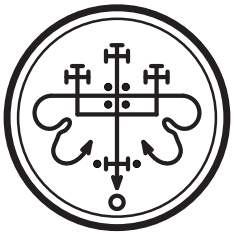
Problemas propuestos
Fundamentos de Informática

Horst H.˜von Brand

16 de octubre de 2015



Borrador

1. Preliminares

1. Explique las diferencias o relaciones entre $f(n) = O(g_1(n))$, $f(n) = \Omega(g_2(n))$, $f(n) = \Theta(g_3(n))$ y $f(n) \sim g(n)$.
2. Explique la diferencia entre $f(n) = O(g(n))$ y $f(n) = o(g(n))$
3. Explique las diferencias o relaciones entre $f(n) = O(g_1(n))$, $f(n) = \Omega(g_2(n))$ y $f(n) = \Theta(g_3(n))$.
4. Dé la diferencia simétrica entre A y B en términos solamente de unión, intersección y complemento.
5. Se dan dos funciones $f(n)$ y $g(n)$. Demuestre que si $\lim_{n\to\infty} f(n)/g(n)$ es finito, entonces $f(n) = O(g(n))$. Si además el límite no es cero, entonces $f(n) = \Theta(g(n))$.
6. Responda *brevemente* las siguientes:
   a) Sea $f(n) = 3n^2 \sin^2 n + n/2$. Demuestre usando las definiciones que $f(n) = O(n^2)$ y que $f(n) = \Omega(n)$.
   b) ¿Si las cotas de la parte 6*a* son las mejores posibles, hay k tal que $f(n) = \Theta(n^k)$?
7. Exprese la diferencia entre conjuntos $A \setminus B$ en términos de unión, intersección y complemento.
8. Demostrar las siguientes identidades:
   a) $m^{\underline{n+k}} = m^{\underline{n}}(m-n)^{\underline{k}}$
   b) $m^{\overline{n+k}} = m^{\overline{n}}(m+n)^{\overline{k}}$
   c) $x^{\underline{k}} = (-1)^k(-x)^{\overline{k}}$
9. Se define el operador $\Delta f(n)$ como

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

   Del mismo modo, se define su operador inverso $\Sigma f(n)$ como sigue

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

   Demuestre que ambos son operadores lineales, es decir, para constantes α y β arbitrarias, las relaciones

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

   se cumplen.
10. Demuestre que las relaciones

    $$\Delta \Sigma f(n) = f(n)$$
    $$\Sigma \Delta f(n) = f(n) + c$$

    Son correctas.
11. Se definen los *coeficientes binomiales* para $k \in \mathbb{N}_0$ y α arbitrario (no necesariamente un entero) mediante:

    $$\binom{\alpha}{k} = \frac{\alpha^{\underline{k}}}{k!}$$

    Demuestre que cumplen:

    $$\binom{\alpha+1}{k+1} = \binom{\alpha}{k} + \binom{\alpha}{k+1}$$

Borrador

2. Relaciones y funciones

1. Sobre $\mathbb{Z}^2 \setminus \{(0,0)\}$ defina la relación $(a,b) \sim (c,d)$ si $a \cdot d = b \cdot c$. Demuestre que es una relación de equivalencia.
2. Una relación R se llama *asimétrica* si para todo a, b, si $a \; R \; b$ entonces $b \not R \; a$, y *antireflexiva* si para todo a es $a \not R \; a$. Demuestre que toda relación asimétrica es antireflexiva.
3. Si R_1 y R_2 son relaciones de equivalencia, demuestre que $R_1 \cap R_2$ es una relación de equivalencia.
4. Considere una relación R y su inversa R^{-1} sobre algún universo $\mathcal{U}$. Explique qué puede decir acerca de R^{-1} si sabe que:
   a) R es simétrica
   b) R es antisimétrica
   c) R es transitiva
   d) R es reflexiva
5. Determine cuáles de las siguientes son relaciones de equivalencia:
   a) En $\mathbb{Z}$, $a \sim b$ siempre que $\gcd(a,b) = 1$
   b) En el plano $\mathbb{R}^2$, los puntos $(x_1, y_1) \sim (x_2, y_2)$ siempre que $x_1^2 + y_1^2 = x_2^2 + y_2^2$
   c) En $\mathbb{R}$, $x \sim y$ siempre que $x - y$ es racional
6. Se define la relación $a \; R \; b$ sobre $\mathbb{N}$ si el máximo dígito de a en decimal es el máximo dígito de b en decimal. ¿Es esta una relación de equivalencia?
7. a) Defina una función $f \colon \mathbb{N} \to \mathbb{N}$ que es uno a uno, pero no sobre
   b) Defina una función $g \colon \mathbb{N} \to \mathbb{N}$ que es sobre, pero no uno a uno
8. ¿Es simétrica la composición de dos relaciones simétricas?
9. ¿Es una relación simétrica y transitiva necesariamente reflexiva?
10. Clasifique las siguientes relaciones:
    a) La relación R_1 entre funciones tal que $f \; R_1 \; g$ siempre que $f(n) = \Theta(g(n))$.
    b) En $\mathbb{R}^2$, $(x,y) \; R_2 \; (u,v)$ siempre que $(x-u)^2 + (y-v)^2 \leq 1$.
11. Dé ejemplos de funciones $f : \mathbb{N} \to \mathbb{N}$ tales que
    a) f es uno a uno, pero no sobre
    b) f es sobre, pero no uno a uno
    c) f es biyectiva
12. Considere una relación simétrica R. ¿Qué puede decir sobre su transpuesta R^{-1}?
13. Considere dos relaciones transitivas R_1 y R_2. ¿Qué puede decir sobre su composición $R_2 \circ R_1$?
14. Una función es un caso particular de relación. ¿La transpuesta de una función es siempre una función?
15. Determine las propiedades y clasifique las siguientes relaciones:
    a) La relación R_1 entre funciones de los naturales a los reales tal que $f \; R_1 \; g$ siempre que $f(n) = \Omega(g(n))$ (no considere totalidad).
    b) En $\mathbb{R}$, $x \; R_2 \; y$ siempre que $x - y \in \mathbb{Z}$
16. Estudie las propiedades de las relaciones definidas en la lista que sigue, sobre los conjuntos que se indica.
    a) $\mathcal{R}_1$ definida sobre $\mathbb{R}$ por $x \; \mathcal{R}_1 \; y$ si y sólo si $\cos x = \sin y$
    b) $\mathcal{R}_2$ definida sobre $\mathbb{R} \times \mathbb{R}$ por $(u,v) \; \mathcal{R}_2 \; (x,y)$ si y sólo si $(x-u, y-v) \in \mathbb{Z} \times \mathbb{Z}$

Borrador

c) $\mathcal{R}_3$ definida sobre $[1, 500] \times [1, 500]$ por $(u, v)\ \mathcal{R}_3\ (x, y)$ si y sólo si $uy = xv$ (los rangos son de números enteros)

17. Se define la función $f\colon \mathbb{N} \to 2^{\mathbb{N}}$ mediante:

$$f(n) = \{n + 1, n + 2, \dots\}$$

¿Es una inyección? ¿Es sobreyectiva?

18. Sobre $\mathbb{R}^2$ se define $(r, s) \sim (x, y)$ si $r^2 - y^2 = x^2 - s^2$. ¿Es esta una relación de equivalencia?

19. Demuestre que la función $f\colon \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x^3 + 2x^2 + 3x + 4$ es uno a uno.

Borrador

3. Lógica

1. ¿Cuál es el contrapositivo de $P \Rightarrow Q$?

2. Considere los siguientes predicados:

   $D(x, y)$: x dicta el ramo y — $C(x, y)$: x es alumno del ramo y
   $A(x, y)$: x aprueba el ramo y — $E(x, y)$: x estudia para el ramo y
   $R(x)$: x es muy carretero

   En estos términos, exprese los siguientes:

   a) Si Juan toma Fundamentos, y estudia para este ramo, lo aprueba.

   b) Todo alumno que toma un ramo con un profesor muy carretero reprueba ese ramo.

   c) Si un profesor es muy carretero, todos los alumnos no muy carreteros aprueban su ramo.

3. Considere los siguientes predicados:

   $D(x, y)$: x dicta el ramo y — $C(x, y)$: x es alumno del ramo y — $A(x, y)$: x aprueba el ramo y
   $R(x)$: x es muy carretero — $E(x, y)$: x estudia para el ramo y

   En estos términos, exprese los siguientes, justificando *brevemente*:

   a) Ningún profesor muy carretero dicta dos o más ramos.

   b) Hay alumnos muy carreteros que aprueban todos sus ramos.

   c) Si el profesor de un ramo no es muy carretero, sólo aprueban los alumnos que estudian.

4. Traduzca las especificaciones expuestas a continuación como fórmulas preposicionales, utilizando las siguientes definiciones:

   - L ::= sistema de archivos bloqueado
   - Q ::= nuevos mensajes son puestos en cola
   - B ::= nuevos mensajes son enviados al búfer de mensajes
   - N ::= sistema funcionando normalmente

   a) Si el sistema de archivos no está bloqueado, nuevos mensajes serán puestos en cola.

   b) Si el sistema de archivos no está bloqueado, nuevos mensajes serán enviados al búfer de mensajes.

   c) Si el sistema de archivos no está bloqueado, el sistema está funcionando normalmente y, a la inversa, si el sistema está funcionando normalmente, entonces el sistema de archivos no está bloqueado.

   d) Si nuevos mensajes no son puestos en cola, entonces serán enviados al búfer de mensajes.

   e) Nuevos mensajes no son enviados al búfer de mensajes.

5. (Continuación ejercicio anterior) Diremos que la especificación es *consistente* si hay una sola opción de valores de verdad para las variables L, Q, B y N, tal que cada una de las fórmulas preposicionales de la parte anterior son verdaderas. Si las cinco declaraciones son verdaderas para alguna asignación de valores de verdad a las variables, entonces el sistema es consistente. Si para cada una de las 16 posibles asignaciones de verdad, al menos una de las declaraciones es falsa, el sistema es inconsistente. Utilice demostración por casos para encontrar las asignaciones de verdad que confirman que esta especificación de sistema es consistente. Explique por qué sólo hay una asignación que cumple con esto.

Borrador

4. Demostraciones

1. Demuestre por contradicción que si $0 \leq x \leq \pi/2$, entonces $\sin x + \cos x \geq 1$.

   Pista: En este rango $\sin x \geq 0$ y $\cos x \geq 0$. Suponga $\sin x + \cos x < 1$, y eleve al cuadrado.

2. Demostrar que $\log_2 5$ es irracional.

3. Se usa la notación m mód n para indicar el resto de la división de m por n. Por ejemplo, 17 mód 3 = 2. Use el contrapositivo para demostrar que si n mód 4 = 2 ó n mód 4 = 3 entonces n no es un cuadrado perfecto.

4. Demuestre por inducción que

   $$\frac{(2n)!}{n!2^n}$$

   siempre es impar.

5. Demuestre por inducción que:

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

6. Juguemos. Comienza con una torre de n cajas. En cada movida divide una de las torres que tiene en dos. Si divide una torre de $a+b$ cajas en torres de a y b cajas, gana ab puntos. Demuestre que, sea como sea que juega, su puntaje total es $n(n-1)/2$.

7. Demuestre por inducción que:

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

8. Demuestre por inducción que:

   $$\prod_{2\leq k\leq n} \left(1-\frac{1}{k^2}\right) = \frac{n+1}{2n}$$

9. Demuestre la fórmula de de Moivre:

   $$(\cos\theta + \mathrm{i}\sin\theta)^n = \cos n\theta + \mathrm{i}\sin n\theta$$

10. Demuestre por inducción la serie de Mengoli:

    $$\sum_{1\leq k\leq n} \frac{1}{k(k+1)} = \frac{n}{n+1}$$

11. Demuestre por inducción que:

    $$\sum_{0\leq k\leq n} k\cdot k! = (n+1)! - 1$$

12. Demuestre por inducción que para $n \in \mathbb{N}$ si $x > 0$ entonces $(1+x)^n \geq 1 + nx$.

13. Demostrar que para $n \geq 2$ es $4^n > 3^n + 2^n$.

14. Los números de tribonacci T_n se definen mediante $T_0 = 0, T_1 = T_2 = 1$ y $T_{n+3} = T_{n+2} + T_{n+1} + T_n$ para $n \geq 0$. Demostrar que $T_n < 2^n$.

Borrador

15. Demuestre por inducción que

$$\frac{(2n)!}{n!2^n}$$

siempre es impar.

16. Usando el contrapositivo, demuestre que si $n \equiv 2 \pmod 3$, entonces n no es un cuadrado perfecto.

17. Para $0 \leq x \leq \pi/2$ demuestre por contradicción que $\sin x + \cos x \geq 1$.

18. Demuestre que $5^{2n} - 1$ es siempre divisible por 24, cuando n es un número natural.

19. Demuestre que la suma de los primeros n números impares es n^2. Exprese su demostración formalmente.

20. Encuentre una fórmula para la suma

$$\sum_{1 \leq k \leq n} ak + b$$

y demuéstrela por inducción.

