{r \in \mathbb{N} | r \notin S\}$$

es no vacío. Por el axioma del buen orden, $S^c$ tiene un menor elemento $m$. Por 1) el 1 pertenece a $S$, luego $m \neq 1$. Se sigue que $m-1$ pertenece a $\mathbb{N}$ y como $m$ es el mínimo de $S^c$, $m-1$ debe pertenecer a $S$. Poniendo $k = m-1$ en la condición 2), concluimos que $m$ esta en $S$, lo cual contradice el hecho de que $m$ pertenece a $S^c$.

De este modo, la suposición $S \neq \mathbb{N}$ nos lleva a un absurdo, y por lo tanto tenemos $S = \mathbb{N}$ y $P(n)$ es verdadera para todo $n \in \mathbb{N}$. □

En la notación del teorema anterior, *a)* es llamado el *caso base*, *b)* es llamado el *paso inductivo* y $P(k)$ es llamada la *hipótesis inductiva*. El paso inductivo consiste en probar que $P(k) \Rightarrow P(k+1)$ o, equivalentemente, podemos suponer $P(k)$ verdadera y a partir de ella probar $P(k+1)$.

El principio de inducción es útil para probar la veracidad de propiedades relativas a los números naturales. Por ejemplo, consideremos las siguientes propiedades $P(n)$, $Q(n)$ y $R(n)$:

*a)* $P(n)$ es la propiedad: si $0 < a$, entonces $0 < a^n$ para todo $n \in \mathbb{N}$.

*b)* $Q(n)$ es la afirmación: si $n$ es par entonces $n$ es divisible por 4,

*c)* $R(n)$ es la afirmación: $2n < n-1$.

Intuitivamente notamos que $P(n)$ es verdadera para cualquier $n$ natural, $Q(n)$ lo es para algunos valores de $n$ y es falsa para otros y $R(n)$ es falsa para todo valor de $n$. Sin embargo, para verificar realmente que la propiedad $P(n)$ es verdadera para todo $n$ natural no podemos hacerlo probando para cada $n$ en particular y entonces lo podemos probar por el principio de inducción.

*Ejemplo* (Serie aritmética). Probar que asi $n > 0$,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

*Solución.* Primero observemos que lo que debemos probar es equivalente a demostrar que

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

(*Caso base* $n = 1$) Debemos ver que $\sum_{i=1}^{1} i = \frac{1(1+1)}{2}$. Ahora bien, $\sum_{i=1}^{1} i = 1$ por definición de sumatoria y $\frac{1(1+1)}{2} = \frac{2}{2} = 1$, luego la igualdad se verifica.

(*Paso inductivo*) Supongamos que el resultado es verdadero para $n = k$, es decir que

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}, \tag{HI}$$

la hipótesis inductiva. Entonces debemos probar que

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}. \tag{1.4.1}$$

Partiremos del lado izquierdo de la igualdad (1.4.1) y obtendremos el lado derecho:

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \sum_{i=1}^{k} i + (k+1) && \text{(definición de sumatoria)} \\
&= \frac{k(k+1)}{2} + (k+1) && \text{(hipótesis inductiva)} \\
&= \frac{k(k+1) + 2(k+1)}{2} && \text{(común denominador)} \\
&= \frac{(k+1)(k+2)}{2} && \text{(factor común } k+1\text{).}
\end{aligned}$$

Luego hemos obtenido (1.4.1) y por el principio de inducción concluimos que el resultado es verdadero para todo $n \geqslant 1$. □

*Ejemplo.* Sea $a \in \mathbb{Z}$ tal que $0 < a$. Probemos que $0 < a^n$ para todo $n \in \mathbb{N}$.

*Solución.*

(*Caso base*) El resultado es verdadero cuando $n = 1$ pues $a^1 = a > 0$.

(*Paso inductivo*) Supongamos que el resultado verdadero cuando $n = k$, o sea, que la hipótesis inductiva es $0 < a^k$. Como $0 < a$, multiplicando por

$a$ ambos lados de la desigualdad obtenemos, por la compatibilidad de $<$ con el producto, que $a \cdot 0 < a^k \cdot a$, es decir $0 < a^{k+1}$. Luego el resultado es verdadero cuando $n = k+1$ y por el principio de inducción, es verdadero para todos los enteros positivos $n$. □

Existen varias formas modificadas del principio de inducción. A veces es conveniente tomar como base inductiva el valor $n = 0$, por otro lado puede ser apropiado tomar un valor como 2 o 3 porque los primeros casos pueden ser excepcionales. A veces, el caso base puede ser una secuencia de números enteros. Cada problema debe ser tratado según sus características. Otra modificación útil es tomar como hipótesis inductiva la suposición de que el resultado es verdadero para todos los valores $n \leqslant k$, más que para $n = k$ solamente. Esta formulación es llamada *el principio de inducción completa*. Todas esas modificaciones pueden justificarse con cambios triviales en la demostración del teorema 1.4.1

El siguiente teorema incorpora todas las modificaciones del principio de inducción mencionadas más arriba.

**Teorema 1.4.2** (Principio de inducción completa)**.** *Sean* $m_0 \leqslant n_0$ *números enteros y sea* $P(n)$ *una propiedad para* $n \geqslant m_0$ *tal que:*

*a)* $P(m_0), P(m_0+1), \ldots, P(n_0)$ *son verdaderas.*

*b) Si* $P(h)$ *verdadera para toda* $h$ *tal que* $m_0 \leqslant h \leqslant k$*, entonces* $P(k+1)$ *verdadera.*

*Entonces* $P(n)$ *es verdadera para todo* $n \geqslant m_0$*.*

*Demostración (*).* Sea $Q(n) = P(h)$ verdadera para toda $h$ tal que $m_0 \leqslant h \leqslant n$. A partir de aquí la demostración es completamente análoga a la del teorema 1.4.1.

Sea

$$S = \{n \in \mathbb{Z}_{\geqslant m_0} : Q(n)\}.$$

Entonces $S$ es un subconjunto de $\mathbb{Z}_{\geqslant m_0}$. Por *a)*, 1) $m_0 \in S$. Por *a)* y *b)*, 2) si $k \in S$ entonces $k+1 \in S$.

Si la conclusión es falsa, tenemos que $S \neq \mathbb{Z}_{\geqslant m_0}$ y entonces el conjunto complementario $S^c$ definido por

$$S^c = \{r \in \mathbb{Z}_{\geqslant m_0} | r \notin S\}$$

es no vacío. Por el axioma del buen orden, $S^c$ tiene un menor elemento $m$. Por 1) el entero $m_0$ pertenece a $S$, luego $m > m_0$. Se sigue que $m-1$ pertenece a $\mathbb{Z}_{\geqslant m_0}$ y como $m$ es el mínimo de $S^c$, $m-1$ debe pertenecer a $S$.

Poniendo $k = m - 1$ en la condición 2), concluimos que $m$ esta en $S$, lo cual contradice el hecho de que $m$ pertenece a $S^c$.

De este modo, la suposición $S \neq \mathbb{Z}_{\geqslant m_0}$ nos lleva a un absurdo, y por lo tanto tenemos $S = \mathbb{Z}_{\geqslant m_0}$ y $Q(n)$ es verdadera para todo $n \in \mathbb{Z}_{\geqslant m_0}$. □

Como en el principio de inducción, *a)* es llamado el *caso base* y *b)* el *paso inductivo*.

*Ejemplo.* Sean

$$u_1 = 3, \qquad u_2 = 5, \qquad u_n = 3u_{n-1} - 2u_{n-2}, \qquad n \geqslant 3.$$

Probemos que $u_n = 2^n + 1$, para todo $n \in \mathbb{N}$.

*Solución.* En este caso, el caso base es $n = 1$ y $n = 2$.

(*Caso base*) El resultado es verdadero cuando $n = 1$ pues $3 = 2^1 + 1$ y para $n = 2$ pues $5 = 2^2 + 1$.

(*Paso inductivo*) Sea $k \geqslant 2$ y supongamos que el resultado es cierto para los $h$ tales que $1 \leqslant h \leqslant k$. Es decir que $u_h = 2^h + 1$ para $1 \leqslant h \leqslant k$ (hipótesis inductiva), entonces

$$\begin{aligned} u_{k+1} &= 3u_k - 2u_{k-1} && \text{(por definición recursiva)} \\ &= 3(2^k + 1) - 2(2^{k-1} + 1) && \text{(por hipótesis inductiva)} \\ &= 3 \cdot 2^k + 3 - 2 \cdot 2^{k-1} - 2 \\ &= 3 \cdot 2^k + 1 - 2^k \\ &= 2 \cdot 2^k + 1 \\ &= 2^{k+1} + 1. \end{aligned}$$

□

*Ejemplo.* Sea $a \in \mathbb{Z}$ y $n \in \mathbb{N}$. Definimos $a^n$ de la siguiente manera:

$$a^1 = a, \qquad a^{n+1} = a^n \cdot a \qquad \text{para } n > 1. \tag{1.4.2}$$

Si $n, m \in \mathbb{N}$ verifiquemos las siguientes propiedades

*a)* $a^n \cdot a^m = a^{n+m}$.

*b)* $(a^n)^m = a^{nm}$

*Solución.* Veamos la afirmación *a)*. Se fijará $n$ y se hará inducción sobre $m$.

(*Caso base*) Debemos ver que $a^n \cdot a^1 = a^{n+1}$, lo cual es verdadero por la definición recursiva (1.4.2).

(*Paso inductivo*) Supongamos que el resultado es verdadero para $m = k$, es decir que $a^n \cdot a^k = a^{n+k}$ (hipótesis inductiva). Veamos que $a^n \cdot a^{k+1} = a^{n+k+1}$. Ahora bien,

$$\begin{aligned} a^n \cdot a^{k+1} &= a^n \cdot a^k \cdot a && \text{(definición (1.4.2))} \\ &= a^{n+k} \cdot a && \text{(hipótesis inductiva)} \\ &= a^{n+k+1} && \text{(definición (1.4.2)).} \end{aligned}$$

Probemos ahora *b)*. Al igual que antes, Se fijará $n$ y se hará inducción sobre $m$.

(*Caso base*) Debemos ver que $(a^n)^1 = a^n$, lo cual es verdadero por la definición recursiva (1.4.2).

(*Paso inductivo*) Supongamos que el resultado es verdadero para $m = k$, es decir que $(a^n)^k = a^{nk}$ (hipótesis inductiva). Veamos que $(a^n)^{k+1} = a^{n(k+1)}$.

$$\begin{aligned} (a^n)^{k+1} &= (a^n)^k \cdot a^n && \text{(definición (1.4.2))} \\ &= a^{nk} \cdot a^n && \text{(hipótesis inductiva)} \\ &= a^{nk+n} && \text{(por } a\text{)} \\ &= a^{n(k+1)}. \end{aligned}$$

□

*Ejemplo* (Serie geométrica). Sea $q$ número real positivo distinto de 1. Probar que si $n \geqslant 0$, entonces

$$\sum_{i=0}^{n} q^i = \frac{q^{n+1} - 1}{q - 1}.$$

*Solución.* Lo probaremos haciendo inducción sobre $n$.

(*Caso base* $n = 0$) Debemos ver que $\sum_{i=0}^{0} q^i = \frac{q^1 - 1}{q-1}$. Ahora bien, por definición de sumatoria $\sum_{i=0}^{0} q^i = q^0 = 1$ y como $\frac{q^1-1}{q-1} = \frac{q-1}{q-1} = 1$, la igualdad se verifica.

(*Paso inductivo*) Supongamos que el resultado es verdadero para $n = k$, es decir que

$$\sum_{i=0}^{k} q^i = \frac{q^{k+1} - 1}{q - 1}, \tag{HI}$$

la hipótesis inductiva. Entonces debemos probar que

$$\sum_{i=0}^{k+1} q^i = \frac{q^{k+2} - 1}{q - 1}. \tag{1.4.3}$$

Partiremos del lado izquierdo de la igualdad (1.4.3) y obtendremos el lado derecho:

$$\begin{aligned}
\sum_{i=0}^{k+1} q^i &= \sum_{i=0}^{k} q^i + q^{k+1} && \text{(definición de sumatoria)}\\
&== \frac{q^{k+1}-1}{q-1} + q^{k+1} && \text{(hipótesis inductiva)}\\
&= \frac{q^{k+1}-1+(q-1)q^{k+1}}{q-1} && \text{(común denominador } q-1\text{)}\\
&= \frac{q^{k+1}-1+q\cdot q^{k+1}-q^{k+1}}{q-1} && \text{(distributiva)}\\
&= \frac{q^{k+1}-1+q^{k+2}-q^{k+1}}{q-1}\\
&= \frac{q^{k+2}-1}{q-1}.
\end{aligned}$$

Luego hemos obtenido (1.4.3) y por el principio de inducción concluimos que el resultado es verdadero para todo $n \geqslant 0$. □

§ *Ejercicios*

1) Usar el principio de inducción para demostrar que

$$1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$$

para todos los enteros positivos $n$.

2) Hacer una tabla de valores de

$$S_n = 1^3 + 2^3 + \cdots + n^3$$

para $1 \leqslant n \leqslant 6$. Basándose en su tabla sugiera una fórmula para $S_n$. [Ayuda: los valores de $S_n$ son cuadrados perfectos.] Usar el principio de inducción para establecer que la fórmula es correcta para todo $n \geqslant 1$. (Si el método falla ¡su fórmula es equivocada!)

3) Probar que

$$1^4 + 2^4 + \cdots + n^4 = \frac{1}{30}n(n+1)(2n+1)(3n^2+3n-1).$$

4) Usar el principio de inducción para probar que $2^n > n+1$ para todo entero $n \geqslant 2$.

5) Encontrar el menor entero positivo $n_0$ para el cual sea verdadero que $n! \geqslant 2^n$. Tomando el caso $n = n_0$ como la base inductiva, demostrar que el resultado vale para $n \geqslant n_0$.

6) En los siguientes casos encontrar los valores apropiados de $n_0$ para la base inductiva y demostrar que la afirmación es verdadera para todos los $n \geqslant n_0$.

   *a)* $n^2 + 6n + 9 \geqslant 0$,

   *b)* $n^3 \geqslant 6n^2$.

# 2

# CONTEO

Intuitivamente, diremos que un conjunto $A$ es finito si podemos contar la cantidad de elementos que tiene. En ese caso denotaremos $|A|$ la cantidad de elementos de $A$ y la llamaremos el *cardinal de* $A$.

Formalmente, un conjunto $A$ es finito y tiene cardinal $n$ si existe una función $f : \{1, \ldots, n\} \to A$ biyectiva. Sin embargo, a lo largo del curso usaremos sólo la definición intuitiva y no formal de cardinal, más que suficiente para aprender los principios básicos de conteo.

## 2.1 PRINCIPIOS BÁSICOS DE CONTEO

### *El principio de adición*

Se puede realizar una acción $X$ de $n$ formas distintas o, alternativamente, se puede realizar otra acción $Y$ de $m$ formas distintas. Entonces el número de formas de realizar la acción "$X$ o $Y$" es $n + m$.

*Ejemplo* 2.1.1. Supongamos que una persona va a salir a pasear y puede ir al cine donde hay 3 películas en cartel o al teatro donde hay 4 obras posibles. Entonces, tendrá un total de $3 + 4 = 7$ formas distintas de elegir el paseo.

Este principio es el más básico del conteo y más formalmente dice que si $A$ y $B$ son conjuntos finitos disjuntos, entonces

$$|A \cup B| = |A| + |B|.$$

El principio es fácilmente generalizable a varios conjuntos.

**Proposición 2.1.2.** *Sean* $A_1, \ldots, A_n$ *conjuntos finitos tal que* $A_i \cap A_j = \emptyset$ *cuando* $i \neq j$, *entonces*

$$|A_1 \cup \cdots \cup A_n| = |A_1| + \cdots + |A_n|.$$

*Demostración.* La prueba se hace por inducción en $n$. Debemos probar

$$P(n) = \text{Si } A_1, \ldots, A_n \text{ conjuntos finitos disjuntos dos a dos, entonces } |A_1 \cup \cdots \cup A_n| = |A_1| + \cdots + |A_n|.$$

(*Caso base* $n = 1$) En este caso no hay nada que probar pues $|A_1| = |A_1|$.

(*Paso inductivo*) La hipótesis inductiva es $P(k)$ y debemos probar que $P(k) \Rightarrow P(k+1)$. Si denotamos $B = A_1 \cup \cdots \cup A_k$, entonces

$$A_1 \cup \cdots \cup A_{k+1} = B \cup A_{k+1}$$

Ahora bien, si $x \in B \cap A_{k+1}$, entonces $x \in A_i$ para algún $i < k+1$ y $x \in A_{k+1}$. Como $A_i \cap A_{k+1} = \emptyset$, se produce un absurdo que viene de suponer que existía un elemento en $B \cap A_{k+1}$. Luego $B \cap A_{k+1} = \emptyset$ y por el principio de adición $|B \cup A_{k+1}| = |B| + |A_{k+1}|$.

Por la hipótesis inductiva tenemos que

$$|B| = |A_1 \cup \cdots \cup A_k| = |A_1| + \cdots + |A_k|,$$

Luego

$$|A_1 \cup \cdots \cup A_k \cup A_{k+1}| = |B| + |A_{k+1}| = |A_1| + \cdots + |A_k| + |A_{k+1}|.$$

□

Si $A$ y $B$ no son disjuntos, cuando sumamos $|A|$ y $|B|$ estamos contando $A \cap B$ dos veces. Entonces, para obtener la respuesta correcta debemos restar $|A \cap B|$ y obtenemos

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Generalizar la fórmula de arriba a más conjuntos no es del todo sencillo y es el llamado principio del tamiz o principio de inclusión-exclusión (ver apéndice B).

*El principio de multiplicación*

Suponga que una actividad consiste de 2 etapas y la primera etapa puede ser realizada de $n_1$ maneras y la etapa 2 puede realizarse de $n_2$ maneras, independientemente de como se ha hecho la etapa 1. Entonces toda la actividad puede ser realizada de $n_1 \cdot n_2$ formas distintas.

*Ejemplo.* Supongamos que la persona del ejemplo 2.1.1 tiene suficiente tiempo y dinero para ir primero al cine y luego al teatro. Entonces tendrá $3 \cdot 4 = 12$ formas distintas de hacer el paseo.

Formalmente, si $A, B$ conjuntos y definimos el *producto cartesiano* entre $A$ y $B$ por

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

Entonces si $A$ y $B$ son conjuntos finitos se cumple que

$$|A \times B| = |A| \cdot |B|.$$

## 2.2 SELECCIONES ORDENADAS CON REPETICIÓN

Un aplicación inmediata del principio de multiplicación es que nos permite calcular la cantidad de selecciones ordenadas con repetición.

*Ejemplo.* Sea $X = \{1, 2, 3\}$ ¿de cuántas formas se pueden elegir dos de estos números en forma ordenada? Es decir, debemos elegir dos números $a$ y $b$ teniendo en cuenta que si $a \neq b$ no es lo mismo elegir $a$ y luego $b$ que $b$ y $a$.

Para no escribir demasiado vamos a adoptar una notación muy conveniente: si elegimos $a$ y $b$ en forma ordenada, denotamos $ab$. Entonces, en muy breve espacio seremos capaces de escribir todas las selecciones ordenadas de 2 elementos del conjunto $\{1, 2, 3\}$:

| | | |
|---|---|---|
| 11 | 12 | 13 |
| 21 | 22 | 23 |
| 31 | 32 | 33 |

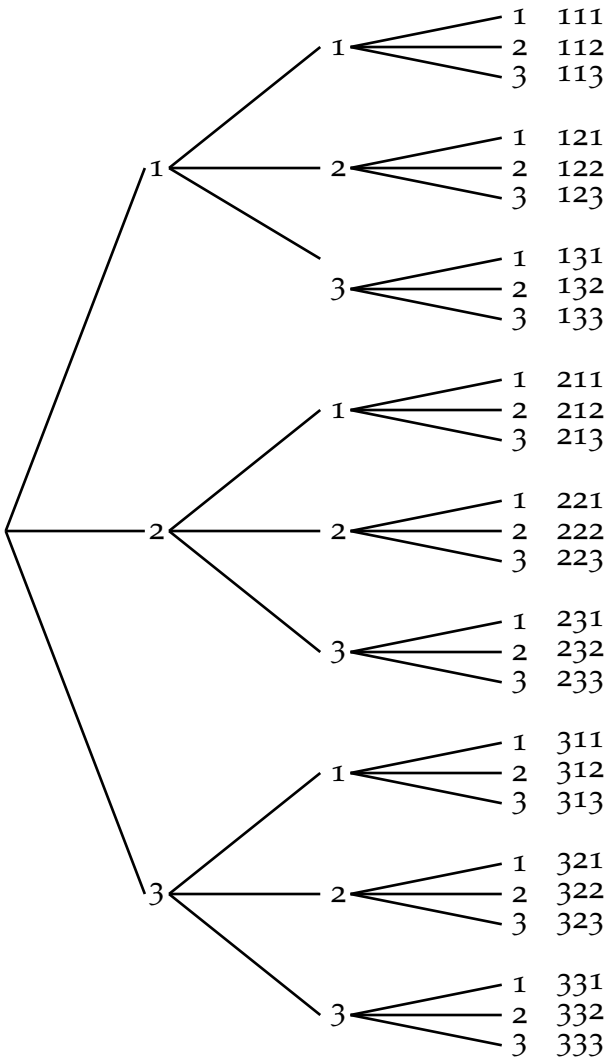
Son $9 = 3^2$ formas. ¿Cómo justificamos esto? Es claro que para la primera elección tenemos 3 valores posibles y para la segunda elección tenemos también 3 valores posibles, entonces, por el principio de multiplicación, tenemos en total $3 \cdot 3$ elecciones posibles.

Avancemos un poco más y ahora elijamos en forma ordenada 3 elementos de $[[1, 3]]$, es claro que estas elecciones son

| | | |
|---|---|---|
| 111 | 211 | 311 |
| 112 | 212 | 312 |
| 113 | 213 | 313 |
| 121 | 221 | 321 |
| 122 | 222 | 322 |
| 123 | 223 | 323 |
| 131 | 231 | 331 |
| 132 | 232 | 332 |
| 133 | 233 | 333. |

El total de elecciones posibles $27 = 3^3$. Esto se justifica usando dos veces el principio de multiplicación: para la primera elección tenemos 3 valores posibles. Para la segunda elección tenemos también 3 valores posibles, entonces, por el principio de multiplicación, tenemos en total $3 \cdot 3$ valores posibles para la elección de los dos primeros números. Como para la tercera elección tenemos 3 valores posibles, por el principio de multiplicación nuevamente, tenemos $3 \cdot 3 \cdot 3$ elecciones posibles.

Un diagrama arbolado ayuda a pensar.




Cada rama del árbol representa una selección ordenada de elementos de $\{1, 2, 3\}$.

El razonamiento anterior se puede extender:

**Proposición 2.2.1.** *Sean* $m, n \in \mathbb{N}$. *Hay* $n^m$ *formas posibles de elegir ordenadamente* $m$ *elementos de un conjunto de* $n$ *elementos.*

*Idea de la prueba.* La prueba de esta proposición se basa en aplicar el principio de multiplicación $m - 1$ veces, es decir debemos hacer inducción sobre $m$ y usar el principio de multiplicación en el paso inductivo. □

*Ejemplo.* ¿Cuántos números de cuatro dígitos pueden formarse con los dígitos $1, 2, 3, 4, 5, 6$?

Por la proposición anterior es claro que hay $6^4$ números posibles.

*Ejemplo.* ¿Cuántos números de 5 dígitos y capicúas pueden formarse con los números dígitos $1, 2, 3, 4, 5, 6, 7, 8$? Un número capicúa de cinco dígitos es de la forma

$$xyzyx$$

Se reduce a ver cuántos números de tres dígitos pueden formarse con aquéllos dígitos. Exactamente $8^3$.

*Ejemplo.* Sea $X$ un conjunto de $m$ elementos. Queremos contar cuántos subconjuntos tiene este conjunto. Por ejemplo, si $X = \{a, b, c\}$ los subconjuntos de $X$ son exactamente

$$\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}.$$

Es decir que existen 8 subconjuntos de $X$, un conjunto de 3 elementos. ¿Cómo podemos encontrar razonando este número? Un forma sería la siguiente: cuando elijo un subconjunto el $a$ puede estar o no estar en el subconjunto, es decir hay dos posibilidades. Con el $b$ pasa lo mismo, puede estar o no estar y por lo tanto hay 2 posibilidades. Con el $c$ se hace un razonamiento análogo y por lo tanto tenemos que hay en total

$$2 \cdot 2 \cdot 2 = 2^3 = 8$$

posibles subconjuntos de $X$.

Otra forma de verlo: podemos identificar cada subconjunto de $X$ con una terna ordenada de 0's y 1's de la siguiente manera: si $a$ está en el subconjunto la primera coordenada de la terna es 1, si no es 0; si $b$ está en el subconjunto la segunda coordenada de la terna es 1, si no es 0; si $c$ está en el subconjunto la tercera coordenada de la terna es 1, si no es 0. Es decir tenemos la identificación

$$\begin{array}{lcl}
\emptyset & \leftrightarrow & 000 \\
\{a\} & \leftrightarrow & 100 \\
\{b\} & \leftrightarrow & 010 \\
\{c\} & \leftrightarrow & 001 \\
\{a, b\} & \leftrightarrow & 110 \\
\{a, c\} & \leftrightarrow & 101 \\
\{b, c\} & \leftrightarrow & 011 \\
\{a, b, c\} & \leftrightarrow & 111.
\end{array}$$

Observar entonces que seleccionar un subconjunto de $X$ es equivalente a elegir en forma ordenada 3 elementos del conjunto $\{0, 1\}$; y sabemos entonces que en ese caso tenemos $2^3$ posibilidades.

En general, cuando X tiene $n$ elementos, elegir un subconjunto de X es equivalente a elegir en forma ordenada $n$ elementos del conjunto $\{0,1\}$ y por lo tanto

*Proposición* 2.2.2. *La cantidad de subconjuntos de un conjunto de* $n$ *elementos es* $2^n$.

Dado X un conjunto, denotamos $\mathcal{P}(X)$ el conjunto formado por todos los subconjuntos de X, por ejemplo

$$\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}.$$

Si X es un conjunto finito la proposición 2.2.2 nos dice que

$$|\mathcal{P}(X)| = 2^{|X|}$$

## 2.3 SELECCIONES ORDENADAS SIN REPETICIÓN

Sea $n \in \mathbb{N}$. Recordemos que definimos recursivamente *factorial de* $n$ al número denotado

$$n!,$$

tal que

$$1! = 1$$
$$(n+1)! = n!(n+1)$$

Definimos también

$$0! = 1$$

Por ejemplo

$$2! = 2 \cdot 1 = 2$$
$$3! = 3 \cdot 2 \cdot 1 = 6$$
$$4! = 3! \cdot 4 = 6 \cdot 4 = 24.$$

Si $n \in \mathbb{N}$, denotaremos $[[1,n]]$ al conjunto de los primeros $n$ números naturales. Es decir:

$$[[1,n]] = \{1, 2, \ldots, n\}.$$

Ahora estudiaremos las selecciones ordenadas de $m$ elementos entre $n$ donde *no* se permite la repetición. Es decir si el conjunto es $A = \{a_1, a_2, \ldots, a_n\}$, las selecciones deben ser del tipo

$$a_{i_1} a_{i_2} \cdots a_{i_m}$$

donde $a_{i_j} \neq a_{i_k}$ si $i \neq k$.

Por ejemplo, las selecciones de 3 elementos en forma ordenada y sin repetición de $[[1,3]]$ son exactamente

$$123,\ 132,\ 213,\ 231,\ 312,\ 321$$

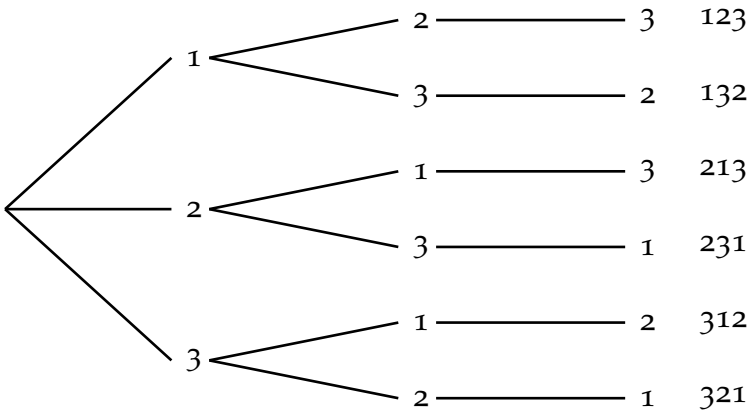
(son las ternas donde los tres números son distintos). O sea hay 6 selecciones ordenadas y sin repetición de elementos de $[[1,3]]$.

Notemos que

$$3 \cdot 2 \cdot 1 = 6 = 3!$$

Esta forma de escribir nos da la razón de que haya 6 selecciones ordenadas y sin repetición de elementos de $[[1,3]]$: para la elección del primer elemento tenemos 3 posibilidades (el 1, 2 o 3). Cuando elegimos el segundo elemento, si queremos que no haya repetición, debemos excluir el valor elegido en primer lugar, o sea que tenemos solo 2 elecciones. Análogamente para la tercera elección solo hay solo una posibilidad, pues debemos descartar los valores elegidos en el primer y segundo lugar. Tenemos entonces $3 \cdot 2 \cdot 1$ selecciones posibles.

En un diagrama arbolado la selección se puede representar de la siguiente forma:




El número total es entonces $3 \cdot 2 \cdot 1 = 6$.

Pensemos ahora que queremos elegir en forma ordenada y sin repetición 3 elementos entre 5. Entonces para la primera elección tenemos 5 posibilidades, para la segunda 4 posibilidades y para la tercera 3 posibilidades haciendo un total de

$$5 \cdot 4 \cdot 3$$

selecciones posibles.

**Proposición 2.3.1** (Principio de las casillas)**.** *Si* $n < m$*, no hay ninguna selección ordenada y sin repetición de* $m$ *elementos de un conjunto de* $n$ *elementos.*

El principio de las casillas, también llamado *principio del palomar* o *principio de Dirichlet*, es intuitivamente trivial: si hay más personas que asientos, ¡alguien se quedará parado!. Su demostración no es difícil y se basa en la definición formal de conteo, con el uso de funciones biyectivas e inyectivas.

**Proposición 2.3.2.** *Si* $n \geqslant m$ *entonces existen*

$$n \cdot (n-1) \cdots (n-(m-1)), \qquad m \text{ - factores}$$

*selecciones ordenadas y sin repetición de* $m$ *elementos de un conjunto de* $n$ *elementos.*

*Demostración.* La prueba es una generalización del razonamiento aplicado más arriba en los ejemplos: debemos seleccionar $m$-veces elementos de un conjunto que tiene $n$ elementos. La primera selección puede ser de cualquiera de los $n$ objetos; la segunda selección debe recaer en uno de los $n-1$ elementos restantes. De manera similar, hay $n-2$ posibilidades para la tercera selección, y así sucesivamente. Cuando hacemos la $m$-ésima selección, $m-1$ elementos ya han sido seleccionados, y entonces el elemento seleccionado debe ser uno de los $n-(m-1)$ elementos restantes. Por consiguiente el número total de selecciones es el propuesto. □

*Observación.* El resultado anterior en particular nos dice que existen

$$n \cdot (n-1) \cdots (n-(n-1)) = n \cdot (n-1) \cdots 1 = n!$$

selecciones ordenadas y sin repetición de $n$ elementos en un conjunto con $n$ elementos y esta podría ser una motivación natural del factorial.

Las selecciones ordenadas y sin repetición de $n$ elementos en un conjunto con $n$ elementos se denominan *permutaciones* de grado $n$. Hay, pues, $n!$ permutaciones de grado $n$.

Volviendo al resultado de la proposición 2.3.2, por ejemplo hay

- $7 \cdot 6 \cdot 5$ selecciones ordenadas y sin repetición de 3 elementos de $[[1,7]]$,
- $7 \cdot 6 \cdot 5 \cdot 4 \cdot 3$ selecciones ordenadas y sin repetición de 5 elementos de $[[1,7]]$ y
- $7!$ selecciones ordenadas y sin repetición de todos los elementos de $[[1,7]]$.

Notemos que si $n \geqslant m$ entonces

$$n \cdot (n-1) \cdots (n-(m-1)) = \frac{n!}{(n-m)!}$$

pues

$$n! = n \cdot (n-1) \cdots (n-(m-1)) \cdot (n-m)!$$

Por lo tanto la proposición 2.3.2 se puede reescribir de la siguiente manera:

**Proposición 2.3.3.** *Si* $n \geqslant m$ *entonces existen*

$$\frac{n!}{(n-m)!}$$

*selecciones ordenadas y sin repetición de* $m$ *elementos de un conjunto de* $n$ *elementos.*

*Ejemplo.* Si en un colectivo hay 10 asientos vacíos. ¿De cuántas formas pueden sentarse 7 personas? Se trata de ver cuantas selecciones ordenadas y sin repetición de 7 asientos entre 10.

Este número es

$$10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4, \qquad 7 \text{ - factores.}$$

*Ejemplo.* ¿Cuántas permutaciones pueden formarse con las letras de *silvia*?

Afirmamos que se pueden formar $\frac{6!}{2!}$ palabras usando las letras de *silvia*.

Si escribo en lugar de *silvia*,

$$s\ i\ l\ v\ i'\ a$$

Es decir si cambio la segunda $i$ por $i'$, todas las letras son distintas, luego hay 6! permutaciones, pero cada par de permutaciones del tipo

$$\cdots i \cdots i' \cdots$$
$$\cdots i' \cdots i \cdots$$

coinciden, por lo tanto tengo que dividir por 2 el número total de permutaciones.

Tomemos la palabra

*ramanathan*

el número total de permutaciones es $\frac{10!}{4!2!}$.

En efecto, escribiendo el nombre anterior así

$$r\ a_1\ m\ a_2\ n_1\ a_3\ t\ h\ a_4\ n_1$$

el número total de permutaciones es 10! Pero permutando las $a_i$ y las $n_i$ sin mover las otras letras obtenemos la misma permutación de *ramanathan*.

Como hay 4! permutaciones de las letras $a_1$, $a_2$, $a_3$, $a_4$, y 2! de $n_1$, $n_2$ el número buscado es

$$\frac{10!}{4!2!}.$$

Dejamos a cargo del lector probar que el número total de permutaciones de las letras de *arrivederci* es

$$\frac{11!}{3!2!2!}$$

§ *Ejercicios*

1) Simplificar las siguientes expresiones, sea $n \in \mathbb{N}$

   *a)* $\dfrac{n!}{(n-2)!}$, si $n \geqslant 2$.

   *b)* $\dfrac{(n+2)!}{(n-2)!}$, si $n \geqslant 2$.

   *c)* $\dfrac{n!}{(n-2)!2!}$, si $n \geqslant 2$.

   *d)* $\dfrac{(n+2)!}{n!}$.

   *e)* $\dfrac{(n-1)!}{(n+2)!}$.

2) En este ejercicio decimos que una *palabra* es una sucesión de letras (tenga sentido o no).

   *a)* ¿Cuántas palabras de 4 letras o menos se pueden hacer con un alfabeto de 26 letras?

   *b)* ¿De cuántas formas pueden ordenarse las letras de la palabra PREPOTENTE?

## 2.4 SELECCIONES SIN ORDEN

Consideremos un conjunto $X$ finito de $n$ elementos. Nos proponemos averiguar cuántos subconjuntos de $m$ elementos hay en $X$.

*Ejemplo.* Por ejemplo, sea $X = \{1, 2, 3, 4, 5\}$ y nos interesan los subconjuntos de tres elementos. ¿Cuántos habrá? Una forma de individualizar un subconjunto de tres elementos en $X$, consiste en, primero, seleccionar ordenadamente 3 elementos de $[[1, 5]]$.

Habría, a priori, $5 \cdot 4 \cdot 3$ subconjuntos pues ese es el número de selecciones ordenadas y sin repetición de 3 elementos de $[[1, 5]]$.

Pero es claro que algunas de las selecciones ordenadas pueden determinar el mismo subconjunto. En efecto, por ejemplo, cualesquiera de las selecciones

$$123, \qquad 132, \qquad 213, \qquad 231, \qquad 312, \qquad 321$$

determina el subconjunto $\{1,2,3\}$ . Es decir las permutaciones de $\{1,2,3\}$ determinan el mismo subconjunto. Y así con cualquier otro subconjunto de tres elementos. Por lo tanto, el número total de subconjuntos de 3 elementos debe ser

$$\frac{5\cdot 4\cdot 3}{3!} = \frac{5!}{3!(5-3)!}$$

En el caso general de subconjuntos de $m$ elementos de un conjunto de $n$ elementos ($m \leqslant n$) podemos razonar en forma análoga. Cada subconjunto de $m$ elementos está determinado por una selección ordenada y todas las permutaciones de esta selección.

Por lo tanto el número total de subconjunto de $m$ elementos de $X$ es

$$\frac{n\cdot(n-1)\cdots(n-(m-1))}{m!} = \frac{n!}{(n-m)!\ m!}$$

**Definición 2.4.1.** Sean $n, m \in \mathbb{N}_0$, $m \leqslant n$. Definimos

$$\binom{n}{m} = \frac{n!}{(n-m)!\ m!}$$

y por razones que se verán más adelante se denomina el *coeficiente binomial* o *número combinatorio* asociado al par $n$, $m$ con $m \leqslant n$.

Definimos también

$$\binom{n}{m} = 0, \qquad \text{si } m > n.$$

*Observación.* Hay unos pocos números combinatorios que son fácilmente calculables:

$$\binom{n}{0} = \binom{0}{0} = 1 \qquad \text{y} \qquad \binom{n}{1} = \binom{n}{n-1} = n.$$

Estos resultados se obtienen por aplicación directa de la definición (recordar que $0! = 1$).

Concluyendo, el razonamiento de la página 35 se puede resumir en la siguiente proposición.

**Proposición 2.4.2.** *Sean $n, m \in \mathbb{N}_0$, $m \leqslant n$, y supongamos que el conjunto $X$ tiene $n$ elementos.*

*Entonces, la cantidad de subconjuntos de $X$ con $m$ elementos es $\binom{n}{m}$.*

Como vimos anteriormente el número combinatorio suele resultar de utilidad para resolver problemas de conteo. Veamos un ejemplo.

*Ejemplo.* ¿Cuántos comités pueden formarse de un conjunto de 6 mujeres y 4 hombres, si el comité debe estar compuesto por 4 mujeres y 2 hombres?

*Solución.* Debemos elegir 4 mujeres entre 6, y la cantidad de elecciones posibles es $\binom{6}{4}$. Por otro lado, hay $\binom{4}{2}$ formas de elegir 2 hombres entre 4. Luego, por el principio de multiplicación, el resultado es

$$\binom{6}{3} \cdot \binom{4}{2} = \frac{6!}{2!4!} \cdot \frac{4!}{2!2!} = \frac{6 \cdot 5}{2} \cdot \frac{4 \cdot 3}{2} = 15 \cdot 6 = 90.$$

□

**Proposición 2.4.3** (Simetría del número combinatorio)**.** *Sean* $m, n \in \mathbb{N}_0$*, tal que* $m \leqslant n$*. Entonces*

$$\binom{n}{m} = \binom{n}{n-m}.$$

*Demostración.*

$$\binom{n}{n-m} = \frac{n!}{(n-(n-m))!\,(n-m)!} = \frac{n!}{m!\,(n-m)!} = \frac{n!}{(n-m)!\,m!} = \binom{n}{m}.$$

□

*Observación.* El hecho de que

$$\binom{n}{m} = \binom{n}{n-m}.$$

se puede interpretar en términos de subconjuntos: $\binom{n}{m}$ es el número de subconjuntos de $m$ elementos de un conjunto de $n$ elementos. Puesto que con cada subconjunto de $m$ elementos hay unívocamente asociado un subconjunto de $n-m$ elementos, su complemento en $X$, es claro que $\binom{n}{m} = \binom{n}{n-m}$.

**Teorema 2.4.4** (Fórmula del triángulo de Pascal)**.** *Sean* $m, n \in \mathbb{N}$*, tal que* $m \leqslant n$*. Entonces*

$$\binom{n+1}{m} = \binom{n}{m-1} + \binom{n}{m}$$

*Demostración.* El enunciado nos dice que debemos demostrar que

$$\frac{(n+1)!}{(n-m+1)!\,m!} = \frac{n!}{(n-m+1)!\,(m-1)!} + \frac{n!}{(n-m)!\,m!}$$

Hay varias forma de operar algebraicamente las expresiones y obtener el resultado. Nosotros partiremos de la expresión de la derecha y obtendremos la de la izquierda:

$$\begin{aligned}
\frac{n!}{(n-m+1)!\,(m-1)!} + \frac{n!}{(n-m)!\,m!} &= \\
&= \frac{n!}{(n-m)!\,(m-1)!}\left(\frac{1}{(n-m+1)} + \frac{1}{m}\right) \\
&= \frac{n!}{(n-m)!\,(m-1)!}\left(\frac{m+n-m+1}{(n-m+1)m}\right) \\
&= \frac{n!}{(n-m)!\,(m-1)!}\left(\frac{n+1}{(n-m+1)m}\right) \\
&= \frac{n!(n+1)}{(n-m)!(n-m+1)\,(m-1)!\,m} \\
&= \frac{(n+1)!}{(n-m+1)!\,m!}.
\end{aligned}$$

□

Aunque por razones de conteo es obvio que los números combinatorios son números naturales, esto no es claro por la definición formal.

**Corolario 2.4.5.** *Si* $n \in \mathbb{N}$ *y* $0 \leqslant m \leqslant n$ *entonces* $\binom{n}{m} \in \mathbb{N}$.

*Demostración.* Haremos inducción en $n$. Si $n = 1$ los posibles números combinatorios son

$$\binom{1}{1} = \binom{1}{0} = 1 \in \mathbb{N}.$$

Ahora supongamos que el resultado sea cierto para $n \in \mathbb{N}$. Es decir, $\binom{n}{m} \in \mathbb{N}$ cualquiera sea $m$ tal que $0 \leqslant m \leqslant n$ (hipótesis inductiva).

Probaremos entonces que

$$\binom{n+1}{m} \in \mathbb{N}$$

para todo $m \in \mathbb{N}$ tal que $0 \leqslant m \leqslant n+1$.

Consideremos tres casos: $m = 0$, $1 \leqslant m \leqslant n$ y $m = n+1$.