21. Demuestre que:

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

¿Para qué valores naturales m y n vale esta identidad?

22. Sabiendo que $1 + 2 + \ldots + n = n(n+1)/2$, demuestre que para $n \geq 1$:

$$1^3 + 2^3 + \ldots + n^3 = (1 + 2 + \ldots + n)^2$$

23. Demuestre que para todo $n \in \mathbb{N}$ se cumple que:

$$\sum_{1 \leq k \leq n} k(k+1) = 1 \cdot 2 + 2 \cdot 3 + \ldots + n(n+1) = \frac{n(n+1)(n+2)}{3}$$

24. Los *números de Fibonacci* se definen por la recurrencia:

$$F_{n+2} = F_n + F_{n+1} \qquad F_0 = F_1 = 1$$

Demuestre que:

$$\sum_{0 \leq k \leq n} F_k^2 = F_n F_{n+1}$$

25. Demuestre que:

$$\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$$

26. Demuestre que $\sqrt{10}$ es irracional.

27. Demuestre que φ, la raíz positiva de $x^2 - x - 1 = 0$, es irracional.

28. Demuestre que $\sqrt[3]{2}$ es irracional, y que no hay un polinomio $a_2x^2 + a_1x + a_0$ con coeficientes enteros que tiene $\sqrt[3]{2}$ como raíz.

Pista: Considere $x^3 - 2 = (a_2x^2 + a_1x + a_0)(b_1x + b_0)$

Borrador

29. Demuestre formalmente que $\sqrt{2}+\sqrt{3}$ es irracional.
    Pista: Si a es racional, lo es a^2.

30. Demuestre que para todo $n \in \mathbb{N}$:

$$\sum_{1\leq k\leq n} k^3 = \left(\sum_{1\leq k\leq n} k\right)^2$$

31. Demuestre formalmente que no existen números naturales a y b tales que $a^2 - b^2 = 1$.

32. Demuestre que:

$$\sum_{1\leq k\leq n} 2k-1 = n^2$$

33. Demuestre que:

$$\sum_{1\leq k\leq n} k^{\underline{2}} = \frac{(n+1)^{\underline{3}}}{3}$$

34. Demuestre por inducción que $\forall n \in \mathbb{N}, n \geq 13, n^2 < \left(\frac{3}{2}\right)^n$.

35. Demuestre por inducción que si $x \geq 0$, entonces $\forall n \in \mathbb{N}, (1+x)^n \geq 1 + x^n$.

36. *a*) Demuestre que para todo $n \in \mathbb{N}$:

$$\frac{1}{\sqrt{n+1}} \geq 2\left(\sqrt{n+2} - \sqrt{n+1}\right)$$

    (Multiplique por la cantidad positiva $\sqrt{n+2}+\sqrt{n+1}$)

    b) Usando lo anterior, demuestre que para $n \geq 1$:

$$1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} \geq 2\left(\sqrt{n+1} - 1\right)$$

37. Demuestre por inducción sobre n que:

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

    Asimismo demuestre que si $\Delta x_k = x_{k+1} - x_k$, entonces:

$$\Delta k^{\underline{m}} = m k^{\underline{m-1}}$$

38. Demostrar que $(x+1)^{2n+1} + x^{n+2}$ es divisible por $x^2 + x + 1$ para todo $n \in \mathbb{N}_0$.

39. La secuencia de números positivos $u_1, u_2, u_3, \ldots$ es tal que $u_1 < 4$ y:

$$u_{n+1} = \frac{5u_n + 4}{u_n + 2}$$

    Considerando $4 - u_n$ demuestre por inducción que $u_n < 4$ para todo $n \geq 1$. Demuestre además que $u_{n+1} > u_n$.

40. Demostrar que para $n \geq 3$ es $n^{n+1} > (n+1)^n$.

41. Demostrar que:

$$\sum_{1\leq k\leq n} \frac{k}{(k+1)!} = 1 - \frac{1}{(n+1)!}$$

Borrador

42. Demostrar que:

$$\frac{(2n)!}{2^n n!}$$

es un entero para $n \in \mathbb{N}_0$.

43. Demuestre que $\log_2 5$ es irracional.

44. Demuestre que la secuencia definida por:

$$a_{n+1} = \frac{a_n}{na_n + 1}$$

cumple:

$$a_n = \frac{2a_0}{n(n-1)a_0 + 2}$$

45. Los números de Fibonacci F_n se definen mediante $F_0 = 0, F_1 = 1$ y $F_{n+2} = F_{n+1} + F_n$ para $n \geq 0$. Demostrar que $F_n < 2^n$.

Borrador

5. Estructuras algebraicas

1. Encuentre los subgrupos de $\mathbb{Z}_{12}$ con la suma. Verifique que cumplen el teorema de Lagrange.
2. Descomponga $\mathbb{Z}_{100}$ en una suma directa de anillos.
3. ¿Cuántos grupos de orden 3 hay?
4. ¿Cuántos grupos abelianos de orden 4 hay?
5. ¿Cuántos grupos de orden 1 hay? ¿Cuántos de órdenes 2, 3, y 4, respectivamente?
6. Sea G un grupo, y H_1, H_2 subgrupos de G. Demuestre que $H_1 \cap H_2$ es un subgrupo de G.
7. Sea G un grupo finito con elemento neutro e. Si se definen potencias de la forma tradicional, demuestre que para todo elemento $a \in G$ existe $n \in \mathbb{N}$ tal que $a^n = e$ (el *orden* de a en G).
8. Sea G un grupo, y H_1 y H_2 subgrupos de G. Demuestre que $H_1 \cap H_2$ también es un subgrupo de G.
9. Demuestre que todo subgrupo H de un grupo cíclico G es cíclico a su vez
   Pista: Sea g un generador de G, y considere el elemento de H que es la mínima potencia de g
10. Demuestre que en un anillo finito un elemento o es un divisor de cero o es una unidad.
11. Sea F un campo, G y H subcampos de F. Demuestre que $G \cap H$ es un campo.
12. Sean a y b unidades del anillo $\mathfrak{R}$. ¿Es $a + b$ siempre una unidad?
13. Un grupo $\mathfrak{G}$ se dice *cíclico* si todo elemento de $\mathfrak{G}$ puede escribirse g^k para algún $g \in \mathfrak{G}$ fijo. En tal caso, se llama a g un *generador* de $\mathfrak{G}$. Demuestre que los grupos aditivos $\mathbb{Z}$ y $\mathbb{Z}_n$ para todo n son cíclicos.
14. Considere el conjunto de racionales que en mínimos términos tienen denominador impar. Demuestre que con las operaciones de $\mathbb{Q}$ forman un dominio integral (anillo conmutativo sin divisores de cero).
15. Suele denotarse mediante R^* al grupo de las unidades del anillo $(R, +, \cdot)$. Demuestre que el grupo $\mathbb{R}^*$ es isomorfo a la suma directa de $\mathbb{Z}_2$ y el grupo de los reales positivos con multiplicación.
16. Considere el conjunto de elementos de la forma $p + q\sqrt{3}$, donde p y q son números racionales, junto con las operaciones de suma y multiplicación tradicionales. ¿Es esto un anillo? En caso de serlo, ¿cuáles son las unidades, y cuáles son sus inversos? ¿Hay divisores propios de cero?
17. Sea G un grupo, se define la relación R sobre G mediante $a\ R\ b$ si y solo si $b = gag^{-1}$ para un elemento $g \in G$. ¿Es esta una relación de equivalencia?
18. Demuestre que en un anillo finito R, un elemento $x \in R$ solo puede ser cero, una unidad o un divisor de cero.
19. Sea τ la raíz positiva de $x^2 - x - 1 = 0$. Demuestre que $\mathbb{Z}[\tau] = \{a + b\tau \colon a, b \in \mathbb{Z}\}$ es un dominio integral (anillo conmutativo sin divisores propios de cero).
20. Sea $(G, \otimes)$ un grupo finito. Si S es un subconjunto de G cerrado con respecto a $\otimes$, demuestre que $(S, \otimes)$ es un subgrupo de G.
21. Determine para qué valores de k y m $(\mathbb{Z}, \oplus, \otimes)$ es un anillo, si las operaciones están definidas como:

    $$a \oplus b = a + b - k$$
    $$a \otimes b = a + b + mab$$

    ¿Que elemento es el cero? ¿Existe un uno? ¿Cuáles son las unidades?

Borrador

22. Sea $(R, +, \cdot)$ un anillo conmutativo. Considere $R[\![x]\!]$, el conjunto de *series de potencias formales* sobre R. O sea:

$$\begin{aligned} a(x) &= \sum_i a_i x^i \\ b(x) &= \sum_i b_i x^i \\ a(x) + b(x) &= \sum_i (a_i + b_i) x^i \\ a(x) \cdot b(x) &= \sum_i \left(\sum_{0 \le j \le i} a_j \cdot b_{i-j} \right) x^i \end{aligned}$$

Demuestre que esto es un anillo.

23. Demuestre sucesivamente las siguientes:

    a) Si G es un grupo, y $a \in G$, el subgrupo generado por a es el menor subgrupo de G que contiene a a (o sea, es un subgrupo de G que contiene a a, y es subconjunto de todo subgrupo de G que contiene a a).

    b) Demuestre que el grupo G es cíclico si y sólo si G es el subgrupo generado por un elemento $g \in G$.

    c) Demuestre que todo grupo de orden primo es cíclico.

24. Demuestre que la intersección de subgrupos de un grupo es a su vez un subgrupo.

25. Considere el conjunto de números reales $C = \{a + b\sqrt{2} \colon a, b \in \mathbb{Q}\}$. Demuestre que C con las operaciones de suma y multiplicación de los números reales conforman un campo.

26. Demuestre que el grupo de elementos invertibles del anillo $\mathbb{R}$ no es cíclico.

27. Sea A un anillo, no necesariamente conmutativo. Defina $a \ R \ b$ para $a, b \in A$ si hay un elemento invertible $g \in A$ tal que $gag^{-1} = b$. ¿Es R una relación de equivalencia?

28. Sea A un anillo finito. Demuestre que $a \in A$ es invertible o es un divisor de cero.

    Pista: Considere el conjunto $\{a \cdot x \colon x \in A \text{ y } x \neq 0\}$, y analice los casos en que tiene elementos repetidos y en que no los tiene.

29. Considere bytes de 8 bits con la operación $\oplus$ que corresponde a o exclusivo bit a bit.

    a) Demuestre que este conjunto de elementos forma un grupo abeliano con esta operación.

    b) ¿Cuál es el orden del grupo?

    c) ¿Cuál es el máximo orden de un elemento en este grupo?

30. Determine si es cierta o falsa la siguiente aseveración: Sea G un grupo abeliano finito, y sean H, I subgrupos de G tales que $|H| \le |I|$. Entonces H es subgrupo de I.

31. Sea R un dominio integral (anillo conmutativo sin divisores propios de cero). Demuestre que el mapa $\phi \colon R[x] \to R$ definido mediante

    $$a_0 + a_1 x + \cdots + a_n x^n \mapsto a_0$$

    es un homomorfismo de anillo.

32. Factorize $x^4 + x^3 + x$ lo más posible en $\mathbb{Z}_3[x]$.

33. Factorize el polinomio $x^3 + x^2 + 1$ sobre $\mathbb{Z}_3$.

34. Factorize $x^4 + 1$ sobre $\mathbb{Z}_3$.

Borrador

35. Dados los polinomios en $\mathbb{Q}[x]$:

$$a(x) = 15x^5 - 11x^4 - 5x^3 + 16x^2 - 10x + 4$$
$$b(x) = 3x^4 + 2x^3 - 15x^2 + 16x - 6$$

muestre paso a paso cómo calcular $\gcd(a(x), b(x))$ usando el algoritmo de Euclides.

36. El campo $\mathbb{F}_{27}$ puede representarse como $\mathbb{Z}_3[x]/(x^3 + x^2 + 2)$.

a) Demuestre que $x^3 + x^2 + 2$ es irreductible sobre $\mathbb{Z}_3$.

b) Se le llama *elemento primitivo* del campo a un generador de su grupo de unidades. ¿Cuántos elementos primitivos tiene $\mathbb{F}_{p^n}$?

c) ¿Cómo puede determinar si $p(x)$ es un elemento primitivo de $\mathbb{F}_{p^n}$ *sin* calcular todas sus potencias?