Si $m = 0$, entonces

$$\binom{n+1}{m} = \binom{n+1}{0} = 1 \in \mathbb{N}.$$

Si $1 \leqslant m \leqslant n$, entonces por el teorema anterior (en la segunda parte)

$$\binom{n+1}{m} = \binom{n}{m-1} + \binom{n}{m}$$

Como $\binom{n}{m-1}$ y $\binom{n}{m}$ pertenecen a $\mathbb{N}$ por la hipótesis inductiva, su suma es también un número natural, o sea

$$\binom{n+1}{m} \in \mathbb{N}$$

para $1 \leqslant m \leqslant n$.

Si $m = n+1$, entonces

$$\binom{n+1}{n+1} = 1 \in \mathbb{N}.$$

Por lo anterior, se concluye que

$$\binom{n+1}{m} \in \mathbb{N}$$

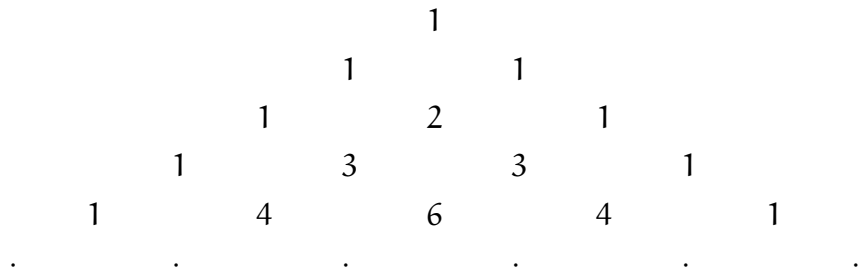
cualquiera sea $m$ , $0 \leqslant m \leqslant n+1$.

Por lo tanto, es válido el paso inductivo y así nuestra afirmación queda probada. □

El teorema precedente permite calcular los coeficientes binomiales inductivamente. Escribamos en forma de triángulo

$$\begin{array}{ccccccccccc}
 & & & & \binom{0}{0} & & & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & \\
. & & . & & . & & . & & . & & .
\end{array}$$

En virtud del teorema 2.4.4 cada término interior es suma de los dos términos inmediatos superiores. Los elementos en los lados valen 1 por lo tanto se puede calcular cualquiera de ellos.




(Lector: calcule el valor de la suma total de cada fila del triángulo.)

El triángulo es denominado *triángulo de Pascal*. Entre las propiedades que cuenta el triángulo de Pascal está la de ser simétrico respecto de su altura, como consecuencia de la simetría de los números combinatorios (ver proposición 2.4.3).

## 2.5 EL TEOREMA DEL BINOMIO

En álgebra elemental aprendemos las formulas

$$(a+b)^2 = a^2 + 2ab + b^2, \qquad (a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3,$$

y a veces nos piden desarrollar la formula para $(a+b)^4$ y potencias mayores de $a+b$. El resultado general que da una formula para $(a+b)^n$ es conocido como el *teorema del binomio*.

**Teorema 2.5.1.** *Sea $n$ un entero positivo. El coeficiente del termino $a^{n-r}b^r$ en el desarrollo de $(a+b)^n$ es el número binomial $\binom{n}{r}$. Explícitamente,*

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n}b^n,$$

*o, escrito en forma más concisa,*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i}b^i. \tag{2.5.1}$$

*Demostración.* (Primera) Consideremos que ocurre cuando multiplicamos $n$ factores: $(a+b)(a+b)\cdots(a+b)$.

Un término en el producto se obtiene seleccionando o bien $a$ o bien $b$ de cada factor. El número de términos $a^{n-r}b^r$ es solo el número de formas de

seleccionar $r$ b's (y consecuentemente $n-r$ a's), y por definición éste es el número binomial $\binom{n}{r}$. □

*Observación* 2.5.2. Antes de hacer una segunda demostración del teorema del binomio veamos el siguiente resultado que nos resultará útil: sea $a_k, a_{k+1}, \ldots, a_{m-1}, a_m$ una sucesión de números reales ($k \leqslant m$) y sea $r \in \mathbb{N}_0$. Entonces

$$\sum_{i=k}^{m} a_i = \sum_{i=r}^{m-k+r} a_{i+k-r}.$$

La sumatoria de la derecha es la de la izquierda con un "cambio de variable" en el índice. La demostración de este hecho se puede hacer por inducción sobre $m$ (caso base $m = k$) o simplemente escribiendo ambas sumatorias con la notación de puntos suspensivos y verificando que ambas son iguales a

$$a_k + a_{k+1} + \cdots + a_{m-1} + a_m.$$

*Observación.* Por la simetría del número binomial la fórmula (2.5.1) es equivalente a

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{n-i} a^{n-i} b^i.$$

Haciendo el cambio de variable $i \leftrightarrow n-i$, se obtiene la fórmula equivalente

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

La fórmula anterior es también, muy utilizada para enunciar el teorema del binomio.

*Demostración (*).* (Segunda) Se hace por inducción en $n$. Si $n = 1$, el resultado es trivial. Supongamos que el resultado es cierto para $n-1$, es decir, de acuerdo a la fórmula (2.5.1),

$$(a+b)^{n-1} = \sum_{i=0}^{n-1} \binom{n-1}{i} a^{n-1-i} b^i.$$

Luego

$$\begin{aligned}
(a+b)^n &= (a+b)(a+b)^{n-1} \\
&= (a+b)\left(\sum_{i=0}^{n-1}\binom{n-1}{i}a^{n-1-i}b^i\right) && \text{(hip. ind.)} \\
&= \sum_{i=0}^{n-1}\binom{n-1}{i}a^{n-i}b^i + \sum_{i=0}^{n-1}\binom{n-1}{i}a^{n-1-i}b^{i+1} && \text{(distributiva)} \\
&= \sum_{i=0}^{n-1}\binom{n-1}{i}a^{n-i}b^i + \sum_{i=1}^{n}\binom{n-1}{i-1}a^{n-i}b^i && \text{( obs. 2.5.2)} \\
&= a^n + \sum_{i=1}^{n-1}\left\{\binom{n-1}{i} + \binom{n-1}{i-1}\right\}a^{n-i}b^i + b^n \\
&= a^n + \sum_{i=1}^{n-1}\binom{n}{i}a^{n-i}b^i + b^n && \text{(teor. 2.4.4)} \\
&= \sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^i.
\end{aligned}$$

□

Los coeficientes en el desarrollo pueden ser calculados con el método recursivo usado para los números binomiales (triángulo de Pascal) o usando la formula. Por ejemplo,

$$\begin{aligned}
(a+b)^6 = &\binom{6}{0}a^6 + \binom{6}{1}a^5b + \binom{6}{2}a^4b^2 + \binom{6}{3}a^3b^3 \\
&+ \binom{6}{4}a^2b^4 + \binom{6}{5}ab^5\binom{6}{6}b^6 \\
&= a^6 + 6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 + b^6.
\end{aligned}$$

Por supuesto, podemos obtener otras formulas útiles si reemplazamos $a$ y $b$ por otras expresiones. Algunos ejemplos típicos son:

$$\begin{aligned}
(1+x)^4 &= 1 + 4x + 6x^2 + 4x^3 + x^4; \\
(1-x)^7 &= 1 - 7x + 21x^2 - 35x^3 + 35x^4 - 21x^5 + 7x^6 - x^7; \\
(x+2y)^5 &= x^5 + 10x^4y + 40x^3y^2 + 80x^2y^3 + 80xy^4 + 32y^5; \\
(x^2+y)^4 &= x^8 + 4x^3y + 6x^4y^2 + 4x^2y^3 + y^4.
\end{aligned}$$

La expresión $a+b$ es conocida como un expresión *binómica* porque tiene dos términos. Como los números $\binom{n}{r}$ aparecen como los coeficientes en el desarrollo de $(a+b)^n$, generalmente se los llama, como ya fue dicho,

coeficientes binomiales. De todos modos esta claro por la primera prueba del teorema 2.5.1 que estos números aparecen en este contexto porque representan el número de formas de hacer ciertas selecciones. Por esta razón continuaremos usando el nombre de números binomiales, que se aproxima más al concepto que simbolizan.

Además de ser extremadamente útil en manipulaciones algebraicas, el teorema del binomio puede usarse para deducir identidades en que estén involucrados los números binomiales.

*Ejemplo.* Probemos que

$$\sum_{i=0}^{n} \binom{n}{i} = \binom{n}{0} + \binom{n}{1} + \binom{n}{3} + \cdots + \binom{n}{n} = 2^n.$$

*Demostración.* Observar que $1 + 1 = 2$, luego, por el teorema del binomio,

$$\begin{aligned} 2^n = (1+1)^n &= \sum_{i=0}^{n} \binom{n}{i} 1^{n-i} 1^i \\ &= \sum_{i=0}^{n} \binom{n}{i} 1 \cdot 1 \\ &= \sum_{i=0}^{n} \binom{n}{i}. \end{aligned}$$

□

*Ejemplo.* Probemos que

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{3}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n}. \tag{2.5.2}$$

*Demostración.* Usamos la igualdad

$$(1+x)^n (1+x)^n = (1+x)^{2n}.$$

El resultado se demostrará encontrando el coeficiente del termino $x^n$ de ambos términos de esta igualdad.

De acuerdo con el teorema del binomio el miembro izquierdo es el producto de dos factores, ambos iguales a

$$\binom{n}{0} 1 + \binom{n}{1} x + \cdots + \binom{n}{r} x^r + \cdots + \binom{n}{n} x^n.$$

Cuando los dos factores se multiplican, un termino en $x^n$ se obtiene tomando un termino del primer factor de tipo $x^i$ y un termino del segundo factor de tipo $x^{n-i}$. Por lo tanto los coeficientes de $x^n$ en el producto son

$$\binom{n}{0}\binom{n}{n} + \binom{n}{1}\binom{n}{n-1} + \binom{n}{2}\binom{n}{n-2} + \cdots + \binom{n}{n}\binom{n}{0}. \tag{2.5.3}$$

Como $\binom{n}{n-r} = \binom{n}{r}$, vemos que (2.5.3) es el lado izquierdo de la igualdad (2.5.2). Pero el lado derecho es $\binom{2n}{n}$ que es también el coeficiente de $x^n$ en el desarrollo de $(1+x)^{2n}$, y entonces obtenemos la igualdad que buscábamos. □

*Observación* (Definición de $0^0$). No hay consenso matemático en cual es el valor de $0^0$, pues dependiendo del contexto puede ser conveniente definir su valor de cierta forma o declarar su valor como *indeterminado* (ver el artículo de Wikipedia Cero a la cero).

Sin embargo, para su uso en álgebra, así como en combinatoria se considera conveniente definir $0^0 = 1$. ¿Cuál es la razón para darle este valor? Existen varias razones, pero una de las más importantes proviene del teorema del binomio. Observemos que por el teorema del binomio

$$(1+0)^n = \sum_{i=0}^{n} \binom{n}{i} 1^{n-1} 0^i = \sum_{i=0}^{n} \binom{n}{i} 0^i.$$

Es claro que para $i > 0$, $0^i = 0 \cdot \ldots \cdot 0 = 0$, luego la ecuación se reduce a

$$1 = 1^n = 0^0.$$

No sería muy convincente enunciar el teorema del binomio con algunas excepciones poco naturales (como ser, exigir que $a$ y $b$ sean no nulos) y la formulación más general parece ser la correcta. Esta formulación exige que $0^0 = 1$, como hemos visto más arriba.

Una fundamentación extensa y rigurosa sobre la conveniencia de definir $0^0 = 1$ puede leerse en el artículo de D. Knuth *Two notes on notation* que se encuentra en https://arxiv.org/abs/math/9205211.

§ *Ejercicios*

1) Desarrollar las fórmulas de $(1+x)^8$ y $(1-x)^8$.

2) Calcular los coeficientes de:

   *a)* $x^5$ en $(1+x)^{11}$; *b)* $a^2b^8$ en $(a+b)^{10}$;

   *c)* $a^6b^6$ en $(a^2+b^3)^5$; *d)* $x^3$ en $(3+4x)^6$.

3) Usar la identidad $(1+x)^m(1+x)^n = (1+x)^{m+n}$ para probar que

$$\binom{m+n}{r} = \binom{m}{0}\binom{n}{r} + \binom{m}{1}\binom{n}{r-1} + \cdots \binom{m}{r}\binom{n}{0}$$

donde $m, n$ y $r$ son enteros positivos y, $m \geqslant r$, y $n \geqslant r$.

# 3

# DIVISIBILIDAD

## 3.1 COCIENTE Y RESTO

Cuando somos chicos aprendemos que 6 "cabe" cuatro veces en 27 y el resto es 3, o sea

$$27 = 6 \cdot 4 + 3.$$

Un punto importante es que el resto debe ser menor que 6. Aunque, también es verdadero que, por ejemplo

$$27 = 6 \cdot 3 + 9,$$

debemos tomar el menor valor para el resto, de forma que "lo que queda" sea un número no negativo lo más chico posible. El hecho de que el conjunto de posibles "restos" tenga un mínimo es una consecuencia del axioma del buen orden.

**Teorema 3.1.1.** *Sean* $a$ *y* $b$ *números enteros cualesquiera con* $b \in \mathbb{N}$*, entonces existen enteros únicos* $q$ *y* $r$ *tales que*

$$a = b \cdot q + r \qquad y \qquad 0 \leqslant r < b.$$

*Demostración.* Debemos aplicar el axioma del buen orden al conjunto de los "restos"

$$R = \{x \in \mathbb{N}_0 | a = by + x \text{ para algún } y \in \mathbb{Z}\}.$$

Primero demostraremos que $R$ no es vacío. Si $a \geqslant 0$ la igualdad

$$a = b \cdot 0 + a$$

demuestra que $a \in R$, mientras que si $a < 0$ la igualdad

$$a = b \cdot a + (1 - b) \cdot a$$

demuestra que $(1 - b) \cdot a \in R$ (en ambos casos es necesario controlar que el elemento es no negativo.)

Ahora, como $R$ es un subconjunto no vacío de $\mathbb{N}_0$, tiene un mínimo $r$, y como $r$ esta en $R$ se sigue que $a = bq + r$ para algún $q$ en $\mathbb{Z}$. Además

$$a = bq + r \Rightarrow a = b(q + 1) + (r - b)$$

de manera que si $r \geqslant b$ entonces $r - b$ esta en R. Pero $r - b$ es menor que r, contradiciendo la definición de r como el menor elemento de R. Como la suposición $r \geqslant b$ nos lleva a una contradicción, solo puede ocurrir que $r < b$, como queríamos demostrar.

Es fácil ver que el cociente q y el resto r obtenidos en el teorema son únicos. Supongamos que $q'$ y $r'$, también satisfacen las condiciones, esto es

$$a = bq' + r' \qquad \text{y} \qquad 0 \leqslant r' < b.$$

Si $q > q'$, entonces $q - q' \geqslant 1$ y tenemos que

$$r' = a - bq' = (a - bq) + b(q - q') \geqslant r + b.$$

Como $r + b \geqslant b$, se sigue que $r' \geqslant b$ contradiciendo la segunda propiedad de $r'$. Por lo tanto la suposición $q' > q$ es falsa. El mismo argumento con q y $q'$ intercambiados demuestra que $q < q'$ también es falsa. Entonces debemos tener $q = q'$, y en consecuencia $r = r'$, puesto que

$$r = a - bq = a - bq' = r'.$$

□

*Ejemplo.*

- Si $a = 10$ y $b = 3$, entonces $10 = 3 \cdot 3 + 1$. Es decir $q = 3$, $r = 1$.
- Si $a = 2$ y $b = 5$, entonces $2 = 5 \cdot 0 + 2$. Es decir $q = 0$, $r = 2$.
- Si $a = -10$ y $b = 3$, entonces $-10 = 3 \cdot (-4) + 2$. Es decir $q = -4$, $r = 2$. En algunos viejos compiladores del lenguaje C, la división entera estaba mal definida, pues consideraban, por ejemplo, $-10 = 3 \cdot (-3) - 1$. Es decir, si el número a ser dividido era negativo, tomaban el resto también como un número negativo, lo cual no está de acuerdo al teorema 3.1.1.
- Si $a = -2$ y $b = 3$, entonces $-2 = 3 \cdot (-1) + 1$. Es decir $q = -1$, $r = 1$.

§ *Desarrollos en base* b, *(*$b \geqslant 2$*)*

Una consecuencia importante del teorema 3.1.1 es que justifica nuestro método usual de representación de enteros.

*Ejemplo.* Deseamos escribir el número 407 con una expresión de la forma

$$407 = r_n 5^n + r_{n-1} 5^{n-1} + \cdots + r_1 5 + r_0,$$

con $0 \leqslant r_i < 5$. Veamos que esto es posible y se puede hacer de forma algorítmica. La forma de hacerlo es, primero, dividir el número original y los sucesivos cocientes por 5:

$$407 = 5 \cdot 81 + 2 \tag{3.1.1}$$
$$81 = 5 \cdot 16 + 1 \tag{3.1.2}$$
$$16 = 5 \cdot 3 + 1 \tag{3.1.3}$$
$$3 = 5 \cdot 0 + 3. \tag{3.1.4}$$

Observar entonces que

$$\begin{aligned} 407 &= 5 \cdot 81 + 2 && \text{por (3.1.1)} \\ &= 5 \cdot (5 \cdot 16 + 1) + 2 && \text{por (3.1.2)} \\ &= 5^2 \cdot 16 + 5 \cdot 1 + 2 \\ &= 5^2 \cdot (5 \cdot 3 + 1) + 5 \cdot 1 + 2 && \text{por (3.1.3)} \\ &= 5^3 \cdot 3 + 5^2 \cdot 1 + 5 \cdot 1 + 2. \end{aligned}$$

En este caso diremos que el desarrollo en base 5 de 407 es 3112 o, resumidamente, $407 = (3112)_5$. Observar que el desarrollo en base 5 de 407 viene dado por los restos de las divisiones sucesiva, leídos en forma ascendente.

Sea $b \geqslant 2$ un número entero, llamado *base* para los cálculos. Para cualquier entero positivo $x$ tenemos, por la aplicación repetida del teorema 3.1.1,

$$\begin{aligned} x &= bq_0 + r_0 \\ q_0 &= bq_1 + r_1 \\ &\dots \\ q_{n-2} &= bq_{n-1} + r_{n-1} \\ q_{n-1} &= bq_n + r_n. \end{aligned}$$

Aquí cada resto es uno de los enteros $0, 1, \dots, b-1$, y paramos cuando $q_n = 0$. Reemplazando sucesivamente los cocientes $q_i$, como lo hicimos en el ejemplo, obtenemos

$$x = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b + r_0.$$

Hemos representado $x$ (con respecto a la base $b$) por la secuencia de los restos, y escribimos $x = (r_n r_{n-1} \dots r_1 r_0)_b$. Convencionalmente $b = 10$ es la base para los cálculos hechos "a mano" y omitimos ponerle el subíndice, entonces tenemos la notación usual

$$1984 = 1 \cdot 10^3 + 9 \cdot 10^2 + 8 \cdot 10 + 4.$$

Esta notación posicional requiere símbolos solo para los enteros $0, 1, \dots, b-1$. La base $b = 2$ es particularmente adaptable para los cálculos en computadoras porque los símbolos 0 y 1 pueden representarse físicamente por la ausencia o presencia de un pulso de electricidad o luz.

*Ejemplo.* ¿Cuál es la representación en base 2 de $(109)_{10}$?

*Demostración.* Dividiendo repetidamente por 2 obtenemos

$$\begin{aligned} 109 &= 2 \cdot 54 + 1 \\ 54 &= 2 \cdot 27 + 0 \\ 27 &= 2 \cdot 13 + 1 \\ 13 &= 2 \cdot 6 + 1 \\ 6 &= 2 \cdot 3 + 0 \\ 3 &= 2 \cdot 1 + 1 \\ 1 &= 2 \cdot 0 + 1 \end{aligned}$$

Por lo tanto

$$(109)_{10} = (1101101)_2.$$

La base 16 también es usada en computación pues se utiliza el byte como unidad básica de memoria y debido a que un byte puede tomar $2^8$ posibles valores, tenemos que

$$2^8 = 2^4 \cdot 2^4 = 16 \cdot 16 = 1 \cdot 16^2 + 0 \cdot 16^1 + 0 \cdot 16^0.$$

Luego un byte puede representar $(100)_{16}$ valores. Más allá de la justificación, es claro que los dígitos disponibles (del 0 al 9) no nos alcanzan para representar un número en base 16, pues se requieren 16 símbolos. La convención usada es

$$\mathtt{A} = 10, \quad \mathtt{B} = 11, \quad \mathtt{C} = 12, \quad \mathtt{D} = 13, \quad \mathtt{E} = 14, \quad \mathtt{F} = 15.$$

*Ejemplo.* Representemos 12488 en base 16.

$$\begin{aligned} 12488 &= 16 \cdot 780 + 8 \\ 780 &= 16 \cdot 48 + 12 \\ 48 &= 16 \cdot 3 + 0 \\ 3 &= 16 \cdot 0 + 3. \end{aligned}$$

Luego $12488 = (30\mathtt{C}8)_{16}$.

□

§ *Ejercicios*

1) Encontrar $q$ y $r$ que satisfagan el teorema 3.1.1 cuando

   *a)* $a = 1001, \qquad b = 11;$

*b)* $a = 12345, \qquad b = 234.$

2) Encontrar las representaciones de $(1985)_{10}$ en:

*a)* Base 2, *b)* Base 5, *c)* Base 11.

3) Encontrar las representación usual (base 10) de:

*a)* $(11011101)_2$, *b)* $(4165)_7$.

## 3.2 DIVISIBILIDAD

**Definición 3.2.1.** Dados dos enteros $x$ e $y$ decimos que $y$ es un *divisor* de $x$, y escribimos $y|x$, si

$$x = yq \quad \text{para algún} \quad q \in \mathbb{Z}.$$

También decimos que $y$ es un *factor* de $x$, que $y$ *divide* a $x$, que $x$ es *divisible* por $y$, y que $x$ es *múltiplo* de $y$.

Cuando $y|x$ podemos usar el símbolo $\frac{x}{y}$ (o $x/y$) para denotar el entero $q$ tal que $x = yq$. Cuando $y$ no es un divisor de $x$ tenemos que asignar un nuevo significado a la fracción $x/y$, puesto que este número no es un entero. El lector indudablemente, esta familiarizado con las reglas para manejar fracciones, y usaremos esas reglas de tanto en tanto, pero es importante recordar que las fracciones no han sido aún formalmente definidas en el contexto de este apunte. Y es aún más importante recordar que $x/y$ no es un elemento de $\mathbb{Z}$ a menos que $y$ divida a $x$.

*Observación* 3.2.2. Veamos ahora alguna propiedades básicas de la relación "divide a". Sean $a, b, c$ enteros, entonces

*a)* $1|a, \qquad a|0, \qquad a|\pm a;$

*b)* si $a|b$, entonces $a|bc$ para cualquier $c$;

*c)* si $a|b$ y $a|c$, entonces $a|(b+c)$;

*d)* si $a|b$ y $a|c$, entonces $a|(rb+sc)$ para cualesquiera $r, s \in \mathbb{Z}$.

*e)* si $a, b > 0$ y $a|b$, entonces $a \leqslant b$.

*Demostración.* La demostración de estos hechos es sencilla, por ejemplo *c)*: como $a|b$, existe $q$ tal que $b = aq$. Análogamente, como $a|c$, existe $q'$ tal que $c = aq'$. Entonces $b + c = aq + aq' = a(q + q')$, luego $a|(b + c)$. Las demás demostraciones, excepto la última, se dejan como ejercicio para el lector.

Demostración de *e)*: como $a|b$ existe $q \in \mathbb{Z}$ tal que $b = aq$, como $a, b > 0$, entonces, por la compatibilidad de $>$ con el producto, $q > 0$. Luego $q - 1 \geqslant 0$ y, de nuevo por la compatibilidad, $a(q-1) \geqslant 0$. Ahora bien, $b = aq = a + a(q-1)m$ luego $b - a = a(q-1) \geqslant 0$, por lo tanto $b \geqslant a$. □

*Ejemplo.* Demostremos que si $c$, $d$ y $n$ son enteros tales que, $d|n$ y $c \left| \frac{n}{d} \right.$, entonces

$$c|n \quad \text{y} \quad d \left| \frac{n}{c} \right.$$

*Demostración.* Como $d|n$ existe un entero $s$ tal que $n = ds$, y $n/d$ denota al entero $s$. Puesto que $c|(n/d)$ existe un entero $t$ tal que

$$s = \frac{n}{d} = ct.$$

Se sigue que

$$n = ds = d(ct) = c(dt)$$

entonces $c|n$ y $n/c$ denota al entero $dt$. Finalmente, como $n/c = dt$ tenemos $d|(n/c)$, como queríamos demostrar. □

**Proposición 3.2.3.** *Sean $a$ y $b$ enteros.*

*a) Si $ab = 1$ entonces $a = b = 1$ o $a = b = -1$.*

*b) Si $x$ e $y$ son enteros tales que $x|y$ e $y|x$, entonces $x = y$ o $x = -y$.*

*Demostración.*

*a)* Si $a$ o $b$ valen $0$, entonces $ab = 0 \neq 1$. Luego $a$ y $b$ son distintos de $0$. Si $a > 0$ y $b < 0$ por los axiomas de compatibilidad del orden con el producto $ab < 0$. Lo mismo ocurre si $a < 0$ y $b > 0$.

Es decir podemos suponer que o bien $a > 0$ y $b > 0$, o bien $a < 0$ y $b < 0$.

Si $a > 0$ y $b > 0$, entonces $a \geqslant 1$ y $b \geqslant 1$. Si $a = 1$, como $ab = 1$, tenemos que $b = 1 \cdot b = 1$. Si $a > 1$, como $b > 0$ por compatibilidad de $<$ con el producto tenemos que $ab > 1$, lo cual no es cierto. Es decir, hemos probado que si $a > 0$ y $b > 0$, entonces $a = 1$ y $b = 1$.

Si $a < 0$ y $b < 0$, entonces $-a > 0$ y $-b > 0$ y $(-a)(-b) = ab = 1$. Luego, por el párrafo de arriba, $-a = -b = 1$ y en consecuencia $a = b = -1$.

*b)* Sean $x, y$ tales que $x|y$ e $y|x$. Como $x|y$, existe $q \in \mathbb{Z}$ tal que $y = qx$. Análogamente, como $y|x$ existe $q'$ tal que $x = q'y$. Luego

$$y = qx = q(q'y) = (qq')y.$$

Por el axioma de cancelación (cancelando $y$) obtenemos que $1 = qq'$. Por lo demostrado más arriba tenemos que, o bien $q = q' = 1$ y en consecuencia $x = y$, o bien $q = q' = -1$ y en consecuencia $x = -y$. □

*Observación.* Si $a$ y $b$ son enteros positivos y $a|b$ entonces $a \leqslant b$. Esto se demuestra de la siguiente manera: como $a|b$ existe $q$ tal que $b = aq$. Como $a$ y $b$ son positivos, por la regla de los signos también $q > 0$. Ahora bien $b = aq = a(q-1) + a \geqslant a$. La última desigualdad es verdadera pues

$$q > 0 \;\Rightarrow\; q - 1 \geqslant 0 \;\Rightarrow\; a(q-1) \geqslant 0 \;\Rightarrow\; a(q-1) + a \geqslant a.$$

§ *Ejercicios*

1) Usar el principio de inducción para demostrar que, para todo $n \geqslant 0$ se cumplen;

   *a)* $n^2 + 3n$ es divisible por 2,

   *b)* $n^3 + 3n^2 + 2n$ es divisible por 6.

## 3.3 EL MÁXIMO COMÚN DIVISOR Y EL MÍNIMO COMÚN MÚLTIPLO

Recordemos que por la observación 3.2.2 *e)*, si $x|y$ y ambos son mayores que $0$, entonces $x \leqslant y$. En consecuencia, el conjunto de divisores de un número positivo está compuesto por números menores o iguales al número.

**Definición 3.3.1.** Si $a$ y $b$ son enteros algunos de ellos no nulo, decimos que un entero no negativo $d$ es el *máximo común divisor*, o *mcd*, de $a$ y $b$ si

*a)* $d|a$ y $d|b$;

*b)* si $c|a$ y $c|b$ entonces $c \leqslant d$.

Denotaremos al máximo común divisor de $a$ y $b$ por $\mathrm{mcd}(a, b)$ o, en caso de no haber confusión, por $(a, b)$.

La condición *a)* nos dice que $d$ es un común divisor de $a$ y $b$ y la condición *b)* nos dice que cualquier divisor común de $a$ y $b$ es menor igual que $d$. Podemos resumir la definición en una frase, diciendo: *el máximo común divisor de* $a$ *y* $b$ *es el mayor divisor común a ambos números.*

*Ejemplo.* Los divisores positivos comunes de 60 y 84 son 1, 2, 3, 6 y 12, luego, por ejemplo, 6 es un divisor común y por lo tanto satisface *a)*. Sin embargo, no satisface *b)* de la definición, pues $12|60$ y $12|84$ pero $12 > 6$. En este caso, 12 claramente es el máximo común divisor.

*Ejemplo.* Hallar $\mathrm{mcd}(174, 72)$.

*Solución.*

Divisores de 174: 1, 2, 3, 6, 29, 58, 87, 174

Divisores de 72: 1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72

Luego, 6 es divisor común de 174 y 72, y todos los demás divisores comunes (1, 2 y 3) son menosres que 6. Por lo tanto $\mathrm{mcd}(174, 72) = 6$. □

En los ejemplos anteriores usamos dos enteros pequeños y no tuvimos problemas en encontrar el máximo común divisor. Pero ¿qué pasaría si consideráramos dos enteros muy grandes?

En el desarrollo de esta sección veremos el *algoritmo de Euclides*, un método muy eficiente para calcular el máximo común divisor de dos números.

*Observación* 3.3.2. Sean $a, b$ enteros, alguno de ellos no nulo, y $a', b'$ otro par de enteros tal que se cumple la propiedad:

$$c|a \wedge c|b \quad \Leftrightarrow \quad c|a' \wedge c|b',$$

es decir, $c$ es divisor de $a$ y $b$ si y solo si es divisor de $a'$ y $b'$. Entonces, $\mathrm{mcd}(a, b) = \mathrm{mcd}(a', b')$. Esto es obvio a partir de la definición del mcd.

Podemos enunciar las propiedades más sencillas del mcd en la siguiente proposición.

**Proposición 3.3.3.** *Sean* $a, b$ *enteros con* $a \neq 0$, *entonces*

*(1)* $\mathrm{mcd}(b, a) = \mathrm{mcd}(a, b) = \mathrm{mcd}(\pm a, \pm b)$,

*(2) si* $a > 0$, $\mathrm{mcd}(a, 0) = a$ *y* $\mathrm{mcd}(a, a) = a$,

*(3)* $\mathrm{mcd}(1, b) = 1$.

*Demostración.* Estas propiedades son de demostración casi trivial, por ejemplo para demostrar que $\mathrm{mcd}(1, b) = 1$ comprobamos que 1 cumple con la definición:

*a)* $1|1$ y $1|b$;

*b)* si $c|1$ y $c|b$ entonces $c \leqslant 1$,

propiedades que son obviamente verdaderas.

1. y 2. se dejan a cargo del lector. □

La siguiente propiedad no es tan obvia y resulta muy importante.

**Propiedad 3.3.4.** *Si* $a \neq 0, b \in \mathbb{Z}$, *entonces* $\mathrm{mcd}(a, b) = \mathrm{mcd}(a, b - a)$.

*Demostración.* Sea $d = \mathrm{mcd}(a, b - a)$, luego

*a)* $d|a$ y $d|b-a$;

*b)* si $c|a$ y $c|b-a$ entonces $c \leqslant d$.

Ahora bien, como $d|a$ y $d|b-a$, entonces $d|a+(b-a)=b$. Es decir, para recalcar,

*a')* $d|a$ y $d|b$.

Por otro lado, si $c|a$ y $c|b$, entonces $c|b-a$, luego por *b)* tenemos que $c \leqslant d$. Es decir,

*b')* si $c|a$ y $c|b$, entonces $c \leqslant d$.

Luego, por definición de mcd, obtenemos que $d = \text{mcd}(a,b)$. □

La propiedad anterior nos provee un método práctico para encontrar el máximo común divisor entre dos números. Veamos su aplicación en el siguiente ejemplo.

*Ejemplo.* Encontrar el mcd entre 72 y 174.

*Solución.* Observar que

$$\begin{aligned}\text{mcd}(72,174) &= \text{mcd}(72,174-72) = \text{mcd}(72,102) = \text{mcd}(72,30) = \text{mcd}(42,30)\\ &= \text{mcd}(12,30) = \text{mcd}(12,18) = \text{mcd}(12,6) = \text{mcd}(6,6) = 6.\end{aligned}$$

□

En general no es sencillo encontrar todos los divisores de un número entero grande. Por ejemplo, para los números de más de cien dígitos no es posible, en general, calcular sus divisores ni con las computadoras más poderosas de la actualidad. Por lo tanto, no es factible calcular el mcd de números grandes revisando todos los divisores comunes. El algoritmo que nos provee la propiedad 3.3.4 nos da un método práctico y relativamente eficiente para calcular el mcd. Veremos a continuación un método similar pero mucho más eficiente para calcular el mcd de dos enteros no negativos $a, b$ con $b \neq 0$. Este método esta basado en el algoritmo de división y el siguiente resultado.

**Proposición 3.3.5.** *Sean* $a, b$ *enteros no negativos con* $b \neq 0$*, entonces*

$$a = bq + r \quad \Rightarrow \quad \text{mcd}(a,b) = \text{mcd}(b,r). \tag{3.3.1}$$

*Demostración.* Se puede demostrar por definición directamente y en ese caso la demostración es similar a la de la propiedad 3.3.4.

Sin embargo, para mostrar que un problema se puede encarar de forma diferente, haremos la demostración utilizando la observación 3.3.2. Es decir probaremos que los divisores comunas de $a$ y $b$ son los mismos que los divisores comunes de $b$ y $r$.

Para demostrar esto debemos observar que si $c$ divide $a$ y $b$, entonces también divide a $a - bq$; y como $a - bq = r$, tenemos que $c|r$. De este modo cualquier divisor común de $a$ y $b$ es también divisor común de $b$ y $r$. Por otro lado si $c$ divide $b$ y $r$ también divide a $a = bq + r$. Es decir, $c$ es divisor común de $a$ y $b$ si y sólo si $c$ es divisor común de $b$ y $r$. Por lo tanto, por observación 3.3.2, obtenemos que $d = \text{mcd}(b, r)$. □

La aplicación repetida de este simple resultado, en combinación con el algoritmo de división, nos da un método para calcular el mcd.

*Ejemplo.* Encuentre el mcd de 2406 y 654.

*Solución.* Tenemos

$$\begin{aligned}
\text{mcd}(2406, 654) &= \text{mcd}(654, 444) && \text{porque} && 2406 = 654 \cdot 3 + 444,\\
&= \text{mcd}(444, 210) && \text{porque} && 654 = 444 \cdot 1 + 210,\\
&= \text{mcd}(210, 24) && \text{porque} && 444 = 210 \cdot 2 + 24,\\
&= \text{mcd}(24, 18) && \text{porque} && 210 = 24 \cdot 8 + 18,\\
&= \text{mcd}(18, 6) && \text{porque} && 24 = 18 \cdot 1 + 6,\\
&= \text{mcd}(6, 0) = 6 && \text{porque} && 18 = 6 \cdot 3 + 0
\end{aligned}$$

Por lo tanto, $\text{mcd}(2406, 654) = 6$. □

Este ejemplo es un caso particular o una aplicación del algoritmo que nos permite calcular el máximo común divisor: sean $a$ y $b$ enteros con $b > 0$, sea $r_0 = a$, $r_1 = b$ y suponiendo definidos $r_{i-1}$ y $r_i$ definimos recursivamente $r_{i+1}$ por la siguiente ecuación

$$r_{i-1} = r_i q + r_{i+1} \quad \text{con} \quad 0 < r_{i+1} < r_i.$$

Observar que $r_{i+1]}$ está bien definido por el algoritmo de división. Detenemos el proceso cuando uno de los restos $r_i$ es igual a $0$. Ahora bien, cada resto no nulo es positivo y estrictamente menor que el anterior. Entonces, queda claro que el proceso se va a detener.

El proceso se explica esquemáticamente en el cuadro 1.

Este procedimiento es conocido como el *algoritmo de Euclides*, debido al matemático griego Euclides (300 a. c.). Es extremadamente útil en la práctica, y tiene importantes consecuencias.

**Algoritmo de Euclides**

Por lo general, para calcular el mcd de enteros $a$ y $b$, con $b > 0$, definimos $r_i$ recursivamente de la siguiente manera: $r_0 = a$, $r_1 = b$, y

$$
\begin{array}{lll}
(e_1) & r_0 = r_1 q_1 + r_2 & (0 < r_2 < r_1) \\
(e_2) & r_1 = r_2 q_2 + r_3 & (0 < r_3 < r_2) \\
(e_3) & r_2 = r_3 q_3 + r_4 & (0 < r_4 < r_3) \\
\dots & & \\
(e_i) & r_{i-1} = r_i q_i + r_{i+1} & (0 < r_{i+1} < r_i) \\
\dots & & \\
(e_{k-1}) & r_{k-2} = r_{k-1} q_{k-1} + r_k & (0 < r_k < r_{k-1}) \\
(e_k) & r_{k-1} = r_k q_k + 0, &
\end{array}
$$

Cuadro 1: Algoritmo de Euclides

**Teorema 3.3.6.** *Sean $a$ y $b$ enteros con $b > 0$, entonces el máximo común divisor es el último resto no nulo obtenido en el algoritmo de Euclides (con la notación del cuadro 1 es $r_k$).*

*Demostración.* Observar que aplicando repetidas veces la fórmula (3.3.1) obtenemos

$$
\begin{aligned}
r_k = \operatorname{mcd}(r_k, 0) = \operatorname{mcd}(r_{k-1}, r_k) = \operatorname{mcd}(r_{k-2}, r_{k-1}) = \cdots \\
\cdots = \operatorname{mcd}(r_2, r_3) = \operatorname{mcd}(r_1, r_2) = \operatorname{mcd}(r_0, r_1) = \operatorname{mcd}(a, b)
\end{aligned}
$$

□

*Observación* (*). El algoritmo de Euclides es fácilmente implementable en un lenguaje de programación. A continuación una versión del mismo en pseudocódigo.

ALGORITMO DE EUCLIDES

```
# pre: a y b son números positivos
# post: Obtenemos d = mcd(a,b)
i, j = a, b
while j != 0:
    # invariante: mcd(a, b) = mcd(i, j)
    resto = i % j  # i = q * j + resto
    i, j = j, resto
d = i
```

Observar que en el ciclo `while` los valores que se obtienen en cada repetición son $i' = j$, $j' = i \,\%\, j$, luego

$$i = q \cdot j + j' \;\Rightarrow\; \mathrm{mcd}(i, j) = \mathrm{mcd}(j, j') = \mathrm{mcd}(i', j').$$

**Definición 3.3.7.** Sean $a, b$ enteros, entonces dados $s, t \in \mathbb{Z}$ diremos que

$$sa + tb$$

es una *combinación lineal entera* de $a$ y $b$.

*Observación.* Sean $a, b \in \mathbb{Z}$, alguno de ellos no nulo, y $d$ un máximo común divisor de $a$ y $b$. Entonces, $d$ divide a cualquier combinación lineal entera de $a$ y $b$. Esto es una consecuencia directa de la observación 3.2.2 *d)*.

**Teorema 3.3.8.** *Sean $a, b \in \mathbb{Z}$, alguno de ellos no nulo. Entonces, existen $s, t \in \mathbb{Z}$ tal que*

$$\mathrm{mcd}(a, b) = sa + tb.$$

*Es decir* $\mathrm{mcd}(a, b)$ *es combinación lineal entera de* $a$ *y* $b$.

*Demostración.* Supongamos que $b > 0$ (los otros casos se deducen fácilmente) y sea $d = \mathrm{mcd}(a, b)$. La idea es calcular $s$ y $t$ tales que

$$d = sa + tb.$$

De acuerdo con la notación que utilizamos para explicar el algoritmo de Euclides, $d = r_k$ y usando la ecuación $(e_{k-1})$ tenemos

$$r_k = r_{k-2} - r_{k-1} q_{k-1}.$$

Así, $d$ puede escribirse en la forma $d = s_k r_{k-2} + t_k r_{k-1}$, donde $s_k = 1$ y $t_k = -q_{k-1}$ . Usando la ecuación $(e_{k-2})$, sustituyendo $r_{k-1}$ en términos de $r_{k-3}$ y $r_{k-2}$ obtenemos

$$d = s_k(r_{k-3} - r_{k-2} q_{k-2}) + t_k r_{k-3} = s_{k-1} r_{k-3} + t_{k-1} r_{k-2}$$

donde $s_{k-1} = s_k + t_k$ y $t_{k-1} = -s_k q_{k-2}$. Aplicando repetidas veces las ecuaciones del algoritmo de Euclides obtenemos, en general que

$$d = s_i r_{i-2} + t_i r_{i-1}$$

con $s_i, t_i \in \mathbb{Z}$, para $2 \leqslant i \leqslant k$. En particular

$$d = s_2 r_0 + t_2 r_1 = s_2 a + t_2 b.$$

□

*Ejemplo.* Encontrar usando el algoritmo de Euclides $d = \mathrm{mcd}(470, 55)$ y expresar $d$ como combinación lineal entera entre 470 y 55.

*Solución.*

$$\begin{aligned} 470 &= 55 \cdot 8 + 30 \quad \Rightarrow \quad 30 = 470 + (-8) \cdot 55 \qquad (1) \\ 55 &= 30 \cdot 1 + 25 \quad \Rightarrow \quad 25 = 55 + (-1) \cdot 30 \qquad (2) \\ 30 &= 25 \cdot 1 + 5 \quad \Rightarrow \quad 5 = 30 + (-1) \cdot 25 \qquad (3) \\ 25 &= 5 \cdot 5 + 0. \end{aligned}$$

Luego, el máximo común divisor de 470 y 55 es 5 y de las fórmulas anteriores obtenemos:

$$\begin{aligned} 5 &= 30 + (-1) \cdot 25 && \text{(por (3))} \\ &= 30 + (-1) \cdot (55 + (-1) \cdot 30) = 2 \cdot 30 + (-1) \cdot 55 && \text{(por (2))} \\ &= 2 \cdot (470 + (-8) \cdot 55) + (-1) \cdot 55 = 2 \cdot 470 + (-17) \cdot 55 && \text{(por (1))} \end{aligned}$$

De este modo, la expresión requerida $d = sa + tb$ es

$$5 = 2 \cdot 470 + (-17) \cdot 55.$$

□

**Corolario 3.3.9.** *Sean $a$ y $b$ enteros, unos de ellos no nulo y sea $d = \mathrm{mcd}(a, b)$. Sea $c \in \mathbb{Z}$ tal que $c|a$ y $c|b$, entonces $c|d$.*

*Demostración.* Por la proposición anterior $d$ es combinación lineal entera de $a$ y $b$. Como $c|a$ y $c|b$, por observación 3.2.2 *d)*, se deduce que $c|d$. □

**Definición 3.3.10.** Si $(a, b) = 1$ entonces decimos que $a$ y $b$ son *coprimos*.

**Corolario 3.3.11.** *Sean $a$ y $b$ enteros uno de ellos no nulo, entonces*

$$(a, b) = 1 \Leftrightarrow \textit{existen } s, t \in \mathbb{Z} \textit{ tales que } 1 = sa + tb.$$

*Demostración.* ($\Rightarrow$) Es consecuencia trivial del teorema 3.3.8.