37. Halle todas los ceros en $\mathbb{C}$ del polinomio $x^3 - 2x + 1$.

38. Dé las tablas de suma y multiplicación del campo $\mathbb{Z}_2/(x^2 + x + 1)$.

39. Dé los elementos del campo $\mathbb{Z}_2[x]/(x^2 + x + 1)$.

40. Determine si $x^3 + 2x + 1$ es irreductible sobre $\mathbb{Z}_3$

41. Para qué valores de k es un entero la expresión:

$$\frac{k^2 - 87}{3k + 117}$$

Pista: Multiplique por 3, divida polinomios y vea qué puede concluir.

42. ¿Cuántos polinomios irreductibles de grado 12 hay sobre $\mathbb{Z}_2$?

43. Considere el conjunto $\mathtt{D}_\infty = \mathbb{Z} \times \{-1, 1\}$ (pares formados por un entero y ± 1). Demuestre que $\langle \mathtt{D}_\infty, \circ \rangle$ es un grupo, donde $(x, s) \circ (y, t) = (x + sy, st)$.

44. En un anillo R, a un elemento x se le llama *idempotente* si $x = x^2$.

a) Demuestre que si x es idempotente, $x^n = x$ para todo $n \geq 1$

b) Demuestre que si x es idempotente, lo es $1 - x$

c) Demuestre que si x e y son idempotentes tales que $xy = yx$, son idempotentes xy y $x + y - xy$

Borrador

6. Teoría de números

1. Demuestre que el conjunto de los subconjuntos de $\mathcal{U}$, $2^{\mathcal{U}}$ es un anillo con "suma" la diferencia simétrica y "multiplicación" la intersección. ¿Que elementos toman el lugar de 0 y 1?

2. Sea $\mathscr{A}$ el conjunto de funciones aritméticas. Se define la convolución de Dirichlet entre funciones aritméticas:

   $$(f * g)(n) = \sum_{ab=n} f(a)g(b)$$

   Podemos sumar funciones de la forma habitual:

   $$(f + g)(n) = f(n) + g(n)$$

   donde claramente la función 0 es el elemento neutro, con lo que el conjunto de funciones aritméticas con la suma es un grupo abeliano.

   a) Demuestre que $*$ es cerrada en $\mathscr{A}$, con lo que es una operación.

   b) Demuestre que $*$ es conmutativa.

   c) Demuestre que $*$ es asociativa

   d) Determine el elemento neutro $\epsilon(n)$ para $*$ en $\mathscr{A}$.

   e) Dada una función aritmética f, determine cuándo existe su inversa de Dirichlet, f^{-1} tal que $f * f^{-1} = \epsilon$.

   f) Demuestre que la convolución de Dirichlet distribuye sobre la suma:

   $$f * (g + h) = f * g + f * h$$

   Concluya que $(\mathscr{A}, +, *)$ es un anillo conmutativo.

3. Encuentre el máximo entero n tal que n^2 divide 10!.

4. Explique cuándo tiene soluciones para x la ecuación:

   $$ax + b = c \pmod{m}$$

5. Explique cuándo tiene soluciones la ecuación diofántica (sólo se admiten soluciones enteras):

   $$ax + by = c$$

   Acá a, b y c son constantes dadas, se buscan valores de x e y. Dé todas las soluciones, de haberlas. ¿Bajo qué condiciones hay infinitas soluciones positivas?

6. Halle todas las soluciones a la ecuación:

   $$x^2 - 17y^2 = 1$$

   Use sus resultados para hallar una aproximación racional de $\sqrt{17}$ con cuatro decimales de precisión.

   Pista: Es una ecuación de Pell, y también es $4^2 - 17 \cdot 1^2 = -1$.

7. La ecuación de Pell es de la forma $x^2 - dy^2 = 1$ para d entero, e interesan valores enteros de (x, y). La solución $(1, 0)$ se conoce como la *solución trivial*. Demuestre las siguientes:

   a) Si d es un cuadrado perfecto, la única solución es la trivial

   b) En toda solución x e y son relativamente primos.

8. Demuestre que si $a^n - 1$ es primo, entonces $n = 1$ y $a - 1$ es primo, o n es primo y $a = 2$.

9. Los *números de Fermat* se definen por $F_n = 2^{2^n} + 1$.

   a) Demuestre que si $a \equiv b \pmod{c}$, entonces $\gcd(a, c) = \gcd(b, c)$ para todo $c \in \mathbb{Z}$.

Borrador

b) Demuestre que $\gcd(n+1, n^{2k}+1) = \gcd(n+1, 2)$. Puede usar el resultado 9*a*.

c) Demuestre que $\gcd(F_n, F_m) = 1$ si $n < m$.

10. Demuestre que $7u^2 = x^2 + y^2 + z^2$ sólo tiene la solución $u = x = y = z = 0$ en $\mathbb{Z}$.

11. ¿Que puede concluir respecto de la primalidad de 949 de la información siguiente?

    a) $3^{948} \equiv 1 \pmod{949}$

    b) $3^{237} \equiv 703 \pmod{949}$, $3^{474} \equiv 729 \pmod{949}$ y $3^{948} \equiv 1 \pmod{949}$

12. Determine para qué valores de x son enteras ambas expresiones:

$$\frac{3x-17}{4} \qquad \frac{5x+18}{7}$$

13. Determine los valores de n para los que son simultáneamente enteros $(n+1)/3$, $(3n+1)/4$ y $(7n-3)/5$.

14. Sean a y b números primos. ¿Cuántas raíces cuadradas tiene 1 módulo ab?

15. Un grupo G se dice *cíclico* si hay un elemento $g \in G$ (un *generador*) tal que $G = \langle g \rangle$, o sea, todos los elementos de G pueden escribirse como potencias de g. Demuestre que todo grupo de orden primo es cíclico.

16. Demostrar que $k!$ divide el producto de cualquier secuencia de k enteros consecutivos.

17. Resuelva las ecuaciones:

$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$
$$x \equiv 6 \pmod{8}$$

18. Determine las soluciones (si existen) del sistema de congruencias:

$$x \equiv 6 \pmod{9}$$
$$x \equiv 5 \pmod{12}$$

19. Demuestre que $\binom{n}{i}$ es par para $1 \leq i \leq n-1$ sólo si $n = 2^k$ para algún k.

20. Encuentre el valor de:

$$(73^{33} + 5) \bmod 64$$

    Indique paso a paso los resultados que usa.

21. Sean tres números enteros a, b y c, y sea d el máximo común divisor de los tres, $d = (a, b, c)$. Demuestre que existen enteros x, y y z tales que $d = ax + by + cz$.

22. Demuestre que para todo entero m

$$m^2 \equiv 0 \text{ ó } 1 \pmod{4}$$

    En consecuencia, explique porqué 10 003 no puede ser la suma de los cuadrados de dos números enteros.

23. Determine si $117^{100} + 1$ es divisible por 11.

24. Calcule el valor de $\phi(1\,268\,064)$

25. Demuestre que $a \in \mathbb{Z}_n$ es un generador del grupo (aditivo) $\mathbb{Z}_n$ (véase el problema 13) si y sólo si a es una unidad del anillo $\mathbb{Z}_n$.

26. Encuentre 117^{-1} en $\mathbb{Z}_{144}$

Borrador

27. Descomponga el grupo aditivo $\mathbb{Z}_{30}$ en la suma directa de los más grupos que pueda.

28. Demuestre que si $\mathfrak{A}$ y $\mathfrak{B}$ son subgrupos de $\mathfrak{G}$, entonces lo es $\mathfrak{A} \cap \mathfrak{B}$.

29. ¿El grupo $\mathbb{Z}_7^\times$ es isomorfo a $\mathbb{Z}_6$, que tiene el mismo orden?

30. Compare los grupos aditivos $\mathbb{Z}_8$ y $\mathbb{Z}_2 \oplus \mathbb{Z}_4$.

31. Encuentre todas las soluciones del sistema de ecuaciones:

$$\begin{aligned} x &\equiv 37 \pmod{39} \\ x &\equiv 10 \pmod{13} \\ x &\equiv 1 \pmod{2} \end{aligned}$$

32. Descomponga el grupo $\mathbb{Z}_{31}^*$ (unidades de $\mathbb{Z}_{31}$) en la suma directa de los más grupos que pueda.

33. Encuentre los generadores de $\mathbb{Z}_{31}^*$, si este grupo es cíclico (véanse 13 y 32).

34. Demuestre que si n es un número natural, entonces $\sqrt{n}$ o es un entero o es irracional (nunca es una fracción).

35. Considere la ecuación de Pell, en que las variables son todas enteras:

$$x^2 - dy^2 = 1$$

Siempre está la solución trivial $x = 1$ e $y = 0$.

a) Demuestre que si $d = a^2$ es un cuadrado perfecto no hay soluciones no triviales.

b) Si x_0, y_0 es la menor solución positiva no trivial de la ecuación (su *solución fundamental*), las demás soluciones x_n, y_n se obtienen de:

$$x_n + y_n\sqrt{d} = (x_0 + y_0\sqrt{d})^n$$

Encuentre recurrencias para x_n, y_n en términos de x_0, y_0, y d.

36. Sean $a, b, c \in \mathbb{Z}$, donde $a, b, c \geq 0$, y considere el conjunto $I = \{ax + by + cz : x, y, z \in \mathbb{Z}\}$. El mínimo elemento m de I (si existe) divide a todos los elementos de I.

37. Demuestre que si $\gcd(a^m, b^n) = 1$, donde $m, n \in \mathbb{N}$, entonces $\gcd(a, b) = 1$.

38. Demuestre que la congruencia:

$$ax \equiv b \pmod{m}$$

tiene solución si y sólo si $\gcd(a, m) \mid b$.

39. Sea el número entero x escrito en decimal $d_n d_{n-1} \ldots d_0$, donde $0 \leq d_i \leq 9$. Demuestre:

a) $x \equiv d_0 + d_1 + \ldots + d_n \pmod{9}$

b) $x \equiv d_0 - d_1 + d_2 - \ldots + (-1)^n d_n \pmod{11}$

40. ¿Cuáles son las posibilidades para los últimos dos dígitos de n^2, si n es un entero?

41. ¿Para qué valores de n es par $\phi(n)$? ¿Cuándo es una potencia de 2?

42. Demuestre que si p es primo, entonces:

$$(a + b)^p \equiv a^p + b^p \pmod{p}$$

43. El sistema criptográfico ElGamal funciona como sigue: Se elige un primo p, los cálculos de ahora en adelante son siempre en $\mathbb{Z}_p$. Se encuentra un generador g de $\mathbb{Z}_p^*$, y se elige un entero $x \in \mathbb{Z}_p$ al azar, y se calcula $h = g^x$. La clave pública es (p, g, h), la clave privada es x. Para cifrar un mensaje $m \in \mathbb{Z}_p$ se elige $y \in \mathbb{Z}_p$ al azar, y se calculan $c_1 = g^y$, $c_2 = m \cdot h^y$. El mensaje cifrado es el par (c_1, c_2). Para descifrar se calcula $m' = c_2 \cdot c_1^{-x}$ Demuestre que m' es el mensaje original.

Borrador

44. ¿Cuántos enteros positivos entre 1 y 100 son divisibles por 2 ó 5? Generalice su respuesta para el caso en que le dan un límite N y un conjunto de números primos p_1, p_2, p_3.

45. Demuestre que $ac \equiv bc \pmod{m}$, donde a, b, c y m son enteros, no necesariamente implica $a \equiv b \pmod{m}$. ¿Bajo qué condiciones se cumple esto?

46. Calcule $29^{3965} \pmod{31}$.

47. *a*) Demuestre que $\gcd(a, b) = 1$ si y sólo si $\gcd(a^2, b^2) = 1$.

    b) Usando el resultado de la parte 47*a*, demuestre que $\gcd(a^2, b^2) = (\gcd(a, b))^2$

48. ¿Cuándo tiene solución para x la ecuación $ax + b \equiv c \pmod{m}$?

49. Demuestre que si p es primo entonces $(a + b)^p \equiv a^p + b^p \pmod{p}$ para enteros a y b

50. ¿Para qué valores de n son enteros $(5n + 1)/7$ y $(3n - 4)/5$?

51. Se usaba la *prueba del nueve* para verificar operaciones (sumas, restas y multiplicaciones). Se calcula la suma de los dígitos de los datos sucesivamente hasta reducir a un dígito, se hacen los mismos cálculos con éstos y se compara con el resultado obtenido para verificar. Demuestre que si $n = (a_{k-1}a_{k-2}\ldots a_0)_{10}$ entonces $n \equiv a_0 + a_1 + \ldots + a_{k-1} \pmod{9}$, y con esto justifique este método de verificación.

    Demuestre que $n \equiv a_0 - a_1 + a_2 - \ldots \pm a_{k-1} \pmod{11}$. Basado en esto, describa una técnica afín a la prueba del nueve. ¿Tiene sentido usar ambas técnicas en la esperanza de detectar más errores?

52. Sea $f(x)$ un polinomio. Demuestre que el número de raíces de $f(x) = 0$ módulo $m_1 m_2 \ldots m_r$ es el producto de los números de raíces módulo m_i si los m_i son relativamente primos en pares.