($\Leftarrow$) Sea $d = (a, b)$, entonces $d|a$ y $d|b$ y por lo tanto $d|sa + tb$ para cualesquiera $s, t \in \mathbb{Z}$. En particular, la hipótesis implica que $d|1$ y, en consecuencia $d = 1$. □

*Ejemplo.* Sean $a$ y $b$ enteros coprimos y $c \in \mathbb{Z}$, entonces,

$$a|c \wedge b|c \quad \Rightarrow \quad ab|c.$$

*Solución.* como $a$ y $b$ son coprimos, existen $s, t \in \mathbb{Z}$ tales que $1 = sa + tb$. Por lo tanto, multiplicando por $c$ la ecuación, obtenemos $c = csa + ctb$. Como $a|c$, tenemos que $c/a \in \mathbb{Z}$, y

$$\frac{c}{a} = \frac{csa + ctb}{a} = cs + (\frac{c}{a})tb.$$

Como $b|c$ y $b|b$, entonces $b|cs + (c/a)tb = c/a$, luego $(c/a)/b$ entero, es decir $ab|c$. □

El hecho de que el máximo común divisor de dos enteros $a$ y $b$ puede ser escrito como una combinación lineal entera de $a$ y $b$ (proposición 3.3.8) es una herramienta de suma utilidad para trabajar en problemas relacionados con el mcd. Por ejemplo, todos estamos familiarizados con la idea de que una fracción puede reducirse al "mínimo término", o sea a la forma $a/b$ con $a$ y $b$ coprimos. El siguiente ejemplo establece que esta forma es única, y como veremos, el hecho clave de la demostración es que podemos expresar a $1$ como $sa + tb$.

*Ejemplo.* Supongamos que $a$, $a'$, $b$, $b'$ son enteros positivos que satisfacen

*a)* $ab' = a'b$; *b)* $\mathrm{mcd}(a, b) = \mathrm{mcd}(a', b') = 1$.

Entonces $a = a'$ y $b = b'$.

(La condición *a)* podría escribirse como $a/b = a'/b'$, pero preferimos usar esta forma que no asume ningún conocimiento sobre fracciones.)

*Demostración.* Como por *b)* el $\mathrm{mcd}(a, b) = 1$ existen enteros $s$ y $t$ tales que $sa + tb = 1$. En consecuencia

$$b' = (sa + tb)b' = sab' + tbb' \overset{a)}{=} sa'b + tb'b = (sa' + tb')b,$$

y por lo tanto $b|b'$. Por un argumento similar y usando el hecho de que el $\mathrm{mcd}(a', b') = 1$ deducimos que $b|b'$, por lo tanto $b = b'$ o $b = -b'$ y como $b$ y $b'$ son ambos positivos debemos tener $b = b'$ . Ahora de *a)* deducimos que $a = a'$ y el resultado esta demostrado. □

*Observación* (*). El algoritmo explicado anteriormente para obtener el $\mathrm{mcd}(a, b)$ como combinación lineal entera $sa + tb$ no es muy sencillo de programar. Más aún, requiere terminar el cálculo del mcd usando el algoritmo de Euclides, para comenzar a calcular los coeficientes enteros $s, t$. Veremos a continuación un algoritmo que calcula usando el algortimo de Euclides simultáneamente los coeficientes enteros $s$ y $t$ y el máximo común divisor. El algoritmo se basa en el siguiente resultado, que es una forma más precisa de enunciar el teorema 3.3.8 .

**Proposición 3.3.12.** *Sean,* $a, b$ *enteros,* $b > 0$*, y* $r_i, q_i$ *los restos y cocientes obtenidos en el algoritmo de Euclides (ver tabla 1). Entonces,*

*a) para* $0 \leqslant i \leqslant k$*, existen* $s_i, t_i \in \mathbb{Z}$ *tal que*

$$r_i = s_i a + t_i b.$$

*b)* $s_0, t_0 = 1, 0$ , $s_1, t_1 = 0, 1$ *y*

$$s_i = s_{i-2} - q_{i-1}s_{i-1}, \qquad t_i = t_{i-2} - q_{i-1}t_{i-1}, \tag{3.3.2}$$

*para* $i \geqslant 2$.

*Demostración. a)* Lo haremos por inducción sobre $i$.

Como $r_i$ se define con una recursión que se basa en los dos casos anteriores, el caso base debe hacerse en dos valores: $i = 0$ e $i = 1$, pero como $r_0 = a$ (en este caso $s_0 = 1, s_1 = 0$) y $r_1 = b$ (en este caso $s_0 = 0, s_1 = 1$), se cumple el enunciado para el caso base.

*Paso inductivo.* Si $i > 1$, tenemos

$$\begin{aligned} r_i &= r_{i-2} + (-q_{i-1})r_{i-1} \\ &= s_{i-2}a + t_{i-2}b + (-q_{i-1})(s_{i-1}a + t_{i-1}b) \qquad \text{(hipótesis inductiva)} \\ &= (s_{i-2} - q_{i-1}s_{i-1})a + (t_{i-2} - q_{i-1}t_{i-1})b. \end{aligned}$$

*b)* Es claro por la demostración de *a)*. □

Con el uso de *b)* de la proposición anterior, podemos escribir el algoritmo para obtener $s, t$ tal $\mathrm{mcd}(a, b) = sa + tb$ con el siguiente pseudocódigo.

ALGORITMO DE EUCLIDES 2

```
# pre: a y b son números positivos
# post: Obtenemos s y t tal que mcd(a,b) = a*s + b*t
r[0], r[1] = a, b
s[0], t[0], s[1], t[1] = 1, 0, 0, 1
i = 1
while r[i] != 0:
    # invariante: r[i-1] = a * s[i-1] + b * t[i-1]
    #             y  mcd(a, b) = mcd(r[i-1], r[i])
    q, r[i+1] = r[i-1] // r[i], r[i-1] % r[i]
    s[i+1] = s[i-1] - s[i] * q
    t[i+1] = t[i-1] - t[i] * q
    i = i+1
s, t  = s[i-1], t[i-1]
```

Sin embargo, este algoritmo no es muy conveniente, a nivel de eficiencia de memoria, pues las variables `r`, `s` y `t` van guardando series de valores en forma innecesaria.

Una versión mejorada, aunque menos legible, es la siguiente.

ALGORITMO DE EUCLIDES 2 (VERSIÓN 2)

```
# pre: a y b son números positivos
# post: Obtenemos s y t tal que mcd(a,b) = a*s + b*t
r0, r1 = a, b
s0, t0, s1, t1 = 1, 0, 0, 1
while r1 != 0:
    # invariante: r0 = a * s0 + b * t0  y
    #             mcd(a, b) = mcd(r0, r1)
    resto = r0 % r1
    q, r0, r1 = r0 // r1, r1, resto
    s1p, t1p = s1, t1
    s0, t0, s1, t1 =  s1p, t1p, s0 - s1 * q, t0 - t1 * q
s, t  = s0, t0
```

Este último código y el de la página 55 son códigos válidos en Python 3 y pueden ser incorporados a un programa escrito en ese lenguaje.

### § *Mínimo común múltiplo*

**Definición 3.3.13.** Sean $a$ y $b$ enteros no nulos. Decimos que un entero positivo $m$ es el *mínimo común múltiplo*, o *mcm*, de $a$ y $b$ si

*a)* $a|m$ y $b|m$;

*b)* si $a|n$ y $b|n$ entonces $m|n$.

La condición *a)* nos dice que $m$ es múltiplo común de $a$ y $b$, la condición *b)* nos dice que cualquier otro múltiplo de $a$ y $b$ también debe ser múltiplo de $m$. Por ejemplo hallemos el mínimo común múltiplo entre 8 y 14. Escribamos los múltiplos de ambos números y busquemos el menor común a ambos. Los primeros múltiplos de 8 son: $8, 16, 24, 32, 40, 48, 56, \ldots$. Los primeros múltiplos de 14 son: $14, 28, 42, 56, 72, \ldots$. Luego se tiene $\text{mcm}(8, 14) = 56$. Nos faltaría comprobar que cualquier múltiplo de 8 y 14 es múltiplo de 56, pero eso se deduce fácilmente de los resultados que veremos a continuación.

El siguiente teorema garantiza la existencia del mcm.

**Teorema 3.3.14.** *Sean* $a$ *y* $b$ *enteros no nulos, entonces*

$$\operatorname{mcm}(a,b) = \frac{ab}{\operatorname{mcd}(a,b)}.$$

*Demostración.* Demostraremos que

$$m = \frac{ab}{\operatorname{mcd}(a,b)}$$

es el mínimo común múltiplo de $a$, $b$.

Como

$$m = \frac{ab}{\operatorname{mcd}(a,b)} = \frac{a}{\operatorname{mcd}(a,b)}b = a\frac{b}{\operatorname{mcd}(a,b)}$$

resulta que $m$ es múltiplo de $a$ y $b$, y por lo tanto se satisface (a) de la definición de mínimo común múltiplo. Veamos ahora (b): sea $n \in \mathbb{Z}$ tal que $a|n$ y $b|n$. Como existen enteros $r, s$ tales que

$$\operatorname{mcd}(a,b) = ra + sb, \tag{3.3.3}$$

dividiendo la ecuación (3.3.3) por $\operatorname{mcd}(a,b)$ y multiplicando por $n$, obtenemos la siguiente ecuación:

$$n = r\frac{a}{\operatorname{mcd}(a,b)}n + s\frac{b}{\operatorname{mcd}(a,b)}n. \tag{3.3.4}$$

Escribiendo $n = b'b = a'a$ ($a', b'$ en $\mathbb{Z}$) y haciendo los reemplazos en (3.3.4), resulta finalmente

$$n = rb'\frac{ab}{\operatorname{mcd}(a,b)} + sa'\frac{ab}{\operatorname{mcd}(a,b)} = \frac{ab}{\operatorname{mcd}(a,b)}(rb' + sa')$$

lo cual demuestra que $m$ divide a $n$. □

En particular este resultado implica que si $a$ y $b$ son enteros coprimos, entonces $\operatorname{mcm}(a,b) = ab$.

*Ejemplo.* Encontrar el mcm de 8 y 14.

*Solución.* Es claro que $2 = \operatorname{mcd}(8,14)$, luego $\operatorname{mcm}(8,14) = 8 \cdot 14/2 = 56$. □

§ *Ejercicios*

1) Encontrar el mcd de 721 y 448 y expresarlo en la forma $721m + 448n$ con $m, n \in \mathbb{Z}$.

2) Usar proposición 3.3.8 para demostrar que si $a$, $b$ y $n$ son enteros no nulos, entonces $\mcd(na, nb) = n \mcd(a, b)$.

3) Usar el Ej. 2 para demostrar que si el $\mcd(a, b) = d$ , entonces

$$\mcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

4) Sean $a$ y $b$ enteros positivos y sea $d = \mcd(a, b)$. Probar que existen enteros $x$ e $y$ que satisfacen la ecuación $ax + by = c$ si y solo si $d|c$.

5) Encontrar enteros $x$ e $y$ que satisfagan $966x + 685y = 70$.

## 3.4 FACTORIZACIÓN EN PRIMOS

**Definición 3.4.1.** Se dice que un entero positivo $p$ es *primo* si $p \geqslant 2$ y los únicos enteros positivos que dividen $p$ son $1$ y $p$ mismo.

Luego si un entero $m \geqslant 2$ no es un primo si y sólo si existe $m_1$ divisor de $m$ tal que $m_1 \neq 1, m$, es decir con $1 < m_1 < m$. Sea $m_2$ el cociente de $m$ por $m_1$: es claro que $m_2 \neq 1, m$ y por lo tanto $1 < m_2 < m$. Concluyendo,

*un entero $m \geqslant 2$ no es un primo si y sólo si $m = m_1 m_2$ donde $m_1$ y $m_2$ son enteros estrictamente entre $1$ y $m$.*

Enfaticemos que de acuerdo a la definición, $1$ *no* es primo.

Los primeros primos (los menores que 100) son

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 y 97.

*Observación* (Criba de Eratóstenes *). Un forma de encontrar números primos es con la *criba de Eratóstenes.* Es un algoritmo que permite hallar todos los números primos menores que un número natural dado $n$. Se forma una lista con todos los números naturales comprendidos entre 2 y $n$, y se van tachando los números que no son primos de la siguiente manera: comenzando por el 2, se tachan todos sus múltiplos; comenzando de nuevo, cuando se encuentra un número entero que no ha sido tachado, ese número es declarado primo, y se procede a tachar todos sus múltiplos y así sucesivamente. El proceso termina cuando alcanzamos $n$.

Podemos expresar el algoritmo en pseudocódigo:

CRIBA DE ERATÓSTENES

```
# pre: n número natural
# post: se obtiene ''primos'' la lista de números primos hasta n
primos = [] # lista vacía
tachados = [] # lista de números tachados
for i = 2 to n:
    if i not in tachados:
        primos.append(i) # agregar i a primos
        k = 2
        while k * i <= n:
            tachados.append(k * i) # agrega k*i a tachados
            k = k + 1
```

Este código en si no es eficiente, pero muestra una forma sencilla de obtener primos con el uso de la criba de Eratóstenes. El código puede ser mejorado y su rendimiento aumenta enormemente.

CRIBA DE ERATÓSTENES 2

```
# pre: n número natural
# post: primos[i] = True si y solo si i <= n es primo.
primos = lista de longitud n con todas las coordenadas True
for i = 2 to [n^0.5]:
    if primos[i] == True:
        for j = i**2 to n+1 step i:
            primos[j] = False
```

En el algoritmo `[n^0.5]` denota la parte entera de la raíz cuadrada de `n`. Por otro lado, `for j = k to m step t` simboliza que comenzamos un contador `j` en `k` y lo vamos incrementando en `t` hasta llegar a `m`.

El lector debe estar casi totalmente familiarizado con la idea de que cualquier entero positivo puede expresarse como producto de primos: por ejemplo

$$825 = 3 \cdot 5 \cdot 5 \cdot 11.$$

La existencia de esta factorización en primos para cualquier entero positivo es una consecuencia del axioma del buen orden.

**Teorema 3.4.2.** *Todo entero mayor que* 1 *es producto de números primos.*

*Demostración.* Sea $B$ el conjunto de enteros positivos que no tienen una factorización en primos.

Si $B$ no es vacío entonces, por el axioma del buen orden, tiene un mínimo $m$. Si $m$ fuera un primo $p$ entonces tendríamos la factorización trivial

$m = p$; por lo tanto $m$ no es primo y existen $m_1, m_2$ enteros positivos con $1 < m_1 < m$ y $1 < m_2 < m$ tal que $m = m_1 m_2$.

Como estamos suponiendo que $m$ es el menor entero ($\geqslant 2$) que no tiene factorización en primos, entonces $m_1$ y $m_2$ tienen factorización en primos. Pero entonces la ecuación $m = m_1 m_2$ produce una factorización en primos de $m$, contradiciendo la suposición de que $m$ era un elemento de $B$. Por lo tanto $B$ debe ser vacío, y la afirmación esta probada. □

*Ejemplo.* Encontremos la factorización en números primos de 201 000. Esto se hace dividiendo sucesivamente los números hasta llegar a factores primos:

$$\begin{aligned} 201\,000 &= 201 \cdot 1000 = 3 \cdot 67 \cdot 10 \cdot 10 \cdot 10 \\ &= 3 \cdot 67 \cdot 2 \cdot 5 \cdot 2 \cdot 5 \cdot 2 \cdot 5 \\ &= 2^3 \cdot 3 \cdot 5^3 \cdot 67. \end{aligned}$$

Como vimos más arriba $2, 3, 5$ y $67$ son números primos y por lo tanto hemos obtenido la descomposición prima de 201 000.

Veamos ahora algunas propiedades básicas de los números primos.

*Observación* 3.4.3. Sea $a \in \mathbb{Z}$ y $p$ primo. Entonces

*a)* Si $p \nmid a$, entonces $\mathrm{mcd}(a, p) = 1$.

*b)* Si $p$ y $p'$ son primos y $p|p'$ entonces $p = p'$.

*Demostración.*

*a)* Como los únicos divisores de $p$ son $p$ y $1$, y $p \nmid a$, el único divisor común de $p$ y $a$ es $1$.

*b)* $p'$ es primo, por lo tanto tiene sólo dos divisores positivos $1$ y $p'$. Como $p$ no es $1$, tenemos que $p = p'$. □

Para encontrar una descomposición prima de un número, digamos $n$, debemos ir tomando todos los números menores a $n$ y comprobando si estos lo dividen o no. En lo que sigue veremos el criterio de la raíz, que se utiliza para comprobar si un número es primo en menos pasos que la comprobación directa.

**Lema 3.4.4.** *Si $n > 0$ no es primo, entonces existe $m > 0$ tal que $m|n$ y $m \leqslant \sqrt{n}$.*

*Demostración.* Si $n$ no es primo, entonces $n = m_1 m_2$ con $1 < m_1, m_2 < n$. Supongamos que $m_1, m_2 > \sqrt{n}$, entonces $n = m_1 m_2 > \sqrt{n}\sqrt{n} = n$, lo cual es una contradicción. Por lo tanto, $m_1$ o $m_2$ debe ser menor o igual que $\sqrt{n}$ y por consiguiente encontramos un divisor de $n$ menor o igual a $\sqrt{n}$. □

**Proposición 3.4.5** (Criterio de la raíz)**.** *Sea* $n \geqslant 2$*. Si para todo* $m$ *tal que* $1 < m \leqslant \sqrt{n}$ *se cumple que* $m \nmid n$*, entonces* $n$ *es primo.*

*Demostración.* Supongamos que $n$ no es primo, luego, por el lema anterior, existe $m$ tal que $m|n$ y $1 < m \leqslant \sqrt{n}$ y esto contradice nuestras hipótesis. La contradicción se produce al suponer que $n$ no es primo, por lo tanto $n$ es primo. □

Este criterio reduce enormemente la cantidad de pruebas que debemos hacer para verificar si un número es primo.

*Ejemplo.* Verifiquemos si 467 es primo o no.

*Solución.* Observar primero que si no utilizamos el criterio de la raíz deberíamos hacer 465 divisiones: deberíamos comprobar si $m|467$ con $1 < m < 467$.

Como $\sqrt{467} < 22$, por el criterio de la raíz, sólo debemos comprobar si $m|467$ para $2 \leqslant m \leqslant 21$. Un sencilla comprobación (dividiendo) muestra que los números $2, 3, \cdots, 20, 21$ no dividen a 467 y por lo tanto 467 es primo. □

La facilidad con la que establecemos la existencia de la factorización de primos conlleva dos dificultades importantes. Primero el problema de encontrar los factores primos no es de ningún modo directo; y segundo no es obvio que exista una *única* factorización en primos para todo entero dado $n \geqslant 2$ . El siguiente resultado es un paso clave en la demostración de la unicidad.

**Teorema 3.4.6.** *Sea* $p$ *un número primo.*

*a) Si* $p|xy$ *entonces* $p|x$ *o* $p|y$*.*

*b)* $x_1, x_2, \ldots, x_n$ *son enteros tales que*

$$p|x_1x_2\ldots x_n$$

*entonces* $p|x_i$ *para algún* $x_i$ $(1 \leqslant i \leqslant n)$*.*

*Demostración.*

*a)* Si $p|x$ ya está probado el resultado. Si $p \nmid x$ entonces tenemos $\text{mcd}(x, p) = 1$. Por proposición 3.3.8, existen enteros $r$ y $s$ tales que $rp + sx = 1$. Por lo tanto tenemos

$$y = 1 \cdot y = (rp + sx)y = (ry)p + s(xy).$$

Como $p|p$ y $p|xy$, entonces divide a ambos términos y se sigue que $p|y$.

*b)* Usemos el principio de inducción. El resultado es obviamente verdadero cuando $n = 1$ (base inductiva).

Ahora, supongamos que el resultado es verdadero cuando $n = k$, es decir si $p|x_1x_2\dots x_k$, entonces $p|x_i$ para algún $i$ con $1 \leqslant i \leqslant k$ (hipótesis inductiva).

Debemos probar que si $p|x_1x_2\dots x_kx_{k+1}$, entonces $p|x_i$ para algún $x_i$ $(1 \leqslant i \leqslant k+1)$.

Supongamos $p|x_1x_2\dots x_kx_{k+1}$ y sea $x = x_1x_2\dots x_k$. Si $p|x$ entonces, por la hipótesis inductiva, $p|x_i$ para algún $x_i$ en el rango $1 \leqslant i \leqslant k$. Si $p \not| x$ entonces, por 1), se sigue que $p|x_{k+1}$. De este modo, en ambos casos $p$ divide uno de los $x_i$ $(1 \leqslant i \leqslant k+1)$. □

Un error común es asumir que el teorema 3.4.6 se mantiene verdadero cuando reemplazamos el primo $p$ por un entero arbitrario . Pero esto claramente falso: por ejemplo

$$6|3 \cdot 8 \quad \text{pero} \quad 6 \not| 3 \quad \text{y} \quad 6 \not| 8.$$

Ejemplos como éste nos ayudan a entender que el teorema 3.4.6 expresa una propiedad muy significativa de los números primos. Además veremos que esta propiedad juega un papel crucial en el siguiente resultado, que a veces es llamado el *Teorema Fundamental de la Aritmética*.

**Teorema 3.4.7.** *La factorización en primos de un entero positivo $n \geqslant 2$ es única, salvo el orden de los factores primos.*

*Demostración.* Por el axioma del buen orden, si existe un entero para el cual el teorema es falso, entonces hay un entero mínimo $n_0 \geqslant 0$ con esta propiedad. Supongamos entonces que

$$n_0 = p_1p_2\dots p_k \quad \text{y} \quad n_0 = p'_1p'_2\dots p'_l,$$

donde los $p_i$ $(1 \leqslant i \leqslant k)$ son primos, no necesariamente distintos, y los $p'_i$ $(1 \leqslant i \leqslant l)$ son primos, no necesariamente distintos. La primera ecuación implica que $p_1|n_0$, y la segunda ecuación implica que $p_1|p'_1p'_2\dots p'_l$. Por consiguiente por teorema 3.4.6 tenemos que $p_1|p'_j$ para algún $j$ $(1 \leqslant j \leqslant l)$. Reordenando la segunda factorización podemos asumir que $p_1|p'_1$, y puesto que $p_1$ y $p'_1$ son primos, se sigue que $p_1 = p'_1$ (observación 3.4.3-(3)). Luego por el axioma (**I7**), podemos cancelar los factores $p_1$ y $p'_1$, y obtener

$$p_2p_3\dots p_k = p'_2p'_3\dots p'_l,$$

y llamemos a esto $n_1$. Pero supusimos que $n_0$ tenía dos factorizaciones diferentes, y hemos cancelado el mismo número ($p_1 = p'_1$) en ambas factorizaciones, luego $n_1$ tiene también dos factorizaciones primas diferentes.

Esto contradice la definición de $n_0$ como el mínimo entero sin factorización única. Por lo tanto el teorema es verdadero para $n \geqslant 2$. □

En la práctica a menudo reunimos los primos iguales en la factorización de $n$ y escribimos

$$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r},$$

donde $p_1, p_2, \dots, p_r$ son primos distintos y $e_1, e_2, \dots, e_r$ son enteros positivos. Por ejemplo $7000 = 2^3 \cdot 5^3 \cdot 7$.

La unicidad de la factorización prima de cualquier entero mayor que 1 nos permite hacer la siguiente definición.

**Definición 3.4.8.** Se $n$ entero mayor o igual a 2 y

$$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r},$$

donde $p_i$ primo para todo $i$ ($1 \leqslant i \leqslant r$). Entonces, diremos que $p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ es la *factorización prima de* $n$ y que $p_i$ es un *factor primo de* $n$ ($1 \leqslant i \leqslant r$).

**Proposición 3.4.9.** *Sea $n$ entero mayor o igual a 2 y $p$ número primo. Entonces, $p|n$ si y solo si $p$ es un factor primo de $n$.*

*Demostración.* Si $n = q_1 q_2 \cdots q_s$ donde los $q_i$ son primos no necesariamente distintos. Como $p|n$, entonces $p|q_i$, para algún $i$ (teorema 3.4.6 *b)*), por lo tanto $p = q_i$ (observación 3.4.3 *b)*), es decir, $p$ es factor primo de $n$.

Recíprocamente, si en la factorización prima de $n$ participa $p$, es decir si $n = pp_1 \cdots p_k$, entonces $n = pm$ donde $m = p_1 \cdots p_k$. Por lo tanto, $p|n$. □

La factorización prima nos dice que los números primos son los "ladrillos" esenciales para "construir" los números enteros usando multiplicaciones. Ahora bien, podría ocurrir que haya un número finitos de ellos y que podamos escribir cada número como producto de primos en forma muy sintética. Pero este no es el caso.

**Proposición 3.4.10** (Teorema de Euclides)**.** *Existen infinitos números primos.*

*Demostración.* Haremos la demostración por el absurdo: supongamos que existen en total $r$ números primos $p_1, p_2, \dots, p_r$. Sea $n = p_1 p_2 \dots p_r + 1$. Sea $p$ primo tal que $p|n$. Como la lista de primos es exhaustiva, existe $i$ con $1 \leqslant i \leqslant r$ tal que $p = p_i$. Ahora bien $p_i|n$ y $p_i|p_1 p_2 \dots p_r$, luego $p_i|n - p_1 p_2 \dots p_r = 1$, lo cual es un absurdo que vino de suponer que el número de primos es finito. □

*Ejemplo.* Probemos que si $m$ y $n$ son enteros tales que $m \geqslant 2$ y $n \geqslant 2$, entonces $m^2 \neq 2n^2$.

*Demostración.* Supongamos que la factorización prima de $n$ contiene al 2 elevado a la $x$ (donde $x$ es cero si 2 no es factor primo de $n$). Entonces $n = 2^x h$, donde $h$ es producto de primos más grandes que 2, luego

$$2n^2 = 2(2^x h)^2 = 2^{2x+1} h^2.$$

Por lo tanto 2 está elevado a una potencia *impar* en la factorización prima de $2n^2$.

Por otro lado, si $m = 2^y g$, donde $g$ es producto de primos mayores que 2, entonces

$$m^2 = (2^y g)^2 = 2^{2y} g^2,$$

luego 2 está elevado a una potencia *par* (posiblemente cero) en la factorización prima de $m^2$. se sigue entonces que de ser $m^2 = 2n^2$ deberíamos tener dos factorizaciones primas diferentes del mismo número entero, contradiciendo al teorema 3.4.7. Entonces $m^2 \neq 2n^2$. □

Es claro que la conclusión del ejemplo vale también si nosotros permitimos que alguno de los enteros $m$ o $n$ valga 1. Luego podemos expresar el resultado diciendo que no hay enteros positivos $m$ y $n$ que cumplan

$$\left(\frac{m}{n}\right)^2 = 2$$

o equivalentemente, diciendo que la raíz cuadrada de 2 no puede ser expresada como una fracción $m/n$.

Una notación conveniente para nuestros propósitos será la siguiente: sean $m$ y $n$ dos enteros positivos, a veces es conveniente escribir la factorización prima de ambos números usando los mismos primos, y los primos que usamos son los que se encuentran en la factorización prima de ambos. Es decir escribimos

$$m = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}, \qquad n = p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}.$$

con $e_i, f_i \geqslant 0$ para $i = 1, \dots, r$ y $e_i$ o $f_i$ distinto de cero.

Veremos ahora un resultado que se puede deducir fácilmente del Teorema Fundamental de la Aritmética (TFA).

**Proposición 3.4.11.** *Sean* $m, n \geqslant 2$ *con*

$$m = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}, \qquad n = p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}.$$

*donde* $p_i$ *primo y* $e_i, f_i \geqslant 0$ *para* $i = 1, \dots, r$.

*Entonces* $m|n$ *si y sólo si* $e_i \leqslant f_i$ *para todo* $i$.

*Demostración.*

($\Rightarrow$) Por la descomposición de $m$ es claro que $p^{e_i}|m$. Como $m|n$ entonces $p^{e_i}|n$. Es decir $n = p^{e_i}u$. Es claro por TFA entonces que $e_i \leqslant f_i$.

($\Leftarrow$) Como $e_i \leqslant f_i$, tenemos que $p^{e_i}|p^{f_i}$, para $1 \leqslant i \leqslant r$. Luego

$$p_1^{e_1}p_2^{e_2}\dots p_r^{e_r}|p_1^{f_1}p_2^{f_2}\dots p_r^{f_r}.$$

Es decir $m|n$. □

**Corolario 3.4.12.** *Sea $n \geqslant 2$ y $p$ un número primo, entonces $p|n$ si y solo si $p$ es un factor primo de $n$.* □

Ahora veremos que es posible calcular el mcd y el mcm de un par de números sabiendo sus descomposiciones primas.

**Proposición 3.4.13.** *Sean $m$ y $n$ enteros positivos cuyas factorizaciones primas son*

$$m = p_1^{e_1}p_2^{e_2}\dots p_r^{e_r}, \qquad n = p_1^{f_1}p_2^{f_2}\dots p_r^{f_r}.$$

*a) El mcd de $m$ y $n$ es $d = p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}$ donde, para cada $i$ en el rango $1 \leqslant i \leqslant r$, $k_i$ es el mínimo entre $e_i$ y $f_i$.*

*b) El mcm de $m$ y $n$ es $u = p_1^{h_1}p_2^{h_2}\dots p_r^{h_r}$ donde, para cada $i$ en el rango $1 \leqslant i \leqslant r$, $h_i$ es el máximo entre $e_i$ y $f_i$.*

*Demostración.*

*a)* Sea $c$ tal que $c|n$ y $c|m$, entonces los primos que intervienen en la factorización de $c$ son $p_1, \dots, p_r$ y por lo tanto $c = p_1^{t_1}p_2^{t_2}\dots p_r^{t_r}$. Además, como $c|n$ y $c|m$ tenemos que $t_i \leqslant e_i, f_i$ y por lo tanto $t_i \leqslant k_i = \min(e_i, f_i)$. De esto se deduce que $c|p_1^{k_1}p_2^{k_2}\dots p_r^{k_r} = d$. Por otro lado, es claro que $p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}$ divide a $m$ y $n$ y se deduce el resultado.

*b)* Se deja como ejercicio. □

*Observación.* La proposición anterior nos puede llevar a pensar que una forma sencilla de encontrar el mcd y mcm es usando la descomposición en factores primos de los números involucrados. Esto, en general, no es así para números grandes: no hay un método eficiente para encontrar la descomposición prima de un número grande. Esencialmente, el mejor método para encontrar un divisor de un número grande es el criterio de la raíz, es decir probando si algún número menor que la raíz del número original lo divide. El criterio de la raíz baja el número de comprobaciones de $n$ a $\sqrt{n}$ y eso no ayuda mucho cuando $n$ es grande.

Ahora bien, ¿qué es un "número grande"? En la actualidad, por ejemplo, con todos los recursos computacionales de que se disponen, no es posible factorizar números de 200 dígitos o más. Por lo tanto, no podríamos encontrar el mcd de dos números de 200 dígitos o más a partir de la factorización prima de ambos. Sin embargo, con el algoritmo de Euclides el mcd de estos números se obtendría en pocos segundos.

*Ejemplo.* Encontremos el mcd y el mcm de 825 y 385 utilizando las factorizaciones primas de ambos.

*Solución.* Como $825 = 3 \cdot 5^2 \cdot 11$ y $385 = 5 \cdot 7 \cdot 11$, tenemos que

$$\mathrm{mcd}(825, 385) = 5 \cdot 11 = 55, \qquad \mathrm{mcm}(825, 385) = 3 \cdot 5^2 \cdot 7 \cdot 11 = 5775.$$

□

§ *Ejercicios*

1) Sean $m, n$ enteros con $m, n \geqslant 2$. Probar que, $m$ y $n$ son coprimos si y sólo si no comparten ningún primo en la factorización.

   En otras palabras, sean

   $$m = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}, \qquad n = q_1^{f_1} q_2^{f_2} \dots q_s^{f_s},$$

   las descomposiciones primas de $m$ y $n$ con $e_i, f_j > 0$. Entonces $\mathrm{mcd}(m, n) = 1$ si y sólo si con $p_i \neq q_j$ para todos los $i, j$.

2) Probar que si $m$ y $n$ son enteros positivos, tales que $m \geqslant 2$ y $n \geqslant 2$, y $m^2 = kn^2$, entonces $k$ es el cuadrado de un entero.

3) Usar la identidad

   $$2^{rs} - 1 = (2^r - 1)(2^{(s-1)r} + 2^{(s-2)r} + \dots + 2^r + 1)$$

   para probar que si $2^n - 1$ es primo, entonces $n$ es primo.

4) Encontrar el mínimo $n$ para el cual la recíproca del ejercicio anterior es falsa: esto es, $n$ es primo pero $2^n - 1$ no lo es.

5) Para $n \in \mathbb{N}$ sea $q_n$ el factor primo más pequeño de $n! + 1$.

   *a)* Probar que $q_n > n$.

   *b)* Probar, usando el resultado del item anterior, que existen infinitos números primos (demostración de Hermite).

# 4

# ARITMÉTICA MODULAR

## 4.1 CONGRUENCIAS

Una de las más familiares particiones de un conjunto es la partición de $\mathbb{Z}$ en enteros pares y enteros impares. Es decir $\mathbb{Z}$ es la unión disjunta del conjunto de números pares y el de los números impares. Es claro que dos números $a, b$ tienen la misma paridad si $a - b$ es divisible por 2. Para expresar este hecho es usual la notación

$$a \equiv b \pmod{2}$$

y se dice que $a$ es *congruente* a $b$ *módulo* 2. Es decir $a$ y $b$ son ambos pares o ambos impares si y solo si $a$ es congruente a $b$ módulo 2.

Claramente esta definición se puede extender a cualquier entero positivo $m$.

**Definición 4.1.1.** Sean $a$ y $b$ enteros y $m$ un entero positivo. Diremos que $a$ es *congruente* a $b$ *módulo* $m$, y escribimos

$$a \equiv b \pmod{m}$$

si $a - b$ es divisible por $m$, o, escrito de otra forma, $m|a - b$.

Observar que $a \equiv 0 \pmod{m}$ si y sólo si $m|a$ y que $a \equiv b \pmod{m}$ si y sólo si $a - b \equiv 0 \pmod{m}$.

*Notación.* $a \equiv b \pmod{m}$ también lo denotamos $a \equiv b\ (m)$.

*Ejemplo.* Algunos ejemplos numéricos:

- $7 \equiv 3\ (2)$, pues $2|7 - 3 = 4$.
- $17 \equiv 8\ (3)$, pues $3|17 - 8 = 9$.
- $8 \equiv 17\ (3)$, pues $3|8 - 17 = -9$.
- $35 \equiv 13\ (11)$, pues $11|35 - 13 = 22 = 2 \cdot 11$.

**Proposición 4.1.2.** *Sean $a$ entero y $m$ un entero positivo. Sea $r$ el resto de dividir $a$ por $m$, entonces*

$$a \equiv r \pmod{m}.$$

*Demostración.* $a = mq + r$ con $0 \leqslant r < m$. Luego,

$$a - r = mq \quad \Rightarrow \quad m|a - r \quad \Rightarrow \quad a \equiv r \pmod{m}.$$

□

Es fácil verificar que la congruencia módulo $m$ es una relación de equivalencia.

**Proposición 4.1.3.** *Sea $m$ entero positivo y $x, y, z \in \mathbb{Z}$. Entonces la relación de congruencia es*

*a) reflexiva, es decir* $x \equiv x \pmod{m}$,

*b) simétrica, es decir si* $x \equiv y \pmod{m}$, *entonces* $y \equiv x \pmod{m}$, *y*

*c) transitiva, es decir si* $x \equiv y \pmod{m}$ *e* $y \equiv z \pmod{m}$, *entonces* $x \equiv z \pmod{m}$.

*Demostración.* Las tres propiedades son sencillas de demostrar y se deducen de propiedades de "divide a".

*a)* $m|x - x = 0$ y por lo tanto $x \equiv x \pmod{m}$.

*b)* $x \equiv y\ (m) \Rightarrow m|x - y \Rightarrow m|-(x - y) \Rightarrow m|y - x \Rightarrow y \equiv x\ (m)$.

*c)* $x \equiv y\ (m) \wedge y \equiv z\ (m) \quad \Rightarrow \quad m|x - y \wedge m|y - z \quad \Rightarrow$

$m|(x - y) + (y - z) = x - z \quad \Rightarrow \quad x \equiv z\ (m)$.

□ □

*Observación.* Dado un conjunto $X$ una relación que cumple las propiedades de ser reflexiva, simétrica y transitiva es llamada una *relación de equivalencia*.

Ejemplos de relación de equivalencia son la igualdad y el paralelismo de rectas. Veremos otra relación de equivalencia en el capítulo de grafos.

Por la proposición 4.1.2 y por ser "congruencia módulo $m$" una relación de equivalencia se deduce el siguiente resultado.

**Proposición 4.1.4.** *Sean $a$ y $b$ enteros y $m$ un entero positivo. Entonces* $a \equiv b \pmod{m}$ *si y sólo si $a$ y $b$ tienen el mismo resto en la división por $m$.*

*Demostración.* ($\Rightarrow$) Si $a = mh + r$ y $b = mk + s$, con $0 \leqslant r, s < m$, entonces por la proposición 4.1.2 tenemos que

$$a \equiv r \pmod{m} \quad \wedge \quad b \equiv s \pmod{m}.$$

Por la propiedad transitiva de "congruencia módulo $m$", $r \equiv s \pmod{m}$, luego $m|r-s$. Podemos suponer, sin perdida de generalidad, que $s \leqslant r$, luego $0 \leqslant r-s < m$, lo cual implica que $r-s=0$, es decir $r=s$.

($\Leftarrow$) Si $a$ y $b$ tienen el mismo resto en la división por $m$, entonces $a = mh+r$ y $b = mk+r$, luego $a-b = m(h-k)$ que es divisible por $m$. □

Así como antes podíamos separar $\mathbb{Z}$ en los números pares e impares, la propiedad anterior nos permite expresar $\mathbb{Z}$ como una unión disjunta de $m$ subconjuntos. Es decir sea $\mathbb{Z}_{[r]} = \{x \in \mathbb{Z} : \text{el resto de dividir } x \text{ por } m \text{ es } r\}$, o más formalmente

$$\mathbb{Z}_{[r]} = \{x \in \mathbb{Z} : \ x \equiv r \pmod{m}\}, \qquad 0 \leqslant r < m.$$

Entonces,

$$\mathbb{Z} = \mathbb{Z}_{[0]} \cup \mathbb{Z}_{[1]} \cup \cdots \cup \mathbb{Z}_{[m-1]}.$$

La utilidad de las congruencias reside principalmente en el hecho de que son compatibles con las operaciones aritméticas. Específicamente, tenemos el siguiente teorema.

**Teorema 4.1.5.** *Sea $m$ un entero positivo y sean $x_1$, $x_2$, $y_1$, $y_2$ enteros tales que*

$$x_1 \equiv x_2 \pmod{m}, \qquad y_1 \equiv y_2 \pmod{m}.$$

*Entonces*

*a)* $x_1 + y_1 \equiv x_2 + y_2 \pmod{m}$,

*b)* $x_1 y_1 \equiv x_2 y_2 \pmod{m}$,

*c) Si* $x \equiv y \pmod{m}$ *y* $j \in \mathbb{N}$, *entonces* $x^j \equiv y^j \pmod{m}$.

*Demostración.* La hipótesis nos dice que

$$m|x_1 - x_2 \qquad \wedge \qquad m|y_1 - y_2.$$

*a)* Como $m|x_1 - x_2$ y $m|y_1 - y_2$, entonces

$$m|(x_1 - x_2) + (y_1 - y_2) = (x_1 + y_1) - (x_2 + y_2).$$

Es decir, $x_1 + y_1 \equiv x_2 + y_2 \pmod{m}$.

*b)* Aquí tenemos,

$$\begin{aligned} m|x_1 - x_2 \wedge m|y_1 - y_2 &\Rightarrow m|(x_1 - x_2)y_1 \wedge m|x_2(y_1 - y_2) \\ &\Rightarrow m|(x_1 - x_2)y_1 + x_2(y_1 - y_2) \\ &\Rightarrow m|x_1 y_1 - x_2 y_1 + x_2 y_1 - x_2 y_2 \\ &\Rightarrow m|x_1 y_1 - x_2 y_2. \end{aligned}$$

Luego $x_1y_1 \equiv x_2y_2 \pmod{m}$.

*c)* Lo haremos por inducción sobre $j$.

Es claro que si $j = 1$ el resultado es verdadero. Supongamos ahora que el resultado vale para $j-1$, es decir que si $x \equiv y \pmod{m}$, entonces

$$x^{j-1} \equiv y^{j-1} \pmod{m}.$$

Como $x \equiv y \pmod{m}$, por (b) tenemos que

$$x^{j-1}x \equiv y^{j-1}y \pmod{m},$$

es decir

$$x^j \equiv y^j \pmod{m}.$$

□

Veremos ahora una aplicación interesante de las congruencias y sus propiedades.