53. Calcule $45^{17} + 31^9$ mód 16

54. Una manera de demostrar la fórmula para $\phi(pq)$ con p y q primos es considerar los números entre 1 y pq, y restar los que son múltiplos de p y q. Complete los detalles de lo anterior.

55. Calcule el valor de 55^{50} mód 52. Nótese que $52 = 4 \cdot 13$.

56. Calcule el valor de $(33^{193} + 25^9)$ mód 16.

57. ¿Cuándo es impar $\phi(n)$?

58. Discutimos los métodos de factorización siguientes:

    a) Intentar dividir por los primos 2, 3, 5, 7, ...

    b) El método ρ de Pollard

    c) El método $p - 1$ de Pollard

    d) El método de Fermat

    Explique *someramente* cómo funciona cada uno de éstos. ¿En qué casos funciona mejor cada uno de ellos?

59. Suponga que a y b son relativamente primos. ¿Qué valores puede tomar $\gcd(a + b, a - b)$?

60. ¿Tiene inverso multiplicativo módulo 175 el número $22^{12\,007}$?

61. Demuestre que si p es primo, entonces $p \mid a^p - a$ para cualquier entero a.

62. Defina la función $\phi(m)$.

63. Demuestre que hay valores $1 \leq a, b, c < m$ tales que $ac \equiv bc \pmod{m}$, pero $a \not\equiv b \pmod{m}$.

64. ¿Cuánto es $\phi(360)$?

Borrador

65. Los *números de Fibonacci* se definen mediante:

$$F_0 = 0 \quad F_1 = 1 \quad F_{n+2} = F_{n+1} + F_n \text{ (para } n \geq 0)$$

Demuestre que F_n y F_{n+1} son siempre relativamente primos.

`Pista:` Use la identidad de Bézout para $\gcd(F_{n+1}, F_n)$ con la recurrencia para obtener una relación entre F_{n+1} y F_{n+2}, y use inducción.

66. Considere el polinomio $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ con coeficientes enteros, tal que $a_n \neq 0$, $a_0 \neq 0$ y $\gcd(a_n, a_{n-1}, \ldots, a_0) = 1$. Demuestre que si $p(x)$ tiene una raíz racional $x = u/v$ con $\gcd(u, v) = 1$, entonces $u \mid a_0$ y $v \mid a_n$.

Pista: Substituya $x = u/v$ en $p(x)$ y elimine fracciones.

67. Considere el polinomio $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ con coeficientes enteros (un *polinomio mónico*). Demuestre que si $p(x)$ tiene una raíz racional $x = u/v$, ésta necesariamente es entera.

Pista: Substituya $x = u/v$ en $p(x)$ y elimine fracciones.

68. Calcule el valor de $(33^{193} + 25^9)$ mód 16.

69. Demuestre que si $\gcd(a, b^2) = 1$, entonces $\gcd(a, b) = 1$.

70. Encuentre todos los valores de n para los que son enteros tanto $(5n + 2)/3$ como $(7n - 3)/5$.

71. Un conjunto de elementos con propiedades afines a los enteros los ponen los polinomios. Acá consideraremos polinomios con coeficientes racionales:

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$$

donde $a_i \in \mathbb{Q}$. Si $a_n \neq 0$, se dice que el *grado* de p, $\deg(p(x)) = n$. Para el caso particular del polinomio cero (todos los coeficientes cero) se dice que su grado es $-\infty$. Si el polinomio no es cero, podemos dividir todos los coeficientes por a_n, y obtenemos *polinomios mónicos* (en ellos el coeficiente de x^n es uno).

Pueden sumarse y multiplicarse polinomios, y se cumplen:

$$\deg(p(x) + q(x)) \leq \text{máx}(\deg(p(x)), \deg(q(x)))$$
$$\deg(p(x) \cdot q(x)) = \deg(p(x)) + \deg(q(x))$$

a) Demuestre que dados polinomios $n(x)$ y $d(x)$, hay polinomios $q(x)$, $r(x)$ únicos tales que:

$$n(x) = q(x) \cdot d(x) + r(x)$$

con $\deg(r(x)) < \deg(d(x))$ (algoritmo de división para polinomios).

b) Demuestre que al multiplicar polinomios mónicos se obtiene un polinomio mónico como producto. Además, si un polinomio mónico puede expresarse como el producto de dos polinomios, puede expresarse como el producto de polinomios mónicos.

c) Un polinomio mónico se dice *irreducible* si no puede escribirse como producto de polinomios de menor grado. Demuestre que todo polinomio mónico puede expresarse como producto de polinomios mónicos irreducibles.

Pista: Proceda como en la factorización de los enteros, eligiendo el contraejemplo con mínimo grado y llegando a una contradicción.

72. Sea $ax + by = c$ una ecuación lineal donde a, b y c son coeficientes enteros. Si $\gcd(a, b) \mid c$, entonces la ecuación posee soluciones enteras de la forma

$$x = x_0 - k\frac{b}{d}$$
$$y = y_0 + k\frac{a}{d}$$

donde $k \in \mathbb{Z}$ y $d = \gcd(a,b)$. Acá x_0, y_0 representan una solución particular de la ecuación.

Dado este contexto, se les pide que realicen las siguientes tareas:

Borrador

a) Demostrar que en el caso indicado la solución indicada es correcta, y todas las soluciones están dadas por esa expresión.

b) Encontrar un método para encontrar una solución particular (x_0, y_0) de la ecuación, usando la identidad de Bézout para $\gcd(a, b)$.

73. Calcule el valor de las siguientes expresiones en $\mathbb{Z}_{14}$, o explique porqué no se puede hacer:

$$3 \cdot 17 - 4/5$$
$$5/6 + 8$$
$$(4 + 22) \cdot 4 - 21/7$$

74. Resuelva las ecuaciones siguientes, indicando *todas* las soluciones (si las hay) en $\mathbb{Z}_{15}$:

$$3x + 10 = 7$$
$$4x - 5 = 8$$
$$5x + 11 = 0$$

75. Determine las unidades y los divisores de cero en $\mathbb{Z}_{24}$ y en $\mathbb{Z}_{31}$. ¿Son campos estos anillos?

76. Encuentre todas las raíces cuadradas de cada elemento de $\mathbb{Z}_{24}$ y de $\mathbb{Z}_{31}$.

77. Resuelva la ecuación $x^2 + x + 1 = 0$ en los anillos $\mathbb{Z}_{24}$, en $\mathbb{Z}_{26}$ y $\mathbb{Z}_{31}$. ¿Puede aplicarse la tradicional fórmula para las raíces de la cuadrática en estos casos? Explique.

78. Calcule

a) 7^{401} mód 41

b) 50^{50} mód 45

Explique cómo hace el cálculo a mano, sin ayuda de calculadoras.

79. El profesor Carroll quiere dividir su curso en grupos. Pero al dividirlo en tres grupos, hay dos estudiantes que quedan fuera. Al intentar con cinco grupos, sobran tres. Finalmente intenta con siete grupos, y quedan dos sin grupo. ¿Cuál es el mínimo número de estudiantes en el curso?

80. Encuentre todas las soluciones enteras (x, y) para la ecuación $119x + 399y = \gcd(119, 399)$.

81. La *sección áurea* es el cero positivo del polinomio $x^2 - x - 1$. Demuestre que este número es irracional.

82. La ecuación de Pell es $x^2 - dy^2 = 1$, donde todas las variables son enteras.

a) Demuestre que si d es un cuadrado perfecto no hay soluciones.

b) Demuestre que para todas sus soluciones $\gcd(x, y) = 1$.

83. La fórmula para resolver ecuaciones de segundo grado se obtiene con manipulaciones que son válidas en un anillo conmutativo, siempre que las raíces e inversos existan. Encuentre las raíces en $\mathbb{Z}_7$ (un generador de $\mathbb{Z}_7^*$ es 3) de la ecuación:

$$4x^2 + 3x + 4 = 0$$

84. Sea p un factor primo del número de Fermat $F_n = 2^{2^n} + 1$. Demuestre que el orden de 2 módulo p es 2^{n+1}.

85. Demuestre que los números de Fermat $F_n = 2^{2^n} + 1$ cumplen:

$$F_n = \prod_{0 \le k < n} F_k + 2$$

Borrador

86. A un número a que verifique la congruencia

$$a \equiv x^2 \pmod{m}$$

se le denomina *residuo cuadrático* (módulo m). El *símbolo de Legendre* se define para un entero a y un primo impar p, con $p \nmid a$, como:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ es residuo cuadrático módulo } p \\ -1 & \text{si } a \text{ es no-residuo cuadrático módulo } p \end{cases}$$

Veremos que $\mathbb{Z}_p^*$ es cíclico si p es primo, con lo que sus elementos pueden escribirse como potencias de una *raíz primitiva* r. Es claro que las potencias pares de r tienen raíz cuadrada en $\mathbb{Z}_p$, las impares no.

a) Demuestre que módulo un primo impar p hay tantos residuos cuadráticos como no-residuos cuadráticos.

b) De las reglas al sumar números pares e impares, demuestre que:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

c) Sabemos que $r^{(p-1)/2} \equiv -1 \pmod{p}$, ya que el orden de r es $p-1$ y en $\mathbb{Z}_p$ sólo 1 y -1 cumplen $x^2 \equiv 1 \pmod{p}$. Demuestre que:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

87. Demostrar que si $\gcd(a, b) = 1$ entonces $\gcd(a + b, a - b)$ es 1 o 2.

88. El objetivo es demostrar un resultado de Fermat.

a) Usando el teorema fundamental de la aritmética, demuestre que si $\gcd(a, b) = 1$ y $ab = c^n$ entonces a y b son n-ésimas potencias perfectas.

b) Usando la parte 88*a*, demuestre que las únicas soluciones enteras de $x^3 = y^2 + y$ son $(0, 0)$ y $(0, -1)$.

89. Demostramos que si f es multiplicativa, y $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ con p_i primos distintos y $e_i \geq 1$ entonces:

$$\sum_{d|n} \mu(d) f(d) = \prod_{1 \leq i \leq r} (1 - f(p_i))$$

Partiendo de la identidad de Gauß:

$$\sum_{d|n} \phi(d) = n$$

halle una fórmula para $\phi(n)$.

90. El número ISBN de una publicación consta de 9 dígitos, y un dígito verificador que se calcula como:

$$\sum_{1 \leq k \leq 9} k d_k \text{ mód } 11$$

Si el dígito verificador es 10, se anota X.

a) ¿Puede este código detectar todos los errores en un único dígito?

b) ¿Puede este código detectar todas las transposiciones (dos dígitos intercambiados)?

91. Demuestre que $19 \mid 10a + b$ si y solo si $19 \mid a + 2b$.

92. Demuestre que si $a^n - 1$ es primo, es $n = 1$ y $a - 1$ primo, o $a = 2$ y n es primo.

Borrador

93. Resuelva las congruencias:

$$x \equiv 1 \pmod 3$$
$$x \equiv 2 \pmod 4$$
$$x \equiv 3 \pmod 5$$

94. Sea $\omega(n)$ el número de primos distintos que dividen a n (por ejemplo, $\omega(2) = \omega(27) = 1$, $\omega(12) = 2$). Se define:

$$\gamma(n) = (-1)^{\omega(n)}$$

Demuestre que γ es multiplicativa.

95. La ecuación de Pell es de la forma $x^2 - dy^2 = 1$ para $d > 1$ entero, interesan valores enteros de (x, y). La solución $(1, 0)$ se conoce como la *solución trivial*. Demuestre las siguientes:

a) Si d es un cuadrado perfecto, la única solución es la trivial

b) En toda solución x e y son relativamente primos.

c) Si (x_0, y_0) es una solución de la ecuación de Pell, otras soluciones están dadas por:

$$x_n + y_n\sqrt{d} = (x_0 + y_0\sqrt{d})^n$$

Pista: Aproveche que:

$$(a_1 + b_1\sqrt{d}) \cdot (a_2 + b_2\sqrt{d}) = (a_1a_2 + b_1b_2d) + (a_1b_2 + b_1b_2)\sqrt{d}$$
$$(a_1 - b_1\sqrt{d}) \cdot (a_2 - b_2\sqrt{d}) = (a_1a_2 + b_1b_2d) - (a_1b_2 + b_1b_2)\sqrt{d}$$

Borrador

7. Criptografía

1. El estándar PKCS#1 sobre criptografía de clave pública define la función $\lambda(n)$ para $n = p_1 \cdot p_2 \cdot \ldots \cdot p_u$ donde los p_i son números primos diferentes:

   $$\lambda(n) = \text{lcm}(p_1 - 1, p_2 - 1, \ldots, p_u - 1)$$

   Acá lcm es la función mínimo común múltiplo. PKCS#1 indica usar un par de números primos p y q y un exponente e tal que $(e, \lambda(n)) = 1$. La clave pública acá es $n = p \cdot q$ y e, dado el mensaje $m < n$ se cifra mediante:

   $$M = m^e \pmod{n}$$

   Para descifrar se usa la clave privada d tal que $d \cdot e \equiv 1 \pmod{\lambda(n)}$ y:

   $$m' = M^d \pmod{n}$$

   Demuestre que $m' \equiv m \pmod{n}$.