**Proposición 4.1.6.** *Sea* $(x_nx_{n-1}\dots x_0)_{10}$ *la representación del entero positivo* $x$ *en base* 10*, entonces*

$$x \equiv x_0 + x_1 + \cdots + x_n \pmod{9}$$

*Demostración.* Observemos primero que como $10 \equiv 1 \pmod{9}$, entonces $10^k \equiv 1^k \equiv 1 \pmod{9}$. Esto es debido al teorema 4.1.5 *c)*

Por la definición de representación en base 10, tenemos que

$$x = x_0 + 10x_1 + \cdots + 10^n x_n,$$

por el párrafo anterior y teorema 4.1.5 *b)* obtenemos que $x_k10^k \equiv x_k \pmod{9}$ y por teorema 4.1.5 *a)* se deduce que $x \equiv x_0 + x_1 + \cdots + x_n \pmod{9}$. □

**Corolario 4.1.7.** *ea* $(x_nx_{n-1}\dots x_0)_{10}$ *la representación del entero positivo* $x$ *en base* 10*, entonces* $x$ *es divisible por 9 si y solo si* $x_0 + x_1 + \cdots + x_n$ *es divisible por 9.*

*Demostración.*

$$\begin{aligned} 9|x &\Leftrightarrow 0 \equiv x \pmod{9} \\ &\Leftrightarrow 0 \equiv x_0 + x_1 + \cdots + x_n \pmod{9} \quad \text{(prop. 4.1.6 y transitividad)} \\ &\Leftrightarrow 9|x_0 + x_1 + \cdots + x_n. \end{aligned}$$

□

El procedimiento anterior a veces es llamado *regla del nueve.*

*Ejemplo.* Usando la regla del 9 es sencillo verificar que $X = 3475682568$ es divisible por 9, pues

$$3+4+7+5+6+8+2+5+6+8 = 54$$

y como $5+4 = 9$ es divisible por 9, también lo es 54 y, luego, también lo es $x$.

También la proposición 4.1.6 es útil para verificar si una multiplicación larga es incorrecta.

*Ejemplo.* Verifiquemos el siguiente cálculo

$$54\,321 \cdot 98\,765 = 5\,363\,013\,565.$$

*Demostración.* En la notación de la proposición 4.1.6 escribamos $\Sigma\, x$ en vez de

$$\sum_{i=0}^{n} x_i = x_0 + x_1 + \cdots + x_n.$$

Hemos visto que $\Sigma\, x \equiv x \pmod 9$. Por la parte *b)* del teorema 4.1.5 tenemos

$$\Sigma\, x \cdot \Sigma\, y \equiv xy \pmod 9,$$

y por consiguiente si $xy = z$ debemos tener $\Sigma\, x \cdot \Sigma\, y \equiv \Sigma\, z \pmod 9$. En el cálculo que se tiene en el ejemplo

$$\Sigma\, 54\,321 = 15, \quad \Sigma\, 98\,765 = 35, \qquad \Sigma\, 5\,363\,013\,565 = 37,$$

y

$$\Sigma\, 15 = 6, \qquad \Sigma\, 35 = 8, \quad \Sigma\, 37 = 10.$$

Puesto que $6 \cdot 8$ no es congruente a $10 \pmod 9$ se sigue que $15 \cdot 35$ no es congruente a $37 \pmod 9$ y que $54\,321 \cdot 98\,765$ no es congruente a $5\,363\,013\,565 \pmod 9$. En consecuencia el cálculo está errado. □

También a este verificación suele llamársela la regla del 9. Observar que esta última aplicación solo sirve para comprobar que una multiplicación es incorrecta, y no es útil para verificar que una multiplicación es correcta, pues $xy \equiv z \pmod 9$ no garantiza que $xy = z$.

§ *Ejercicios*

1) Sin hacer ninguna "multiplicación larga" probar que

*a)* $1\,234\,567 \cdot 90\,123 \equiv 1 \pmod{10}$

*b)* $2\,468 \cdot 13\,579 \equiv -3 \pmod{25}$

2) Usar la regla del nueve para verificar que dos de las siguientes ecuaciones son falsas. ¿Qué se puede decir de la otra ecuación?

*a)* $5\,783 \cdot 40\,162 = 233\,256\,846$,

*b)* $9\,787 \cdot 1\,258 = 12\,342\,046$,

*c)* $8\,901 \cdot 5\,743 = 52\,018\,443$.

3) Encontrar el resto de dividir $3^{15}$ por 17 y el de dividir $15^{81}$ por 13.

4) Sea $(x_n x_{n-1} \dots x_0)_{10}$ la representación en base 10 de un entero positivo $x$.

*a)* Probar que

$$x \equiv x_0 - x_1 + x_2 + \cdots + (-1)^n x_n \pmod{11}.$$

*b)* Enuncie la *regla del* 11.

*c)* Probar que $1\,213\,141\,516\,171\,819$ es divisible por 11.

5) ¿Cuál es el último dígito de la representación en base 10 de $7^{93}$.

6) Usar que $1\,001 = 7 \cdot 11 \cdot 13$ para construir una prueba para la división simultanea por los números 7, 11 y 13, similar a la prueba del 9.

7) Si $m$ coprimo con $n$, entonces $ma \equiv mb \pmod{n}$ si y solo si $a \equiv b \pmod{m}$.

## 4.2 ECUACIÓN LINEAL DE CONGRUENCIA

Se trata primero de estudiar en general el problema de resolución de la ecuación en $x$

$$ax \equiv b \pmod{m}. \tag{4.2.1}$$

Es fácil ver que el problema no admite siempre solución, por ejemplo $2x \equiv 3 \pmod{2}$ no posee ninguna solución en $\mathbb{Z}$, pues cualquiera se $k \in \mathbb{Z}$, $2k - 3$ es impar, luego no es divisible por 2.

Notemos además que si $x_0$ es solución de la ecuación (4.2.1), también lo es $x_0 + km$ de manera que si la ecuación posee una solución, posee infinitas soluciones. Para evitar la ambigüedad de infinitas soluciones, nos limitaremos a considerar las soluciones tales que $0 \leqslant x < m$.

*Ejemplo.* La solución general de la ecuación $3x \equiv 7 \pmod{11}$ es $6 + k7$ con $k \in \mathbb{Z}$.

*Demostración.* Si probamos con los enteros $x$ tal que $0 \leqslant x < 11$, veremos que la ecuación admite una única solución, a saber $x = 6$. Otras soluciones se obtienen tomando $6 + 11k$. Por otra parte si $u$ es también solución de la ecuación, se tiene $3u \equiv 3 \cdot 6 \pmod{11}$, por lo tanto $3(u-6)$ es múltiplo de 11. Como 11 no divide a 3 se tiene que $11|(u-6)$, o sea $u = 6 + 11k$. □

Analicemos ahora la situación general de la ecuación $ax \equiv b \pmod{m}$. Si $\mathrm{mcd}(a, m) = 1$, entonces sabemos que existen enteros $r$ y $s$ tales que $1 = ra + sm$ y por lo tanto $b = (rb)a + (sb)m$, o sea que

$$a(rb) \equiv b \pmod{m},$$

es decir $rb$ es solución de la ecuación. Veremos que el caso general se hace en forma análoga a lo anterior.

**Teorema 4.2.1.** *Sean $a, b$ números enteros y $m$ un entero positivo y denotemos $d = \mathrm{mcd}(a, m)$. La ecuación*

$$ax \equiv b \pmod{m} \tag{4.2.2}$$

*admite solución si y sólo si $d|b$, y en este caso dada $x_0$ una solución, todas las soluciones son de la forma*

$$x = x_0 + kn, \qquad \text{con } k \in \mathbb{Z} \text{ y } n = \frac{m}{d}$$

*Demostración.* Como $d = \mathrm{mcd}(a, m)$, existen $r, s \in \mathbb{Z}$ tales que

$$d = ra + sm.$$

Si $d|b$, entonces existe $h \in \mathbb{Z}$ tal que $b = dh$. Si multiplicamos por $h$ la ecuación de arriba obtenemos

$$dh = (rh)a + (sh)m.$$

Luego $a(rh) \equiv a(rh) + (sh)m \equiv dh \equiv b \pmod{m}$, y por lo tanto $rh$ es solución de la ecuación lineal de congruencia.

Por otro lado si $ax \equiv b \pmod{m}$, entonces $ax - b = km$ para algún $k$, o sea

$$b = ax + (-k)m$$

de la cual se sigue que si $d|a$ y $d|m$, entonces $d|b$ y por lo tanto $\mathrm{mcd}(a, m)|b$.

Por lo tanto hemos demostrado que la condición necesaria y suficiente para que la ecuación $ax \equiv b \pmod{m}$ admita una solución es que $\mathrm{mcd}(a, m)|b$.

En el caso que $d|b$ veamos ahora cuales son todas las soluciones posibles de la ecuación (4.2.2). Sean $x_1, x_2$ soluciones, es decir

$$\begin{aligned} ax_1 &\equiv b \pmod{m} \\ ax_2 &\equiv b \pmod{m}, \end{aligned}$$

entonces, restando miembro a miembro, obtenemos

$$ax_1 - ax_2 \equiv b - b \equiv 0 \pmod{m}.$$

Es decir, $x_1, x_2$ son soluciones de la ecuación (4.2.2) si y sólo si $y = x_1 - x_2$ es solución de la ecuación lineal de congruencia

$$ay \equiv 0 \pmod{m}.$$

Si $\mathrm{mcd}(a, m) = 1$ es claro que la ecuación $ay \equiv 0 \pmod{m}$ tiene como solución todos los $y$ tales que $m|ay$. Como $m$ y $a$ son coprimos, las soluciones son todos los $y$ tal $m|y$, es decir todos los múltiplos de $m$.

Si $\mathrm{mcd}(a, m) = d > 1$, la ecuación $ay \equiv 0 \pmod{m}$ tiene como solución todos los $y$ tales que $ay = mk$ para algún $k$. Si dividimos por $d$, podemos decir que las soluciones son todos los $y$ tales que $(a/d)y = (m/d)k$, es decir todos los $y$ tal que $(m/d)|(a/d)y$. Como $m/d$ y $a/d$ son coprimos, las soluciones son todos los múltiplos de $m/d$.

Sean $x_0$ y $x$ tal que $ax_0 \equiv b \pmod{m}$ y $ax \equiv b \pmod{m}$, entonces $a(x_0 - x) \equiv 0 \pmod{m}$ y por lo tanto $x_0 - x = kn$ para algún $k$. Es decir, cualquier $x$ que es solución lineal de congruencia es de la forma $x_0 = x + kn$ para algún $k$. □

De las demostraciones podemos obtener un método general para encontrar soluciones de la ecuación lineal de congruencia

$$ax \equiv b \pmod{m}.$$

con $\mathrm{mcd}(a, m)|b$

*a)* Encontrar, usando el algoritmo de Euclides, $r, s$ tales que

$$d = \mathrm{mcd}(a, m) = ra + sm. \tag{4.2.3}$$

*b)* Como $d|b$, tenemos que $b = td$ y multiplicamos la ecuación (4.2.3) por $t$:

$$dt = (rt)a + (st)m.$$

*c)* $b = dt = (rt)a + (st)m \equiv (rt)a \pmod{m}$.

Luego $x_0 = rt$ es solución de la ecuación lineal de congruencia.

*d)* Toda solución de la ecuación lineal de congruencia es $x = x_0 + k(m/d)$ con $k \in \mathbb{Z}$.

Observemos que, en las hipótesis del teorema, si $\text{mcd}(a, m) = 1$, entonces siempre existen soluciones a la ecuación $ax \equiv b \pmod{m}$ y todas las soluciones son de la forma $x_0 + km$, donde $x_0$ es una solución particular. Más aún, debido a esto, hay una única solución $x$, con $0 \leqslant x < m$.

*Ejemplo.* Hallemos las soluciones de la ecuación $13x \equiv 7 \pmod{15}$ con $0 \leqslant x < 15$.

*Demostración.* Hagamos, paso a paso, el procedimiento explicado anteriormente.

*a)* Usando el algoritmo de Euclides obtenemos el $\text{mcd}(13, 15)$.

$$\begin{aligned} 15 &= 13 \cdot 1 + 2 \\ 13 &= 2 \cdot 6 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

Luego $1 = \text{mcd}(13, 15)$. Como 1 divide a cualquier número, en este caso la ecuación tiene solución. Del algoritmo de Euclides deducimos

$$\begin{aligned} 1 &= 13 - 2 \cdot 6 \\ &= 13 - (15 - 13) \cdot 6 \\ &= 13 \cdot 7 - 15 \cdot 6. \end{aligned}$$

Es decir

$$1 = 13 \cdot 7 - 15 \cdot 6. \tag{4.2.4}$$

*b)* Multiplicando la ecuación (4.2.4) por 7 obtenemos

$$7 = 13 \cdot 49 - 15 \cdot 42.$$

*c)* Luego $13 \cdot 49 \equiv 7 \pmod{15}$, es decir 49 es solución de la ecuación.

*d)* Todas las soluciones son de la forma $x = 49 + 15k$.

Debemos ver ahora cuales soluciones $x$ cumplen $0 \leqslant x < 15$. La forma más sencilla de hacerlo es buscando por tanteo: $49 + 15(-1) = 34$, $49 + 15(-2) = 19$, , $49 + 15(-3) = 4$, $49 + 15(-4) = -11$. Es decir la solución que buscamos es $x = 4$. □

*Ejemplo.* Hallemos las soluciones de la ecuación $42x \equiv 50 \pmod{76}$ con $0 \leqslant x < 76$.

*Demostración.* Como antes, hagamos paso a paso el procedimiento explicado anteriormente.

*a)* Usando el algoritmo de Euclides obtenemos el $\mcd(42,76)$.

$$\begin{aligned} 76 &= 42\cdot 1 + 34\\ 42 &= 34\cdot 1 + 8\\ 34 &= 8\cdot 4 + 2\\ 8 &= 2\cdot 4 + 0. \end{aligned}$$

Luego $2 = \mcd(42,76)$. Como $2|50$ la ecuación tiene solución. Del algoritmo de Euclides deducimos

$$\begin{aligned} 2 &= 34 - 8\cdot 4\\ &= 34 - (42-34)\cdot 4 = 34\cdot 5 - 42\cdot 4\\ &= (76-42)\cdot 5 - 42\cdot 4\\ &= 76\cdot 5 - 42\cdot 9. \end{aligned}$$

Es decir

$$2 = (-9)\cdot 42 + 5\cdot 76.$$

*b)* $50 = 2\cdot 25$ y tenemos que

$$\begin{aligned} 50 &= (-9\cdot 25)\cdot 42 + (5\cdot 25)\cdot 76\\ 50 &= (-225)\cdot 42 + 125\cdot 76 \end{aligned}$$

*c)* Luego $x_0 = -225$ es una solución de la ecuación lineal de congruencia.

*d)* Todas las soluciones son de la forma $-225 + (76/2)k$, es decir $x = -225 + 38k$.

Debemos ver ahora cuales soluciones $x$ cumplen $0 \leqslant x < 76$. Como en el caso anterior podemos hacer esto por tanteo, pero aquí la forma más sencilla de hacerlo es escribir las inecuaciones

$$\begin{aligned} 0 &\leqslant -225 + 38k < 76\\ 225 &\leqslant 38k < 76 + 225 = 301\\ 225/38 &\leqslant k \leqslant 301/38\\ 5.9 &\leqslant k \leqslant 7.9 \end{aligned}$$

Luego $k = 6$ o $k = 7$ y entonces $x_1 = -225 + 38\cdot 6 = 3$ y $x_2 = -225 + 38\cdot 7 = 41$ son las soluciones que buscamos. □

Operativamente es útil el siguiente resultado.

**Proposición 4.2.2.** *Sean* $a, b$ *números enteros y* $m$ *un entero positivo, denotemos* $d = \mathrm{mcd}(a, m)$ *y supongamos que* $d|b$. *Entonces las soluciones de la ecuación*

$$ax \equiv b \pmod{m}$$

*son las misma que las de la ecuación*

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

*Demostración.* $x_0$ cumple que $ax_0 \equiv b \pmod{m}$ si y solo si $m|ax_0 - b$, es decir, si y solo si existe $q \in \mathbb{Z}$ tal que $ax_0 - b = mq$. Si dividimos por $d$ la ecuación $ax_0 - b = mq$, obtenemos $\frac{a}{d}x_0 - \frac{b}{d} = \frac{m}{d}q$ y esto vale si y solo si $\frac{a}{d}x_0 \equiv \frac{b}{d} \pmod{\frac{m}{d}}$. □

*Observación.* Sean $a, b$ números enteros y $m$ un entero positivo, denotemos $d = \mathrm{mcd}(a, m)$ y supongamos que $d|b$. Entonces es fácil ver que

$$\mathrm{mcd}(\frac{a}{d}, \frac{m}{d}) = 1,$$

Lo cual implica, por la proposición anterior, que encontrar las soluciones de la ecuación lineal de congruencia se puede reducir al caso que $\mathrm{mcd}(a, b) = 1$.

*Ejemplo.* Hallemos las soluciones de la ecuación $21x \equiv 48 \pmod{114}$ con $0 \leqslant x \leqslant 1000$.

*Demostración.* Los divisores de 21 son 3 y 7, $3|114$ y $7 \not| 114$, por lo tanto $\mathrm{mcd}(21, 114) = 3$. Por la proposición 4.2.2, dividimos por 3 la ecuación y tenemos que el problema original es equivalente a encontrar todos los $x$ tal que

$$7x \equiv 12 \pmod{38} \quad \text{tal que} \quad 0 \leqslant x \leqslant 1000.$$

Ahora bien, usando el algoritmo de Euclides, obtenemos el $\mathrm{mcd}(7, 38)$:

$$\begin{aligned} 38 &= 7 \cdot 5 + 3 \quad \Rightarrow \quad 3 = 38 - 7 \cdot 5 \\ 7 &= 3 \cdot 2 + 1 \quad \Rightarrow \quad 1 = 7 - 3 \cdot 2 \qquad (*) \\ 3 &= 1 \cdot 3 + 0. \end{aligned}$$

Luego $1 = \mathrm{mcd}(7, 38)$ y de (*) deducimos

$$\begin{aligned} 1 &= 7 - 3 \cdot 2 \\ &= 7 - (38 - 7 \cdot 5) \cdot 2 \\ &= 7 + (-2) \cdot 38 + 10 \cdot 7 \\ &= 11 \cdot 7 + (-2) \cdot 38. \end{aligned}$$

Por lo tanto

$$1 \equiv 11 \cdot 7 \pmod{38},$$

o equivalentemente,

$$7 \cdot 11 \equiv 1 \pmod{38}.$$

Si multiplicamos por 12 la ecuación obtenemos:

$$7 \cdot (11 \cdot 12) \equiv 12 \pmod{38}.$$

Por lo tanto, $x_0 = 11 \cdot 12 = 132$ es solución de la ecuación original.

Como $\mcd(7, 38) = 1$, por el teorema 4.2.1 deducimos que todas las soluciones de la ecuación $7x \equiv 12 \pmod{38}$ son de la forma $x = x_0 + 38k$ donde $k \in \mathbb{Z}$.

Debemos ver ahora cuales soluciones $x$ cumplen $0 \leqslant x \leqslant 1000$. Lo haremos escribiendo las inecuaciones:

$$\begin{aligned} 0 &\leqslant 132 + 38k \leqslant 1000 \\ -132 &\leqslant 38k \leqslant 1000 - 132 = 868 \\ -\frac{132}{38} &\leqslant k \leqslant \frac{868}{38} \\ -3.4 &\leqslant k \leqslant 22.8 \end{aligned}$$

Luego $-4 \leqslant k \leqslant 22$, es decir $k$ recorre todos los valores enteros desde $-4$ a $22$.

Concluyendo: los $x$ tales que $21x \equiv 48 \pmod{114}$ y $0 \leqslant x \leqslant 1000$ son los $x = 132 + 38k$ donde $k \in \mathbb{Z}$ y $-4 \leqslant k \leqslant 22$. □

§ *Ejercicios*

1) Resolver las siguientes ecuaciones lineales de congruencia

   *a)* $2x \equiv 1 \pmod{7}$.

   *b)* $3\,970\,x \equiv 560 \pmod{2755}$.

2) Determinar todas las posibles soluciones de las congruencias

   *a)* $5x \equiv 1 \pmod{11}$,

   *b)* $5x \equiv 7 \pmod{15}$.

3) Sea $m$ un número entero $\geqslant 2$ y sea

$$\mathbb{Z}_m := \{0, 1, \ldots, m-1\}$$

el conjunto de restos de dividir por $m$. En $\mathbb{Z}_m$ definimos suma y producto de la siguiente manera: sean $a, b \in \mathbb{Z}_m$, entonces

$$\begin{array}{lll} a+b & = c & \text{si} \quad a+b \equiv c \pmod{m} \quad \wedge \quad 0 \leqslant c \leqslant m-1, \\ a \cdot b & = d & \text{si} \quad a \cdot b \equiv d \pmod{m} \quad \wedge \quad 0 \leqslant d \leqslant m-1. \end{array}$$

*a)* Probar que $\mathbb{Z}_m$ es un *anillo conmutativo con unidad*, es decir se cumplen los axiomas **I1**,...,**I6** de la sección 1.1 (cambiando $\mathbb{Z}$ por $\mathbb{Z}_m$).

*b)* Probar que si $p$ es un número primo, entonces $\mathbb{Z}_p$ es *cuerpo*, es decir se cumplen los axiomas **I1**,...,**I6** de la sección 1.1 y además, para todo $a \in \mathbb{Z}_p$, $a \neq 0$, existe un único $b \in \mathbb{Z}_p$ tal que $ab = 1$ [Ayuda: usar la ecuación lineal de congruencia].

4) Sea $p$ número entero positivo.

*a)* (Teorema de Wilson). Probar que si $p$ es un número primo, entonces

$$(p-1)! \equiv -1 \pmod{p}.$$

[Ayuda: $1 \cdot (p-1) \equiv -1 \pmod{p}$ y debido al ejercicio 3 *b)* los números $2, \ldots, p-2$ se pueden ordenar de a pares $m_1, m_2$ tal que $m_1 m_2 \equiv 1 \pmod{p}$].

*b)* Probar que si $(p-1)! \equiv -1 \pmod{p}$, entonces $p$ es un número primo. [Ayuda: probar el contrarrecíproco y usar el hecho que si $p$ es compuesto existe $m$ con $1 < m < p$ y tal que $m|p$].

## 4.3 TEOREMA DE FERMAT

El siguiente lema nos sirve de preparación para la demostración del Teorema (o fórmula) de Fermat.

**Lema 4.3.1.** *Sea $p$ un número primo, entonces*

*a)* $p \left| \binom{p}{r} \right.$, *con* $0 < r < p$,

*b)* $(a+b)^p \equiv a^p + b^p \pmod{p}$.

*Demostración.*

*a)* Escribamos el número binomial de otra forma:

$$\binom{p}{r} = \frac{p!}{r!(p-r)!} = p \cdot \frac{(p-1)!}{r!(p-r)!}$$

es un número entero, digamos $k$, luego

$$k \cdot r!(p-r)! = p \cdot (p-1)! \tag{4.3.1}$$

Como $p-1$, $r$ y $p-r$ son menores que $p$, entonces $(p-1)!$, $r!$ y $(p-r)!$ son producto de números menores que $p$ y por lo tanto son producto de primos menores que $p$. Por lo tanto, el primo $p$ no aparece en la descomposición prima de $(p-1)!$, $r!$ y $(p-r)!$. Por la igualdad de la ecuación (4.3.1), $p$ debe ser factor de $k = \binom{p}{r}$, luego $p|\binom{p}{r}$.

*b)* Por el teorema del binomio (teorema 2.5.1) sabemos que

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}.$$

Por *a)* es claro que $\binom{p}{i} a^i b^{p-i} \equiv 0 \pmod{p}$, si $0 < i < p$. Luego se deduce el resultado. □

El siguiente es el llamado teorema de Fermat o teorema pequeño de Fermat.

**Teorema 4.3.2.** *Sea $p$ un número primo y $a$ número entero. Entonces*

$$a^p \equiv a \pmod{p}.$$

*Demostración.* Supongamos que $a \geqslant 0$, entonces hagamos inducción en $a$. Si $a = 0$, el resultado es trivial. Supongamos el resultado probado para $k$, es decir $k^p \equiv k \pmod{p}$. Entonces $(k+1)^p \equiv k^p + 1^p \equiv k+1 \pmod{p}$. La primera congruencia es debido al lema 4.3.1 *b)* y la segunda es válida por hipótesis inductiva. Luego $a^p \equiv a \pmod{p}$ cuando $a > 0$.

Si $a < 0$, entonces $-a > 0$ y ya vimos que $(-a)^p \equiv -a \pmod{p}$, es decir que $(-1)^p a^p \equiv (-1)a \pmod{p}$. Si $p \neq 2$, entonces $(-1)^p = -1$ y se deduce el resultado. Si $p = 2$, entonces $(-1)^p = 1$, pero como $1 \equiv -1 \pmod{2}$, obtenemos también $a^p \equiv a \pmod{p}$. □

**Corolario 4.3.3.** *Sea $p$ primo y $a$ entero tal $p \nmid a$, entonces $a^{(p-1)} \equiv 1 \pmod{p}$.*

*Demostración.* Por Fermat $a^p \equiv a \pmod{p}$, es decir

$$p|(a^p - a) = a(a^{(p-1)} - 1).$$

Como $p$ no divide a $a$, tenemos que $p|(a^{(p-1)} - 1)$ (teorema 3.4.6), es decir $a^{(p-1)} \equiv 1 \pmod{p}$. □

Este último corolario es también conocido como teorema de Fermat.

La función de Euler $\phi(n)$, para $n \geqslant 1$, está definida como el cardinal del conjunto de los $x$ entre $1$ y $n$ que son coprimos con $n$. El teorema de Fermat admite la siguiente generalización.

**Teorema 4.3.4** (Teorema de Euler). *Sea $n$ un entero positivo y $a$ un número entero coprimo con $n$, entonces*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

*Demostración.* Ver ejercicios 2 y 3, a continuación. □

§ *Ejercicios*

1) Usar el teorema de Fermat para calcular el resto de dividir $3^{47}$ por 23.

2) Sean $x_1, \ldots, x_k$ los números coprimos con $n$ comprendidos entre 1 y $n$ (es decir $k = \phi(n)$) y sea $y$ coprimo con $n$. Entonces hay un reordenamiento de $yx_1, \ldots, yx_k$, es decir una permutación $\sigma$ de $1, \ldots, k$, tal que $x_i \equiv yx_{\sigma_i} \pmod{n}$, para $1 \leqslant i \leqslant k$. [Ayuda: como $y$ coprimo con $n$, existe $v$ tal que $yv \equiv 1 \pmod{n}$].

3) Demostrar el teorema de Euler. [Ayuda: Sean $x_1, \ldots, x_k$ los números coprimos con $n$ comprendidos entre 1 y $n$, por el ejercicio anterior $y^{\phi(n)}x_1 \ldots x_k = yx_1 \ldots yx_k \equiv x_1 \ldots x_k \pmod{n}$. Como $u = x_1 \ldots x_k$ coprimo con $n$, existe $v$ tal que $uv \equiv 1 \pmod{n}$].

## 4.4 EL CRIPTOSISTEMA RSA

Una de las aplicaciones más elementales y difundidas de la aritmética es en el diseño de sistemas criptográficos. El RSA es el más conocido de ellos y será presentado en esta sección.

Por criptosistema nos referimos a sistemas de encriptamiento o codificación esencialmente pensados para proteger la confidencialidad de datos que se desean transmitir. Entre los criptosistemas encontramos los simétricos y los de clave pública o asimétricos.

Los sistemas criptográficos simétricos son aquellos en que tanto el emisor como el receptor conocen una función, digamos $f$ y una palabra, digamos $x$ (la clave), tanto la función como la clave deben ser confidenciales o más comúnmente solo la clave debe ser confidencial. Cuando el emisor desea enviar un mensaje $M$, entonces aplica la función a $M$ y $x$, es decir

$M' = f(M, x)$, envía $M'$ y el receptor aplica la función inversa y recupera $M$, es decir $M = f^{-1}(M', x)$. Es llamada *simétrica* porque tanto el emisor como el receptor manejan las mismas claves y el emisor puede pasar a receptor y viceversa usando la misma encriptación.

En los sistemas de clave pública el receptor conoce una clave privada $y$ (no compartida por nadie) y publicita una clave pública $x$, de la misma manera que antes, si alguien desea enviar un mensaje $M$ al receptor debe hacer $M' = f(M, x)$, pero el receptor para decodificar debe hacer $M = g(M', y)$, donde $g$ es una función adecuada. Una ventaja evidente de los sistemas de clave pública es que no es necesario poner en conocimiento del emisor ninguna clave confidencial, más aún cualquier persona puede enviar en forma confidencial datos a otra persona que ha publicitado su clave.

Rivest, Shamir y Adleman descubrieron el primer criptosistema práctico de clave pública, que es llamado RSA. La seguridad del RSA se basa en la dificultad de factorizar números enteros grandes. Este sistema es el más comúnmente recomendado para uso en sistemas de clave pública. La mayor ventaja del RSA es que puede ser usado para proveer privacidad y autenticación (firma digital) en las comunicaciones. Su principal desventaja es que su implementación se basa en exponenciación de números enteros grandes, una operación que consume recursos de la computadora, aunque esto es cada vez menos significativo.

Antes de describir el RSA digamos que se basa fuertemente en el teorema de Fermat visto en la sección anterior.

En el sistema RSA deben realizarse algunos paso previos para fijar ciertos parámetros que luego nos permitirán encriptar y desencriptar los mensajes.

*Idea del algoritmo*

Supongamos que la persona $B$ quiere enviar a la persona $A$ un mensaje $m$ pero encriptado de tal forma que sólo $A$ pueda leer su contenido. Por su parte $A$ hace públicos dos números $e$ y $n$ que son los que se utilizarán para encriptar los mensajes que le envíen.

Entonces a partir de $m$ la persona $B$ genera un mensaje cifrado $c$ mediante la siguiente operación:

$$c \equiv m^e \pmod{n},$$

donde $e$ y $n$ es la clave pública de $A$.

Ahora $A$ recupera le mensaje $m$ a partir del mensaje en clave $c$ mediante la operación inversa dada por

$$m \equiv c^d \pmod{n},$$

donde $d$ es la clave privada que solo $A$ conoce.

*Elección de claves*

Sean $p$ y $q$ primos distintos suficientemente .

- La *clave pública* es $(n, e)$ con $n = pq$ y $e$ tal que $1 < e < (p-1)(q-1)$ y $\text{mcd}(e, (p-1)(q-1)) = 1$.
- La *clave privada* es un entero $d$ tal que $ed \equiv 1 \pmod{(p-1)(q-1)}$ y $0 \leqslant d < (p-1)(q-1)$.

*Observación.* Algunos comentarios sobre la elección de $p, q, e, d$.

- Los dos primos $p$ y $q$ deberían tener alrededor de 100 dígitos cada uno (longitud considerada segura en este momento).
- El número $e$ puede elegirse pequeño y se selecciona haciendo prueba y error con el algoritmo de Euclides, es decir probando hasta encontrar un $e$ tal que $\text{mcd}(e, (p-1)(q-1)) = 1$.
- La existencia de $d$ está garantizada por el teorema 4.2.1 (ecuación lineal de congruencia), pues $e$ y $(p-1)(q-1)$ son coprimos.

*Encriptar y desencriptar mensajes*

El receptor de mensajes publicita la clave pública $(n, e)$. Obviamente no da a conocer ni $p$, ni $q$ y mantiene segura la clave privada $d$. Como mencionamos anteriormente, el envío del mensaje y su decodificación requiere dos pasos

*a)* El emisor desea *encriptar* un número $m \in \{0, \ldots, n-1\}$ y para ello calcula $c \equiv m^e \pmod{n}$ y envía $c$ al receptor.

*b)* El receptor desea *desencriptar* el mensaje, es decir usando la clave pública $(n, e)$ y $c$, desea recuperar $m$: calcula $c^d \pmod{n}$ y veremos a continuación que este número es $m$.

*Demostración del método*

Debemos probar que el método anterior funciona y lo haremos en la siguiente proposición.

**Proposición 4.4.1.** *Sean*

- $n = pq$ *producto de dos números primos,*
- $e$ *coprimo con* $(p-1)(q-1)$, *y*
- $d$ *tal que* $ed \equiv 1 \pmod{(p-1)(q-1)}$.

*Entonces si* $m \in \{0, \ldots, n-1\}$,

$$c \equiv m^e \pmod{n} \quad \Rightarrow \quad m \equiv c^d \pmod{n}.$$

*Demostración.* Como $ed \equiv 1 \pmod{(p-1)(q-1)}$, entonces existe $k$ tal que

$$ed = 1 + k(p-1)(q-1). \tag{4.4.1}$$

Consideremos el mensaje $m$ y si es o no coprimo con $p$.

Si $\mcd(m,p) = 1$, el Teorema de Fermat dice que $m^{p-1} \equiv 1 \pmod{p}$. Entonces $(m^{p-1})^x \equiv 1 \pmod{p}$ para cualquier $x$. En particular, para $x = k(q-1)$. Asi que tenemos:

$$m^{k(p-1)(q-1)} = (m^{p-1})^{k(q-1)} \equiv 1 \pmod{p}.$$

Multiplicando esta ecuación por $m$ obtenemos

$$m^{1+k(p-1)(q-1)} \equiv m \pmod{p}. \tag{4.4.2}$$

Usando las ecuaciones (4.4.1) y (4.4.2) obtenemos:

$$m^{ed} \equiv m \pmod{p} \tag{4.4.3}$$

Esto, si $\mcd(m,p) = 1$. Pero si esto último no es cierto, entonces al ser $p$ primo debemos tener $m \equiv 0 \pmod{p}$ y en ese caso la ecuación (4.4.3) es trivial (dice que $0 \equiv 0$). Concuyendo, la ecuación (4.4.3) se cumple para todo $m$.

Obviamente podemos reemplazar $p$ por $q$ en el razonamiento anterior, así que la ecuación (4.4.3) también es verdadera si reemplazamos $p$ por $q$. De esa forma obtenemos:

$$p|(m^{ed} - m) \qquad \text{y} \qquad q|(m^{ed} - m).$$

Como $p$ y $q$ son primos distintos, entonces concluimos que $pq|(m^{ed} - m)$, es decir,

$$m^{ed} \equiv m \pmod{pq}.$$

□

*Ejemplo.* Probemos el sistema en forma práctica usando primos pequeños, por ejemplo $p = 31$, $q = 73$. En este caso $n = pq = 2\,263$.

Busquemos ahora un $e$: tenemos que $(p-1)(q-1) = 30 \cdot 72 = 2\,160$. Vemos que 2, 3, 5 dividen a $2\,160$, pero 7 es coprimo con $2\,160$. Tomemos entonces $e = 7$.

Usando el algoritmo de Euclides obtenemos $1 = 2 \cdot 2\,160 + (-617) \cdot 7$. Luego, $-617$ es solución de $7x \equiv 1 \pmod{2\,160}$, pero como queremos que la solución sea positiva menor que $2\,160$, podemos tomar $d = 2\,160 - 617 = 1\,543$.

Por lo tanto el receptor tiene clave pública $(2\,263, 7)$ y conserva en secreto su clave privada $1\,543$

- Supongamos que el emisor ha nacido en el año 1993 y quiere enviarle en secreto al receptor su año de nacimiento. Entonces encripta el año haciendo

$$1\,993^7 \equiv 10 \pmod{2\,263},$$

y envía, por una vía insegura, por ejemplo un email, el número $1\,417$ al receptor.

- El receptor calcula

$$10^{1\,543} \pmod{2\,263}$$

y obtiene nuevamente $1\,993$ (si quiere convencerse de esto ingrese `10^1543 mod 2263` en la ventana de búsqueda de Wolfram Alpha).

Pese a que el cálculo de desencriptado (en este caso $10^{1\,543} \pmod{2\,263}$) puede parecer costoso computacionalmente, hay métodos eficientes para hacerlo como veremos en la sección 4.5.

*Firma digital*

Una propiedad importante del RSA es que puede ser usado para firma digital o autenticación. En las hipótesis de la proposición 4.4.1, es claro que lo que probamos es que

$$(m^e)^d \equiv m \pmod{n},$$

para $m \in \{0, \ldots, n-1\}$. Ahora bien

$$(m^e)^d = m^{ed} = (m^d)^e,$$

es decir

$$(m^d)^e \equiv m \pmod{n},$$

para $m \in \{0, \ldots, n-1\}$. Por lo tanto, el receptor puede codificar un número o mensaje $m$ calculando $b \equiv m^d \pmod{n}$ y cualquiera que conozca la clave pública puede obtener el original calculando $b^e \pmod{n}$.

Lo interesante de esto es que si el receptor envía $m$ (el mensaje) y $b$ (la codificación de $m$), cualquiera puede comprobar que el mensaje ha sido codificado por el receptor (y no por otra persona) verificando que $m \equiv b^e \pmod{n}$.

*Ejemplo.* Como ya hemos mencionado, podemos ver que el RSA también puede ser usado para un sistema de *autenticación*, es decir es posible comprobar quien es la persona que envía el mensaje. Veamos una forma de hacerlo: la persona A tiene clave pública $(e, n)$ y clave privada $d$ y la persona B tiene clave pública $(e', n')$ y clave privada $d'$.

*a)* La persona B desea enviar un mensaje $m$ (en forma segura) a la persona A y quiere certificar que el mensaje fue enviado por él.

*b)* B calcula $x \equiv m^{d'} \pmod{n'}$. Es decir encripta su mensaje usando su clave privada.

*c)* Ahora B codifica $m$ y $x$ con la clave pública de A, es decir calcula $c \equiv m^e \pmod{n}$ e $y \equiv x^e \pmod{n}$.

*d)* B envía $c$ e $y$ al receptor A.

*e)* La persona A recupera $m$ y $x$ calculando $m \equiv c^d \pmod{n}$ y $x \equiv y^d \pmod{n}$.

*f)* A comprueba que el mensaje proviene de B o, mejor dicho, proviene de la persona con clave pública $(e', n')$, verificando que $m \equiv x^{e'} \pmod{n'}$.

## 4.5 MÉTODO BINARIO PARA EXPONENCIACION MODULAR (*)

Vimos en la sección anterior que para implementar el criptosistema RSA es esencial tener una forma eficiente de calcular exponenciación modular, es decir tener la capacidad de calcular el resto de dividir por cierto número la potencia muy grande de otro número.

Más explícitamente, sean $a, d, n$ enteros positivos se desea calcular $r$ tal que $a^d \equiv r \pmod{n}$ con $0 \leqslant r < n$. En otras palabras, se desea calcular el resto de de dividir $a^d$ por $n$. Estaríamos tentados de calcular $a^d$ y luego hacer la congruencia módulo $n$, pero cuando $d$ es grande, por ejemplo $d > 10^{20}$, este cálculo es imposible para cualquier computador.

Para realizar el cálculo de $a^d \equiv r \pmod{n}$ en forma eficiente podemos utilizar el *método binario de exponenciación modular* que explicaremos a continuación.

Primero, recordemos la definición recursiva de la potencia de un número: sea $a$ número (entero, racional, real, etc.), entonces

$$a^d = \begin{cases} 1 & , \quad \text{si } d = 0, \\ a \cdot a^{d-1} & , \quad \text{si } d > 0. \end{cases} \tag{4.5.1}$$

Aplicar esta definición tiene el inconveniente de que si $d$ es un número grande, la cantidad de pasos que se deben realizar para calcular $a^d$ es directamente proporcional (y mayor) a $d$, número que puede ser inmanejable para una computadora.

Una definición alternativa de las potencias de un número nos permite bajar el número de operaciones en forma significativa. Sea $a$ número (entero, racional, real, etc.), entonces

$$a^d = \begin{cases} 1 & , \quad \text{si } d = 0, \\ a \cdot a^{d-1} & , \quad \text{si } d > 0 \text{ y } d \text{ impar;} \\ (a^2)^{\frac{d}{2}} & , \quad \text{si } d > 0 \text{ y } d \text{ par.} \end{cases} \tag{4.5.2}$$

Con esta definición la cantidad de operaciones necesarias para calcular la potencia de un número decrece enormemente. Observemos que mientras que con la definición (4.5.1) la cantidad de operaciones es del orden de $d$, con la definición (4.5.2) la cantidad de operaciones es del orden de $\log_2(d)$.

*Ejemplo* 4.5.1. Supongamos que queremos calcular $9^{17}$. En este caso, podríamos hacer este cálculo directamente, multiplicando 17 veces 9 y así obtenemos 16677181699666569 con 17 multiplicaciones. Este sería el método que se deduce de la definición recursiva (4.5.4).

Probemos con la segunda definición recursiva:

$$\begin{aligned} 9^{17} &= 9 \cdot 9^{16} \\ &= 9 \cdot (9^2)^8 && = 3 \cdot 81^8 \\ &= 9 \cdot (81^2)^4 && = 3 \cdot 6561^4 \\ &= 9 \cdot (6561^2)^2 && = 3 \cdot 43046721^2 \\ &= 9 \cdot 1853020188851841 && = 16677181699666569. \end{aligned} \tag{4.5.3}$$

Es decir, en bastante menos pasos hemos podido calcular $9^{17}$.

Pasemos ahora al problema de calcular exponenciación modular.

Supongamos ahora que queremos calcular $r$ tal que

$$5^{1125899986842625} \equiv r \pmod{100000037},$$

y $0 \leqslant r < 100000037$. Hacer este cálculo directamente no nos da un resultado satisfactorio, ni siquiera con un programa de computadora. Pueden hacer

el intento con un lenguaje de programación, Python por ejemplo, y verán que el programa no termina. Esto se debe a que $5^{1125899986842625}$ es un número inmenso cuya representación no cabría en la memoria de ninguna computadora ni actual ni futura. La clave para poder calcular $r$ es usar un análogo a la definición (4.5.2), pero con congruencias. Sea $a$ número entero y sean $d \geqslant 0$ y $n \geqslant 1$. Definimos $\%$ el *operador módulo* de tal forma que $a \% n$ devuelve el resto de dividir $a$ por $n$. Hay muchas forma de calcular $a^d \% n$, y nosotros elegimos la siguiente forma recursiva:

$$a^d \% n = \begin{cases} 1 & , \quad \text{si } d = 0, \\ a \cdot (a^{n-1} \% n) \% n & , \quad \text{si } d > 0 \text{ y } d \text{ impar}; \\ (a^2 \% n)^{\frac{n}{2}} \% n & , \quad \text{si } d > 0 \text{ y } d \text{ par}. \end{cases} \tag{4.5.4}$$

Esta definición no solo reduce la cantidad de pasos para calcular $r$, si no que, veremos un poco más adelante, también mantiene la cantidad de dígitos de los cálculos intermedios acotada.

*Ejemplo* 4.5.2. Sea $n = 23$, calculemos usando la definición 4.5.4, $r$ tal que $9^{17} \equiv r \pmod{23}$ con $0 \leqslant r < 23$, es decir $9^{17} \% 23$. Apliquemos la definición (4.5.4) y aprovechemos los cálculos hechos en el ejemplo 4.5.1:

$$\begin{aligned} 9^{17} &\equiv 9 \cdot 9^{16} \\ &\equiv 9 \cdot (9^2)^8 \quad \equiv \quad 9 \cdot 12^8 && (\text{pues } 9^2 \equiv 12 \pmod{23}) \\ &\equiv 9 \cdot (12^2)^4 \quad \equiv \quad 9 \cdot 6^4 && (\text{pues } 12^2 \equiv 6 \pmod{23}) \\ &\equiv 9 \cdot (6^2)^2 \quad \equiv \quad 9 \cdot 13^2 && (\text{pues } 6^2 \equiv 13 \pmod{23}) \\ &\equiv 9 \cdot 8 && (\text{pues } 13^2 \equiv 8 \pmod{23}) \\ &\equiv 3 && (\text{pues } 9 \cdot 8 \equiv 3 \pmod{23}). \end{aligned}$$

Es decir, $9^{17} \equiv 3 \pmod{23}$. Observar que pese a que $9^{17}$ es un número de 17 dígitos, los cálculos que hacemos (módulo 23) involucran pocos dígitos.

Como observamos en el ejemplo, en cada paso donde $d$ es par tenemos que calcular el cuadrado de un número y elevarlo a una potencia que es la mitad que la anterior. Luego, si el exponente es $d < 2^k$ en alrededor de $k$ pasos (unos pocos más en realidad) obtendremos el resultado deseado.

En el caso que habíamos planteado: calcular $5^{1125899986842625} \equiv r \pmod{100000037}$, como $1125899986842625 < 2^{51}$, si lo resolvemos usando el método de la fórmula (4.5.4) necesitaremos poco más de 50 pasos.

La definición (4.5.4) nos muestra como casi inmediátamente podemos obtener una fórmula recursiva para la exponenciación modular: sea $n > 0$, definimos $//$ el *operador cociente* de tal forma que $a // n$ es el cociente entero

de dividir $a$ por $n$. Entonces, nuestro interés es calcular $f(a,d) = a^d \,\%\, n$ en forma eficiente y la fórmula (4.5.4) es equivalente a

$$f(a,d) = \begin{cases} 1 & , \quad \text{si } d = 0, \\ (a \cdot f(a, d-1)) \,\%\, n & , \quad \text{si } d > 0 \text{ y } d \text{ impar;} \\ f(a^2 \,\%\, n, d \,//\, 2) & , \quad \text{si } d > 0 \text{ y } d \text{ par.} \end{cases} \tag{4.5.5}$$

Observar que en la definición hay dos $\%\, n$ que podrían haber sido reemplazados por una instancia de la función $f$ pues $x \,\%\, n = f(x,1)$. Pero, en este caso, se pueden calcular directamente por el algorimo de división, pues están aplicados en números considerados "no grandes".

Esta función recursiva es fácilmente trasladable a pseudocódigo.

EXPONENCIACIÓN MODULAR RECURSIVA

```
def f(a, d):
    if d == 0:
        res = 1
    elif d % 2 == 1:
        res =  (a * f(a, d - 1)) % n
    else:
        res =  f(a**2 % n, d // 2)
    return res
```

En pseudocódigo una versión iterativa de la exponenciacion modular se puede describir de la siguiente forma.

EXPONENCIACIÓN MODULAR

```
def exp_modular(a, d, n):
    res = 1
    base, exponente = a, d
    while exponente > 0:
        # invariante: (a**d) % n = (res * base**exponente) % n
        if exponente % 2 == 1:
            res = (res * base) % n
            exponente = exponente // 2
            base = base**2 % n
        elif exponente % 2 == 0:
            exponente = exponente // 2
            base = base**2 % n
    return res
```

## 4.6 PRUEBAS DE PRIMALIDAD (*)

En la implementación del criptosistema RSA es fundamental el uso de primos de grandes dimensiones, por ejemplo de más de 100 dígitos. Ahora bien, tratar de demostrar que un número (grande) es primo buscando sus divisores es imposible con una arquitectura de computadoras determinística, como la es la de las computadoras actuales. Justamente en la dificultad de la descomposición prima se basa la fortaleza del criptosistema RSA.

Sin embargo, veremos en esta parte del apunte que hay algoritmos que permiten determinar en forma probabilística si un número es primo o no. También mencionaremos, al final de esta sección, algoritmos que determinan eficientemente y en forma determinística si un número es primo a o no.

El algoritmo que veremos principalmente es el test de primalidad Miller-Rabin probabilístico. Como su nombre lo indica es una prueba probabilística de primalidad: un algoritmo que determina si un número dado es probable que sea primo.

Este test es ampliamente utilizado en la práctica (en RSA, por ejemplo) y es una de las pruebas más simples y rápidas conocidas.

Describamos en forma amplia el método del test: dado $m$ un entero positivo.

- Si le hacemos el test a $m$ y no supera la prueba, entonces el número no es primo.
- Si hacemos $k$ veces el test y $m$ supera las $k$ pruebas, entonces $m$ tiene la probabilidad $1 - (1/4^k)$ de ser primo.

El test de Miller-Rabín se basa en comprobar $k$ veces (para un $k$ dado) si el número es fuertemente probable primo respecto a una base. Veamos a continuación las definiciones necesarias para comprender este concepto.

**Definición 4.6.1.** Sea $n > 2$ un entero impar, entonces $n = 2^s \cdot d + 1$ con $d$ impar. Sea $a$ entero tal que $0 < a < n$. Entonces diremos que $n$ es *fuertemente probable primo (FPP) respecto a la base* $a$ si se cumple

- $a^d \equiv 1 \pmod{n}$, o
- $a^{2^r \cdot d} \equiv -1 \pmod{n}$ para algún $r$ tal que $0 \leqslant r < s$.

Con la aplicación del teorema de Fermat y la ecuación lineal de congruencia probaremos que todo número primo es FPP respecto a cualquier base. El contrarrecíproco de esta afirmación nos dice que un número que no es FPP respecto a alguna base es compuesto.

**Lema 4.6.2.** *Sea $n$ un primo impar, entonces las únicas raíces cuadradas de 1 modulo $n$ son 1 y $-1$. Es decir,*

$$x^2 \equiv 1 \pmod{n} \quad \Rightarrow \quad x \equiv \pm 1 \pmod{n}.$$

*Demostración.* Sea $x$ tal que $x^2 \equiv 1 \pmod{n}$, luego $x^2 - 1 \equiv 0 \pmod{n}$, como $x^2 - 1 = (x-1)(x+1)$, obtenemos $(x-1)(x+1) \equiv 0 \pmod{n}$. Esto quiere decir que $n|(x-1)(x+1)$. Como $n$ es primo, $n|x-1$ o $n|x+1$, es decir $x \equiv 1 \pmod{n}$ o $x \equiv -1 \pmod{n}$. □

**Teorema 4.6.3.** *Si $n$ es un primo impar, entonces $n$ es FPP para cualquier base $a$ con $0 < a < n$.*

*Demostración.* Consideremos la sucesión $a^{2^s \cdot d}, a^{2^{s-1} \cdot d}, \ldots, a^{2d}, a^d$ y observemos que cada término de la sucesión es el cuadrado del siguiente.

Por el teorema de Fermat, $a^{2^s \cdot d} = a^{n-1} \equiv 1 \pmod{n}$. Luego $(a^{2^{s-1} \cdot d})^2 \equiv 1 \pmod{n}$ y por lo tanto $a^{2^{s-1} \cdot d}$ es una raíz cuadrada de 1 módulo $n$. Por el lema anterior obtenemos que $a^{2^{s-1} \cdot d} \equiv \pm 1 \pmod{n}$.

Si $a^{2^{s-1} \cdot d} \equiv -1 \pmod{n}$, obtenemos el resultado. En caso contrario $a^{2^{s-1} \cdot d} \equiv 1 \pmod{n}$, luego $(a^{2^{s-2} \cdot d})^2 \equiv 1 \pmod{n}$ y por lo tanto $a^{2^{s-2} \cdot d}$ es una raíz cuadrada de 1 módulo $n$ y en consecuencia $a^{2^{s-2} \cdot d} \equiv \pm 1 \pmod{n}$.

Iterando el razonamiento anterior concluimos que alguno de los términos de la sucesión $a^{2^r \cdot d}$ es congruente a $-1$ módulo $n$ o bien todos los términos son congruentes a 1, en particular $a^d \equiv 1 \pmod{n}$, con lo cual $n$ resulta ser probable primo fuerte. □

Ahora bien, también es cierto el recíproco (que no demostraremos): un número $n$ que es FPP respecto a todas las bases $0 < a < n$ es primo. Podríamos intentar ver que un número es primo probando que es FPP para cualquier base, pero este cálculo es computacionalmente imposible para primos grandes.

Por otro lado, un número $n$ que es FPP respecto alguna base $0 < a < n$ podría ser compuesto, pero hay una probabilidad mayor que 0.75 de que sea primo. La verificación con diferentes bases de que un número es FPP acerca a 1 la probabilidad de que el número sea primo.

El test probabilístico de primalidad de Miller-Rabin se basa en las observaciones realizadas más arriba: sea $n$ entero positivo impar y sea $k$ entero positivo.

(1) Elegir al azar $a$ entero tal que $0 < a < n$.

(2) Verificar que $n$ es FPP respecto a la base $a$.

(3) Repetir (1) y (2) $k$ veces.

Si $n$ es FPP las $k$ veces, entonces decimos que $n$ supera el test probabilístico de primalidad de Miller-Rabin y tiene probabilidad $1 - (1/4^k)$ de ser primo (y lo consideramos primo).

Mostramos a continuación una implementación en pseudocódigo.

TEST DE PRIMALIDAD DE MILLER-RABIN

```
def test_Miller_Rabin(n: int, k: int) -> bool:
    s, d = satisfacen n = 2**s * d + 1, s impar
    repetir k veces:
        a = entero al azar entre 2 y n-1
        fpp = False # suponemos n no es fuertemente primo en base a
        if 1 == a**d % n:
            fpp = True
        else:
            r = 0
            while r <= s and fpp == False:
                if n - 1 == a**(2**r * d) % n:
                    fpp = True
                r = r + 1
            if fpp == False: # si n no pasa la prueba
                return False
    return True # n pasó las k pruebas
```

Observemos que el test de primalidad de Miller-Rabin hace uso de la exponenciación modular y por lo tanto debe ser implementado usando el método binario de exponenciación modular.

El test de Miller-Rabin probabilístico se deriva del test de Miller: asumiendo que es válida la Hipótesis de Riemman, sea $n$ entero positivo, si comprobamos que $n$ es FPP en base $a$ con $2 < a < 2\ln(n)^2$, entonces $n$ es primo.

El test de Miller no se utiliza en la práctica. Para la mayoría de los propósitos, el uso adecuado de la prueba probabilística de Miller-Rabin es mucho más rápida y brinda suficente seguridad del resultado. Para fines teóricos que requieren un algoritmo de tiempo polinomial determinista, el test de Miller fue reemplazado por la prueba de primalidad de Agrawal–Kayal–Saxena (AKS), que no se basa en suposiciones no probadas.

Parte II

# GRAFOS

# 5

# GRAFOS

## 5.1 GRAFOS Y SUS REPRESENTACIONES

Los objetos a los cuales llamaremos *grafos* son muy útiles en matemática discreta. Su nombre se deriva del hecho de que pueden ser entendidos con una notación gráfica (o pictórica), y en este aspecto solamente se parecen a los familiares gráficos de funciones que son estudiados en matemática elemental. Pero nuestros grafos son bastante diferentes de los gráficos de funciones y están más relacionados con objetos que en el lenguaje diario llamamos *redes* (networks).

Usaremos la siguiente definición en lo que sigue: dado un conjunto $X$ un 2-*subconjunto* es un subconjunto de $X$ de dos elementos.

**Definición 5.1.1.** Un *grafo* $G$ consiste de un conjunto finito $V$, cuyos miembros son llamados *vértices*, y un conjunto de 2-subconjuntos de $V$, cuyos miembros son llamados *aristas*. Nosotros usualmente escribiremos $G = (V, E)$ y diremos que $V$ es el *conjunto de vértices* y $E$ es el *conjunto de aristas*.

La restricción a un conjunto finito no es esencial, pero es conveniente para nosotros debido a que no consideraremos "grafos infinitos" en este apunte.

Un ejemplo típico de un grafo $G = (V, E)$ es dado por los conjuntos

$$V = \{a, b, c, d, z\}, \qquad E = \{\{a, b\}, \{a, d\}, \{b, z\}, \{c, d\}, \{d, z\}\}. \tag{5.1.1}$$

Este ejemplo y la definición misma no son demasiado esclarecedores, y solamente cuando consideramos la *representación pictórica* de un grafo es cuando se hace la luz.

Nosotros representamos los vértices como puntos, y unimos dos puntos con una linea siempre y cuando el correspondiente par de vértices está en una arista. Luego la Fig. 4 es una representación pictórica del grafo dado en el ejemplo arriba. Esta clase de representación es extremadamente conveniente para trabajar "a mano" con grafos relativamente pequeños. Más aún, esta representación es de gran ayuda para formular y comprender argumentos abstractos.

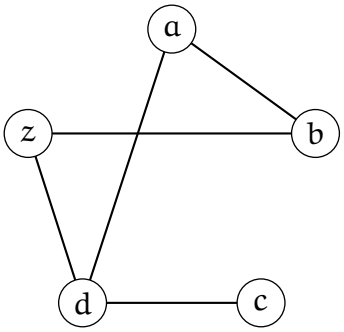



Figura 4: Una representación pictórica del grafo definido en (5.1.1).

**Definición 5.1.2.** La *valencia* o *grado* de un vértice $v$ en un grafo $G = (V, E)$ es el número de aristas de $G$ que contienen a $v$. Usaremos la notación $\delta(v)$ para la valencia de $v$, formalmente

$$\delta(v) = |D_v|, \quad \text{donde} \quad D_v = \{e \in E | v \in e\}.$$

Por ejemplo, el grafo descrito en Fig. 4 tiene $\delta(a) = 2$, $\delta(b) = 2$, $\delta(c) = 1$, $\delta(d) = 3$, $\delta(z) = 2$.

Nosotros damos a continuación un ejemplo frívolo de un problema que se resuelve pensándolo como un grafo.

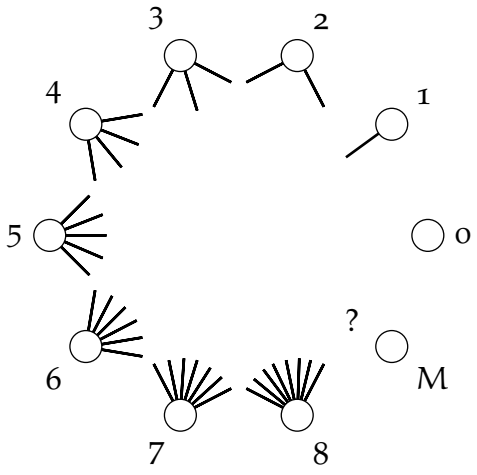



Figura 5: La fiesta de Abril

*Ejemplo.* Mario y su mujer Abril dan una fiesta en la cual hay otras cuatro parejas de casados. Las parejas, cuando arriban, estrechan la mano a algunas personas, pero, naturalmente, no se estrechan la mano entre marido y mujer. Cuando la fiesta finaliza el profesor pregunta a los otros a cuantas personas han estrechado la mano, recibiendo 9 respuestas diferentes. ¿Cuántas personas estrecharon la mano de Abril?

*Solución.* Construyamos un grafo cuyos vértices son las personas que asisten a la fiesta. Las aristas del grafo son las $\{x, y\}$ siempre y cuando $x$ e $y$ se hayan estrechado las manos. Puesto que hay nueve personas aparte de Mario, y que una persona puede estrechar a lo sumo a otras 8 personas, se sigue que las 9 respuestas diferentes que ha recibido el profesor deben ser $0, 1, 2, 3, 4, 5, 6, 7, 8$. Denotemos los vértices con estos números y usemos $M$ para Mario. Así obtenemos la representación pictórica de la Fig. 5

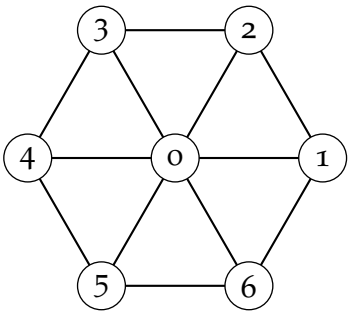
Ahora, el vértice 8 alcanza a todos los otros vértices excepto uno, el cual debe por lo tanto representar a la esposa de 8. Este vértice debe ser el 0 el cual por cierto que no está unido al 8 (ni obviamente a ningún otro). Luego 8 y 0 son una pareja de casados y 8 está unido a $1, 2, 3, 4, 5, 6, 7$ y $M$. En particular el 1 está unido al 8 y ésta es la única arista que parte del 1. Por consiguiente 7 no esta unido al 0 y al 1 (únicamente), y la esposa de 7 debe ser 1, puesto que 0 esta casado con 8. Continuando con este razonamiento vemos que 6 y 2, y 5 y 3 son parejas de casados. Se sigue entonces que $M$ y 4 están casados, luego el vértice 4 representa a Abril, quien estrechó la mano de cuatro personas. □

*Ejemplo* 5.1.3. Los senderos de un jardín han sido diseñados dándoles forma de *grafo rueda* $W_n$ ($n \geqslant 2$), cuyos vértices son $V = \{0, 1, 2, \ldots, n\}$ y sus aristas son

$$\begin{array}{llllll} \{0,1\}, & \{0,2\}, & \ldots, & \{0,n-1\}, & \{0,n\}, & \text{(los rayos de la rueda)} \\ \{1,2\}, & \{2,3\}, & \ldots, & \{n-1,n\}, & \{n,1\}. & \text{(el perímetro de la rueda)} \end{array}$$

Describir una ruta por los senderos de tal forma que empiece y termine en el vértice 0 y que pase por cada vértice una sola vez.

*Solución.* Primero dibujemos el grafo para darnos cuenta de por que se llama "rueda". Dibujemos $W_6$. El dibujo nos orienta de como puede ser una ruta: $0, 1, 2, 3, 4, 5, 6, 0$.




En general una respuesta para $W_n$ es: $0, 1, 2, 3, \cdots, n-1, n, 0$. □

Aunque la representación pictórica es intuitivamente atractiva para los seres humanos, es claramente inútil cuando deseamos comunicarnos con una computadora. Para lograr esto debemos representar el grafo mediante el conjunto de aristas, como en la definición formal, o cierta clase de lista o tabla. Diremos que dos vértices $x$ e $y$ de un grafo son *adyacentes* cuando $\{x, y\}$ es una arista. (o también diremos que $x$ e $y$ son *vecinos*). Entonces podemos representar un grafo $G = (V, E)$ por su *lista de adyacencia*, donde cada vértice $v$ encabeza una lista de aquellos vértices que son adyacentes a $v$. El grafo de Fig. 4 tiene la siguiente lista de adyacencia:

| a | b | c | d | z |
|---|---|---|---|---|
| b | a | d | a | b |
| d | z | | c | d |
| | | | z | |

Las listas de adyacencia son redundantes (cada arista está representada dos veces) pero como todo lenguaje de programación de alto nivel maneja la estructura tipo lista, preferimos esta representación pues un grafo resulta ser una lista de listas o un arreglo de listas.

*Observación.* ¿Por qué es más eficiente la representación de un grafo por una lista de adyacencia que por los conjuntos que lo definen?. En los algoritmos sobre grafos una de las operaciones más utilizadas es encontrar los vértices adyacentes a un vértice dado $v$. En la implementación natural por conjuntos esto supone recorrer todas las aristas del grafo para determinar en cuales de ellas se encuentra $v$. En un grafo con gran cantidad de aristas esto supone muchísimas operaciones. En cambio si trabajamos con listas de adyacencia es simplemente devolver la lista correspondiente a $v$ y la cantidad necesaria de operaciones para hacer esto es del orden de la valencia de $v$ (que puede ser un número muy pequeño comparada la número de aristas).

**Definición 5.1.4.** Por cada entero positivo $n$ definimos el *grafo completo* $K_n$ como el grafo con $n$ vértices y en el cual cada par de vértices es adyacente.

¿Cuántas aristas tiene $K_n$? ¿Cuál es la valencia de cada vértice? De cada vértice "salen" $n-1$ aristas, las que van a otros vértices. Luego, cada vértice tiene valencia $n-1$. Si sumamos $n$-veces las $n-1$ aristas que salen de cada vértice es claro que estamos contando cada arista dos veces, luego el número total de aristas es $n(n-1)/2$ (observar que esta es una demostración, usando grafos, de que $\sum_{i=1}^{n} i = n(n-1)/2$).

§ *Ejercicios*

1) A tres casas $A, B, C$ se les debe conectar el gas, el agua y la electricidad: $G, W, E$. Escribir la lista de adyacencia para el grafo que representa este problema y construir una representación pictórica del mismo. ¿Puede usted encontrar un dibujo en el cual las líneas que representan las aristas no se crucen?

2) ¿Para cuales valores de $n$ se puede hacer una representación pictórica de $K_n$ con la propiedad que las líneas que representan las aristas no se corten?

3) Un *3-ciclo* en un grafo es un conjunto de tres vértices mutuamente adyacentes. Construir un grafo con cinco vértices y seis aristas que no contenga 3-ciclos.

## 5.2 ISOMORFISMO DE GRAFOS

En este punto nosotros debemos enfatizar que un grafo esta definido como una entidad matemática abstracta. Es en este contexto que nosotros discutiremos el importante problema de que queremos decir cuando decimos que dos grafos son "el mismo".

Claramente lo importante de un grafo no son los nombres con que designamos a los vértices, ni su representación pictórica o cualquier otra representación. La propiedad característica de un grafo es la manera en que los vértices están conectados por aristas.

Antes de definir isomorfismo de grafos repasaremos el concepto de función o aplicación biyectiva. Dado dos conjuntos $X, Y$ diremos que una aplicación $f : X \to Y$ es *biyectiva* si para cada $y \in Y$ existe un único $x \in X$ tal que $f(x) = y$. Un propiedad importante, de las funciones biyectivas es que $f$ es biyectiva si y sólo sí $f$ tiene *inversa*, es decir existe $f^{-1} : Y \to X$, tal que $f(f^{-1}(y)) = y$, $\forall\, y \in Y$ y $f^{-1}(f(x)) = x$, $\forall\, x \in X$.

*Ejemplo.* La función

$$f : \{1, 2, 3\} \to \{a, b, c\} \quad \text{definida } f(1) = c, f(2) = b, f(3) = a$$

es biyectiva y su inversa es

$$f^{-1}(a) = 3,\ f^{-1}(b) = 2,\ f^{-1}(c) = 1.$$

También es biyectiva la aplicación

$$g : \{x, y\} \times \{u, w, z\} \to \{1, 2, 3, 4, 5, 6\} \quad \text{definida}$$

$$g(x, u) = 1,\ g(x, w) = 2,\ g(x, z) = 3,\ g(y, u) = 4,\ g(y, w) = 5,\ g(y, z) = 6.$$

**Definición 5.2.1.** Dos grafos $G_1$ y $G_2$ se dicen que son *isomorfos* cuando existe una biyección $\alpha$ entre el conjunto de vértices de $G_1$ y el conjunto de vértices de $G_2$ tal que si $\{x, y\}$ es una arista de $G_1$ entonces $\{\alpha(x), \alpha(y)\}$ es una arista de $G_2$ y recíprocamente si $\{z, w\}$ es una arista de $G_2$ entonces $\{\alpha^{-1}(z), \alpha^{-1}(w)\}$ es una arista de $G_1$. La biyección $\alpha$ es llamada un *isomorfismo*.

Es importante notar que, debido a al definición, un isomorfismo de grafos se extiende a un biyección de aristas del primer grafo en el segundo grafo. Por lo tanto, para demostrar que $\alpha$ es un isomorfismo entre dos grafos $G_1$ y $G_2$ alcanza con verificar que lleva en forma inyectiva todas las aristas de $G_1$ en todas las aristas de $G_2$.

Por ejemplo, considere los dos grafos de la Fig. 6. En este caso hay una biyección entre el conjunto de vértices de $G_1$ y el conjunto de vértices de $G_2$ la cual tiene la propiedad requerida; esta biyección es dada por

$$\alpha(a) = t, \quad \alpha(b) = v, \quad \alpha(c) = w, \quad \alpha(d) = u.$$

Podemos comprobar que a cada arista de $G_1$ le corresponde una arista de $G_2$ y viceversa. Por ejemplo, a la arista $bc$ de $G_1$ le corresponde la arista $vw$ de $G_2$, y así siguiendo. (Usaremos la abreviación $xy$ para la arista $\{x, y\}$, recordando que una arista es un par desordenado, es decir $xy$ es lo mismo que $yx$.)

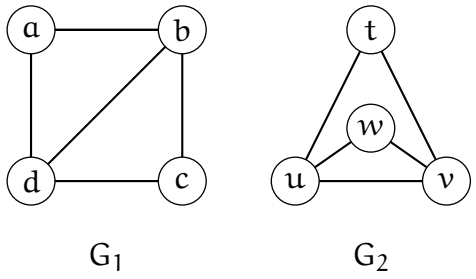



Figura 6: $G_1$ y $G_2$ son isomorfos

Cuando, como en la Fig. 6, dos grafos $G_1$ y $G_2$ son isomorfos usualmente nos referiremos a ellos como que son "el mismo" grafo.

Para mostrar que dos grafos no son isomorfos, nosotros debemos demostrar que no hay una biyección entre el conjunto de vértices de uno con el conjunto de vértices de otro, que lleve las aristas de uno en las aristas del otro.

Si dos grafos tienen diferente número de vértices, entonces no es posible ninguna biyección, y los grafos no pueden ser isomorfos. Si los grafos tienen el mismo número de vértices, pero diferente número de aristas, entonces hay biyecciones de vértices pero ninguna de ellas puede ser un isomorfismo.

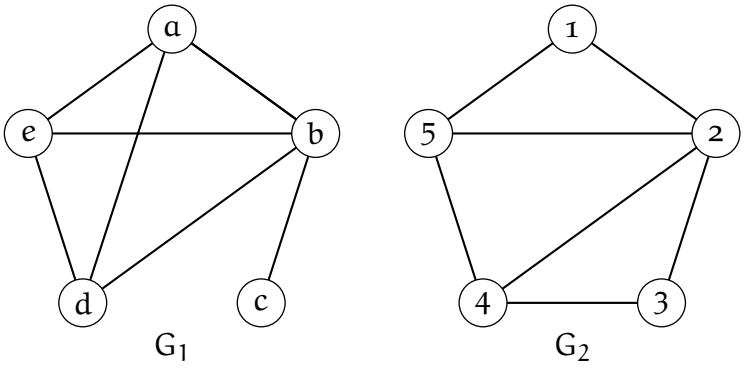



Figura 7: $G_1$ y $G_2$ no son isomorfos

**Definición 5.2.2.** Sea $G = (V, E)$ un grafo. Se dice que $G' = (V', E')$ es *subgrafo* de $G = (V, E)$ si $V' \subset V$, $E' \subset E$ y todos los vértices que son extremos de las aristas de $E'$ están en $V'$.

Es claro, pero no lo demostraremos aquí, que un isomorfismo lleva un subgrafo a un subgrafo isomorfo. Este resultado es una herramienta que puede ser útil para ver si dos grafos no son isomorfos.

Por ejemplo, los dos grafos de la Fig. 7 tienen cada uno cinco vértices y siete aristas pero no son isomorfos. Una manera de ver esto es observar que los vértices $a$, $b$, $d$, $e$ forman un subgrafo completo de $G_1$ (cada par de ellos está conectado por una arista). Cualquier isomorfismo debe llevar estos vértices en cuatro vértices de $G_2$ con la misma propiedad, y puesto que no hay tal conjunto de vértices en $G_2$ no puede haber ningún isomorfismo.

§ *Ejercicios*

1) Probar que los grafos mostrados en la Fig. 8 no son isomorfos.

2) Encontrar un isomorfismo entre los grafos definidos por las siguientes listas de adyacencias. Ambas listas especifican versiones de un grafo famoso conocido como *grafo de Petersen*.

| a | b | c | d | e | f | g | h | i | j |
|---|---|---|---|---|---|---|---|---|---|
| b | a | b | c | d | a | b | c | d | e |
| e | c | d | e | a | h | i | j | f | g |
| f | g | h | i | j | i | j | f | g | h |

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 0 | 1 | 0 | 2 | 6 |
| 5 | 0 | 1 | 2 | 3 | 4 | 4 | 3 | 5 | 7 |
| 7 | 6 | 8 | 7 | 6 | 8 | 9 | 9 | 9 | 8 |

3) Sea $G = (V, E)$ el grafo definido como sigue: el conjunto de vértices $V$ es el conjunto de todas las palabras de longitud tres en el alfabeto $\{0, 1\}$, y el conjunto de aristas $E$ contiene aquellos pares de palabras

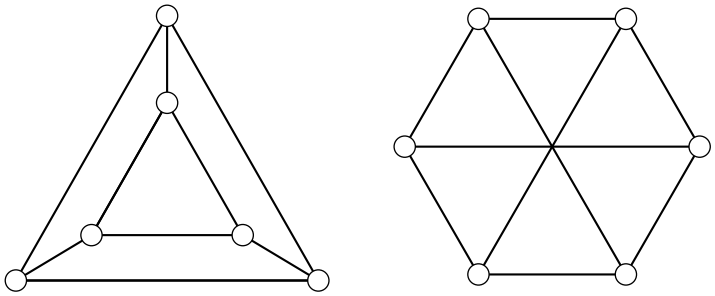



Figura 8: Probar que estos grafos no son isomorfos

que difieren exactamente en una posición. Probar que G es isomorfo al grafo formado por las esquinas y aristas de un cubo.

## 5.3 VALENCIAS DE UN GRAFO

El primer teorema de la teoría de grafos nos dice que la suma de las valencias de un grafo es dos veces el número de aristas.

**Teorema 5.3.1.** *La suma de los valores de las valencias $\delta(v)$, tomados sobre todos los vértices $v$ del grafo $G = (V, E)$, es igual a dos veces el número de aristas:*

$$\sum_{v \in V} \delta(v) = 2|E|.$$

*Demostración.* La valencia de un vértice $v$ indica la cantidad de "extremos" de aristas que "tocan" a $v$. Es claro que hay $2|E|$ extremos de aristas, luego la suma total de las valencias de los vértices es $2|E|$. □

Hay un útil corolario de este resultado. Diremos que un vértice de G es *impar* si su valencia es impar, y *par* si su valencia es par. Denotemos $V_i$ y $V_p$ los conjuntos de vértices impares y pares respectivamente, luego $V = V_i \cup V_p$ es una partición de $V$. Por teorema 5.3.1, tenemos que

$$\sum_{v \in V_i} \delta(v) + \sum_{v \in V_p} \delta(v) = 2|E|.$$

Ahora cada término en la segunda suma es par, luego esta suma es un número par. Puesto que el lado derecho también es un número par, la primera suma debe ser también par. Pero la suma de números impares solo puede ser par si el número de términos es par. En otra palabras:

**Teorema 5.3.2.** *El número de vértices impares es par.*

Este resultado es a veces llamado el "handshaking lemma" (handshak = estrechar la mano, darse la mano), debido a que se puede interpretar en términos de gente y darse la mano: dado un conjunto de personas, el número de personas que le ha dado la mano a un número impar de miembros del conjunto es par.

*Observación.* Cuando representamos un grafo por una lista de adyacencia, como cada arista se encuentra dos veces (si $w$ está en la columna de $v$, entonces $v$ está en la columna de $w$) podemos llegar a pensar que la representación por listas de adyacencia utiliza "demasiado espacio" (el doble de lo necesario). Sin embargo, esta representación ocupa el mismo espacio que la de conjuntos: en la lista de adyacencia de un grafo $G$, en cada columna $v$ se encuentran $\delta(v)$ vértices. Por lo tanto la tabla tiene $\sum_{v\in V}\delta(v)$ entradas. Por el teorema 5.3.1 tenemos que $\sum_{v\in V}\delta(v) = 2|E|$, es decir el número de entradas de la tabla es dos veces el número de aristas. Por otro lado, como cada arista ocupa 2 espacios (los dos vértices), el número de espacios necesario para representar $G$ como conjunto es también $2|E|$.

Un grafo en el cual todos los vértices tienen la misma valencia $r$ se llama *regular* (con valencia $r$), o $r$-*valente*, o de *grado* $r$. En este caso, el de un grafo de grado $r$, el resultado del teorema 5.3.1 se traduce a

$$r|V| = 2|E|.$$

Muchos de los grafos que aparecen en las aplicaciones son regulares. Ya conocemos los grafos completos $K_n$; ellos son regulares, con valencia $n-1$. De geometría elemental conocemos los polígonos de $n$ lados, los cuales en teoría de grafos son llamados *grafos cíclicos* $C_n$. Formalmente, podemos decir que el conjunto de vértices de $C_n$ es $\mathbb{Z}_n$, y los vértices $i$ y $j$ están unidos si $j = i+1$ o $j = i-1$ en $\mathbb{Z}_n$. Claramente, $C_n$ es un grafo regular con valencia 2, si $n \geqslant 3$.

Una aplicación importante de la noción de valencia es en el problema de determinar si dos grafos son o no isomorfos. Si $\alpha : V_1 \to V_2$ es un isomorfismo entre $G_1$ y $G_2$, y $\alpha(v) = w$, entonces cada arista que contiene a $v$ se transforma en una arista que contiene a $w$. En consecuencia $\delta(v) = \delta(w)$. Por otro lado, si $G_1$ tiene un vértice $x$, con valencia $\delta(x) = \delta_0$, y $G_2$ no tiene vértices con valencia $\delta_0$, entonces $G_1$ y $G_2$ no pueden ser isomorfos. Esto nos da otra manera para distinguir los grafos de la Fig 7, puesto que el primer grafo tiene un vértice de valencia 1 y el segundo no.

Una extensión de esta idea se da en la siguiente proposición.

**Proposición 5.3.3.** *Sean* $G_1$ *y* $G_2$ *grafos isomorfos. Para cada* $k \geqslant 0$ *sea* $n_i(k)$ *el número de vértices de* $G_i$ *que tienen valencia* $k$ *(*$i = 1, 2$*). Entonces* $n_1(k) = n_2(k)$.

*Demostración.* Hemos visto más arriba que si $\alpha : V_1 \to V_2$ es un isomorfismo entre $G_1$ y $G_2$ y $v \in V_1$, entonces $\delta(v) = \delta(\alpha(v))$. Luego la cantidad de vértices con valencia $k$ en $G_1$ es igual a la cantidad de vértices con valencia $k$ en $G_2$. □

*Ejemplo.* Revisemos los grafos de la Fig. 7 y la Fig. 8 de la sección anterior. Los dos grafos de la Fig. 7 no son isomorfos debido a que en el primer grafo existen tres vértices con valencia 3 mientras que en el segundo existen sólo dos.

Observar que los criterios vistos hasta ahora relativos a cantidad de vértices, cantidad de aristas y valencias, incluyendo el de la proposición 5.3.3, no son útiles para determinar si los grafos de la Fig. 8 son isomorfos o no: ambos tienen 6 vértices, 9 aristas y todos los vértices son de valencia 3. Sin embargo, en el caso de la Fig. 8 podemos determinar que los grafos no son isomorfos observando los subgrafos de cada uno. Ahora bien, no hay ningún criterio general eficiente para determinar si dos grafos son isomorfos o no: en los casos difíciles esencialmente debemos probar con todas las biyecciones posibles de los vértices de un grafo a los vértices del otro y eso es no computable para casos no demasiado grandes.

§ *Ejercicios*

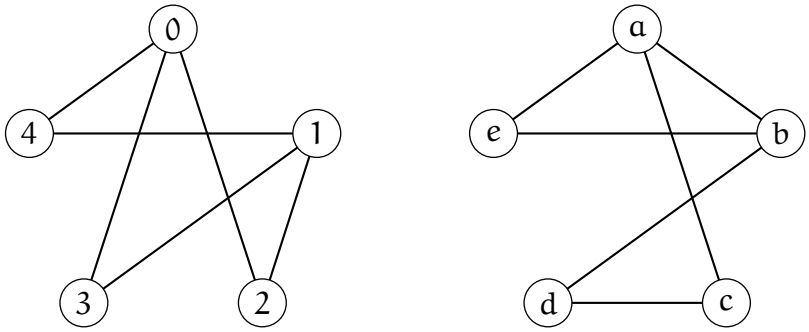
1) ¿Es posible que las siguientes listas sean las valencias de todos los vértices de un grafo? Si así lo fuera, dar una representación pictórica de tal grafo. (Recordar que hay a lo más una arista que una un par de vértices dados.)

   *a)* $2, 2, 2, 3$.
   *b)* $1, 2, 2, 3, 4$.
   *c)* $2, 2, 4, 4, 4$.
   *d)* $1, 2, 3, 4$.

2) Si $G = (V, E)$ es un grafo, el *complemento* $G^c$ de $G$ es el grafo cuyo conjunto de vértices es $V$ y cuyas aristas unen aquellos vértices que no son unidos por $G$. Si $G$ tiene $n$ vértices y sus valencias son $d_1, d_2, \ldots, d_n$, ¿cuáles son las valencias de $G^c$?

3) Probar que dos grafos $G_1$ y $G_2$ son isomorfos si y solo si $G_1^c$ y $G_2^c$ son isomorfos.

4) Usando la propiedad anterior probar que los siguientes grafos no son isomorfos.




$G_1$ $G_2$

5) Encontrar todos los grafos posibles (no isomorfos) que pueda, que sean regulares, 4-valentes y con 7 vértices. [Ayuda: considere el complemento de esos grafos.]

6) Probar que si G es un grafo con al menos dos vértices, entonces G tiene dos vértices con la misma valencia.

## 5.4 CAMINOS Y CICLOS

Frecuentemente usamos grafos como modelos de situaciones prácticas que involucran rutas: los vértices representan ciudades o cruces, y cada arista representa una ruta o cualquier otra forma de comunicación. Las definiciones de esta sección se comprenderán mejor con esta clase de ejemplo en mente.

**Definición 5.4.1.** Una *caminata* en un grafo G es una secuencia de vértices

$$v_1, v_2, \ldots, v_k,$$

tal que $v_i$ y $v_{i+1}$ son adyacentes ($1 \leqslant i \leqslant k-1$). Si todos los vértices son distintos, una caminata es llamada un *camino*.

Un *recorrido* es una caminata $v_1, v_2, \ldots, v_k$ donde todas las aristas $\{v_i, v_{i+1}\}$ con $1 \leqslant i \leqslant k-1$ son distintas.

Llamaremos *ciclo* a una caminata $v_1, v_2, \ldots, v_{r+1}$ con $r \geqslant 3$ y cuyos vértices son distintos exceptuando los extremos, es decir que $v_1, v_2, \ldots, v_r$ es un camino de al menos tres vértices y $v_1 = v_{r+1}$. A menudo diremos que es un $r$-*ciclo*, o un ciclo de *longitud* $r$ en G.

Es decir, una caminata especifica una ruta en G: del primer vértice vamos a uno adyacente, de éste a otro adyacente y así siguiendo. En una caminata podemos visitar cualquier vértice varias veces, y en particular, podemos ir de un vértice $x$ a otro $y$ y luego tomar la dirección contraria y regresar a $x$. En un camino, cada vértice es visitado solo una vez.

Escribamos $x \sim y$ siempre y cuando $x = y$ o $x \neq y$ y los vértices $x$ e $y$ de $G$ puedan ser unidos por un camino en $G$. Hablando en forma rigurosa, esto significa que cuando $x \neq y$ que hay un camino $v_1, v_2, \ldots, v_k$ en $G$ con $x = v_1$ e $y = v_k$.

**Lema 5.4.2.** *Sea $G$ un grafo y $x$, $y$ vértices distintos. Entonces, $x \sim y$ si y sólo si $x$ e $y$ pueden ser unidos por una caminata*

*Demostración.* Es claro que si $x$ e $y$ están unidos por un camino, como un camino es un caso especial de caminata, $x$ e $y$ están unidos por una caminata.

Veamos que si $x$ e $y$ están unidos por una caminata, entonces están unidos por un camino. Sea

$$x = x_1, x_2, \ldots, x_k = y,$$

una caminata entre $x$ e $y$. Si ninguno de los $x_i$ se repite, entonces tenemos un camino y terminado el problema. Si hay repetición, entonces existe $j$ tal que $x_j = x_{j+r}$ con $r > 0$, es decir tenemos una caminata

$$x = x_1, x_2, \ldots, x_j, \ldots, x_{j+r}, \ldots, x_k = y,$$

Como $x_j = x_{j+r}$ podemos eliminar la subcaminata $x_{j+1}, \ldots, x_{j+r}$ (un "bucle" dentro de la caminata) y nos queda

$$x = x_1, x_2, \ldots, x_j, x_{j+r+1}, \ldots, x_k = y,$$

una caminata, más corta, entre $x$ e $y$. Esto se ejemplifica en la figura 9.

Podemos repetir este procedimiento hasta eliminar todos los "bucles" y obtener un camino. □

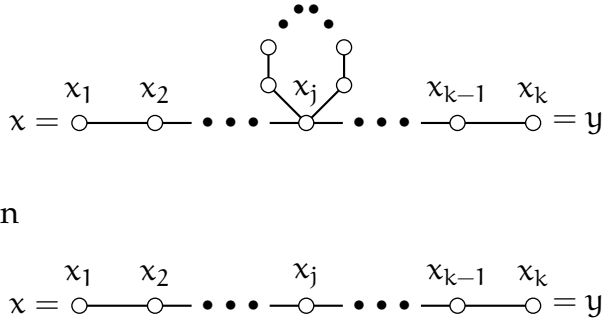



Figura 9: Eliminando "bucles" de una caminata

**Definición 5.4.3.** Diremos que un grafo $G$ es *conexo* si para cualesquiera dos vértices $x, y$ existe un camino de $x$ a $y$, es decir si $x \sim y$.

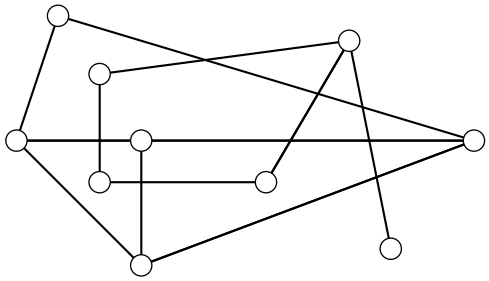


Figura 10: Un grafo con dos componentes

Debido al lema que probamos más arriba, es sencillo verificar la siguientes propiedades: sea G grafo y sean $x, y, z$ vértices de G, entonces

*a)* $x \sim x$ (reflexividad de $\sim$).

*b)* $x \sim y$, entonces $y \sim x$ (simetría de $\sim$).

*c)* $x \sim y$, $y \sim z$, entonces $x \sim z$ (transitividad de $\sim$).