   ¿Que ventajas trae consigo esta variante de RCS?

2. Considere la siguiente propuesta para una variante de RSA: Se eligen 3 números primos diferentes, llamémosles p_1, p_2, y p_3. El módulo es $m = p_1 \cdot p_2 \cdot p_3$, y se elige un exponente e tal que $a^e \pmod{m}$ (la operación de cifrado) sea cómoda de calcular (por ejemplo, $e = 65$, que en su representación binaria tiene sólo dos bits 1).

   a) ¿Cómo se descifra en este esquema?

   b) ¿Que ventajas podría tener el usar tres primos en vez de dos, como en RSA tradicional?

3. El sistema para intercambio de claves de Diffie-Hellman usa un número primo grande p y una raíz primitiva g módulo p.

   a) Explique cómo funciona este sistema.

   b) Se sugiere reutilizar p y g. ¿Porqué esto no afecta la seguridad del sistema?

   c) Explique porqué es crítico que las potencias elegidas por A y B se mantengan secretas.

4. El sistema de clave pública ElGamal es como sigue:

   - Alice elige un grupo cíclico G de orden q y un generador g del grupo. Elige x al azar entre $\{1, \ldots, q-1\}$. Calcula $h = g^x$. Su clave pública es (G, q, g, h), su clave privada es (G, q, g, h, x).
   - Para cifrar el mensaje m (que suponemos es un elemento de G) con la clave de Alice, Bob elige y al azar en $\{1, \ldots, q-1\}$, y calcula $c_1 = g^y$, $s = h^y$ y $c_2 = m \cdot s$, luego envía (c_1, c_2) a Alice.
   - Para decifrar el mensaje (c_1, c_2) de Bob, Alice calcula $s = c_1^x$, y obtiene $m' = c_2 \cdot s^{-1}$

   Generalmente se usa el grupo $G = \mathbb{Z}_p^\times$ para un primo p grande.

   a) Demuestre que Alice realmente recupera el mensaje enviado por Bob, o sea que $m = m'$.

   b) Se indica que el valor de y no debe reusarse, es una clave efímera. Explique cómo romper el sistema si se ha interceptado un mensaje cifrado (c_1, c_2) para el que se conoce el mensaje original m, y se reusa y para cifrar mensajes adicionales.

5. Una informática paranoica, Alice, desea usar el método de Diffie-Hellman para intercambiar claves con un amigo, Bob. Alice elige el número primo $p = 1031$. ¿Cuál es el mínimo generador de $\mathbb{Z}_p^*$? Muestre cómo generan la clave final Alice y Bob si Alice usa el generador mínimo y $a = 117$, y Bob elige $b = 32$.

6. El sistema de secreto compartido de Shamir para compartir s entre n participantes, elige un primo p tal que $s < p$, y genera $k - 1$ coeficientes a_1 hasta a_{k-1} al azar, obteniendo el polinomio $f(x) = a_{k-1}x^{k-1} + \ldots + a_0$, donde $a_0 = s$. Para cada los participantes elige un valor x_1 hasta x_n, todos distintos. Al participante i se le entrega el par $(x_i, f(x_i) \bmod p)$. Demuestre que sólo si al menos k participantes cooperan es posible determinar el secreto s.

Borrador

7. El sistema de cifrado ElGamal consiste en lo siguiente: Alice elige un número primo p y una raíz primitiva r. Elige x al azar en el rango $0 \leq x < p$, y calcula $h = r^x \bmod p$. Su clave pública es (p, r, h). Si Bob desea comunicarle m a ella, con $0 \leq m < p$, elige y al azar en el rango $0 \leq y < p$ y calcula $c_1 = r^y \bmod p$ y $s = h^y \bmod p$. Luego calcula $c_2 = (m \cdot s) \bmod p$ y envía el par (c_1, c_2) a Alice.

   Para descifrar, Alice calcula en $\mathbb{Z}_p$:

   $$s' = c_1^x$$
   $$m' = c_2 \cdot (s')^{-1}$$

   Demuestre que esto es válido, en el sentido que Alice obtiene el mensaje original ($m' = m$).

8. Suponga que Alice define su clave RSA con primos p y q, dando módulo $n = pq$, y elige el exponente primo e. Bob le envía un mensaje de contenido kp. ¿Puede Alice descifrar el mensaje recibido?

   Pista: Use (el padre de) el teorema chino de los residuos.

9. El sistema de Mignotte comparte el secreto s entre n personas de forma que se requieren a lo menos k cualquiera de ellas para tener acceso al secreto.

   Se eligen n enteros relativamente primos $m_1 < m_2 < \ldots < m_n$. El secreto s a compartir es un entero menor a $m_1 \cdot m_2 \cdot \ldots \cdot m_k$ (el producto de los k m_i más pequeños) pero mayor a $m_{n-k+2} \cdot m_{n-k+3} \cdot \ldots \cdot m_n$ (el producto de los $k-1$ m_i más grandes). Claramente los m_i deben elegirse de forma de tener un rango suficiente entre estos dos límites. A cada participante i se le da el par ($s \bmod m_i, m_i$).

   a) Dado que cooperan k de los participantes, explique cómo se obtiene el secreto.

   b) Explique porqué sólo si al menos k de los participantes cooperan pueden obtener el secreto.

10. Alan Turing propuso un sistema criptográfico basado en teoría de números en su juventud. No sobreviven demasiados detalles, damos dos interpretaciones de lo que se sabe al respecto:

    Versión 1: Se elige un número grande k como clave. El mensaje m (interpretado como entero) se multiplica por k para dar el mensaje cifrado $c = m \cdot k$. Para que no sea demasiado fácil descifrar, se exige que m sea primo también (basta "rellenar" al final para hacerlo primo). Descifrar es simplemente dividir por k.

    Versión 2: Se elige un primo grande p (que se publica) y una clave k, $1 \leq k \leq p-1$. para cifrar se calcula $c = m \cdot k \bmod p$, descifrar es multiplicar por k^{-1} en $\mathbb{Z}_p$.

    Explique los problemas con estos sistemas criptográficos. Considere situaciones como varios mensajes que se saben cifrados con la misma clave, o casos en que se conoce el mensaje original y el mensaje cifrado (esto se da por ejemplo con comienzo de archivos en un formato, donde se conoce gran parte del encabezado y se puede "adivinar" el resto).

Borrador

8. Combinatoria elemental

1. La bolsa en Wall Street identifica a las empresas mediante un código de cuatro consonantes. Así por ejemplo, Red Hat es `RDHT`. ¿Cuántas posibles empresas hay en Wall Street? Supóngase que se integran las empresas de América Latina, y se quedan cortos de opciones. Deciden entonces permitir una única vocal en cualquiera de las cuatro posiciones, como en `ABCD`. ¿Cuántas opciones hay ahora?

2. Finalmente se acabarán los números de patentes nuevas (4 consonantes y 2 dígitos). En reemplazo, se sugieren las siguientes propuestas (las letras son 21 consonantes y 5 vocales, en total 26):

   a) 4 letras seguidas por 3 dígitos

   b) 4 letras y 3 dígitos, alternadamente (letra - dígito - letra - dígito - letra - dígito - letra)

   c) 4 consonantes y 3 dígitos en cualquier orden

   d) Por una módica suma adicional, se ofrecerán patentes personalizadas de largo entre tres y seis, formadas por letras y a lo más un dígito en cualquier orden

   Muestre paso a paso cómo calcula el número de posibilidades para cada propuesta.

3. ¿Cuántos subconjuntos tiene el multiconjunto $\{a_1^{n_1} a_2^{n_2} \dots a_k^{n_k}\}$? ¿Cuántos de ellos tienen m elementos?

4. La Universidad de Miskatonic envía su imbatible sexteto de voleibol a una competencia.

   a) Para el viaje les preparan sándwich. Si hay elección entre pan batido y hallula, y pueden ser de salame, de jamón o de palta, ¿cuántos tipos de sándwich son posibles?

   b) ¿Cuántas posibilidades hay en total si cada jugador elige un sándwich, una bebida (agua mineral o té) y una fruta (manzana, naranja o plátano)?

   c) En el camino paran en una heladería, que tiene 17 sabores diferentes de helado que se sirven en conos con tres sabores. ¿Cuántos helados distintos pueden servirse, si no importa el orden de los sabores?

   d) ¿Cuántas opciones de helados hay si la regla de la heladería es que no se pueden repetir sabores?

5. Para apelar a su espíritu lúdico.

   a) En el dominó tradicional las piezas tienen dos lados numerados de 0 a 6, sin que hayan piezas repetidas. ¿Cuántas piezas hay?

   b) Una variante es el *triominó*, en el cual hay piezas triangulares con tres números, nuevamente sin repeticiones. Si la numeración va de 0 a 5, ¿cuántas piezas hay?

   Explique claramente cómo calcula los valores que entrega.

6. Dados n y k, encuentre una expresión para el número de secuencias de números naturales $1 \leq a_1 \leq a_2 \leq \dots \leq a_k \leq n$.
   Pista: Use las variables auxiliares $x_1 = a_1 - 1$, $x_2 = a_2 - a_1$, $\dots$, $x_{k+1} = n - a_k$.

7. Encuentre el número de permutaciones de las 26 letras del alfabeto inglés que no contengan *hoy*, *prueba*, *fea* ni *nota*.

8. Al salir de la tienda, María y Fernanda vieron cómo dos hombres huían de una joyería, en la cual sonaba la alarma. María está segura que el último dígito de la patente del auto en que huyeron los asaltantes era 5 ó un 6, y el segundo era un 3, mientras Fernanda asevera que la primera letra era una O o una D, y que el primer dígito era 1 ó 7. ¿Cuántas patentes cumplen con estas restricciones, suponiendo tres letras y cuatro dígitos?

9. Al planificar las actividades de la semana, Matías ve que tiene 12 tareas que debe llevar a cabo. ¿De cuántos órdenes distintos puede ejecutarlas, si no hay otras restricciones? ¿Cuántas alternativas hay si considera que 4 de las tareas son más importantes, y deben estar completas antes de comenzar cualquiera de las otras 8? ¿Cuántas formas hay si los divide en tres grupos, 4 de máxima prioridad, 5 de prioridad media, y 3 de mínima prioridad?

Borrador

10. Pamela tiene 10 libros y 3 repisas. ¿De cuántas formas puede disponer sus libros en las repisas, si deben haber al menos dos libros por repisa? Nótese que a ella le importa el orden de izquierda a derecha en que están los libros en cada repisa.

11. Muestre que para cualquier par de enteros $n, r \geq 0$, si $n + 1 > r$, entonces:

$$P(n+1, r) = \frac{n+1}{n+1-r} P(n, r)$$

12. Encuentre los valores de n que satisfacen cada uno de los casos

    a) $P(n, 2) = 90$

    b) $P(n, 3) = 3P(n, 2)$

    c) $2P(n, 2) + 50 = P(2n, 2)$

13. ¿Cuántas trayectorias entre $(0, 0)$ y $(5, 17)$ formadas únicamente por pasos hacia la derecha (D) y hacia arriba (A) hay? ¿Cómo puede generalizarse esto a trayectorias entre (x_1, y_1) y (x_2, y_2)?

14. En un rectángulo de $m \times n$ se permiten sólo movimientos hacia el norte y el este. Partiendo en la esquina inferior izquierda y llegando a la superior derecha, ¿cuántos caminos diferentes pueden seguirse?

15. ¿Cuántos enteros de seis dígitos (no comienzan con cero) hay? ¿Cuántos hay si no se permiten dígitos repetidos?

16. ¿De cuántas formas se pueden distribuir 12 naranjas entre 5 niños? ¿Cuántas si cada uno recibe al menos una naranja? ¿Si además el mayor recibe al menos dos naranjas? ¿El menor recibe un número impar de naranjas?

17. En MS-DOS se admiten nombres de archivo formados por letras y dígitos. Un archivo tiene un nombre de a lo más 8 caracteres, y una extensión opcional de a lo más tres caracteres. ¿Cuántos nombres de archivo distintos admite MS-DOS?

18. La primeras versiones de Unix admitían nombres de archivo de a lo más 14 caracteres, elegidos de entre los 128 caracteres ASCII, excluyendo únicamente el caracter nulo (`NUL`) y el '/'. ¿Cuántos nombres de archivo eran posibles?

19. ¿Cuántas palabras de 5 letras se pueden formar con las letras de MISSISSIPI? ¿Cuántas tienen exactamente una letra repetida? ¿Cuántas tienen a lo menos una letra repetida?