En un lenguaje formal, una relación que cumple las tres propiedades anteriores es llamada una *relación de equivalencia* del conjunto, en este caso tenemos una relación de equivalencia del conjunto de vértices V de G. Como ya vimos en el capítulo 4, página 72, la congruencia módulo es también una relación de equivalencia, y hay muchísimos ejemplos en matemática de estos tipos de relaciones.

Estas tres propiedades que posee la relación de equivalencia permiten partir a V en conjuntos disjuntos: dos vértices están en el mismo conjunto si ellos pueden ser unidos por un camino, y están en conjuntos diferentes si no podemos encontrar tal camino. llamaremos a estos conjuntos disjuntos las *clases de equivalencia de* $\sim$.

**Definición 5.4.4.** Supongamos que $G = (V, E)$ es un grafo y que la partición de V en las clases de equivalencia de $\sim$ es

$$V = V_1 \cup V_2 \cup \cdots \cup V_r.$$

Denotemos con $E_i$ $(1 \leqslant i \leqslant r)$ al subconjunto de E que contiene todas las aristas cuyos finales están en $V_i$. Entonces los grafos $G_i = (V_i, E_i)$ son llamados las *componentes* de G. Si G tiene solo una componente entonces, claramente, el grafo es conexo.

La terminología casi explica por si misma el significado de estas definiciones. El grafo mostrado en la Fig. 10 tiene dos componentes, y por consiguiente no es conexo. La descomposición de un grafo en componentes es muy útil, puesto que muchas propiedades de los grafos pueden ser

establecidas considerando las componentes separadamente. Por esta razón, teoremas acerca de grafos a menudo son probados solo para la clase de grafos conexos.

Cuando un grafo de moderado tamaño es dado por una representación pictórica es bastante fácil determinar si es o no conexo. Sin embargo, cuando un grafo es dado por una lista de adyacencia necesitaremos un algoritmo eficiente para decidir si es o no conexo.

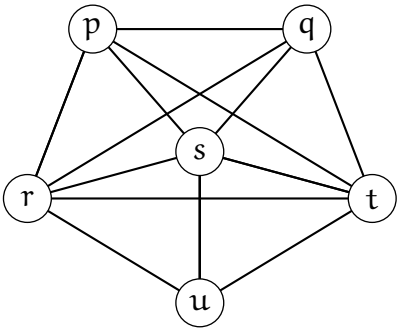



Figura 11: El gran tour

*Ciclos hamiltonianos, caminatas eulerianas*

*Ejemplo* 5.4.5. Leandro y Juan, dos amigos, planean tomar sus vacaciones en determinada isla. La Fig. 11 representa los lugares de interés turístico de la isla y las carreteras que los unen. Leandro es un turista por naturaleza, y desea visitar cada lugar una vez y volver al punto de partida. Juan es un explorador, y desea atravesar todos los caminos solo una vez, a él lo tiene sin cuidado si regresa o no al lugar del cual partió. ¿Podrán encontrar las rutas que desean Leandro y Juan?

*Solución.* Leandro puede usar diferentes rutas para alcanzar su objetivo: una posibilidad es el ciclo $p, q, t, s, u, r, p$.

Sin embargo, Juan está en un apuro. Llamemos $x$ al punto de partida y llamemos $y$ al punto de llegada, y supongamos por el momento que $x \neq y$. Entonces él usa una arista con extremo en $x$ para partir y cada vez que vuelve a $x$ debe arribar y partir por nuevas aristas. Luego, usa un número impar de aristas con extremo en $x$, y por consiguiente $x$ debe ser un vértice impar. De manera análoga, $y$ debe ser también un vértice impar, puesto que Juan usa dos aristas cada vez que pasa por $y$, y una más al finalizar en $y$. Los restantes vértices deben ser pares, puesto que cada vez que Juan llega a un vértice intermedio parte de nuevo, y por consiguiente usa dos aristas.

Resumiendo, una ruta para Juan que empiece y finalice en vértices distintos $x$ e $y$, es solo posible si hay dos vértices impares (que son $x$ e $y$) y el resto de los vértices es par. Pero en el grafo de la Fig. 11 el valor de las valencias es: $\delta(p) = 4$, $\delta(q) = 4$, $\delta(r) = 5$, $\delta(s) = 5$, $\delta(t) = 5$, y $\delta(u) = 3$. Luego hay demasiados vértices impares, y por lo tanto no existe la ruta que Juan desea. Si permitimos la posibilidad de que $x = y$ , la situación es aún peor, pues en este caso todos los vértices deberían ser pares. □

En general, la ruta de Leandro es un ciclo que contiene todos los vértices del grafo dado. Tales ciclos fueron estudiados por el matemático irlandés W.R. Hamilton ($1\,805 - 65$), y en consecuencia un ciclo con esta propiedad es llamado un *ciclo hamiltoniano*. En nuestro ejemplo, fue muy fácil encontrar un ciclo hamiltoniano, pero este fue un caso muy especial y no representativo. Para ciertos grafos, puede ser un problema difícil decidir si un ciclo hamiltoniano existe o no.

Por otro lado, el problema de Juan puede ser fácilmente resuelto. Una caminata que use cada arista de un grafo solo una vez, o equivalentemente un recorrido que use todas las aristas, es llamada una *caminata euleriana*, debido a que Euler fue el primero en estudiar estas caminatas y encontró que si $x \neq y$, una condición necesaria para que exista una caminata euleriana que comience en $x$ y finalice en $y$ es que $x$ e $y$ deben ser vértices impares y el resto debe ser par, mientras que si $x = y$ la condición es que todos los vértices deben ser pares. Es decir que una condición necesaria para que exista una caminata euleriana en un grafo $G$ es que $G$ debe tener a lo más dos vértices impares. Más aún, puede probarse que esta condición es también suficiente. Puesto que es sencillo calcular las valencias de los vértices de un grafo, es relativamente sencillo decidir si un grafo tendrá o no una caminata euleriana.

Resumiendo las definiciones de más arriba:

**Definición 5.4.6.** Un *ciclo hamiltoniano* en un grafo $G$ es un ciclo que contiene a todos los vértices del grafo. Una *caminata euleriana* en un grafo $G$ es un recorrido que usa todas las aristas de $G$. Una caminata euleriana que comienza y termina en un mismo vértice se llama también *circuito euleriano*.

*Ejemplo.* En el ejemplo 5.1.3 vimos que dado $n \in \mathbb{N}$, entonces el grafo rueda $W_n$ tiene ciclos hamiltonianos. Con el resultado del teorema 5.4.7 veremos que el grafo rueda nunca tiene caminatas eulerianas.

El siguiente teorema resume los resultados sobre caminatas eulerianas. La demostración no es demasiada complicada, pero la veremos más adelante.

**Teorema 5.4.7.** *Un grafo conexo con más de un vértice posee una caminata euleriana de $v$ a $w$, con $v \neq w$ si y sólo si $v$ y $w$ son los únicos vértices de grado impar. Un grafo conexo con más de un vértice tiene un circuito euleriano si y sólo si todos los vértices tienen grado par.*

*Observación* 5.4.8. El caso de un grafo donde todas las valencias son pares se puede reducir al anterior: si deseamos una caminata euleriana que empiece y termine en $v$, eliminamos una arista del grafo que contenga a $v$, digamos la arista $\{v, w\}$ (con lo cual queda un grafo con solo dos vértices, $v$ y $w$, de valencia impar), aplicamos el caso anterior, con lo cual hacemos una caminata euleriana que termina en $w$, y terminamos la caminata agregando la arista $\{v, w\}$.

*Observación* 5.4.9. Recíprocamente, el caso de un grafo G con dos valencias impares y todas las demás valencias pares se puede reducir al caso en que todas las valencias son pares. Sean p y q los dos vértices de valencia impar, entonces tenemos dos casos (1) $\{p, q\}$ es arista de G y (2) $\{p, q\}$ no es arista de G. En el caso (1), eliminamos la arista $\{p, q\}$ del grafo y nos queda un grafo con todos los vértices de valencia par. Por lo tanto, hay un circuito euleriano de p a p. Agregamos al final la arista $\{p, q\}$ y obtenemos una caminata euleriana de p a q. El caso (2) es un poco más complicado: agregamos al grafo G la arista $\{p, q\}$ y obtenemos un grafo con todos los vértices de valencia par. Luego hay un circuito euleriano de q a q. Podemos describir el circuito como

$$q, v_1, \ldots, v_k, q, p, w_1, \ldots, w_r, q.$$

A partir de este circuito podemos obtener la caminata

$$p, w_1, \ldots, w_r, q, v_1, \ldots, v_k, q,$$

que es una caminata euleriana.

*Algoritmo de Hierholzer*

C. Hierholzer (1840-1871) mostró, poco antes de su muerte, un algoritmo fácilmente implementable para encontrar un circuito euleriano para cualquier grafo con vértices de grado par. El algoritmo de Hierholzer fue la primera demostración del teorema 5.4.7 para el caso de grafos con vértices de grado par. Nosotros veremos aquí una versión del algoritmo de Hierholzer que se aplica tanto a los grafos con todos los vértices de valencia par como, a los que tienen dos vértices de valencia impar.

Para explicar el algoritmo de Hierholzer nos es útil la siguiente definición: un *recorrido maximal* es un recorrido que respetando la condición de no

repetir aristas no es posible continuarlo como recorrido desde el último vértice.

La idea clave del algoritmo de Hierholzer es la siguiente.

**Lema 5.4.10.** *(1) En un grafo de valencias pares (conexo o no conexo) todo recorrido maximal termina en el vértice original.*

*(2) En un grafo conexo con dos vértices de valencia impar todo recorrido maximal que parte de un vértice de valencia impar termina en el otro vértice de valencia impar.*

*Demostración.* (1) Observar que no es posible quedarse atascado en ningún vértice que no sea el vértice original, porque el grado par de todos los vértices garantiza que, cuando se ingresa a un vértice distinto al original debe haber una arista sin usar que nos permite dejarlo.

(2) Saliendo del vértice original, y razonando en forma análoga a (1), podemos ver fácilmente que el recorrido maximal termina en el vértice impar que no es el origen. □

Teniendo en cuenta las consideraciones anteriores podemos plantear el siguiente algoritmo:

Sea G un grafo conexo con vértices de grado par o con dos vértices de grado impar y los demás de grado par.

(1) **Paso 0.** Elija el vértice inicial $v$. Si G tiene todos sus vértices de grado par, elija cualquier vértice. Si G tiene dos vértices de grado impar, elija un vértice de valencia impar.

(2) **Paso 1.** Haga un recorrido maximal partiendo de $v$.

(3) **Paso iterativo**

- Mientras en la caminata ya realizada exista un vértice $u$ que tenga aristas que no formen parte de la caminata, realice otro recorrido maximal que parte de $u$ siguiendo las aristas no utilizadas.
- Inserte en $u$ este recorrido a la caminata anterior obteniendo una nueva caminata (más larga).
- Si aún queda alguna arista sin recorrer vuelva al inicio del paso iterativo.

Observemos que el recorrido del paso 1 en el caso del grafo con todas las valencias pares, es un recorrido cerrado. En el caso del grafo con dos valencias impares es un recorrido que va de un vértice impar al otro.

En cualquier de los dos casos, en el paso 1 el recorrido maximal puede no cubrir todos los vértices y aristas del grafo inicial. Además, observemos que el subgrafo que se obtiene eliminando las aristas del recorrido tiene todas las valencias pares.

En el paso iterativo el subgrafo de las aristas disponibles tiene todos los vértices de valencia par y por lo tanto el recorrido comienza y termina en el mismo vértice y allí se inserta.

Puesto que suponemos que el grafo original es conexo, repetir el paso iterativo agotará todos las aristas del grafo.

*Ejemplo.* Dado el grafo de de la Fig. 12, encontremos un circuito euleriano con origen en $u$.

Debemos primero observar que debe existir un circuito euleriano, pues $\delta(p) = 4$, $\delta(q) = 4$, $\delta(r) = 4$, $\delta(s) = 4$, $\delta(t) = 4$, y $\delta(u) = 2$, es decir todos los vértices tienen grado par.

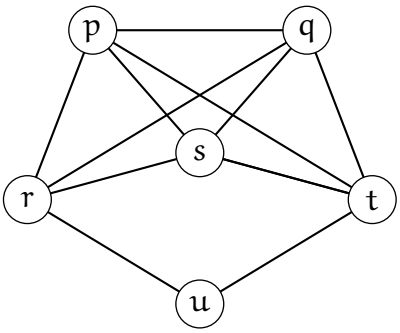



Figura 12: El gran tour, de nuevo.

Apliquemos el algoritmo de Hierholzer partiendo desde $u$. Una caminata posible con origen en $u$ y que vuelva a $u$ es

$$u, r, p, q, s, t, u.$$

Ahora elijamos $q$ que es un vértice que pertenece a la caminata pero que tiene aristas que no son parte de la caminata (ver figura 13). Una caminata que no toca aristas usadas y que parte de $q$ y regresa a $q$ es $q, t, p, s, r, q$. Insertamos en $q$ esta caminata a la caminata anterior y obtenemos:

$$u, r, p, \mathbf{q, t, p, s, r, q}, s, t, u.$$

(En negrita la caminata insertada).

*Observación.* Escribiremos en pseudocódigo el algoritmo de Hierholzer para hallar un circuito euleriano en un grafo $G$ con $n$ vértices de valencia par o una caminata euleriana en un grafo con dos valencias impares.

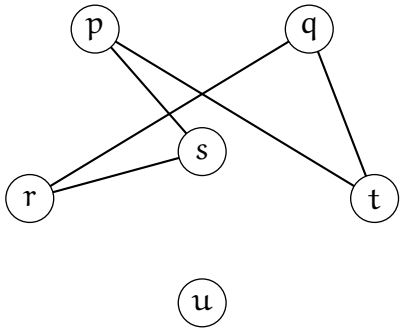



Figura 13: El subgrafo de aristas no utilizadas.

Como ya mencionamos anteriormente, a un grafo G lo representaremos por una lista de adyacencia. Supongamos que los vértices de G son $0, \ldots, k$, entonces $G[i] = [i_0, i_1, \ldots]$ serán los vértices adyacentes al vértice $i$. Tomamos como comienzo del recorrido el vértice $0$. En el caso de los grafos con valencia impar el vértice $0$ debe ser impar.

Primero daremos el pseudocódigo para encontrar un recorrido maximal.

RECORRIDO MAXIMAL

```
def r_max(L, v_ini):
    # pre: L grafo, v_ini vértice de L
    # post: devuelve un recorrido maximal que comienza en v_ini
    # mod: se quitan de L las aristas utilizadas
    sub_caminata = [v_ini]  # sub caminata
    p0 = v_ini
    while len(L.adyacentes(p0)) > 0:
        p1 = L.adyacentes(p0)[0] # p1 primer adyacente a p0
        sub_caminata.append(p1) # agrega p1 a caminata
        L.quitar_arista((p0,p1)) # quita arista {p0, p1}
        p0 = p1
    return sub_caminata
```

Ahora, implementamos el circuito euleriano o caminata euleriana, según corresponda, con el uso de la función `r_max()`.

### Circuito/Caminata euleriana

```
# pre: G grafo con todos los vértices de valencia par o dos impares
# post: cuando termina 'cam' es una lista de vértices que es
#       una caminata o circuito euleriano que empieza en 0.
libres = G.copiar() # sub grafo de aristas no utilizadas
cam = r_max(libres, 0) # recorrido maximal desde v = 0
while len(libres.aristas()) > 0:
    for v in libres.vertices():
        if len(libres.adyacentes(v)) > 0 and v in cam:
            pos = cam.index(v)
            cam  =  cam[:pos] + r_max(libres, v) + cam[pos+1:]
```

Cuando el algoritmo termina la variable `cam` es una lista que describe la caminata o circuito euleriano. En el algoritmo, `cam.index(v)` indica en que lugar de la caminata se encuentra `v` y `libres.adyacentes(v)` indica la lista de vértices adyacentes a `v` en el grafo `libres`.

§ *Ejercicios*

1) Encontrar el número de componentes de el grafo cuya lista de adyacencia es

| a | b | c | d | e | f | g | h | i | j |
|---|---|---|---|---|---|---|---|---|---|
| f | c | b | h | c | a | b | d | a | a |
| i | g | e | | g | i | c | | f | f |
| j | | g | | | j | e | | | |

2) ¿Cuántas componentes conexas tiene el grafo de la fiesta de Abril (sección 5.1)?

3) Encontrar un ciclo hamiltoniano en el grafo formado por los vértices y aristas de un cubo.

4) El año que viene el Leandro y Juan desean visitar otra isla, donde los lugares interesantes y las caminos que los unen están representados por el grafo que tiene la siguiente lista de adyacencia

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 0 | 3 | 0 | 1 | 0 | 1 |
| 3 | 2 | 3 | 2 | 5 | 4 | 5 | 2 | 3 |
| 5 | 6 | 7 | 4 | | 6 | 7 | 6 | 5 |
| 7 | 8 | | 8 | | 8 | | 8 | 7. |

¿Es posible encontrar rutas para Leandro y Juan que satisfagan lo pedido en el ejemplo 5.4.5?

5) Un ratón intenta comer un $3 \cdot 3 \cdot 3$ cubo de queso. Él comienza en una esquina y come un subcubo de $1 \cdot 1 \cdot 1$, para luego pasar a un subcubo adyacente. ¿Podrá el ratón terminar de comer el queso en el centro?

## 5.5 ÁRBOLES

**Definición 5.5.1.** Diremos que un grafo conexo $T$ es un *árbol* si no hay ciclos en $T$.

Algunos árboles típicos han sido dibujados en la Fig. 14. A causa de su particular estructura y propiedades, los árboles aparecen en diversas aplicaciones de la matemática, especialmente en investigación operativa y ciencias de la computación. Comenzaremos el estudio de ellos estableciendo algunas propiedades sencillas.

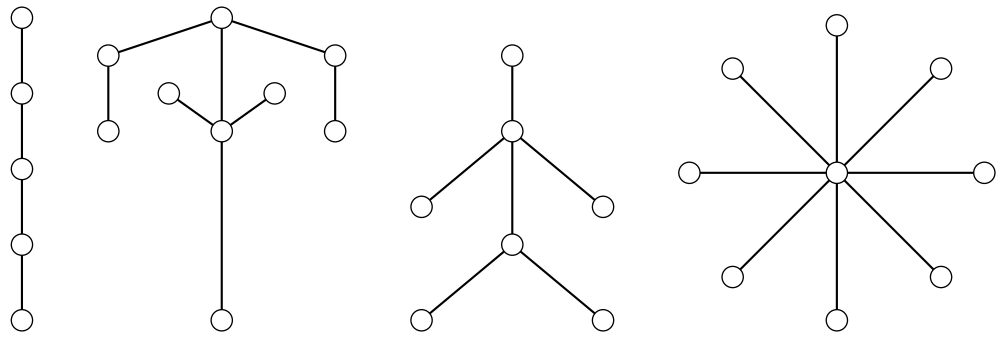


Figura 14: Algunos árboles

El siguiente lema nos resultará útil para probar una parte del teorema fundamental de esta sección.

**Lema 5.5.2.** *Sea* $G = (V, E)$ *un grafo conexo, entonces* $|E| \geqslant |V| - 1$.

*Demostración.* Como $G$ es conexo existe una caminata que recorre todos los vértices de $G$:

$$v_1, v_2, \ldots, v_r.$$

Renombremos los vértices de $G$ con números naturales de tal forma que el primer vértice de la caminata sea 1, el segundo 2 y cada vez que aparece un vértice que no ha sido renombrado se le asigna el número siguiente. Luego la caminata comienza en 1 y termina en $n$, donde $n = |V|$. Observar que cada vez que renombramos un vértice (excepto el primero) su antecesor es menor, es decir dado $i$ tal que $1 < i \leqslant n$ tenemos que la caminata tiene la forma

$$1, \ldots, j_i, i, \ldots, j_n, n$$

donde $j_i < i$, luego es claro que

$$\{j_2, 2\}, \{j_3, 3\}, \ldots, \{j_n, n\}$$

forman un conjunto de $n-1$ aristas distintas en $G$. □

**Teorema 5.5.3.** *Si $T = (V, E)$ es un grafo conexo con al menos dos vértices, entonces son equivalentes las siguientes propiedades*

***(T1)*** *$T$ no tiene ciclos.*

***(T2)*** *Para cada par $x$, $y$ de vértices existe un único camino en $T$ de $x$ a $y$.*

***(T3)*** *El grafo obtenido de $T$ removiendo cualquier arista tiene dos componentes conexas.*

***(T4)*** $|E| = |V| - 1$.

*Demostración.* Vamos a probar **(T1)** $\Rightarrow$ **(T2)** $\Rightarrow$ **(T3)** $\Rightarrow$ **(T1)**, lo cual prueba las equivalencias entre **(T1)**, **(T2)**, **(T3)**. También probaremos que **(T2)** $\Leftrightarrow$ **(T4)**, lo cual prueba la equivalencia entre todas las afirmaciones.

**(T1)** $\Rightarrow$ **(T2)**. Puesto que $T$ es conexo, existe un camino de $x$ a $y$, digamos

$$x = v_0, v_1, \ldots, v_r = y.$$

Si existiera otro camino, digamos

$$x = u_0, u_1, \ldots, u_s = y,$$

consideremos $i$ el más pequeño subíndice para el cual se cumple que $u_{i+1} \neq v_{i+1}$ Fig. 15.

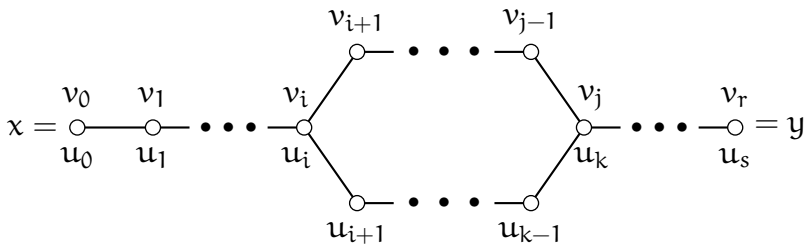



Figura 15: Dos caminos diferentes determinan un ciclo

Puesto que ambos caminos finalizan en $y$ ellos se encontrarán de nuevo, y entonces podemos definir $j$ como el más pequeño subíndice tal que

$$j > i \quad y \quad v_j = u_k \quad \text{para algún } k.$$

Entonces $v_i, v_{i+1}, \ldots, v_j, u_{k-1}, u_{k-2}, \ldots, u_{i+1}, v_i$ es un ciclo en $T$, y esto contradice a las hipótesis. Por consiguiente solo existe un camino en $T$ de $x$ a $y$.

**(T2)** $\Rightarrow$ **(T3)**. Sea $uv$ arista de $T$ y sea $F = T - uv$, es decir el grafo con el mismo conjunto de vértices que $T$ y con el conjunto de aristas $E' = E - uv$.

Como hay un único camino de $u$ a $v$, si eliminamos $uv$ el grafo se parte en dos componentes conexas: $T_1$ el subgrafo que es la componente conexa de $u$ y $T_2$ el subgrafo que es la componente conexa de $v$.

Más explícitamente, los vértices de $T_1$ son los $x \in V$ tales que el camino que que une $x$ con $u$ no pasa por $v$ y los vértices de $T_2$ son los $x \in V$ tales que el camino que que une $x$ con $u$ pasa por $v$.

**(T3)** $\Rightarrow$ **(T2)**. Supongamos que exista $T$ con la propiedad **(T3)** y que no cumple la propiedad **(T2)**, es decir existen $u, v$ vértices tales que hay dos caminos distintos $C_1$ y $C_2$ de $u$ a $v$. Como $C_1 \neq C_2$, existe una arista $xy$ tal que $C_2 = u \cdots xy \cdots v$ y $xy$ no es parte del $C_1$. $C_2$ es la concatenación $C_2 = C_3 xy C_4$ donde $C_3 = u \cdots x$ y $C_4 = y \cdots v$ son el subcamino inicial y final, respectivamente, de $C_2$.

Sea $G' = T - xy$, veamos que $G'$ es conexo. Sean $a, b$ vértices, como el grafo $T$ es conexo hay un camino $C$ de $a$ a $b$. Si el camino no utiliza la arista $xy$ entonces hay un camino de $a$ a $b$ en $G'$. En caso contrario el camino es $C = a \cdots xy \cdots b$ (o, análogamente $b \cdots xy \cdots a$ ). De este camino obtenemos dos subcaminos $C_5 = a \cdots x$ y $C_6 = b \cdots y$ tal que $C = C_5 xy C_6$. Por lo tanto, podemos hacer un camino concatenando subcaminos:

$$a \overset{C_5}{\cdots} x \overset{C_3^{-1}}{\cdots} u \overset{C_1}{\cdots} v \overset{C_4^{-1}}{\cdots} y \overset{C_6}{\cdots} b$$

(ver Fig. 16). Aquí denotamos $C_3^{-1}$ el camino $C_3$ recorrido en sentido inverso. Análogo para $C_4^{-1}$.

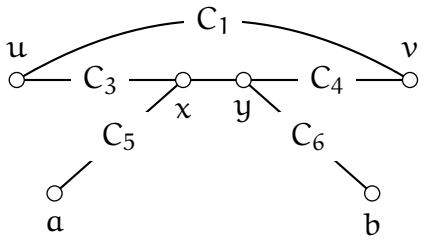



Figura 16: Caminos entre dos vértices

El camino $C_5 C_3^{-1} C_1 C_4^{-1} C_6$ une $a$ con $b$ sin pasar por $xy$ y en consecuencia es un camino en $G'$. Es decir, bajo las hipótesis, para cualesquiera $a, b$ siempre hay un camino de $a$ a $b$ en $G'$ y por lo tanto $G'$ es conexo. Esto nos lleva a un absurdo que vino de suponer que $T$ no cumple **(T2)**.

**(T2)** $\Rightarrow$ **(T4)**. Se hará por inducción completa en $|V|$.

Si $|V| = 2$ el resultado es obviamente cierto.

Veamos el caso $|V| > 2$. Sea $uv$ arista de $T$ y sea $F = T - uv$, es decir el grafo con el mismo conjunto de vértices que $T$ y con el conjunto de aristas $E' = E - uv$.

Por **(T2)** $\Rightarrow$ **(T3)**, $F$ tiene dos componentes conexas $T_1 = (V_1, E_1)$ y $T_2 = (V_2, E_2)$. En cada componente conexa hay un único camino de un vértice a otro, pues sino esa propiedad no se cumpliría en $T$. Además,

$$|V_1| + |V_2| = |V|, \qquad |E_1| + |E_2| = |E| - 1.$$

Aplicando la hipótesis inductiva a $T_1$ y $T_2$ obtenemos que

$$|E| = |E_1| + |E_2| + 1 \overset{(HI)}{=} |V_1| - 1 + |V_2| - 1 + 1 = |V| - 1,$$

como nosotros deseábamos.

**(T4)** $\Rightarrow$ **(T1)**. Supongamos que $T$ satisface **(T4)** pero tiene ciclos. Si eliminamos una arista del ciclo, el grafo sigue siendo conexo, pero con una arista menos (y la misma cantidad de vértices), es decir obtenemos un grafo $G' = (V', E')$ conexo y con $|E'| = |V'| - 2$. Pero esto contradice el resultado obtenido en el lema 5.5.2.

□

Las propiedades **(T2)**, **(T3)** y **(T4)** nos dan maneras alternativas de definir árboles. Por ejemplo la propiedad **(T2)** puede ser considerada como la propiedad que define un árbol, en vez de **(T1)**.

*Observación.* El teorema anterior nos muestra un recurso muy usado para probar que una cierta cantidad de afirmaciones son equivalentes. En el caso de 4 afirmaciones $P_1$, $P_2$, $P_3$, $P_4$, uno debería probar

$$P_1 \Leftrightarrow P_2, \quad P_1 \Leftrightarrow P_3, \quad P_1 \Leftrightarrow P_4, \quad P_2 \Leftrightarrow P_3, \quad P_2 \Leftrightarrow P_4, \quad P_3 \Leftrightarrow P_4.$$

Estas son 12 demostraciones que nos garantizan la equivalencia entre $P_1$, $P_2$, $P_3$ y $P_4$. Sin embargo, podemos ahorrar trabajo demostrando solamente

$$P_1 \Rightarrow P_2, \qquad P_2 \Rightarrow P_3, \qquad P_3 \Rightarrow P_4, \qquad P_4 \Rightarrow P_1$$

que son 4 demostraciones o, por ejemplo, como en el teorema anterior,

$$P_1 \Rightarrow P_2, \qquad P_2 \Leftrightarrow P_3, \qquad P_2 \Rightarrow P_4, \qquad P_4 \Rightarrow P_1,$$

que son 5 demostraciones.

En cualquiera de los dos casos podemos hacer una cadena de "implicas" que nos permite probar $P_i \Rightarrow P_j$ para cualesquiera $i, j$ y, por lo tanto, $P_i \Leftrightarrow P_j$ para cualesquiera $i, j$.

§ *Ejercicios*

1) Hay seis diferentes (es decir, no isomorfos entre si) árboles con seis vértices: hacer un dibujo de ellos.

2) Sea $T = (V, E)$ un árbol con $|V| \geqslant 2$. Usando la propiedad **(T4)** y el teorema 5.3.1 probar que $T$ tiene al menos dos vértices con valencia 1.

3) Una *foresta* es un grafo que satisface que no contiene ciclos pero no necesariamente es conexo. Probar que si $F = (V, E)$ es una foresta con $c$ componentes entonces

$$|E| = |V| - c.$$

## 5.6 COLOREO DE LOS VÉRTICES DE UN GRAFO

Un problema que se nos presenta frecuentemente en la vida moderna es aquel de confeccionar un horario para un conjunto de eventos de tal manera de evitar interferencias. Consideremos ahora un caso muy simple, que nos servirá de ejemplo para mostrar como la teoría de grafos puede ayudar al estudio de este problema.

Supongamos que deseamos hacer un horario con seis cursos de una hora, $v_1, v_2, v_3, v_4, v_5, v_6$. Entre la audiencia potencial hay gente que desea asistir a $v_1$ y $v_2$, $v_1$ y $v_4$, $v_3$ y $v_5$, $v_2$ y $v_6$, $v_4$ y $v_5$, $v_5$ y $v_6$ y $v_1$ y $v_6$. ¿Cuántas horas son necesarias para poder confeccionar un horario en el cual no haya interferencias?

Podemos representar la situación por un grafo Fig. 17. Los vértices corresponden a las seis clases, y las aristas indican las interferencias potenciales.

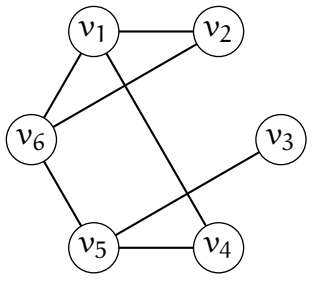



Figura 17: El grafo para un problema de horarios

Un horario el cual cumple con la condición de evitar interferencias es el siguiente:

| Hora 1 | Hora 2 | Hora 3 | Hora 4 |
|---|---|---|---|
| $v_1$ y $v_3$ | $v_2$ y $v_4$ | $v_5$ | $v_6$ |

(ver Fig. 18).

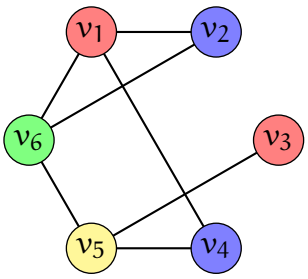



Figura 18: Un grafo coloreado con 4 colores

En términos matemáticos, tenemos una partición del conjuntos de vértices en cuatro partes, con la propiedad que ninguna parte contiene un par de vértices adyacentes del grafo. Un descripción más gráfica utiliza la función

$$c : \{v_1, v_2, v_3, v_4, v_5, v_6\} \to \{1, 2, 3, 4\}$$

la cual asigna cada vértice (curso) a la hora que le corresponde. Usualmente, nosotros hablamos de colores asignados a los vértices, en vez de horas, pero claramente la naturaleza exacta de los objetos $1, 2, 3, 4$ no es importante. Podemos usar el nombre de colores reales, rojo, verde, azul , amarillo, o podemos hablar del color 1, color 2, etc. Lo importante es que los vértices que son adyacentes en el grafo deben tener diferentes colores.

**Definición 5.6.1.** Una *coloración de vértices* de un grafo $G = (V, E)$ es una función $c : V \to \mathbb{N}$ con la siguiente propiedad:

$$c(x) \neq c(y) \quad \text{si} \quad \{x, y\} \in E.$$

El *número cromático* de $G$, denotado $\chi(G)$, se define como el mínimo entero $k$ para el cual existe una coloración de vértices de $G$ usando $k$-colores. En otra palabras, $\chi(G) = k$ si y sólo si existe una coloración de vértices $c$ la cual es una función de $V$ a $\mathbb{N}_k$, y $k$ es el mínimo entero con esta propiedad.

Volviendo al ejemplo de la Fig. 17, vemos que nuestro primer intento de horario es equivalente a una coloración de vértices con cuatro colores. El mínimo número de horas necesarias será el número cromático del grafo, y la pregunta es ahora si este número es cuatro o menor que cuatro. Un rápido intento con tres colores nos da la solución de este problema:

| Color 1 | Color 2 | Color 3 |
|---|---|---|
| $v_1$ | $v_2$ y $v_5$ | $v_3, v_4$ y $v_6$ |

(ver Fig. 19). Más aún, hacen falta por lo menos tres colores, puesto que $v_1$, $v_2$, y $v_6$ son mutuamente adyacentes y por lo tanto deben tener diferentes colores. Luego concluimos que el número cromático del grafo es 3.

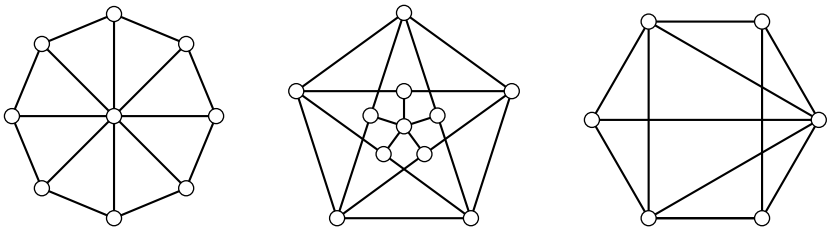
En general, para probar que el número cromático de un grafo dado es $k$, debemos hacer dos cosas:

*a)* encontrar una coloración de vértices usando $k$ colores;

*b)* probar que ninguna coloración de vértices usa menos de $k$ colores.

§ *Ejercicios*

1) Encontrar el número cromático de los siguientes grafos:
   *a)* un grafo completo $K_n$;
   *b)* un grafo cíclico $C_{2r}$ con un número par de vértices;
   *c)* un grafo cíclico $C_{2r+1}$ con un número impar de vértices.
2) Determinar los números cromáticos en los siguientes grafos:



3) Describir todos los grafos $G$ tales que $\chi(G) = 1$.

## 5.7 ALGORITMOS GREEDY EN GRAFOS

Es bastante difícil encontrar el número cromático de un grafo dado. En realidad, no se conoce ningún algoritmo para este problema que trabaje en "tiempo polinomial", y la mayoría de la gente cree que tal algoritmo no existe. Sin embargo hay un método simple de hacer una coloración cromática usando un "razonable" número de colores.

El método consiste en asignar los colores de los vértices en orden, de tal manera que cada vértice recibe el primer color que no haya sido ya asignado a alguno de sus vecinos. En este algoritmo insistimos en hacer la mejor elección que podemos en cada paso, sin mirar más allá para ver si esta elección nos traerá problemas luego. Un algoritmo de esta clase se llama a menudo un *algoritmo greedy (goloso)*.

El algoritmo greedy para coloración de vértices es fácil de programar. Supóngase que hemos dado a los vértices algún orden $v_0, v_1, \ldots, v_n$. Asignemos el color $0$ a $v_0$ y luego le vamos asignando un color a los subsiguientes

vértices: para cada $v_i$ ($1 \leqslant i \leqslant n$) formamos el conjunto $S$ de colores asignados a los vértices $v_j$ ($0 \leqslant j < i$) que son adyacentes a $v_i$, y le damos a $v_i$ el primer color que no está en $S$. (En la práctica, pueden ser usados métodos más sofisticados de manejar los datos.)

ALGORITMO GREEDY PARA COLORACIÓN DE VÉRTICES

```
# pre: 0,...,n los vértices de un grafo G
# post: devuelve v[0],...,v[n] una coloración de G
color = []  #  color[j] = c dirá que el color de j es c.
for i = 0 to n:
    S = []  # S conjunto de colores asignados a los vértices j
            # (1 <= j <i) que son adyacentes a i (comienza vacío)
    for j = 0 to i-1:
        if j es adyacente a i:
           S.append(color[j])  # agrega el color de j a  S
    k = 0
    while k in S:
        k = k + 1
    color.append(k) # Asigna el color k a i, donde k es el primer
                    # color que no esta en S.
```

Debido a que la estrategia greedy es corta de vista, el número de colores que usará será normalmente más grande que le mínimo posible. Por ejemplo, el algoritmo greedy aplicado en el grafo de Fig. 17 con el orden $v_1, v_2, v_3, v_4, v_5, v_6$ da precisamente la coloración de vértices con cuatro colores que fue propuesta anteriormente (ver de la Fig. 18).

*Ejemplo.* Sea G el grafo de la Fig. 17, si aplicamos el algoritmo greedy de coloración de vértices con el orden $v_3, v_4, v_6, v_2, v_5, v_1$ obtenemos la coloración de vértices de la Fig. 19.

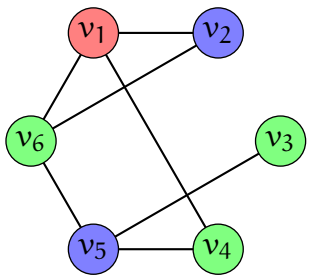



Figura 19: Un grafo coloreado con 3 colores

Cuando aplicamos greedy la coloración depende del orden que se elige inicialmente para los vértices. Es bastante fácil ver que si se elige el orden correcto, entonces el algoritmo greedy nos da la mejor coloración posible

(ejercicio 5.7-(2)). Pero hay $n!$ órdenes posibles, y si tuviéramos que controlar cada uno de ellos, el algoritmo requeriría "tiempo factorial" que en la práctica no es computable para $n$ relativamente pequeño.

Más allá de esto, el algoritmo greedy es útil tanto en la teoría como en la práctica. Probaremos ahora dos teoremas por medio de la estrategia greedy.

**Teorema 5.7.1.** *Si* $G$ *es un grafo con valencia máxima* $k$*, entonces*

*a)* $\chi(G) \leqslant k+1$,

*b) Si* $G$ *es conexo y no regular ,* $\chi(G) \leqslant k$.

*Demostración.*

*a)* Sea $v_1, v_2, \ldots, v_n$ un ordenamiento de los vértices de G. Cada vértice tiene a lo más $k$ vecinos, y por consiguiente el conjunto $S$ de los colores asignados por el algoritmo greedy a los vértices $v_j$ que son adyacentes a $v_i$ $(1 \leqslant j < i)$ tiene como máximo cardinal $k$. Por consiguiente al menos uno de los colores $1, 2, \ldots, k+1$ no está en $S$, y el algoritmo greedy asigna entonces el primero de estos a $v_i$.

*b)* Para probar esta parte debemos elegir un orden especial de los vértices.

1. Sea $v_n$ un vértice con $\delta(v_n) < k$. Este vértice existe, pues el grafo es no regular.
2. Sean $v_{n-1}, v_{n-2}, \ldots, v_{n-r}$ los adyacentes a $v_n$.
3. Luego se van listando consecutivamente los adyacentes a $v_i$ que no están listados antes $(n > i \geqslant 1)$.

Puesto que $G$ es conexo, este método garantiza que podremos listar todos los vértices de $G$.

Por la forma de construir la lista, si $i < n$ el vértice $v_i$ tiene un adyacente a nivel superior, es decir un $v_j$ con $j > i$, luego, como $\delta(v_i) \leqslant k$,

$$\text{si } i < n,\ v_i \text{ tiene a lo más } k-1 \text{ adyacentes a nivel inferior.} \qquad (*)$$

Hagamos el coloreo del grafo usando el algoritmo greedy considerando el orden $v_1, \ldots, v_n$.

Cuando $i < n$, por (*), se puede colorear $v_i$ con un color en $\{1, \ldots, k\}$.

Cuando $i = n$, como $\delta(v_n) < k$, se puede colorear $v_n$ con un color en $\{1, \ldots, k\}$.

De esta forma concluimos que se puede colorear $G$ con $k$ colores.

□

La parte *b)* del teorema es falsa si permitimos que G sea regular. El lector que haya respondido correctamente al ejercicio *1* de la sección 5.6 será capaz de dar dos ejemplos de este hecho: los grafos cíclicos de longitud impar tienen grado 2 y número cromático 3 y los grafos completos de $k+1$ vértices tienen grado $k$ y número cromático $k+1$. Si embargo, puede ser demostrado que estos son los únicos contraejemplos.

Otra consecuencia útil del algoritmo greedy se refiere a grafos G son $\chi(G) = 2$. Para tales grafos, los conjuntos $V_1$ y $V_2$ de vértices de colores 1 y 2 respectivamente, forman una partición de $V$, con la propiedad que cada arista tiene un vértice en $V_1$ y el otro en $V_2$. Por esta razón, cuando $\chi(G) = 2$, diremos que G es *bipartito*. Una coloración de vértices con dos colores de un cubo se ilustra en la Fig. 20, junto a un dibujo alternativo que enfatiza la naturaleza bipartita del grafo. Usualmente usaremos esta clase de dibujo, la de la derecha, cuando trabajemos con grafos bipartitos.

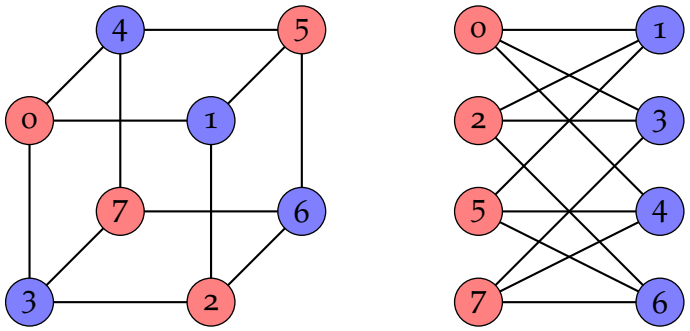



Figura 20: El cubo es un grafo bipartito

**Teorema 5.7.2.** *Un grafo es bipartito si y sólo si no contiene ciclos de longitud impar.*

*Demostración.* Si hay un ciclo de longitud impar, entonces se requieren tres colores, solamente para colorear este ciclo, y el número cromático del grafo es por ende al menos tres. Luego si el grafo es bipartito, no puede tener ciclos de longitud impar.