20. Si se sacan 13 cartas de un mazo común (sin comodines), ¿Cuál es la probabilidad de que contengan al menos una carta de cada pinta? ¿Cuál es la probabilidad que una pinta particular (p. ej. tréboles) no aparezca? ¿Cuál es la probabilidad que sólo aparezcan 3 pintas? ¿Porqué son diferentes las respuestas anteriores?

21. Interesa el número N_3 de polinomios cúbicos irreductibles sobre $\mathbb{Z}_p$. Indique claramente cómo resuelve los problemas combinatorios que se plantean.

    a) Exprese T_n, el número total de polinomios mónicos de grado n, en términos de n y p.

    b) ¿Cuántos polinomios mónicos de grado 1 son irreductibles? Exprese N_1 en términos de T_1 y p.

    c) ¿Cuántos polinomios mónicos de grado 2 son reductibles? Exprese N_2 en términos de T_2 y N_1 y p.

    d) Sea N_3 el número de polinomios mónicos irreductibles de grado 3, expréselo en términos de T_3, N_2, N_1 y p, y finalmente en términos únicamente de p.

22. Un *multiconjunto* es similar a un conjunto, con la diferencia que un elemento puede aparecer más de una vez. Por ejemplo, $A = \{1, 1, 1, 2, 3, 3\}$ es un multiconjunto, donde 1 aparece 3 veces, 2 aparece 1 vez, y 3 está 2 veces. En lo que sigue, considere un multiconjunto C de los elementos 1 a n en que i aparece k_i veces.

    a) Un *subconjunto* de un multiconjunto contiene a lo más el número de veces que cada elemento aparece. Así, $\{1, 1, 1, 3\} \subseteq A\}$. ¿Cuántos subconjuntos de C hay?

    b) Una *permutación* de un multiconjunto se obtiene escribiendo todos sus elementos en algún orden. Así, $(3, 2, 1, 3, 1, 1)$ es una permutación de A. ¿Cuántas permutaciones de C existen?

Borrador

Una forma de verificar sus respuestas es mostrar que dan los familiares valores para un conjunto.

23. Explique paso a paso cómo determinar cuántas manos de poker (cinco cartas tomadas de entre las 52 cartas del mazo inglés) están formadas por un trío (tres cartas con el mismo valor) y un par (dos cartas con el mismo valor).

24. Considere la palabra `CHUPACABRAS` (acá `C` y `H` son letras separadas)

    a) ¿Cuántas secuencias de 11 letras se pueden obtener?

    b) ¿En cuántas secuencias aparece `SAP`?

    c) ¿Cuántas de las secuencias tienen todas las vocales juntas?

25. Dé una demostración combinatoria para la siguiente identidad:

$$\sum_{i+j+k=n} \binom{r}{i}\binom{s}{j}\binom{t}{k} = \binom{r+s+t}{n}$$

26. Considere el juego de canasta, que se juega con dos mazos de carta ingleses (valores son As (A), 2 a 10, Jack (J), Queen (Q), King (K); pintas son espada, corazón, trébol y diamante; además cada mazo incluye dos Jokers). Indique:

    a) ¿Cuántas manos diferentes de 11 cartas hay?

    b) ¿Cuántas manos tienen los cuatro Joker?

    c) ¿Cuántas manos tienen una *canasta limpia* (siete cartas del mismo valor)?

27. Considerando los subconjuntos de un conjunto de n elementos, dé una demostración combinatoria de:

$$\sum_{0\le i\le n} \binom{n}{i} = 2^n$$

28. ¿Cuántas soluciones tiene $x + y + z = 17$ con $x, y, z \in \mathbb{N}$?

29. En un juego de cartas cada jugador recibe una mano de 7 cartas, elegidas de un mazo inglés. Se reconocen *tríos*, tres cartas del mismo valor; y *escalas*, cuatro cartas de valores seguidos de la misma pinta, que pueden "dar la vuelta" (como $Q\clubsuit\ K\clubsuit\ A\clubsuit\ 2\clubsuit$). Explique cómo calcular cuántas hay de cada una de estas manos:

    a) **Una escala** y tres cartas adicionales

    b) **Dos tríos** y una carta adicional

    c) **Una escala y un trío** sin cartas adicionales

30. Exprese los siguientes:

    a) El número total de secuencias de n símbolos tomados de $\{a, b, c\}$

    b) El número de secuencias como las del punto 30*a*, que tienen exactamente i símbolos a, j símbolos b, y k símbolos c (obviamente debe ser $i + j + k = n$)

    c) Está claro que la unión de las secuencias del punto 30*b* es simplemente el número de secuencias del punto 30*a*. Exprese esto como una identidad.

31. En el curso de física del profesor Atwood hay 40 hombres. Cada hombre ha estudiado con 6 de las mujeres, y cada una de las mujeres ha estudiado con 5 de los hombres. ¿Cuántos estudiantes en total hay en el curso?

32. ¿De cuántas maneras se pueden ordenar las letras de `MISSISSIPPI`? ¿Cuántas de éstas tienen todas las consonantes juntas?

33. Se eligen 6 cartas de un mazo inglés. ¿De cuántas formas se pueden elegir tal que los valores sean seguidos, sin importar las pintas?

Borrador

34. En el curso de cálculo del profesor Upham hay 32 hombres. Cada hombre ha estudiado con 5 de las mujeres, y cada una de las mujeres ha estudiado con 8 de los hombres. ¿Cuántos estudiantes en total hay en el curso?

35. ¿De cuántas maneras se pueden ordenar las letras de `PELLEGRINI`? ¿Cuántas de éstas tienen todas las vocales juntas?

36. ¿Cuántas manos de poker tienen exactamente 3 ases?

37. Dé expresiones simples para los siguientes números de palabras que se pueden formar reordenando todas las letras de `EMBAJADOR` (no se piden valores numéricos):

    a) El número de palabras que se pueden formar si debe comenzar con `A`

    b) El número de palabras que se pueden formar si las `A` no están juntas

    c) El número de palabras que comienzan con una vocal

    d) El número de palabras en que están juntas todas las vocales

38. ¿Cuántos anagramas tiene la palabra `VUVUZELA`?

39. ¿De cuántas maneras se pueden ordenar las letras de `JABULANI` si debe comenzar con una vocal?

40. ¿Cuántas manos de poker con dos pares de cartas del mismo valor hay?

41. ¿Cuántos anagramas tiene la palabra `RECUPERATIVO`?

42. Considere la palabra `MOVIMIENTO`. ¿De cuántas maneras se pueden ordenar sus letras? ¿De cuántas maneras si las vocales iguales deben estar juntas? ¿Si las `O` no están juntas? Explique cuidadosamente sus razonamientos.

43. ¿Cuántas manos de poker (5 cartas de un mazo inglés) tienen a lo menos 4 cartas `J`, `Q` o `K`? ¿Cuántas tienen exactamente 2 `K` y 2 `Q`? ¿Cuántas de las anteriores tienen las pintas de las `K` y las `Q` iguales? Explique cuidadosamente sus razonamientos.

44. De un mazo inglés se sacan 5 cartas. ¿De cuántas maneras se puede hacer esto sin obtener un par (dos cartas del mismo valor)? ¿De cuántas maneras se puede hacer obteniendo exactamente un par?

45. En una heladería hay 37 sabores distintos de helado, y los helados se sirven en 3 tamaños. Un grupo de 5 no tan aventajados estudiantes de Fundamentos de Informática se juntan a tomar helado, y no saben cómo determinar cuántos pedidos diferentes pueden hacer con la condición que todos elijan sabores distintos. Explique.

46. Considere la palabra `MOVIMIENTO`.

    a) ¿De cuántas maneras se pueden ordenar sus letras?

    b) ¿De cuántas maneras se pueden ordenar si las vocales deben estar separadas por consonantes?

    c) ¿De cuántas maneras se pueden ordenar si no hay letras iguales juntas?

47. La mesa ejecutiva de la Federación de Estudiantes de la Universidad de Miskatonic está formada por 15 personas, tres de las cuales estudian informática. Deben elegir su directiva, formada por presidente, vicepresidente, secretario y tesorero.

    a) ¿De cuántas maneras puede elegirse la directiva?

    b) ¿Cuántas posibles directivas tienen a un informático de presidente?

    c) ¿Cuántas directivas tienen exactamente un informático?

    d) ¿Cuántas directivas tienen al menos un informático?

48. En el sanatorio de Arkham las puertas se abren con botoneras, en las que hay que introducir un código de cuatro dígitos.

    a) ¿Cuántos códigos distintos son posibles?

    b) En una puerta se ve que los dígitos 1, 2, 4 y 5 están gastados. ¿Cuántos códigos distintos da esto?

    c) En otra puerta están gastados sólo 1, 5 y 9. ¿Cuántos códigos son posibles acá?

Borrador

d) Compare los resultados de 48*b* y 48*c*. ¿Cuál es mayor?

49. Para los efectos presentes, un número telefónico es simplemente un número de 7 dígitos. Diremos que un número es *fácil de llamar* si consta de sólo uno o dos dígitos, como 6666666 o 1221212. No es fácil de llamar 1232233. ¿Cuántos números fáciles de llamar hay?

50. Demostrar la suma:

$$\sum_{1\leq k\leq n} k\binom{n}{k} = n\cdot 2^{n-1}$$

51. Una *composición* del entero n es expresarlo como suma. Por ejemplo, las composiciones de 5 son:

$$1+1+1+1=1+1+2=1+2+1=1+3=2+1+1=2+2=3+1=4$$

¿Cuántas composiciones de n hay?

52. Determine el número de maneras de dividir un grupo de 14 personas en parejas.

53. Explique cómo calcular el número de manos de poker (cinco cartas del mazo inglés, trece valores de cada una de cuatro pintas) que tienen todas las pintas y que no repiten valores.

54. Considere la palabra `COMBINATORIA`. ¿De cuántas maneras se pueden ordenar sus letras de manera que comience o termine en `A`?

55. En la Universidad de Miskatonic los exámenes de fin de año se toman en una semana (cinco días), definiendo tres horarios diarios. Asenath White cursa cuatro ramos, y se pregunta cuántos calendarios de exámenes son posibles para ella, si por reglamento solo puede dar un examen al día.

56. ¿Cuántas manos de poker (5 cartas del mazo inglés) pueden formarse tal que contengan exactamente dos pintas y ninguno de los valores se repite?

57. ¿Cuántos multiconjuntos de $2k$ elementos entre n hay tal que el número de repeticiones de cada elemento es par?

58. ¿De cuántas maneras pueden reordenarse las letras de la palabra `REPROBADO` de manera que no hayan letras iguales adyacentes? Plantee cuidadosamente su cálculo.

59. Dé una demostración combinatoria (explicando cómo cada lado cuenta lo mismo de distinta forma) de la identidad:

$$\sum_{0\leq k\leq n} \binom{n}{k}\binom{n}{n-k} = \binom{2n}{n}$$

60. Suponiendo el alfabeto inglés de 5 vocales y 21 consonantes, ¿de cuántas maneras se pueden ordenar 7 letras de forma que la primera y la última sean vocales, y que no hayan letras repetidas?

Borrador

9. Problemas misceláneos

1. En sus extensos viajes, el Enterprise al mando del capitán Picard visitó el sistema Funda. En el planeta Funda II anualmente se lleva a cabo un campeonato. En el juego del caso no hay empates (si nadie gana, se define con una ronda de manotazos entre los rivales), y siempre gana el mejor equipo. Participan 16 equipos, que mediante algún mecanismo misterioso se dividen en 4 grupos de 4 equipos, que llamaremos 1 a 4. En la primera ronda en cada grupo todos juegan con todos, y pasan a la segunda ronda los dos que ganan más partidos de cada grupo. En la segunda ronda juegan pares, en el primer partido el 1º del grupo 1 con el 2º del grupo 2, luego el 1º del grupo 2 con el 2º del grupo 3, después el 1º del grupo 3 con el 2º del grupo 4, y finalmente el 1º del grupo 4 con el 2º del grupo 1. En la tercera ronda el ganador del primer partido de la segunda ronda juega con el ganador del segundo, el ganador del tercero juega con el ganador del cuarto. Los dos ganadores de esta ronda disputan la copa.

   Lamentablemente, el planeta Funda I se está haciendo inhabitable debido a una plaga de lepatatas. En Funda II ponen como condición para aceptar a los habitantes de Funda I que les den una solución rigurosa a unos temas de discusión constante en los bares. Picard le encargó a O'Brian que averiguara de qué se trataba, y diera la solución para que los refugiados de Funda I sean aceptados en Funda II. En una extensa noche de tomateras en bares Ferengi de Funda II O'Brian averiguó cuáles son los temas del caso, pero por el hachazo resultante del carrete está imposibilitado de resolverlo, y le encargó a Ud. que diera la solución al capitán. Los problemas que se discuten en los bares de Funda II son:

   a) ¿Cuántas maneras hay de distribuir los equipos entre los grupos?

   b) ¿Cuántos partidos ganaron los que pasan a la segunda ronda en cada grupo?

   c) ¿Siempre gana la copa el mejor equipo?

   d) Los entusiastas reclaman que con estas reglas en años pasados el vice campeón fue un mal equipo. ¿Es posible que no sean los dos mejores equipos los que disputan la final?

Borrador

10. Series de potencias

1. Determine explícitamente los coeficientes siguientes:

   a) $[x^k]\,\dfrac{1}{(1-x^2)^3}$

   b) $\left[\dfrac{x^k}{k!}\right]\sqrt{1-4x}$

   c) $[\alpha x^k]\,\dfrac{1}{(1-\alpha x)(1-\beta x)}$

   d) $[x^k]\,\dfrac{1}{(1-\alpha x)^3}$

   e) $[x^k]\,(1+x^2)^m$

2. Determine los siguientes coeficientes:

   a) $[x^n]\,(a-bx)^{-2}$

   b) $[x^n]\,e^{1-x}$

   c) $[x^n y^k]\,(1+y(1-x))^{-3}$

   d) $[x^n]\,(1-nx)^{-2n}$

3. Determine los siguientes coeficientes:

   a) $[x^k]\,\dfrac{1}{1-x^2}$

   b) $[x^k]\,\dfrac{1}{1-x/3}$

   c) $[x^k]\,\dfrac{1}{(1-x^2)^3}$

4. Calcule los primeros 5 términos de la serie para $\ln^2(1-x)$ (cuadrado del logaritmo)

5. Encuentre el coeficiente:

   $$[x^{15}]\left(3x^2-\frac{2}{x}\right)^{12}$$

6. Evalúe la suma:

   $$\sum_{2\le j\le n} j(j-1)\binom{n}{j}$$

7. Evalúe la suma:

   $$\binom{k}{k}+\binom{k+1}{k}+\binom{k+2}{k}+\cdots+\binom{n}{k}$$

8. Dado un par de funciones $d(z)$, $h(z)$, se define su *matriz de Riordan* $D=(d(z),h(z))$ como la matriz triangular inferior:

   $$d_{n,k}=\begin{cases}[z^n]\,d(z)\,(zh(z))^k & \text{si } k\le n\\ 0 & \text{caso contrario}\end{cases}$$

   a) Encuentre la matriz de Riordan para $d(z)=h(z)=(1-z)^{-1}$.

Borrador

b) Sea:

$$F(z) \overset{\text{ogf}}{\longleftrightarrow} \langle f_n \rangle_{n \geq 0}$$

Demostrar que si $d_{n,k}$ son los elementos de la matriz de Riordan $D = (d(z), h(z))$, entonces:

$$\sum_{0 \leq k \leq n} d_{n,k} f_k = [z^n]\, d(z) F(zh(z))$$

c) Para $d(z) = (1-z)^{-1}$ y $h(z) = 1$ es $d_{n,k} = 1$. ¿Que concluye del resultado de la parte (b)?

Borrador

11. Funciones generatrices

1. Tiene 17 dulces a repartir entre 10 niños, de manera que a cada cual le toque al menos un dulce y a lo más dos. Calcule el número de distribuciones mediante funciones generatrices.

2. La florería de Dunwich vende ramilletes de flores, que incluyen a lo más tres lirios, un número impar de tulipanes y cualquier número de rosas. ¿Cuántos ramilletes diferentes de n flores ofrece?

3. Dado un alfabeto de s símbolos, calcule el número de palabras de n símbolos de largo que contienen todos los símbolos mediante

   a) Funciones generatrices, directamente

   b) Usando el principio de inclusión y exclusión

   En ambos casos aplique la técnica en forma ordenada, sin omitir pasos.

4. *a*) Demuestre que:

$$\left(\sum_{n\geq 0} a_n \frac{z^n}{n!}\right) \cdot \left(\sum_{n\geq 0} b_n \frac{z^n}{n!}\right) = \sum_{n\geq 0} \left(\sum_{0\leq k\leq n} \binom{n}{k} a_k b_{n-k}\right) \frac{z^n}{n!}$$

   b) Partiendo de:

$$\mathrm{e}^z = \sum_{n\geq 0} \frac{z^n}{n!}$$
$$\mathrm{e}^{(a+b)z} = \mathrm{e}^{az} \cdot \mathrm{e}^{bz}$$

   y usando 4*a* para expresar el lado derecho, deduzca el teorema del binomio.

5. Suponga secuencias $\langle a_n \rangle_{n\geq 0}$ y $\langle b_n \rangle_{n\geq 0}$ relacionadas por:

$$b_n = \sum_{0\leq k\leq n} \binom{n}{k} a_k$$

   Demuestre la *inversión binomial*:

$$a_n = \sum_{0\leq k\leq n} (-1)^{n-k} \binom{n}{k} b_k$$

   Pista: Use funciones generatrices exponenciales.

6. Para $\alpha > 0$ se definen los números de α-Fibonacci mediante la recurrencia:

$$F_{n+2}^{(\alpha)} = \alpha F_{n+1}^{(\alpha)} + F_n^{(\alpha)} \qquad F_0^{(\alpha)} = 0, F_1^{(\alpha)} = 1$$

   Encuentre su función generatriz ordinaria:

$$F^{(\alpha)}(z) = \sum_{n\geq 0} F_n^{(\alpha)} z^n$$

7. Encuentre la función generatriz de la secuencia $\langle H_n \rangle_{n\geq 0}$ de números harmónicos, definidos por:

$$H_n = \sum_{1\leq k\leq n} \frac{1}{n}$$

   Pista: Esta suma es una convolución

8. Encuentre la función generatriz exponencial de $u^{\underline{n}}$ para u dado.

Borrador

9. Halle la función generatriz exponencial de la secuencia $\langle u_n \rangle_{n \geq 0}$ y de ella obtenga una expresión cerrada para u_n si:

$$u_n = nu_{n-1} + 1 \qquad u_0 = 1$$

10. Según la *distribución exponencial* con parámetro a la probabilidad de $k \geq 0$ es proporcional a a^k.

    a) Encuentre el promedio de k en función de a.

    b) Para que p_k sea una distribución de probabilidad, debe cumplirse que:

    $$\sum_{k \geq 0} p_k = 1$$

    Encuentre p_k para esta distribución en términos de a.

11. Según la *distribución binomial negativa* con parámetros r y p la probabilidad con la que aparece el valor k es:

    $$f(k; r, p) = \binom{k + r - 1}{k} \cdot p^r \cdot (1 - p)^k$$

    Encuentre el promedio de k en función de r y p.

12. Obtenga la función generatriz para los números de Fibonacci en posiciones pares, o sea, la secuencia $\langle F_{2n} \rangle_{n \geq 0}$. **Pista:** Si $G(z)$ es la función generatriz de $\langle g_k \rangle_{k \geq 0}$, ¿a qué secuencia corresponde $(G(z) + G(-z))/2$?

13. Encuentre funciones generatrices ordinarias para las siguientes secuencias:

    a) $\langle \cos k\pi \rangle_{k \geq 0}$

    b) $\langle k^2 \rangle_{k \geq 0}$

    c) $\langle k(k-1) \rangle_{k \geq 0}$

    d) $\langle (-1)^k \rangle_{k \geq 0}$

    e) $\langle \alpha^k \rangle_{k \geq 0}$

14. Encuentre funciones generatrices exponenciales para las siguientes secuencias:

    a) $\langle k^2 \rangle_{k \geq 0}$

    b) $\langle k(k-1) \rangle_{k \geq 0}$

    c) $\langle (-1)^k \rangle_{k \geq 0}$

    d) $\langle \alpha^k \rangle_{k \geq 0}$

15. Encuentre las funciones generatrices ordinaria y exponencial de las secuencias:

    a) $\langle 1/n^2 \rangle_{n \geq 0}$

    b) $\langle \alpha^n \rangle_{n \geq 1}$

    c) $\langle 1, 0, -1, 0, 1, 0, -1, \ldots \rangle_{n \geq 0}$

    d) $\langle 1, 0, 2, 0, 4, 0, 8, 0, \ldots \rangle_{n \geq 0}$

16. Si la serie $A(x) \overset{\text{ogf}}{\longleftrightarrow} \langle a_k \rangle_{k \geq 0}$ converge, explique a qué corresponden:

    a) $A(x) + A(-x)$

    b) $A(x) - A(-x)$

    c) $A(x) + A(\omega x) + A(\omega^2 x)$, donde $\omega^2 + \omega + 1 = 0$ es una raíz cúbica primitiva de 1, o sea:

    $$\omega = e^{\frac{2\pi i}{3}}$$

Borrador

d) Más en general, si ω es una raíz primitiva r-ésima de 1, por ejemplo:

$$\omega = e^{\frac{2\pi i}{r}}$$

demuestre que:

$$\frac{1}{r}\sum_{0\leq k\leq r-1}\omega^{kn} = \begin{cases} 1 & \text{si } r \mid k \\ 0 & \text{caso contrario} \end{cases}$$

17. Considere la definición de *función generatriz de Poisson*:

$$A(x) \overset{\text{Pgs}}{\longleftrightarrow} \langle a_n \rangle_{n\geq 0}$$
$$A(x) = \sum_{n\geq 0} a_n e^{-x}\frac{x^n}{n!}$$

Si $A(x) \overset{\text{Pgs}}{\longleftrightarrow} \langle a_n \rangle_{n\geq 0}$ y $B(x) \overset{\text{Pgs}}{\longleftrightarrow} \langle b_n \rangle_{n\geq 0}$, ¿A qué secuencia corresponde $A \cdot B$?

18. Considerando la identidad:

$$e^{(x+y)t} = e^{xt} \cdot e^{yt}$$

demuestre el teorema del binomio.

19. Demuestre que los números de Fibonacci cumplen:

$$F_0 + F_1 + \ldots + F_n = F_{n+2} - 1$$

20. Si $\langle F_n \rangle_{n\geq 0}$ son los números de Fibonacci, encuentre el valor de

$$\sum_{0\leq k\leq n} F_k F_{n-k}$$

21. Con la definición de la derivada de series formales de potencias, demuestre que si $A(x)$ y $B(x)$ son series formales:

a) $(\alpha A + \beta B)' = \alpha A' + \beta B'$
b) $(A \cdot B)' = A' \cdot B + A \cdot B'$
c) $(A^n)' = nA^{n-1}A'$, donde n es un número natural.

22. Considere los valores de la siguiente expresión:

$$\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5$$

donde $\alpha_i \in \{0, 1\}$.

a) Demuestre que al menos uno de los valores de esta expresión se puede obtener de 3 maneras diferentes.
b) Exprese el número de maneras que se puede obtener el valor v de la expresión como el coeficiente de un término de un polinomio.

23. Sea $p_r(n)$ el número de particiones de n con la restricción que 1 puede aparecer a lo más 1 vez, 2 puede aparecer a lo más 2 veces, ..., k puede aparecer a lo más k veces. Encuentre la función generatriz

$$P_r(x) = \sum_{n\geq 0} p_r(n)x^n$$

Borrador

24. Evalúe la siguiente suma:

$$\sum_{0\le k\le n} \begin{bmatrix} n \\ k \end{bmatrix}$$

Posible pista: La función generatriz mixta de los números de Stirling de primera especie es:

$$H(z,u) = \sum_{\substack{n\ge 0\\ k\ge 0}} \begin{bmatrix} n \\ k \end{bmatrix} \frac{z^n}{n!} u^k = (1-z)^{-u}$$

25. Al discutir números de Stirling de primera especie vimos que:

$$H(z,u) = \sum_{\substack{n\ge 0\\ k\ge 0}} \begin{Bmatrix} n \\ k \end{Bmatrix} u^k \frac{z^n}{n!} = \sum_{n\ge 0} (-u)^{\underline{n}} \frac{(-z)^n}{n!} = (1-z)^{-u}$$

Demuestre la identidad

$$H(-z,-u)\cdot H(-z,-v) = H(-z,-(u+v))$$

y úsela para expresar $(u+v)^{\underline{n}}$ en términos de $u^{\underline{i}}$ y $v^{\underline{j}}$.

26. ¿Cuál es el número de soluciones enteras de $x_1 + x_2 + \ldots x_n = k$, con las condiciones $\alpha \le x_i \le \beta$?

27. Encuentre el número de subconjuntos de k elementos de n tal que no contengan elementos adyacentes.

28. Obtenga las siguientes funciones generatrices, usando resultados ya demostrados en clase:

    a) Encontrar una fórmula para la función generatriz ordinaria de la secuencia $F_1, 2F_2, 3F_3, 4F_4, \ldots$ (los F_n son los números de Fibonacci)

    b) Encontrar una fórmula para la secuencia de las sumas de los primeros n números de Fibonacci, o sea $F_0, F_0+F_1, F_0+F_1+F_2, \ldots$

29. ¿De cuántas formas se pueden elegir 10 globos si se tienen que elegir:

    a) 1, 3 ó 5 amarillos

    b) 2, 3 ó 4 rojos

    c) 1, 4 ó 5 blancos

30. Se pide diseñar un certamen con 4 preguntas, las cuales deben tener puntajes múltiplos de 5 entre 15 y 35. ¿Cuántas formas hay de crear este certamen?