Recíprocamente, supongamos que G es un grafo sin ciclos de longitud impar. Construiremos un orden de G para el cual el algoritmo greedy producirá una coloración de vértices con dos colores. Elijamos cualquier vértice y llamémoslo $v_1$; diremos que $v_1$ esta en el *nivel* 0. A continuación, listemos la lista de vecinos de $v_1$ y llamemos a estos vértices $v_2, v_3, \ldots, v_r$. Diremos entonces que los vértices $v_2, v_3, \ldots, v_r$ están en el *nivel 1*. Continuando de esta manera, definimos el *nivel* $i$ como todos aquellos vértices adyacentes a los del nivel $i-1$, exceptuando aquellos previamente listados en el nivel

$i-2$. Cuando ningún nuevo vértice puede ser agregado de esta forma, obtenemos la componente $G_0$ de $G$ (si $G$ es conexo $G_0 = G$).

El hecho crucial producido por este orden es que un vértice del nivel $i$ solo puede ser adyacente a vértices de los niveles $i-1$ y $i+1$, y no a vértices del mismo nivel. Supongamos que $x$ e $y$ son vértices en el mismo nivel; entonces ellos son unidos por caminos de igual longitud $m$ a algún vértice $z$ de un nivel anterior, y los caminos pueden ser elegidos de tal manera que $z$ sea el único vértice común Fig. 21. Si $x$ e $y$ fueran adyacentes, habría un ciclo de longitud $2m+1$, lo cual contradice la hipótesis.

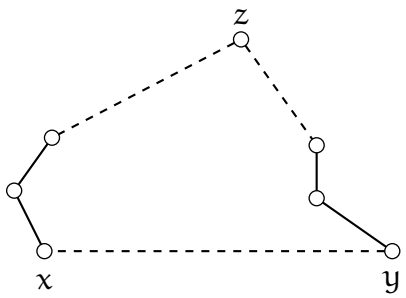



Figura 21: Vértices adyacentes en el mismo nivel inducen un ciclo impar

Se deduce entonces que el algoritmo greedy asigna el color 1 a los vértices en el nivel $0, 2, 4, \ldots$, y el color 2 a los vértices en los niveles $1, 3, 5, \ldots$. Por consiguiente $\chi(G_0) = 2$. Repitiendo el mismo argumento para cada componente de $G$ obtenemos el resultado deseado. □

§ *Ejercicios*

1) Encontrar órdenes de los vértices del grafo del cubo Fig. 20 para los cuales el algoritmo greedy requiera 2, 3 y 4 colores respectivamente.

2) Probar que para cualquier grafo $G$ existe un orden de los vértices para el cual el algoritmo greedy requiera $\chi(G)$ colores. [Ayuda: use un coloreado de vértices de $\chi(G)$ colores para definir el orden.]

3) Denotar $e_i(G)$ el número de vértices del grafo $G$ cuya valencia es estrictamente mayor que $i$. Usar el algoritmo greedy para probar que si $e_i(G) \leqslant i+1$ para algún $i$, entonces $\chi(G) \leqslant i+1$.

4) El grafo $M_r$ ($r \geqslant 2$) se obtiene a partir del grafo cíclico $C_{2r}$ añadiendo aristas extras que unen los vértices opuestos. Probar que

   *a)* $M_r$ es bipartito cuando $r$ es impar,

   *b)* $\chi(M_r) = 3$ cuando $r$ es par y $r \neq 2$,

*c)* $\chi(M_2) = 4$.

# 6

# ÁRBOLES (*)

## 6.1 CONTANDO LAS HOJAS DE UN ÁRBOL CON RAÍZ

Recordemos que un árbol es un grafo conexo que no contiene ciclos. Los árboles aparecen en contextos diferentes y a menudo un vértice del árbol se distingue de los otros. Por ejemplo en el árbol genealógico que describe la descendencia de un rey, nosotros podemos enfatizar la posición especial del rey poniéndolo en lo más alto del árbol. En general, nosotros llamaremos al vértice notable la *raíz* del árbol, y a un árbol con una raíz específica lo llamaremos *árbol con raíz*. (Esta terminología, aunque estándar, tiene el defecto que en la representación pictórica la raíz aparece en lo más alto del árbol y el árbol 'crece' hacia abajo.)

Para el estudio de un árbol con raíz es natural ubicar los vértices en niveles, de la misma manera que lo hicimos para los grafos bipartitos en la sección 5.7. Diremos que el vértice raíz es el *nivel* $0$ y que sus vecinos forman el *nivel* $1$. Para cada $k \geqslant 2$, el *nivel* $k$ está formado por aquellos vértices que son adyacentes a vértices del nivel $k-1$, excepto aquellos que ya pertenecen al nivel $k-2$. El árbol con raíz representado en la Fig. 22 puede ser dibujado nuevamente como se lo muestra a la derecha de manera de visualizar los niveles.

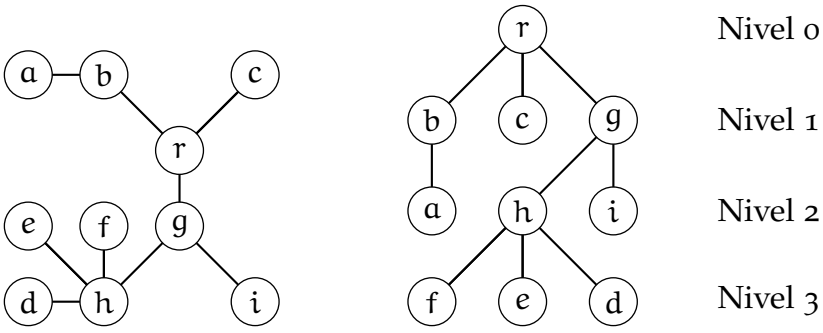



Figura 22: Un árbol con raíz y sus niveles

Un vértice en un árbol con raíz se llama una *hoja* si pertenece al nivel $i$ ($i \geqslant 0$) y no es adyacente a ningún vértice del nivel $i+1$. Un vértice que no es una hoja es llamado *interno*. La *altura* de un árbol con raíz es el máximo

valor de $k$ para el cual el nivel $k$ es no vacío. Luego el árbol de la Fig. 22 tiene seis hojas, cuatro vértices internos y su altura es tres.

Las dos propiedades que usamos en la sección 5.5 para definir un árbol, ser un grafo conexo y sin ciclos, tienen consecuencias obvias cuando pensamos los vértices por niveles. Puesto que todo árbol es conexo entonces cada vértice pertenece a algún nivel. Más importante aún, puesto que un árbol no tiene ciclos cada vértice $v$ del nivel $i$ es adyacente a uno y solo uno $u$ del nivel $i-1$. A veces enfatizaremos esto diciendo que $u$ es el *padre* de $v$ o que $v$ es un *hijo* de $u$. Cada vértice, excepto el raíz, tiene un único padre, pero un vértice puede tener una cantidad arbitraria de hijos (incluso ninguno). Claramente, un vértice es una hoja si y solo si no tiene hijos.

En muchas aplicaciones ocurre que cada padre (vértice interno) tiene la misma cantidad de hijos. Cuando cada padre tiene $m$ hijos diremos que el árbol es $m$-*ario*, en particular cuando $m = 2$ diremos que el árbol es *binario* y cuando $m = 3$ diremos que es *ternario*.

**Teorema 6.1.1.** *La altura de un árbol con raíz $m$-ario con $l$ hojas es por lo menos* $\log_m l$.

*Demostración.* Puesto que

$$h \geqslant \log_m l \quad \Leftrightarrow \quad m^h \geqslant l$$

es suficiente probar la afirmación equivalente: todo árbol con raíz $m$-ario de altura $h$ tiene a lo más $m^h$ hojas. La demostración es por inducción sobre $h$.

Claramente la afirmación es verdadera cuando $h = 0$ puesto que en este caso el árbol es solo un vértice (la raíz) que es una hoja. Supongamos que la afirmación es verdadera cuando $0 \leqslant h \leqslant h_0$ y sea $T$ un árbol con raíz $m$-ario de altura $h_0 + 1$. Si eliminamos la raíz y las aristas a las cuales pertenece obtenemos $m$ árboles $T_1, \ldots, T_m$ cuyas raíces son los vértices del nivel $1$ de $T$. Cada $T_i$ es un árbol con raíz de altura $h_0$ o menos, luego por hipótesis inductiva tiene a lo más $m^{h_0}$ hojas. Pero las hojas de $T$ son precisamente las hojas de los árboles $T_1, \ldots, T_m$ y por consiguiente el número de hojas es a lo más $m \cdot m^{h_0} = m^{h_0+1}$.

Por el principio de inducción completa se sigue que la afirmación es verdadera para todo $h \geqslant 0$. □

Puesto que $\log_m l$ no es generalmente un número entero, el teorema anterior puede ser mejorado un poco. Por ejemplo si $m = 3$ y $l = 10$ la desigualdad

$$h \geqslant \log_m l = 2,0959\ldots$$

implica que $h \geqslant 3$. En general podemos decir que

$$h \geqslant \lceil \log_m l \rceil,$$

donde $\lceil x \rceil$ denota el menor entero $z$ tal que $z \geqslant x$.

Una aplicación frecuente del teorema 6.1.1 es en los *árboles de decisión*. Cada vértice interno de un árbol de decisión representa una decisión y los posibles resultados de esa decisión son las aristas que unen ese vértice con los vértices del nivel siguiente. Los posibles esultados finales del procedimiento son las hojas del árbol. Si el resultado de una decisión puede ser solo verdadero o falso entonces tenemos un árbol binario. A continuación daremos un ejemplo con un árbol ternario.

*Ejemplo* 6.1.2. (El problema de la moneda falsa) Supongamos que tenemos una moneda genuina con la etiqueta 0 y que tenemos otras $r$ monedas indistinguibles de 0 por la apariencia excepto que tienen las etiquetas $1, 2, \ldots, r$. Se sospecha que una moneda podría ser falsa, es decir o más liviana o más pesada. Probemos que son necesarias al menos $\lceil \log_3(2r+1) \rceil$ pesadas en una balanza para decidir que moneda (si hay alguna) es falsa y en ese caso ver si es más pesada o liviana. Mostremos un procedimiento que use exactamente este número de pesadas cuando $r = 4$.

*Solución.* Hay $2r+1$ posibles resultados finales u hojas en el árbol de decisión:

$$B, 1P, 1L, \ldots, rP, rL;$$

donde B significa que todas las monedas son buenas, $iL$ significa que la moneda $i$ es más liviana y $iP$ que es más pesada. El árbol de decisión es ternario, puesto que hay tres posibles resultados de cada decisión (es decir de cada pesada entre un grupo de monedas y otro). Estos son:

$<$ : el grupo de la izquierda es más liviano
$=$ : los dos grupos pesan igual
$>$ : el grupo de la izquierda es más pesado.

Por consiguiente la altura del árbol de decisión es al menos $\lceil \log_3(2r+1) \rceil$.

Cuando $r = 4$ entonces $\lceil \log_3(2r+1) \rceil = 2$, y la solución con dos pesadas se gráfica en la Fig. 23

□

§ *Ejercicios*

1) En la siguiente tabla $n_5(h)$ es el número de árboles con raíz no isomorfos que tienen 5 vértices y altura $h$. (Dos árboles con raíz son isomorfos

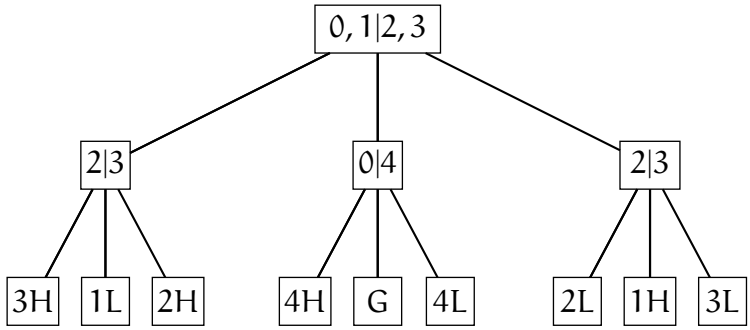



Figura 23: Solución del problema de la moneda falsa cuando $r = 4$

si hay un isomorfismo de grafos, sin considerar la raíz, que lleva la raíz de uno en la del otro.) Verificar la tabla construyendo los ejemplos para cada caso.

| $h$: | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| $n_5(h)$: | 1 | 4 | 3 | 1 |

2) Si se consideran los árboles comunes (sin raíz), ¿cuál es el número de árboles no isomorfos con 5 vértices? Hacer una lista y controlar que la lista del ejercicio anterior sea completa.

3) Construir dos árboles con raíz no isomorfos ambos con 12 vértices, 6 hojas y altura 4.

4) Suponer que se organiza un campeonato de fútbol-5 donde participan 20 equipos. El campeonato es por eliminación simple y no hay empates. Construir un esquema para el torneo basado en un árbol con raíz y pruebar que son necesarias al menos 5 rondas.

5) ¿Cuál es la cota inferior en el número de pesadas necesarias en el problema de la moneda falsa (ver el ejemplo 6.1.2) cuando son seis monedas? Desarrollar un esquema que logre este número de pesadas.

6) Considerar la siguiente variante del problema de la moneda falsa. Hay ocho monedas y sabemos que hay exactamente una que es más liviana. Todas las demás son genuinas pero no hay ninguna moneda con la etiqueta 0. Encontrar una cota inferior teórica del número de pesadas necesarias para detectar la moneda falsa y probar que este número puede ser alcanzado.

## 6.2 ÁRBOLES EXPANDIDOS Y EL PROBLEMA MST

**Definición 6.2.1.** Sea $G = (V, E)$ es un grafo conexo y $T$ es un subconjunto de $E$ tal que

*a)* cada vértice de G pertenece a una arista en T;

*b)* las aristas de T forman un árbol.

En este caso decimos que T es un *árbol expandido* para G.

Por ejemplo, un árbol expandido para el grafo de la Fig. 24 se indica con las líneas más gruesas.

Es fácil hacer "crecer" un árbol expandido: tome un vértice arbitrario $v$ del "árbol parcial" inicial y agregue aristas con un extremo en $v$ y el otro extremo que no pertenezca al árbol parcial inicial. El árbol expandido de la Fig. 24 puede construirse haciéndolo crecer desde el vértice $a$ y conectando los otros vértices en el orden $b$, $c$, $e$, $f$, $d$, $h$, $g$, usando las aristas $ab$, $ac$, $ae$, $cf$, $fd$, $fh$, $hg$. En general, si hay $n$ vértices nosotros deberemos hacer $n-1$ pasos, después de los cuales tendremos $1+(n-1)=n$ vértices y $n-1$ aristas (el cual es el número correcto de acuerdo al teorema 5.5.3).

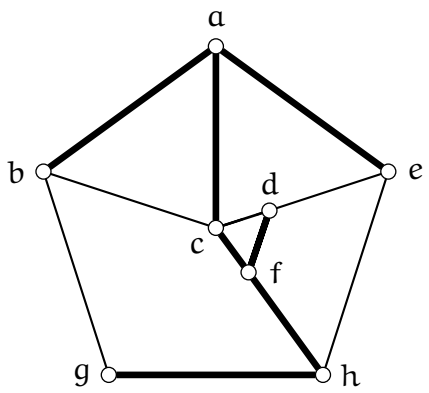



Figura 24: Un grafo y uno de sus árboles expandidos

Verifiquemos que el método siempre funciona: sea S el conjunto de vértices del árbol parcial que se ha logrado en un paso intermedio, es decir que S no es ni vacío ni todo V. Si no existe una arista que tenga un extremo en S y el otro en el complemento $\overline{S}$, entonces no existe un camino entre S y $\overline{S}$ y por lo tanto G es disconexo, lo cual contradice las hipótesis. Por consiguiente siempre existe una arista disponible en cada etapa de la construcción.

Los árboles expandidos son útiles en muchos contextos. Por ejemplo, supongamos que cierta cantidad de ciudades deben ser unidas de a pares por gasoductos de tal forma que quede una red de gasoductos conexa. Algunos pares de ciudades puede ser imposible unirlas por razones geográficas y cada posible conexión tiene asociada un costo de construcción. Formalmente, tenemos un grafo $G=(V,E)$ cuyos vértices son ciudades y sus aristas son las posibles conexiones. Además tenemos una función $w$ de E a $\mathbb{N}$ de tal

forma que $w(e)$ representa el costo de construcción de la arista $e$. Diremos que G y $w$ es un *grafo con pesos* y que $w$ es la *función de pesos*.

En el problema del gasoducto lo que se pretende es construir una red conexa al mínimo costo. Un red de ese tipo corresponde a un árbol expandido T para G cuyo peso total

$$w(T) = \sum_{e \in T} w(e)$$

es lo mas pequeño posible. Nos referiremos a este problema como el *problema MST* (del inglés MST = minimum spanning tree = árbol expandido mínimo) para el grafo con pesos G.

Dado que los valores de $w$ son enteros positivos, claramente el problema MST debe tener solución, puesto que hay solo un número finito de árboles expandidos T para G y cada uno de ellos da un valor entero positivo $w(T)$. En otras palabras, existe un árbol expandido mínimo $T_0$ tal que

$$w(T_0) \leqslant w(T)$$

para todos los árboles expandidos T de G. Sin embargo puede haber varios con la misma propiedad.

Un algoritmo simple para el problema MST se basa en aplicar la estrategia greedy al método explicado anteriormente. Específicamente: en cada paso se agrega la arista "más barata" que une un nuevo vértice al árbol parcial. (Si hay varias aristas con la misma propiedad se selecciona una de ellas.) Por ejemplo, si en la Fig. 25 comenzamos con $u$, luego debemos agregar aristas en el orden $uv$, $ux$, $uy$, $yz$. Por otro lado, si comenzáramos por $y$, entonces agregamos las aristas en el orden $yz$, $yu$, $uv$, $ux$.

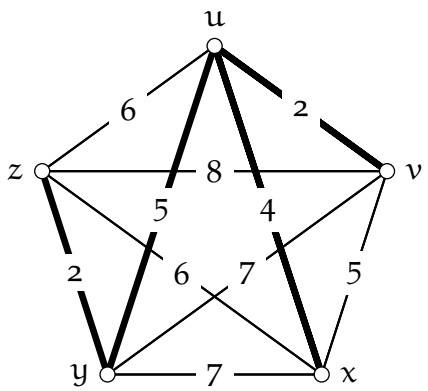



Figura 25: Un árbol expandido mínimo

El algoritmo puede ser descripto informalmente en los siguientes pasos:

- Inicializar un árbol con un sólo vértice (elegido arbitrariamente).

- Agrandar el árbol agregando una arista: entre las aristas que conectan al árbol con vértices que aún no están en el árbol, elegir una de peso mínimo.
- Repetir el paso anterior hasta que todos los vértices estén en el árbol

Un primera impresión nos dice que sería bastante sorprendente que el algoritmo greedy funcione para el problema MST, especialmente cuando recordamos que el algoritmo greedy para el problema de coloración de vértices no siempre produce una coloración con el menor número posible de colores. Pero en el caso del problema MST se tiene más suerte.

**Teorema 6.2.2.** *Sea* $G = (V, E)$ *grafo conexo con función de pesos* $w : E \to \mathbb{N}$*, y supongamos que* $T$ *es el árbol expandido para* $G$ *construido por el algoritmo greedy. Entonces*

$$w(T) \leqslant w(U)$$

*para todo árbol expandido* $U$ *de* $G$*.*

*Demostración.* Denotemos $e_1, e_2, \ldots, e_{n-1}$ las aristas de $T$ en el orden en que aplicamos el algoritmo greedy. Si $U = T$ el resultado es obviamente verdadero. Si $U \neq T$ entonces hay aristas de $T$ que no están en $U$ y supongamos que la primera es $e_k$. Denotemos $S$ el conjunto de vértices en el árbol parcial que se construye por el greedy justo antes de agregar $e_k$ y sea $e_k = xy$ donde $x$ está en $S$ e $y$ no está en $S$. Puesto que $U$ es un árbol expandido existe un camino de $x$ a $y$ y si uno viaja a través de este camino encontrará una arista $e^*$ con un vértice en $S$ y el otro no. Ahora bien, cuando $e_k$ es seleccionada para $T$ en el algoritmo greedy, $e^*$ es también candidata a ser seleccionada, pero no lo es. Por consiguiente debemos tener que $w(e^*) \geqslant w(e)$. Si $e^*$ aparece en $T$, entonces por el razonamiento anterior es una arista que viene después (en el orden dado) de $e_k$.

El resultado de remover $e^*$ de $U$ y reemplazarla por $e_1$ es un árbol expandido $U_1$, para el cual

$$w(U_1) = w(U) - w(e^*) + w(e_k) \leqslant w(U).$$

Más aún, la primera arista de $T$ que no está en $U_1$ aparece después de $e_k$ en el orden dado. En consecuencia podemos repetir el procedimiento obteniendo una sucesión de árboles expandidos $U_1, U_2, \ldots$, con la propiedad que cada uno tiene una secuencia inicial de aristas en común con las aristas de $T$ más larga que el anterior y además $w(U_i) \geqslant w(U_{i+1})$. El proceso termina cuando obtenemos un árbol expandido $U_r$ igual a $T$ y tenemos

$$w(T) = w(U_r) \leqslant w(U_{r-1}) \leqslant \cdots \leqslant w(U_1) \leqslant w(U),$$

como queríamos demostrar. □

En forma más detallada, el algoritmo puede ser implementado con el siguiente pseudocódigo:

ALGORITMO DE PRIM

```
# pre: G grafo con vértices 0,...,n y pesos w(i,j)
#      (w(i,j) = infinito si ij no es arista de G)
# post: devuelve F un MST de G
Q = [1,,...,n]  # lista de vértices aún no utilizados en el MST
S = [0] # lista de vértices ya utilizados en el MST
# L = [[k, 0, pesos[k][0]] : k en Q]
# L se ira modificando de tal forma que si
# Q = [u0,...,uk] no utilizados en F
# S = utilizados en F
# L  = [[ui,vi,w(ui,vi)]: 0 <= i <= k, vi in S tq w(ui,vi) mínimo]
F[i] = [],  0 <= i <= n # grafo con vértices 0,...,n y sin aristas.
while Q != []:
    L.sort(por coordenada 2) # ordena L por pesos
    [u,v,p] = L[0]
    # u en Q, v en S, tal que p = w(u,v) es mínimo
    F.agregar_arista({u, v})
    L.remove([u, v, w(u,v)])
    Q.remove(u)
    S.append(u)
    for i in range(len(L)):
        u' = L[i][0]
        if w[u'][u] < L[i][2]:
            L[i][1] = u
            L[i][2] = w[u'][u]
    # el for actualiza la lista L
return F
```

Notemos que terminamos el proceso no cuando $S$ contiene todos los vértices, si no cuando, de manera equivalente, su complemento $Q$ queda vacío. Existe una forma de ir viendo el progreso del algoritmo por medio de una tabla de tres columnas.

| I | II | III |
|---|---|---|
| $x$ | $y$ | $w(xy)$ |
| . | . | . |
| . | . | . |
| . | . | . |

La Columna I lista los vértices que no están en $S$, que es el conjunto de vértices ya conectados al árbol parcial. Para cada $x$ en la Columna I la correspondiente entrada $y$ en la Columna II es un vértice en $S$ tal que la

arista $xy$ es una de las aristas más baratas que unen el vértice $x$ con alguno de $S$. La Columna III contiene el valor $w(xy)$.

En el $i$-ésimo paso de la construcción tenemos que $|S| = i$ y hay $n-i$ vértices en la Columna I. Tenemos entonces que seleccionar una de las entradas más pequeñas de la Columna III, digamos $w(x_0y_0)$, y esto conlleva $n-i-1$ comparaciones. Ahora debemos actualizar la tabla debido a que agregamos $x_0$ a $S$ por medio de la arista $x_0y_0$. Primero debemos borrar la fila cuya primera posición tiene a $x_0$. Después en cada fila debemos verificar si la entrada correspondiente a la Columna II puede ser reemplazada por $x_0$ o no. Es decir para la fila "$x \quad y \quad w(xy)$" debemos verificar si $xx_0$ es arista y si lo fuera y además $w(xx_0) < w(xy)$, entonces debemos reemplazar $y$ por $x_0$. Esto agrega otras $n-i-1$ comparaciones. El número total de comparaciones requeridas es

$$\sum_{i=1}^{n-1} 2(n-i-1) = (n-1)(n-2).$$

Esto nos dice que para encontrar un MST de un grafo deben hacerse alrededor de $n^2$ operaciones.

§ *Ejercicios*

1) Encontrar árboles expandidos para el cubo Fig. 20 y para el grafo de Petersen.

2) Muestrar esquemáticamente todos los árboles expandidos del grafo completo $K_4$ (hay 16).

3) Usar el algoritmo greedy para encontrar un MST del grafo representado en la Fig. 26. ¿Es en este caso el MST único?

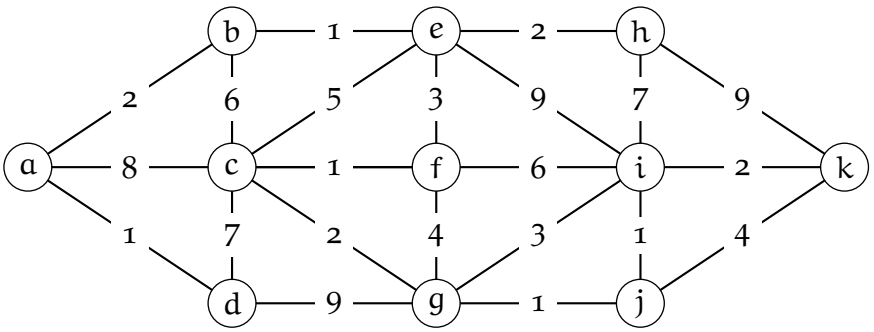



Figura 26: Encontrar el MST

4) Sea $G$ un grafo con pesos cuyos vértices son $x, a, b, c, d, e, f$ y cuyas aristas y pesos vienen dados por la siguiente tabla:

| xa | xb | xc | xd | xe | xf | ab | bc | cd | de | ef | fa |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 6 | 3 | 2 | 4 | 3 | 7 | 6 | 2 | 3 | 1 | 8 | 6. |

Encontrar todos los árboles expandidos mínimos para G.

5) Suponer que T es un árbol expandido mínimo en un grafo con pesos K y sea $e^*$ una arista de K que no es de T. Sea $e$ una arista de T perteneciente al único camino en T que une los vértices de $e^*$. Probar que $w(e) \leqslant w(e^*)$.

6) Escribir un "programa" para el algoritmo greedy basado en el método tabular mostrado más arriba.

Parte III

# APÉNDICES

# A

# PERMUTACIONES

## A.1 PERMUTACIONES

Recordemos que una *permutación* de un conjunto finito no vacío X es una biyección de X en X. (Frecuentemente tomamos X como $[[1,n]] = \{1,2,\ldots,n\}$.) Por ejemplo una permutación típica de $[[1,5]]$ es la función $\alpha$ definida por las ecuación

$$\alpha(1) = 2, \quad \alpha(2) = 4, \quad \alpha(3) = 5, \quad \alpha(4) = 1, \quad \alpha(5) = 3.$$

Denotemos el conjunto de todas las permutaciones de $[[1,n]]$ con $S_n$. Por ejemplo, $S_3$ contiene las $3! = 6$ permutaciones siguientes:

$$\begin{array}{ccc} 1&2&3\\ \downarrow&\downarrow&\downarrow\\ 1&2&3 \end{array} \quad \begin{array}{ccc} 1&2&3\\ \downarrow&\downarrow&\downarrow\\ 1&3&2 \end{array} \quad \begin{array}{ccc} 1&2&3\\ \downarrow&\downarrow&\downarrow\\ 2&1&3 \end{array} \quad \begin{array}{ccc} 1&2&3\\ \downarrow&\downarrow&\downarrow\\ 2&3&1 \end{array} \quad \begin{array}{ccc} 1&2&3\\ \downarrow&\downarrow&\downarrow\\ 3&1&2 \end{array} \quad \begin{array}{ccc} 1&2&3\\ \downarrow&\downarrow&\downarrow\\ 3&2&1 \end{array}$$

En la práctica, usualmente asignamos alguna interpretación concreta a un elemento de $S_n$. Como vimos en la sección 2.3, podemos usar la interpretación "selecciones ordenadas sin repetición" donde, en este caso seleccionamos los elementos de $\{1,2,3,\ldots,n\}$ en algún orden hasta que no queda ninguno. Una interpretación relacionada es que una permutación efectúa un *reacomodamiento* de $\{1,2,3,\ldots,n\}$; por ejemplo, la permutación $\alpha$ vista más arriba efectúa el reacomodamiento de 12 345, en 24 513, así:

$$\begin{array}{ccccc} 1&2&3&4&5\\ \downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\ 2&4&5&1&3 \end{array}$$

En algunas circunstancias es conveniente mirar una permutación y el correspondiente reacomodamiento como la misma cosa, pero esto puede traer dificultades si debemos considerar sucesivos reacomodamientos. Es importante tener en cuenta que

*una permutación es una función con ciertas características.*

Cuando las permutaciones son tratadas como funciones es claro como deben combinarse. Consideremos $\alpha$ la permutación de $[[1,5]]$ antes mencionada, y sea $\beta$ la permutación de $[[1,5]]$ dada por

$$\beta(1) = 3, \quad \beta(2) = 5, \quad \beta(3) = 1, \quad \beta(4) = 4, \quad \beta(5) = 2.$$

La función compuesta $\beta\alpha$ es la permutación definida por $(\beta\alpha)(i) = \beta(\alpha(i))$ $(1 \leqslant i \leqslant 5)$, esto es

$$\beta\alpha(1) = 5, \quad \beta\alpha(2) = 4, \quad \beta\alpha(3) = 2, \quad \beta(4)\alpha = 3, \quad \beta\alpha(5) = 1.$$

(Recordemos que, como siempre, $\beta\alpha$ significa "primero $\alpha$, entonces $\beta$".) En términos de reacomodamientos tenemos

$$\begin{array}{cccccc} & 1 & 2 & 3 & 4 & 5 \\ \alpha & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 2 & 4 & 5 & 1 & 3 \end{array}$$

$$\begin{array}{cccccc} & 1 & 2 & 3 & 4 & 5 \\ \beta & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 5 & 4 & 2 & 3 & 1 \end{array}$$

Existen cuatro características de la composición de permutaciones de gran importancia, y están listadas en el próximo teorema.

**Teorema A.1.1.** *Las siguientes propiedades valen en el conjunto $S_n$ de todas las permutaciones de $\{1, 2, 3, ..., n\}$.*

*a) Si $\pi$ y $\sigma$ pertenecen a $S_n$, entonces $\pi\sigma$ también.*

*b) Para cualesquiera permutaciones $\pi$, $\sigma$, $\tau$ en $S_n$,*

$$(\pi\sigma)\tau = \pi(\sigma\tau).$$

*c) La función identidad, denotada por* id *y definida por* $\mathrm{id}(r) = r$ *para todo* $r$ *en* $\mathbb{N}_n$*, es una permutación y para cualquier $\sigma$ en $S_n$, tenemos*

$$\mathrm{id}\,\sigma = \sigma\,\mathrm{id} = \sigma.$$

*d) Para toda permutación $\pi$ en $S_n$ hay una permutación inversa $\pi^{-1}$ en $S_n$ tal que*

$$\pi\pi^{-1} = \pi^{-1}\pi = \mathrm{id}\,.$$

*Demostración.* Todas las afirmaciones se deducen de propiedades conocidas de funciones en general y funciones biyectivas en particular. Por otro lado, es fácil convencerse de la validez de las mismas mirando las permutaciones como reacomodamiento de elementos. □

Es conveniente tener una notación más compacta para las permutaciones. Consideremos otra vez la permutación $\alpha$ de $\{1, 2, 3, 4, 5\}$, y notemos en particular que

$$\alpha(1) = 2, \qquad \alpha(2) = 4, \qquad \alpha(4) = 1.$$

Así $\alpha$ lleva 1 a 2, 2 a 4 y 4 a 1, y por esta razón decimos que los símbolos $1, 2, 4$ forma un *ciclo* (de longitud 3). Del mismo modo, los símbolos 3 y 5 forman un ciclo de longitud 2, y escribimos:

$$\alpha = (1\,2\,4)(3\,5).$$

Esta es la *notación cíclica* para $\alpha$. Cualquier permutación $\pi$ puede ser escrita cíclicamente de la siguiente manera:

- comencemos con algún símbolo (digamos el 1) y veamos el efecto de $\pi$ sobre él y sus sucesores hasta que alcancemos el 1 nuevamente;
- elijamos un símbolo que todavía no haya aparecido y construyamos el ciclo que se deriva de él;
- repitamos el procedimiento hasta que se terminen los símbolos.

Por ejemplo, la permutación $\beta$ definida antes tiene la notación cíclica

$$\beta = (1\,3)(2\,5)(4),$$

donde observamos que el símbolo 4 forma un ciclo "degenerado" por sí solo, puesto que $\beta(4) = 4$. En algunas ocasiones podemos omitir estos ciclos de longitud 1 cuando escribimos una permutación en notación cíclica, puesto que corresponden a símbolos que no son afectados por la permutación. Sin embargo, usualmente es útil *no* adoptar esta convención hasta que uno se familiariza con la notación.

Aunque la representación de una permutación en notación cíclica es esencialmente única, hay dos manera obvias en las que podemos cambiar la notación sin alterar la permutación. Primero, cada ciclo puede empezar en cualquiera de sus símbolos; por ejemplo $(7\,8\,2\,1\,3)$ y $(1\,2\,7\,8\,2)$ describen el mismo ciclo. Segundo, el orden de los ciclos no es importante; por ejemplo $(1\,2\,4)(3\,5)$ y $(3\,5)(1\,2\,4)$ denotan la misma permutación. Pero las características importantes son el número de ciclos, la longitud del ciclo, y la disposición de los símbolos dentro de los ciclos, y éstas están determinadas de manera única. Por eso, la rotación cíclica nos dice bastantes cosas útiles sobre una permutación.

*Ejemplo* A.1.2. Cartas numeradas del 1 al 12 son distribuidas en una mesa en la manera en que se muestra en la parte izquierda de la tabla que sigue. Luego las cartas son levantadas por filas (de izquierda a derecha y de arriba hacia abajo) y se redistribuyen con el mismo arreglo, pero por columnas, no por filas (de arriba hacia abajo y de izquierda a derecha), apareciendo como se muestra en la parte derecha de la tabla.

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |
| 10 | 11 | 12 |

| | | |
|---|---|---|
| 1 | 5 | 9 |
| 2 | 6 | 10 |
| 3 | 7 | 11 |
| 4 | 8 | 12 |

¿Cuántas veces debe repetirse este procedimiento hasta que las cortas aparezcan dispuestas como estaban inicialmente?

*Solución.* Sea $\pi$ la permutación que efectúa el reordenamiento; esto es $\pi(i) = j$ si la carta $j$ aparece en la posición previamente ocupada por la carta $i$. Trabajando con la notación cíclica para $\pi$ encontramos que

$$\pi = (1)(2\ 5\ 6\ 10\ 4)(3\ 9\ 11\ 8\ 7)(12).$$

Los ciclos degenerados $(1)$ y $(12)$ indican que las cartas 1 y 12 nunca cambian de posición. Las otros ciclos tienen longitud 5, así que cuando el proceso se haya realizado 5 veces las cartas reaparecerán en sus posiciones originales. Otra forma de expresar el resultado es decir que $\pi^5 = \mathrm{id}$, donde $\pi^5$ representa las cinco repeticiones de la permutación $\pi$. □

§ *Ejercicios*

1) Escribir en notación cíclica la permutación que realiza el siguiente reordenamiento:

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|
| ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ |
| 3 | 5 | 7 | 8 | 4 | 6 | 1 | 2 | 9 |

2) Sean $\sigma$ y $\tau$ las permutaciones de $[[1, 8]]$ cuyas representaciones en la notación cíclica son

$$\sigma = (1\,2\,3)(4\,5\,6)(7\,8), \qquad \tau = (1\,3\,5\,7)(2\,6)(4)(8).$$

Escribir en notación cíclica $\sigma\tau$, $\tau\sigma$, $\sigma^2$, $\sigma^{-1}$, $\tau^{-1}$.

3) Resolver el problema presentado en el ejemplo A.1.2 cuando hay 20 cartas acomodadas en 5 filas de 4.

4) Probar que hay exactamente tres elementos de $S_4$ que tienen dos ciclos de longitud 2, escritos en la notación cíclica.

5) Sea K el subconjunto de $S_4$ que contiene la identidad y las tres permutaciones descritas en el ejercicio previo. Escribir la "tabla de multiplicación" para K, interpretando la multiplicación como la composición de permutaciones.

6) Calcular en número total de permutaciones $\sigma$ de $[[1, 6]]$ que satisfacen $\sigma^2 = \mathrm{id}$ y $\sigma \neq \mathrm{id}$.

7) Sean $\alpha$ y $\beta$ permutaciones de $[[1, 9]]$ cuyas representaciones en la notación cíclica son:

$$\alpha = (1237)(49)(58)(6), \qquad \beta = (135)(246)(789).$$

Escribir en notación cíclica $\alpha\beta$, $\beta\alpha$, $\alpha^2$, $\beta^2$, $\alpha^{-1}$, $\beta^{-1}$.

8) Sea $X_1 = \{0, 1\}$, y para $i \geqslant 2$ definamos $X_i$ como el conjunto de subconjuntos de $X_{i-1}$. Encontrar el valor más pequeño para el cual $|X_i| > 10^{100}$.

9) Por cada entero $i$ en el rango $1 \leqslant i \leqslant n-1$ definimos $\tau_i$ como la permutación de $[[1, n]]$ que intercambia $i$ e $i+1$ y no afecta los otros elementos. Explícitamente

$$\tau_i = (1)(2)\cdots(i-1)(i\ i+1)(i+2)\cdots(n).$$

Probar que toda permutación de $[[1, n]]$ puede ser expresada en términos de $\tau_1, \tau_2, \ldots, \tau_{n-1}$.

10) Una permutación de $[[1, n]]$ que tenga solo un ciclo (necesariamente de longitud $n$) es llamada *cíclica* . Probar que hay $(n-1)!$ permutaciones cíclicas de $[[1, n]]$.

11) Un mazo de 52 cartas es dividido en dos partes iguales y luego se alternan las cartas de una y otra parte. Es decir si la numeración original era $1, 2, 3, \ldots, 54$, el nuevo orden es $1, 27, 2, 28, \ldots$ ¿Cuántas veces se debe repetir este procedimiento para obtener de nuevo el mazo original?

# B

# EL PRINCIPIO DEL TAMIZ

## B.1 EL PRINCIPIO DEL TAMIZ

El principio más básico del conteo (proposición 2.1.2) dice que $|A \cup B|$ es la suma de $|A|$ y $|B|$, cuando $A$ y $B$ son conjuntos disjuntos. Si $A$ y $B$ no son disjuntos, cuando sumamos $|A|$ y $|B|$ estamos contando $A \cap B$ dos veces. Entonces, para obtener la respuesta correcta debemos restar $|A \cap B|$:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Un método similar puede aplicarse a tres conjuntos. Cuando sumamos $|A|$, $|B|$ y $|C|$, los elementos de $A \cap B$, $B \cap C$, y $C \cap A$ son contados dos veces (si no están en los tres conjuntos). Para corregir esto, restamos $|A \cap B|$, $|B \cap C|$ y $|C \cap A|$. Pero ahora los elementos de $A \cap B \cap C$, contados originalmente tres veces, han sido descontados tres veces. Luego, para conseguir la respuesta correcta, debemos sumar $|A \cap B \cap C|$. Así

$$|A \cup B \cup C| = \alpha_1 - \alpha_2 + \alpha_3,$$

donde

$$\alpha_1 = |A| + |B| + |C|, \qquad \alpha_2 = |A \cap B| + |B \cap C| + |C \cap A|,$$
$$\alpha_3 = |A \cap B \cap C|.$$

Este resultado es un caso simple de lo que suele ser llamado, por razones obvias, el principio de inclusión y exclusión. También se lo llama el *principio del tamiz*.

**Teorema B.1.1.** *Si $A_1, A_2, \ldots, A_n$ son conjuntos finitos, entonces*

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \alpha_1 - \alpha_2 + \alpha_3 + \cdots + (-1)^n \alpha_n,$$

*donde $\alpha_i$ es la suma de los cardinales de las intersecciones de los conjuntos tomados de a $i$ por vez ($1 \leqslant i \leqslant n$).*

*Demostración.* Debemos demostrar que cada elemento $x$ de la unión hace una contribución neta de 1 al miembro de la derecha. Supongamos que $x$ pertenece a $k$ de los conjuntos $A_1, A_z, \ldots, A_n$. Entonces $x$ contribuye con $k$

en la suma $\alpha_1 = |A_1| + \cdots + |A_n|$. En la suma $\alpha_2$, $x$ contribuye 1 en $|A_i \cap A_j|$ cuando $A_i$ y $A_j$ están entre los $k$ conjuntos que contienen a $x$. Existen $\binom{k}{2}$ de esos pares, por lo tanto $\binom{k}{2}$ es la contribución de $x$ a $\alpha_2$. En general la contribución de $x$ a $\alpha_i$ ($1 \leqslant i \leqslant n$) es $\binom{k}{i}$. Por lo tanto el total con que contribuye $x$ al lado derecho de la igualdad es

$$\binom{k}{1} - \binom{k}{2} + \cdots + (-1)^{k-1}\binom{k}{k},$$

porque los términos con $i > k$ dan cero.

Por el teorema del binomio aplicado a $(1-1)^k = 0$, se deduce que la expresión de arriba es igual a $\binom{k}{0}$, que vale 1. □

Un corolario simple del teorema B.1.1 es a menudo más útil en la práctica. Supongamos que $X$ es un conjuntos finito y $A_1, A_2, \ldots, A_n$ son subconjuntos de $X$ (cuya unión no necesariamente es igual a $X$). Si $|X| = N$, entonces el número de elementos de $X$ que no están en ninguno de esos subconjuntos es

$$\begin{aligned} |X - (A_1 \cup A_2 \cup \ldots \cup A_n)| &= |X| - |A_1 \cup A_2 \cup \ldots \cup A_n| \\ &= N - \alpha_1 + \alpha_2 - \cdots + (-1)^n \alpha_n. \end{aligned}$$

*Ejemplo.* Hay 73 estudiantes en el primer año de la Escuela de Artes de la universidad. De ellos, 52 saben tocar el piano, 25 el violín y 20 la flauta; 17 pueden tocar tanto el piano como el violín, 12 el piano y la flauta; pero solo Juan Rictero puede tocar los tres instrumentos ¿Cuántos alumnos no saben tocar ninguno de esos instrumentos?

*Solución.* Con $V$, $P$ y $F$ denotaremos los conjuntos de estudiantes que saben tocar el violín, el piano y la flauta respectivamente. Usando la información dada tenemos que

$$\begin{aligned} \alpha_1 &= |P| + |V| + |F| = 52 + 25 + 20 = 97 \\ \alpha_2 &= |P \cap V| + |V \cap F| + |P \cap F| = 17 + 7 + 12 = 36 \\ \alpha_3 &= |P \cap V \cap F| = 1. \end{aligned}$$

Por consiguiente, el número de estudiantes que o pertenecen a ninguno de los tres conjuntos $P$, $V$ y $F$ es

$$73 - 97 + 36 - 1 = 11.$$

□

*Ejemplo.* Una secretaria ineficiente tiene $n$ cartas distintas y $n$ sobres con direcciones ¿De cuántas maneras puede ella arreglárselas para meter cada carta en un sobre equivocado? (Esto es comúnmente llamado el *problema del desarreglo* del cual hay varias formulaciones pintorescas.)

*Solución.* Podemos considerar cada carta y su correspondiente sobre como si estuvieran etiquetadas con un entero $i$ en el rango $1 \leqslant i \leqslant n$. El acto de poner las cartas en los sobres puede describirse como una permutación $\pi$ de $\mathbb{N}_n$: $\pi(i) = j$ si la carta $i$ va en el sobre $j$. Necesitamos saber el número de *desarreglos*, esto es, las permutaciones $\pi$ tales que $\pi(i) \neq i$ para todo $i$ en $\mathbb{N}_n$.

Denotemos $A_i$ ($1 \leqslant i \leqslant n$) el subconjunto de $S_n$ (el conjunto de permutaciones de $\mathbb{N}_n$) que contiene aquellos $\pi$ tales que $\pi(i) = i$. Diremos que los elementos de $A_i$ *fijan* $i$. Por el principio del tamiz, el número de desarreglos es

$$d_n = n! - \alpha_1 + \alpha_2 - \cdots + (-1)^n \alpha_n,$$

donde $\alpha_r$ es la suma de los cardinales de las intersecciones de los $A_i$ tomando $r$ por vez. En otras palabras, $\alpha_r$ es el número de permutaciones que fijan $r$ símbolos dados, tomando todas las maneras de elegir los $r$ símbolos. Ahora hay $\binom{n}{r}$ maneras de elegir $r$ símbolos, y el número de permutaciones que los fijan es solo el número de permutaciones de los restantes $n - r$ símbolos, que es $(n-r)!$ Por lo tanto

$$\alpha_r = \binom{n}{r} \cdot (n-r)! = \frac{n!}{r!}, \qquad d_n = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}\right).$$

□

§ *Ejercicios*

1) En una clase de 67 estudiantes de matemática, 47 leen francés, 35 leen alemán y 23 leen ambos lenguajes ¿Cuántos estudiantes no lee ninguno de los dos lenguajes? Si además 20 leen ruso, de los cuales 12 también leen francés, 11 leen alemán y 5 leen los tres lenguajes, ¿cuántos estudiantes no leen ninguno de los tres lenguajes?

2) Encontrar el número de formas de ordenar las letras A, E, M, O, U, Y en una secuencia de tal forma que las palabras ME e YOU no aparezcan.

3) Calcular el número $d_4$ de desarreglos de $\{1, 2, 3, 4\}$ y escriba, en la notación cíclica, las permutaciones relevantes.

4) Usar el principio de inducción para probar que la fórmula para $d_n$ satisface la recursión

$$d_1 = 0, \quad d_2 = 1, \quad d_n = (n-1)(d_{n-1} + d_{n-2}) \ (n \geqslant 3).$$

5) Probar que el número de desarreglos de $\{1, 2, \ldots, n\}$ en el cual un objeto dado (digamos el 1) está en un 2-ciclo es $(n-1)d_{n-2}$. Utilizar

esto para dar una prueba directa de la fórmula recursiva del ejercicio anterior.

# C

# LA FUNCIÓN DE EULER

## C.1 LA FUNCIÓN DE EULER

En esta sección probaremos un útil e importante teorema, usando sólo los conceptos de conteo más básicos.

El teorema se refiere a las propiedades de divisibilidad de los enteros. Recordemos que dos enteros $x$ e $y$ son *coprimos* si el $\mathrm{mcd}(x, y) = 1$. Por cada $n \geqslant 1$ sea $\phi(n)$ el número de enteros $x$ en el rango $1 \leqslant x \leqslant n$ tal que $x$ y $n$ son coprimos. Podemos calcular los primeros valores de $\phi(n)$ haciendo una tabla (tabla 2).

La función es llamada *función de Euler*, debido a Leonhard Euler $(1\,707 - 1\,783)$. Cuando $n$ es primo, digamos $n = p$, cada uno de los enteros $1, 2, \ldots, p-1$ es coprimo con $p$, entonces tenemos

$$\phi(p) = p - 1, \qquad p \text{ primo.}$$

| $n$ | Coprimos a $n$ | $\phi(n)$ |
|---|---|---|
| 1 | 1 | 1 |
| 2 | 1 | 1 |
| 3 | 1,2 | 2 |
| 4 | 1,3 | 2 |
| 5 | 1,2,3,4 | 4 |
| 6 | 1,5 | 2 |
| 7 | 1,2,3,4,5,6 | 6 |
| 8 | 1,3,5,7 | 4 |

Cuadro 2: Primeros valores de $\phi(n)$

Nuestra tarea ahora es probar un resultado respecto a la suma de los valores $\phi(d)$, donde los $d$ son todos los divisores de un número positivo $n$ dado. Por ejemplo, cuando $n = 12$, lo divisores $d$ son 1, 2, 3, 4, 5, 6 y 12, podemos ver que

$$\begin{aligned} &\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) \\ &= 1 + 1 + 2 + 2 + 2 + 4 \\ &= 12. \end{aligned}$$

| d \ f | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | $\phi(d)$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 12 | | | | | | | | | | | | 1 |
| 2 | 6 | | | | | | | | | | | | 1 |
| 3 | 4 | 8 | | | | | | | | | | | 2 |
| 4 | 3 | | 9 | | | | | | | | | | 2 |
| 6 | 2 | | | | 10 | | | | | | | | 2 |
| 12 | 1 | | | | 5 | | 7 | | | | 11 | | 4 |
| | | | | | | | | | | | | | 12 |

Cuadro 3

Debemos demostrar que la suma es siempre igual al entero $n$ dado.

**Teorema C.1.1.** *Para cualquier $n$ entero positivo,*

$$\sum_{d|n} \phi(d) = n.$$

*Demostración.* Sea $S$ el conjunto de pares de enteros $(d, f)$ que satisfacen

$$d|n, \qquad 1 \leqslant f \leqslant d, \qquad \text{mcd}(f, d) = 1.$$

La tabla 3 muestra $S$ cuando $n = 12$; la "marca" que indica que $(d, f)$ pertenece a $S$ es un número cuya importancia explicaremos en seguida. Por lo general, el número de "marcas" en la fila $d$ es el número de $f$'s en el rango $1 \leqslant f \leqslant d$ que satisfacen que el $\text{mcd}(d, f) = 1$; esto es $\phi(d)$. Por lo tanto, contando $S$ por el método de las filas obtenemos

$$|S| = \sum_{d|n} \phi(d).$$

Para demostrar que $|S| = n$ debemos construir una biyección $\beta$ de $S$ en $\mathbb{N}_n$. Dado un par $(d, f)$ en $S$, definimos

$$\beta(d, f) = fn/d.$$

En la tabla, $\beta(d, f)$ es la "marca" en la fila $d$ y la columna $f$. Como $d|n$, el valor de $\beta$, es un entero y como $1 \leqslant f \leqslant d$, entonces $\beta(d, f)$ pertenece a $\mathbb{N}_n$.

Para probar que $\beta$ es una inyección observemos que

$$\beta(d, f) = \beta(d', f') \quad \Rightarrow \quad fn/d = f'n/d' \quad \Rightarrow \quad fd' = f'd.$$

Pero $f$ y $d$ son coprimos, así como también lo son $f'$ y $d'$, así que podemos concluir que $d = d'$ y $f = f'$.

Para demostrar que $\beta$ es una suryección, supongamos que nos dan un $x$ que pertenece a $\mathbb{N}_n$. Sea $g_x$ el mcd de $x$ y $n$, y sea

$$d_x = n/g_x, \qquad f_x = x/g_x.$$

Puesto que $g_x$ es un divisor de $x$ y $n$, entonces $d_x$ y $f_x$ son enteros, y como $g_x$ es el mcd, $d_x$ y $f_x$ son coprimos. Ahora

$$\beta(d_x, f_x) = f_x n/d_x = x,$$

y por lo tanto $\beta$ es suryectiva. Luego $\beta$ es biyectiva y $|S| = n$, como queríamos demostrar. □

§ *Ejercicios*

1) Encontrar los valores de $\phi(19)$, $\phi(20)$, $\phi(21)$.

2) Probar que si $x$ y $n$ son coprimos, entonces lo son $n - x$ y $n$. Deducir que $\phi(n)$ es par para todo $n \geqslant 3$.

3) Probar que, si $p$ es un primo y $m$ es un entero positivo, entonces un entero $x$ en el rango $1 \leqslant x \leqslant p^m$ *no* es coprimo a $p^m$ si y solo si es un múltiplo de $p$. Deducir que $\phi(p^m) = p^m - p^{m-1}$.

4) Encontrar un contraejemplo que confirme que es falsa la conjetura $\phi(ab) = \phi(a)\phi(b)$, para enteros cualesquiera $a$ y $b$. Trate de modificar la conjetura de tal forma que no pueda encontrar un contraejemplo.

5) Probar que para cualesquiera enteros positivos $n$ y $m$ se cumple:

$$\phi(n^m) = n^{m-1}\phi(n).$$

6) Calcular $\phi(1\,000)$ y $\phi(1\,001)$.

## C.2 UNA APLICACIÓN ARITMÉTICA DEL PRINCIPIO DEL TAMIZ

Por cientos de años los matemáticos han estudiado problemas sobre números primos y la factorización de los enteros. Nuestra breve discusión sobre estos temas en los primeros capítulos debería haber convencido al lector de que estos problemas son difíciles, porque los primos mismos se encuentran irregularmente distribuidos, y porque no hay una forma directa de encontrar la factorización en primos de un entero dado. De todos modos, si se nos da la factorización en primos de un entero, es relativamente fácil responder ciertas preguntas sobre sus propiedades aritméticas. Supongamos,

por ejemplo que queremos listar todos los divisores de un entero $n$ y sabemos que la factorización de $n$ es

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}.$$

Entonces un entero $d$ es divisor de $n$ si y solo si no tiene divisores primos distintos de los de $n$, y ningún primo divide más veces a $d$ que a $n$. Visto así, los divisores son precisamente los enteros que pueden escribirse de la forma

$$d = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r},$$

donde cada $f_i$ ($1 \leqslant i \leqslant r$) satisface $0 \leqslant f_i \leqslant e_i$. Por ejemplo dado que $60 = 2^2 \cdot 3 \cdot 5$ podemos listar rápidamente todos los divisores de 60.

Un problema similar es encontrar el número de enteros $x$ en el rango $1 \leqslant x \leqslant n$ que son coprimos con $n$. En la sección C.1 denotamos este número con $\phi(n)$, el valor de la función $\phi$ de Euler en $n$. Ahora demostraremos que si la factorización en primos de $n$ es conocida, entonces $\phi(n)$ puede ser calculado por el principio del tamiz.

*Ejemplo.* ¿Cuál es el valor de $\phi(60)$? En otras palabras, ¿cuántos enteros $x$ en el rango $1 \leqslant x \leqslant 60$ satisfacen $\mathrm{mcd}(x, 60) = 1$?

*Solución.* Sabemos que $60 = 2^2 \cdot 3 \cdot 5$, así que podemos contar el números de enteros $x$ en el rango $1 \leqslant x \leqslant 60$ que no son divisibles por 2, 3 o 5. Con $A(2)$ denotemos el subconjunto de $\mathbb{N}_{60}$ que contiene los enteros que *son* divisibles por 2, con $A(2,3)$ aquellos que *son* divisibles por 2 y 3, y así sucesivamente, entonces tenemos

$$\begin{aligned}\phi(60) &= 60 - |A(2) \cup A(3) \cup A(5)| \\ &= 60 - |A(2) + A(3) + A(5)| \\ &\quad + (|A(2,3) + |A(2,5)| + |A(3,5)|) - |A(2,3,5)|,\end{aligned}$$

por el principio del tamiz. Ahora $|A(2)|$ es el número de múltiplos de 2 en $\mathbb{N}_{60}$ que es $60/2 = 30$. Del mismo modo $|A(2,3)|$ es el número de múltiplos de $2 \cdot 3$, que es $60/(2 \cdot 3) = 10$, y así siguiendo, por lo tanto

$$\phi(60) = 60 - (30 + 20 + 10) + (10 + 6 + 4) - 2 = 16.$$

□

El mismo método puede ser usado para dar una fórmula explícita para $\phi(n)$ en el caso general.

**Teorema C.2.1.** *Sea $n \geqslant 2$ un entero cuya factorización es $n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$. Entonces*

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

*Demostración.* Denotemos $A_j$ el subconjunto de $\mathbb{N}_n$ que contiene los múltiplos de $p_j$ ($1 \leqslant j \leqslant r$). Entonces

$$\begin{aligned}\phi(n) &= n - |A_1 \cup A_2 \cup \cdots \cup A_r| \\ &= n - \alpha_1 + \alpha_2 - \cdots + (-1)^r \alpha_r\end{aligned}$$

donde $\alpha_i$ es la suma de los cardinales de las intersecciones de los conjuntos tomados de a $i$. Una intersección típica como

$$A_{j_1} \cup A_{j_2} \cup \cdots \cup A_{j_i}$$

contiene los múltiplos de $P = p_{j_1} \cdot p_{j_2} \cdots p_{j_i}$ en $\mathbb{N}_n$, y estos son los números

$$P, 2P, 3P, \ldots, \left(\frac{n}{p}\right) P.$$

Luego la cardinalidad de una intersección típica es $n/P$, y $\alpha_i$ es la suma de términos como

$$\frac{n}{P} = n\left(\frac{1}{p_{j_1}}\right)\left(\frac{1}{p_{j_2}}\right)\cdots\left(\frac{1}{p_{j_i}}\right).$$

Se sigue que

$$\begin{aligned}\phi(n) = n - n\left(\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_r}\right) + n\left(\frac{1}{p_1 p_2} + \frac{1}{p_1 p_3} + \cdots\right) + \cdots \\ \cdots + (-1)^r \left(\frac{1}{p_1 p_2 \cdots p_r}\right) = \\ = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).\end{aligned}$$

□

# D

# GRAFOS PLANARES

## D.1 GRAFOS PLANARES

Usualmente el diagrama de un grafo se realiza en el plano por la comodidad que esto representa. Esto no significa que todo grafos sea lo que se denomina un *grafo planar*. ¿Qué es un grafo planar? Es un grafo tal que *existe* un diagrama del grafo en el plano tal que no hay ningún cruce de aristas. Por ejemplo, el grafo $K_3$ es claramente planar Fig. 27-(a). Claro que podríamos dibujar a $K_3$ como en la Fig. 27-(b) y no parecería planar.

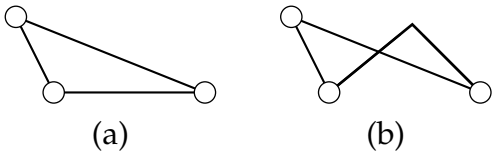



Figura 27: Dibujos de $K_3$

Pero la definición es que un grafo es planar si se *puede* dibujar en el plano sin cruces de aristas, no si *todo* dibujo no tiene cruces. (Si la definición fuera así, ningún grafo seria planar, pues siempre se puede dibujar cualquier grafo con cruces). Otro ejemplo, ya visto, $K_4$ puede ser dibujado como en la Fig. 28-(a) y no parece planar, pero dibujado como en la Fig. 28-(b) muestra que $K_4$ es planar.

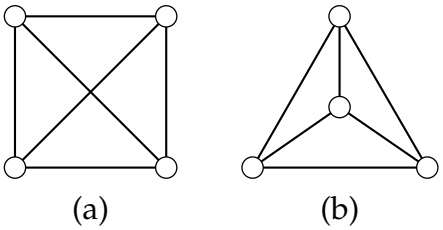



Figura 28: Dibujos de $K_4$

En vista de estos ejemplos, una pregunta es ¿existen grafos no planares? Por ejemplo si dibujáramos $K_{16}$ parecería imposible que fuera planar, dada la gran cantidad de cortes, pero ¿cómo podemos estar seguros?

Observemos primero que si G es planar y H es subgrafo de G, entonces H es planar, pues, si podemos dibujar a G en el plano sin cortes de aristas, entonces H que esta "metido" en G, también puede ser así dibujado. Así, como ya vimos que $K_4$ es planar, sabemos que todo subgrafo de él es planar; es decir, todo grafo con cuatro o menos vértices es planar. Esta observación tiene consecuencias en la otra dirección también: si encontramos un grafo H que *no* sea planar, entonces todo grafo G que lo tenga como subgrafo deberá necesariamente ser no planar, pues si G fuera planar, H también lo seria. Así, si queremos probar que $K_{16}$ no es planar, bastará con encontrar algún subgrafo mas sencillo de el que no lo sea. De hecho, probaremos que $K_5$ no es planar, con lo cual todos los grafos $K_n$, con $n \geqslant 5$ son no planares.

En lo que sigue veremos un arma poderosa para probar que un grafo es no planar: la llamada "fórmula de Euler". Supongamos que un grafo *sí* es planar. Escojamos un diagrama de él en el plano (puede haber muchos, escojamos uno). Este diagrama divide al plano en varias regiones. Por ejemplo, si G esta representado por el dibujo de la Fig. 29, entonces se obtienen regiones que numeraremos como en la Fig. 30 (1 es la región "exterior" a todo el grafo).

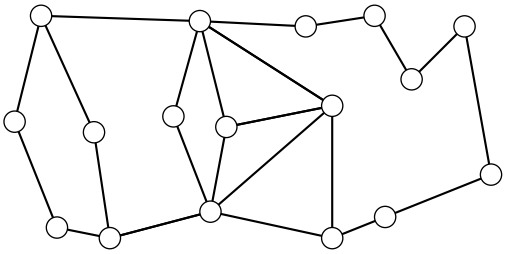


Figura 29: Un grafo planar

En realidad, también podríamos considerar a la región formada por las regiones 3 y 4 juntas, o 2, 5 y 6 juntas, etc. Pero nuestra preocupación estará centrada en una de estas regiones "simples", a las cuales llamaremos *caras*.

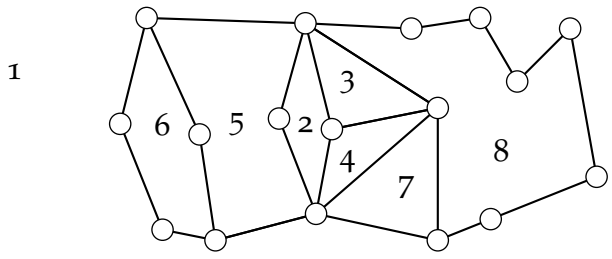



Figura 30: Regiones de un grafo planar

Observemos que no podemos hablar propiamente de las caras del grafo (aunque a veces lo haremos así) pues ellas son en realidad dependientes del diagrama, no del grafo. Sin embargo, algo puede decirse acerca de ellas:

**Teorema D.1.1.** *(Fórmula de Euler) Sea* G *un grafo conexo, con* $v$ *vértices,* $y$ e *aristas. Supongamos que en algún diagrama planar de* G*, existen* f *caras. Entonces,* $v - e + f = 2$.

Antes de ver la prueba, observemos que, puesto que $v$ y $e$ dependen de G y no del diagrama, la fórmula de Euler dice que no importa como dibujemos a G en el plano (siempre y cuando esto sea posible), entonces siempre obtendremos $e - v + 2$ caras. Por lo tanto, el *número* de caras es algo independiente del diagrama, y podemos hablar del "número de caras de un grafo planar". Otra observación es que en el número de caras estamos contando la cara infinita, es decir, la exterior a todo el grafo. Finalmente, observemos que se pide que G sea conexo. La fórmula debe ser alterada en caso contrario.

*Demostración del teorema D.1.1.* Supongamos que la fórmula de Euler no sea cierta. Es decir, supongamos que existen grafos planares para los cuales la fórmula no es válida. Tomemos, de todos estos contraejemplos, alguno con $e$ tan chico como sea posible, y llamemos G a ese grafo. Observemos que G debe tener por lo menos un ciclo, pues si fuera acíclico, como es conexo, sería un árbol. Ahora bien, en un árbol, $e = v - 1$. Además, por ser acíclico, no hay caras, salvo la cara infinita, es decir, f seria 1. Pero entonces $v - e + f = v - (v - 1) + 1 = v - v + 1 + 1 = 2$ y G no sería un contraejemplo. Así pues, G tiene al menos un ciclo. Sea $xy$ alguna arista perteneciente a algún ciclo, y consideremos $H = G - xy$. Como $xy$ pertenece a algún ciclo, es una arista que separa dos caras en G. Esas dos caras ahora son una sola en H. Ver Fig. 31.

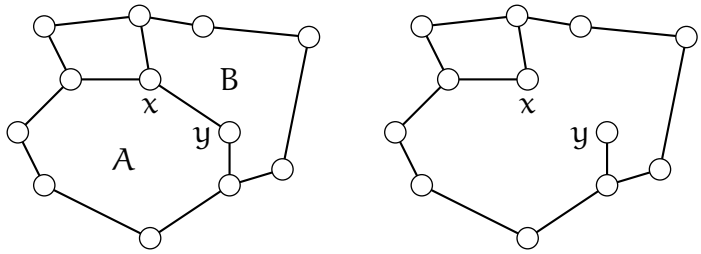



Figura 31: Eliminar una arista

Así, si $f_H, e_H$ y $v_H$ denotan el número de caras, aristas y vértices de H respectivamente, tenemos que $f_H = f - 1$. Además, como borramos una arista, $e_H = e - 1$, y como el número de vértices no cambia, $v_H = v$.

Pero, $e_H = e - 1$ es menor que $e$, y G era un contraejemplo con un número tan chico como fuera posible de aristas, por lo tanto, H no es un contraejemplo, es decir, $v_H - e_H + f_H = 2$. Reemplazando, obtenemos:

$$v - e + f = v_H - (e_H + 1) + f_H + 1 = v_H - e_H - 1 + f_H + 1 = v_H - e_H + f_H = 2,$$

lo cual dice que G no es un contraejemplo, absurdo. □

La fórmula de Euler es una herramienta muy poderosa en la teoría de grafos planares. Para empezar, permite probar que un grafo planar no puede tener muchas aristas, en relación a sus vértices

**Corolario D.1.2.** *Sea* G *un grafo planar con al menos* 3 *vértices. Entonces,* $e \leqslant 3v - 6$, *donde* e *es el número de aristas y* v *el número de vértices de* G.

*Demostración.* Consideremos las caras de G. Si es una cara distinta de la cara infinita, es porque viene de un ciclo. Ahora bien, todo ciclo debe tener por lo menos 3 aristas, así que podemos concluir que hay por lo menos 3 aristas en el borde de esa cara. Si, en cambio, es la cara infinita y el grafo tiene más de tres aristas entonces "toca" 3 o más aristas. Si el grafo tiene menos de 3 aristas (y ningún ciclo), es uno de los de la Fig. 32. Como estamos suponiendo que hay al menos 3 vértices, en realidad solo hay que considerar el último caso, y ese tiene $e = 2$, $v = 3$, y $2 \leqslant 3 \cdot 3 - 6$.

Figura 32: Grafos acíclicos con menos de 3 aristas

Así pues, podemos suponer que en nuestro grafo, todas las caras tienen al menos 3 aristas en su borde. Es decir:

$$\begin{aligned} 3 &\leqslant \text{Número de aristas en el borde de cara 1} \\ 3 &\leqslant \text{Número de aristas en el borde de cara 2} \\ &\vdots \\ 3 &\leqslant \text{Número de aristas en el borde de cara } f. \end{aligned}$$

Si sumamos estas desigualdades, del lado izquierdo obtendremos $3f$. En el lado derecho, cada arista puede, o bordear dos caras, o bordear una. Pero ciertamente, no puede haber aristas que sean borde de 3 caras. Así, si sumamos en el lado izquierdo, la suma nos dará menor o igual a $2e$. Por lo tanto, $3f \leqslant 2e$. Tomando la fórmula de Euler y multiplicándola por 3, obtenemos: $3v - 3e + 3f = 6$. Usando ahora $3f \leqslant 2e$, tenemos

$$6 = 3v - 3e + 3f \leqslant 3v - 3e + 2e = 3v - e,$$

es decir, $e \leqslant 3v - 6$. □

Este corolario nos permite probar inmediatamente la no planaridad de un número significativo de grafos. Por ejemplo, recordemos que queríamos ver que $K_5$ era no planar. Esto lo obtenemos en forma directa, pues $K_5$ tiene 5 vértices y 10 aristas, por lo tanto, si fuera planar debiéramos tener que $10 \leqslant 3 \cdot -6 = 15 - 6 = 9$, lo cual no es cierto.

## D.2 EL PROBLEMA DEL AGUA-LUZ-GAS

Este es un conocido problema de escuela primaria: existen tres casas, y tres centrales: la del agua, la de la luz y la del gas. Trazar las cañerías desde las centrales a las casas sin que se crucen. Una solución (pero haciendo trampa) es mandar las tres cañerías a una casa, y de ella sacarlas las tres a la otra, y de ella las tres a la otra:

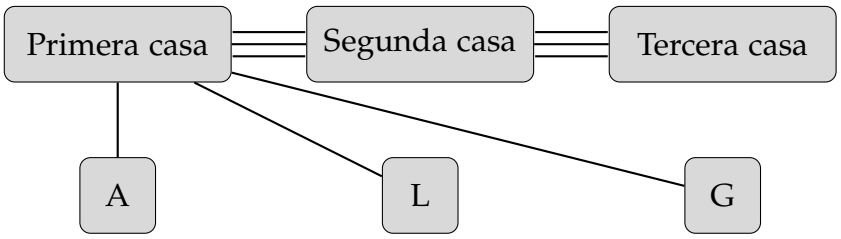



Figura 33: Una solución tramposa

En realidad, no permitiremos el uso de intermediarios, es decir el problema será llevar directamente la cañería desde cada central a cada casa. En el lenguaje de la teoría de grafos, consiste en representar, en el plano, al grafo $K_{3,3}$ Fig. 34.

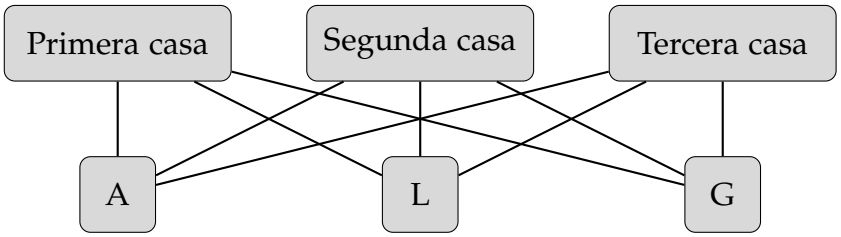



Figura 34: Luz-agua-gas es $K_{3,3}$

La pregunta es entonces si $K_{3,3}$ es planar o no. Veamos si podemos usar esta fórmula que probamos recién: $K_{3,3}$ tiene 9 aristas, y 6 vértices. Desafortunadamente, $3 \cdot 6 - 6 = 18 - 6 = 12$ es ciertamente mayor que 9, así que solo sabemos que quizás es planar. Pero, observemos que $K_{3,3}$, por ser bipartito, no tiene ningún triángulo como subgrafo. Así pues, deduciremos la no planaridad de $K_{3,3}$ del siguiente

**Corolario D.2.1.** *Si* $G$ *es un grafo planar con por lo menos* 3 *vértices y que no tiene ningún triángulo como subgrafo, entonces* $e \leqslant 2v - 4$.

*Demostración.* Es similar a la demostración del corolario D.1.2, pero como no hay triángulos, todo ciclo tiene por lo menos 4 aristas, es decir, cada cara

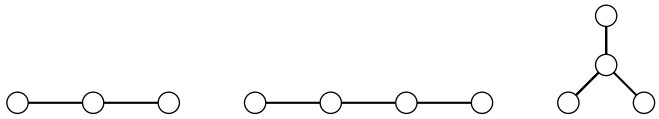


Figura 35: Grafos acíclicos con menos de 4 aristas y al menos 3 vértices

esta bordeada por al menos 4 aristas. Las únicas excepciones con al menos 3 vértices son los de la fig. 35

En el primer caso, $e = 2$, $v = 3$ y $2 \cdot 3 - 4 = 6 - 4 = 2$. En el segundo y terceros, $e = 3$, $v = 4$ y $2 \cdot 4 - 4 = 8 - 4 = 4 \geqslant 3$. Así pues, podemos suponer que cada cara esta bordeada por al menos 4 aristas. Sumando cara a cara, como antes, obtenemos ahora $4f \leqslant 2e$, es decir, $2f \leqslant e$. Multiplicando la fórmula de Euler por 2, tenemos: $4 = 2v - 2e + 2f \leqslant 2v - 2e + e = 2v - e$, es decir, $e \leqslant 2v - 4$. □

Retornando a $K_{3,3}$, como no tiene triángulos, podemos aplicar este corolario, y si fuera planar, debería cumplirlo. Pero habíamos dicho que $K_{3,3}$ tiene 9 aristas y 6 vértices, y $2 \cdot 6 - 4 = 12 - 4 = 8$. Por lo tanto, $K_{3,3}$ no es planar.

Una ultima observación acerca de grafos planares: existe un teorema muy interesante, de difícil demostración (la prueba tiene 31 casos y subcasos para considerar) debido a Kuratowski, que dice que $K_5$ y $K_{3,3}$ son los dos grafos "básicos" no planares, en el siguiente sentido: un grafo G es no planar si y solo si existe un subgrafo de G, digamos H, tal que H se "ve" como $K_5$ o como $K_{3,3}$, es decir, H es uno de ellos, excepto que tal vez, "agregue" en alguna o algunas aristas, vértices en el medio. Por ejemplo, H puede lucir como en la fig. 36.

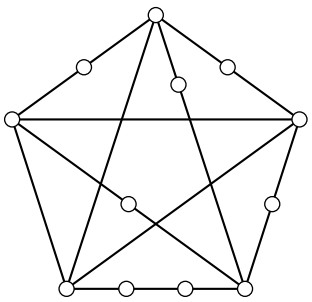


Figura 36: Un grafo no planar "básico"

## D.3 EL TEOREMA DE LOS CUATRO COLORES

Juntaremos ahora lo que hemos visto en esta sección con lo que vimos en la anterior, para tratar uno de los problemas mas famosos y recalcitrantes

de la teoría de grafos, a saber: ¿cuántos colores se necesitan para colorear un grafo planar? En otras palabras, si quiero estar seguro de poder colorear propiamente los vértices de cualquier grafo planar, ¿cuántos colores necesito tener? De hecho, una pregunta más básica sería si existe una cantidad finita de colores que me permitan colorear cualquier tipo de grafo planar, por grande que sea. (Es claro que la respuesta para grafos en general es negativa, pues $K_n$ requiere $n$ colores.) Como $K_4$ es planar, sabemos que necesitamos por lo menos 4 colores. No podemos decir que necesitamos necesariamente 5, pues hemos visto que $K_5$ no es planar. Pero, podría haber otro grafo, complicado pero planar, que requiera 5, o más, colores. A mediados del siglo pasado la conjetura de que bastan 4 colores fue hecha, y en 1879 A. Kempe publicó una prueba de este hecho, que paso a llamarse el teorema de los cuatro colores. Desafortunadamente para Kempe, en 1889 (diez años después) otro matemático, P. Heawood, probó que la prueba de Kempe contenía un error. Heawood no fue completamente destructivo: mostró que adaptando la prueba de Kempe, podía probarse que con 5 colores bastaba para colorear cualquier grafo planar (el teorema de los cinco colores). Así pues, quedo planteado el problema de saber si el teorema de los cuatro colores era cierto, o bien si existía algún grafo planar para el cual 5 colores fueran necesarios. (Pero, al menos, gracias a Heawood, no era necesario buscar alguno que necesitara 6, o 7 u 8 colores, pues no existen, gracias al teorema de los cinco colores.) De hecho, en ese mismo artículo, Heawood probó más cosas: existe algo llamado género de un grafo, que es un número entero no negativo. Heawood demostró que existía una fórmula (expresión aritmética) que para cada género $g \geqslant 1$ da la cantidad de colores que permite colorear todos los grafos de género $g$. Los grafos planares tiene género igual a 0 y aplicando la fórmula para $g = 0$ obtenemos el número 4. Sin embargo, Heawood pudo probar que la fórmula es válida si $g$ es mayor o igual a 1. El hecho de que esta fórmula existiera "convenció" a mucha gente de que el teorema de los cuatro colores debía ser cierto y que una prueba no tardaría en hallarse. Sin embargo, pese al esfuerzo de muchos matemáticos y pese al desarrollo de la teoría, el teorema de los cuatro colores no pudo probarse hasta 1975, cuando dos matemáticos norteamericanos, K. Appel y W. Haken, lo probaron. Más aún, no pudieron probarlos solos, sino que debieron usar la "ayuda" de un poderoso (para esa época) computador. Así, aún cuando el teorema fue probado, un gran sentimiento de desconfianza se generó, sobretodo en una época en la cual el acceso fácil a tiempo de computador no era común. Veinte años han pasado y la prueba ahora ha sido controlada numerosas veces y no genera tanta resistencia como antes. Aún así, si alguien pudiese publicar una prueba que fuese "leíble por humanos" sería muy bien bienvenido.

Obviamente por lo dicho arriba, no daremos una prueba del teorema de los cuatro colores. Sí daremos una del teorema de los cinco colores,

mencionando donde se encuentra la dificultad de la demostración del teorema de los cuatro colores, y dando una idea de que es lo que Appel y Haken (y el computador) hicieron.

**Lema D.3.1.** *Sea* $G$ *un grafo planar. Entonces, existe un vértice de* $G$ *de valencia* $5$ *o menos.*

*Demostración.* Si el orden de $G$ es menor o igual a 2, esto es obvio, pues la valencia de cualquier vértice no superará 2. Así, podemos suponer que hay al menos 3 vértices, y por lo tanto, sabemos que $e \leqslant 3v - 6$, donde $e$ es el numero de aristas y $v$ el de vértices.

Supongamos ahora que la valencia de todos los vértices sea al menos 6. Entonces, si sumamos las valencias de todos los vértices, la suma sera mayor o igual a $6v$. Pero la suma de todos las valencias es igual a $2e$ (lema del apretón de manos). Así, tenemos que $2e \geqslant 6v$. Por otro lado, como $e \leqslant 3v - 6$, tenemos que $2e \leqslant 6v - 12$, es decir, obtenemos $6v - 12 \geqslant 2e \geqslant 6v$, o $-12 \geqslant 0$, lo cual es un absurdo. □

**Teorema D.3.2.** *(Teorema de los cinco colores) Si* $G$ *es planar,* $\chi(G) \leqslant 5$.

*Demostración.* Supongamos que no sea cierto. De todos los contraejemplos al teorema, escojamos uno con la menor cantidad de vértices posible y llamémosle $G$. Por el lema anterior, existe un vértice $x$ de $G$ con valencia menor o igual a 5. Consideremos $H = G - \{x\}$, que es un grafo con menos vértices que $G$ y por lo tanto no puede ser un contraejemplo; es decir, $\chi(H) \leqslant 5$. Así, podemos colorear $H$ con 5 colores. Si la valencia de $x$ en $G$ es $0, 1, 2, 3$ o $4$, los vértices adyacentes a $x$ "usan" a lo sumo 4 de los 5 colores, así que podemos colorear a $x$ con el quinto color, y tendríamos que $\chi(G) = 5$, lo cual no es posible pues $G$ es un contraejemplo. Así pues, podemos suponer que la valencia de $x$ es 5. Ahora bien, si los cinco vértices adyacentes a $x$ no usan cinco colores, estamos como antes, y podemos colorear a $x$ con el color faltante. Así, no solo podemos suponer que hay cinco vértices adyacentes a $x$, sino también que cada uno esta coloreado con un color distinto. Llamemos a estos vértices $y, z, u, w, t$, y supongamos que $y$ de color 1, $z$ de color 2, etc.

Supongamos primero que no haya, entre $y$ y $u$, ningún camino tal que el color de todos sus vértices sea 1 o 3. Entonces, podemos cambiarle el color a $y$, de color 1 a color 3. Además, a los vértices adyacentes a $y$ que tengan color 3, les cambiamos el color de 3 a 1. A los vértices adyacentes a estos, que tengan color 1, los cambiamos a 3, y así sucesivamente. Después de realizar todos estos cambios, todavía tenemos un coloreo propio. Ahora bien, como estamos suponiendo que no hay ningún camino de color 1 y 3 exclusivamente entre $y$ y $u$, resulta que $u$ no cambia de color, es decir,

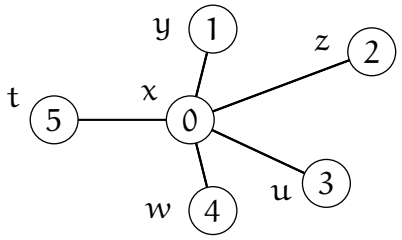



Figura 37: x es un vértice de valencia 5 en el grafo planar.

retiene el color 3. Pero y ahora tiene también el color 3, y ningún otro vértice adyacente a x tiene el color 1. Pero, entonces, podemos colorear a x con el color 1 sin problemas, absurdo pues $\chi(G) \geqslant 6$.

Así pues, existe un camino con todos los vértices de color 1 y 3 entre y y u. Igualmente, si no hubiera ningún camino con todos los vértices de color 2 y 4 entre z y $w$, le podemos cambiar el color a z de 2 a 4 sin problemas, y colorear a x con el color 2. Así, también podemos suponer que existe un camino con todos los vértices de color 2 y 4 entre z y $w$.

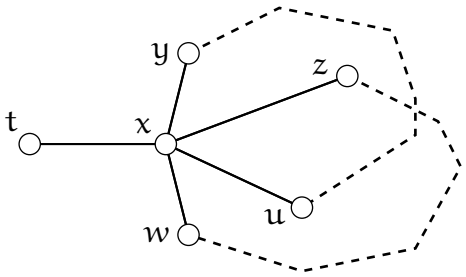



Figura 38: Caminos de y a u y de z a $w$

Por la Fig. 38 es claro que tenemos un problema: ¿por donde se cruzan los caminos A y B? Más precisamente, el camino A, junto con las aristas xy y xu, forma un ciclo C. Este ciclo tiene un interior y un exterior. El ciclo D formado por B y las aristas xz, $xw$ cruza al ciclo C en el punto x, pues la arista xz esta en el interior y la arista $xw$ en el exterior de C. Por lo tanto, D debe cruzar a C en algún otro punto. Pero no puede hacerlo, pues en el resto, C esta coloreado con los colores 1 y 3, y D con los colores 2 y 4. Hemos llegado a una contradicción. □

Analicemos un poco la prueba: hemos probado dos cosas. La primera es que todo grafo planar debe tener una de las siguientes "configuraciones", es decir, parte de él debe lucir como alguno de los grafos de la Fig. 39.

Esto lo probamos con el lema D.3.1. Es decir, probamos que ese conjunto de configuraciones es lo que se llama *inevitable*.

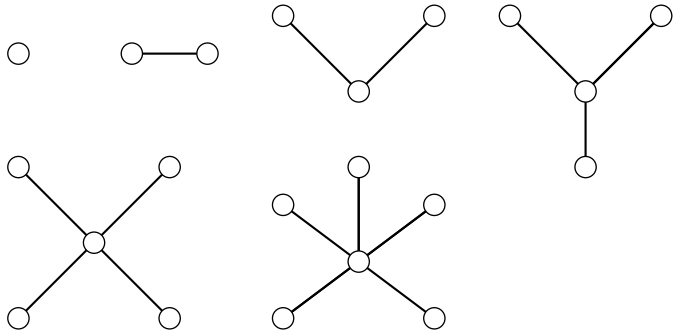


Figura 39: Posibles configuraciones

Además, en segunda instancia, probamos que si un grafo planar tiene una de esas configuraciones, puede ser coloreado con 5 colores (esto es lo que hicimos en el teorema). Es decir, probamos que ese conjunto de configuraciones es lo que se llama *irreducible* (para 5 colores).

Kempe creyó que había sido capaz de probar que todo grafo planar que tuviera esas configuraciones podía ser coloreado con 4 colores, y muchos autores después de Heawood trataron de probar lo mismo. Pero luego se descubrieron nuevas técnicas, tanto para probar que un conjunto de configuraciones es irreducible, como para probar que es inevitable. Lo que no se podía hacer era encontrar un conjunto que fuera al mismo tiempo irreducible (para 4 colores) e inevitable. Finalmente, Appel y Haken encontraron un conjunto que satisfacía esas propiedades. Solo que en vez detener 6 elementos, como en el caso del teorema de 5 colores, el conjunto de Appel y Haken tiene 1 480 elementos, y ningún ser humano es capaz de probarlo, sino que es necesario un computador para comprobar la inevitabilidad e irreducibilidad.

El problema con la prueba de Appel y Haken es que se basa en programas de computadora y entonces uno debe confiar en que no hay errores de programación. Incluso algunos matemáticos han dicho que la prueba contiene varios errores, pero no han podido mostrarlos fehacientemente.

En cierta manera esta polémica si diluyó en el año 2005 cuando Benjamin Werner y Georges Gonthier formalizaron una prueba del teorema con el asistente de pruebas Coq. Esto eliminó la necesidad de confiar en los diversos programas informáticos utilizados para verificar casos particulares; solo es necesario confiar en el kernel de Coq, construido alrededor de un núcleo bien delimitado, el cual la comunidad científica considera que no debe tener errores. A esta altura está claro que esta prueba es mucho más confiable que la demostración de muchos teoremas importantes de la matemática de cientos de páginas propensos a errores humanos.

La prueba con Coq se encuentra en el artículo de G. Gonthier "Formal Proof—The Four-Color Theorem", Notices of the American Mathematical Society, 55 (11): 1382–1393, MR 2463991 (2008).

Parte IV

# ÍNDICE

# ÍNDICE ALFABÉTICO