31. Hallar el número de sucesiones de longitud 8 que pueden formarse usando: 1, 2 ó 3 `A`, 2, 3 ó 4 `B` y 0, 2 ó 4 `C`. importando el orden de los símbolos.

32. Dada la función generatriz ordinaria de la secuencia de los a_n, determine sus valores:

$$A(x) = \frac{1}{(1-2x)^3} - \frac{5}{1+3x} + \frac{e^{-x}}{1-x}$$

33. Considere nuevamente la palabra `BOOKKEEPER`, tan manoseada en Funda I. Use funciones generatrices para determinar:

    a) El número de conjuntos de 5 letras que pueden formarse con sus letras.

    b) El número de palabras de 5 letras que pueden formarse con sus letras.

    Explique porqué estos dos resultados son diferentes.

Borrador

34. Indique el número de soluciones enteras de la ecuación:

$$x_1 + x_2 + x_3 = 11$$

si $0 \leq x_1 \leq 3$, $0 \leq x_2 \leq 4$ y $0 \leq x_3 \leq 6$.

35. Calcule los primeros cuatro términos no nulos de la sucesión cuya función generatriz es

$$\frac{6 + 5x + x^2}{3 - 4x^2 + x^4}$$

36. Se buscan las formas de obtener un canasto de n frutas si:

- El número de manzanas tiene que ser par.
- El número de plátanos debe ser un múltiplo de 5.
- Hay a lo más 4 naranjas.
- Hay a lo más 1 pera.

37. Dada la función generatriz exponencial de los números de Bell:

$$\widehat{B}(z) = \sum_{n \geq 0} B_n \frac{z^n}{n!} = e^{e^z - 1}$$

a) Exprese su derivada en términos de $\widehat{B}(z)$, hallando una ecuación diferencial para $\widehat{B}(z)$

b) Obtenga una recurrencia para B_n interpretando la ecuación diferencial como operaciones con secuencias

38. Evaluar la suma:

$$\sum_{0 \leq k \leq n} (-1)^k \binom{2n - k}{k} 2^{2n-2k}$$

39. Evaluar:

$$\sum_{x+y+z=2014} xy^2z^3$$

40. Hallar el número de soluciones en $\mathbb{N}_0$ para:

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 29$$

tal que hayan exactamente tres de los x_i con valor impar.

41. Demostrar la identidad:

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

42. ¿Cuántas soluciones enteras hay para $x_1 + x_2 + x_3 = n$ si $0 \leq x_i \leq 2$ para $1 \leq i \leq 3$?

Borrador

12. Aceite de serpiente

1. Evalúe:

$$s(n) = \sum_{0 \leq k \leq n} \binom{n}{2k} \binom{2k}{k} 4^{-k}$$

2. Evaluar la suma:

$$\sum_{0 \leq k \leq n} (-1)^k \binom{2n-k}{k} 2^{2n-2k}$$

3. Hallar la suma:

$$\sum_{0 \leq k \leq n} \begin{bmatrix} n \\ k \end{bmatrix} \binom{k}{m}$$

4. Evaluar la suma:

$$\sum_{k} \binom{k}{n-k}$$

5. Evaluar:

$$\sum_{m \leq k \leq n} (-1)^k \binom{n}{k} \binom{k}{m}$$

6. Evaluar:

$$\sum_{m \leq k \leq n} \binom{n}{k} \binom{k}{m}$$

7. Evaluar:

$$\sum_{k} \binom{n}{\lfloor \frac{k}{2} \rfloor} x^k$$

8. Para $m, n \geq 0$ Evaluar la suma:

$$\sum_{k} \binom{n+k}{m+2k} \binom{2k}{k} \frac{(-1)^k}{k+1}$$

9. Demuestre la identidad:

$$\sum_{k} \binom{2n}{2k} \binom{2k}{k} 2^{2n-2k} = \binom{4n}{2n}$$

10. Dados n y p, evalúe (Moriati):

$$\sum_{k} \binom{2n+1}{2p+2k+1} \binom{p+k}{k}$$

11. Usando el método de aceite de serpiente evalúe la suma:

$$S_m = \sum_{m \leq k \leq n} (-1)^k \binom{n}{k} \binom{k}{m}$$

Borrador

13. Recurrencias

1. Plantee una recurrencia para:

$$S_n = \sum_{1 \le k \le n} k^2$$

y resuélvala para obtener la suma de los primeros cuadrados.

2. Resuelva la recurrencia:

$$a_n = 1 + \frac{1}{2} \sum_{0 \le j < n} a_j$$

3. Halle la secuencia definida por:

$$a_n = 6a_{n-1} - 9a_{n-2} \qquad a_0 = 1, a_1 = 9$$

4. Se piden las formas de colorear un rectángulo de $1 \times n$ con rojo, naranja, azul y verde de forma que un número par de bloques se coloreen de rojo y un número impar de naranja.

5. Los *números de Lucas* se definen mediante la recurrencia:

$$L_n = L_{n-1} + L_{n-2} \qquad L_0 = 2, L_1 = 1$$

   a) Encuentre una expresión para L_n

   b) Evalúe las sumas:

$$\sum_{1 \le k \le n} L_k$$

6. Resuelva:

$$a_{n+1} = \frac{2(n+1)a_n + 5(n+1)!}{3} \quad a_0 = 5$$

7. ¿De cuántas maneras pueden agruparse n elementos en grupos de 1 y 2?

8. Resuelva las recurrencias:

$$\begin{aligned} x_{n+1} &= 5x_n + 3 \cdot 5^n - 2 \cdot 5^{-n} + 4 \cdot (-5)^n && x_0 = 3 \\ x_{n+4} + 5x_{n+3} + 7x_{n+2} + 5x_{n+1} + x_n &= 0 && x_0 = x_1 = x_2 = x_3 = 1 \\ x_{n+2} - 10x_{n+1} + 25x_n &= 3 \cdot 5^n - 3 \cdot 5^{-n} && x_0 = 0,\ x_1 = 1 \end{aligned}$$

9. Halle una ecuación para la función generatriz ordinaria $A(z)$ de la secuencia $\langle a_n \rangle_{n \ge 0}$ definida por la recurrencia:

$$a_{n+3} - 2a_{n+1} + a_n = n3^n - 5^{-n} + 1 \qquad a_0 = 1,\ a_1 = 2,\ a_2 = 4$$

10. Los métodos de ordenamiento *inserción* y *burbuja* son ampliamente conocidos. Para el peor caso de ambos (arreglo de entrada ordenado de mayor a menor), calcule cuando se ordenan N elementos:

    a) El número de comparaciones entre elementos

    b) El número de copias (asignaciones) de elementos

    Comente sus resultados.

    (Es posible efectuar un análisis del promedio de estas cantidades, pero eso requiere de propiedades de las permutaciones que no hemos estudiado.)

Borrador

11. Si la secuencia de Fibonacci definida mediante la recurrencia:

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

se calcula mediante el algoritmo recursivo obvio, ¿cuántas llamadas de función se hacen al evaluar F_n?

12. Los coeficientes binomiales cumplen la recurrencia:

$$\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k} \qquad \binom{n}{0} = \binom{n}{n} = 1$$

¿Cuántas llamadas a función involucra `binomial(2n, n)`, si `binomial(n, k)` es la implementación según la recurrencia dada? (Esto da una idea del trabajo a efectuar en el caso general).

13. Determine el máximo número de regiones en el plano que pueden obtener usando N rectas. ¿Cuántas de estas regiones son finitas, y cuántas infinitas?

14. ¿Cuántos volúmenes se pueden obtener con N planos en el espacio?

15. En los números de Fibonacci de la pregunta 11 los últimos dígitos en base 10 se repiten con período 60 (Lagrange descubrió esto). Explique porqué toda secuencia de este tipo tendrá últimos dígitos periódicos, e indique alguna relación entre el largo máximo del período y las características de la recurrencia que define la secuencia.

16. Siendo F_n los números de Fibonacci de la pregunta 11, defina:

$$\begin{aligned} S_n &= F_1F_n + F_2F_{n-1} + \ldots + F_{n-1}F_2 + F_nF_1 \\ &= \sum_{1\le k\le n} F_kF_{n+1-k} \\ S_1 &= F_1F_1 = 1 \\ S_2 &= F_2F_1 + F_1F_2 = 2 \end{aligned}$$

Demuestre que para $n \ge 3$, $S_n = S_{n-1} + S_{n-2} + F_n$

17. Encuentre:

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n}$$

18. Encuentre el límite para las soluciones a las recurrencias de la pregunta 8:

$$\lim_{n\to\infty} \frac{x_{n+1}}{x_n}$$

¿Cuándo importan las condiciones iniciales en el caso de una recurrencia lineal de coeficientes constantes en la respuesta a una pregunta como esta?

19. Encuentre la solución de la recurrencia:

$$a_{n+2} - 3a_{n+1} + 2a_n = 4^n - 2^n \qquad a_0 = a_1 = 1$$

No es necesario que efectúe toda el álgebra, pero debe explicar *claramente* y *en detalle* cómo se obtienen los coeficientes de la solución.

20. Los generadores de números aleatorios mediante el método congruencial hacen:

$$x_{n+1} = (ax_n + c) \text{ mód } m$$

para constantes a, c y m adecuadas, y partiendo de x_0 "al azar" (por ejemplo, el instante actual en milisegundos). Encuentre la solución a esta recurrencia si m es primo.

Borrador

21. Usando funciones generatrices, resuelva la recurrencia:

$$x_{n+2} = 4x_n + 3 \cdot 2^n - 2 \cdot 5^{-n} + 4 \cdot (-2)^n \qquad x_0 = 3$$

22. Encuentre la función generatriz para la secuencia definida por la recurrencia:

$$a_{n+2} + a_n = 0 \qquad a_0 = 0,\ a_1 = 1$$

23. Encuentre la función generatriz para la secuencia definida por la recurrencia:

$$b_n = 2^n + \sum_{0 \le k \le n-1} (n - k - 1) b_k \qquad b_0 = 1$$

24. Encuentre la función generatriz para la secuencia definida por la recurrencia:

$$nc_{n+1} - c_n = n(n-1) \qquad c_0 = 2$$

25. Considere los subconjuntos de $\{1, 2, \ldots, n\}$. ¿Cuántas veces aparece en promedio un par de vecinos, vale decir, i e $i+1$, en estos conjuntos?

26. Resuelva la recurrencia:

$$d_{n+1} = n(d_n + d_{n-1}) \qquad d_0 = 1,\ d_1 = 0$$

usando funciones generatrices exponenciales.

27. Resuelva la recurrencia del problema 26 mediante funciones generatrices ordinarias.

28. Encuentre una función generatriz para la secuencia que resuelve la recurrencia:

$$a_{n+3} + a_n = 2 \cdot 5^n \qquad a_0 = 1,\ a_1 = 2,\ a_2 = 3$$

29. Encuentre una función generatriz para la secuencia que resuelve la recurrencia:

$$b_n = n + \sum_{0 \le k \le n-1} b_k \qquad b_0 = 0$$

30. Sea a_n el número de árboles con raíz que tienen n arcos, y $A(z) = \sum_{n \ge 0} a_n z^n$ la función generatriz respectiva. Entonces $(zA(z))^k$ es la función generatriz para tales árboles con k hijos de la raíz, y:

$$A(z) = \sum_{k \ge 0} (zA(z))^k$$

Encuentre a_n.

31. Considere la definición de *potencias crecientes*:

$$x^{\overline{n}} = x \cdot (x+1) \cdot \ldots \cdot (x+n-1)$$

o, formalmente:

$$x^{\overline{0}} = 1$$
$$x^{\overline{n+1}} = x^{\overline{n}} \cdot (x+n)$$

Expresse estos en la forma:

$$x^{\overline{n}} = \sum_{0 \le k} \begin{bmatrix} n \\ k \end{bmatrix} x^k$$

y encuentre una recurrencia para los coeficientes (números de Stirling de primera especie).

Borrador

32. Resuelva la recurrencia:

$$a_{n+2} = 2a_{n+1} - a_n + n2^n \qquad a_0 = 0,\ a_1 = 1$$

33. Halle una ecuación para una función generatriz para la secuencia definida por:

$$b_n = \sum_{0 \le k \le n-1} \binom{n-1}{k} b_k \qquad b_0 = 1$$

34. Halle una ecuación para una función generatriz para la secuencia definida por:

$$nc_n = \sum_{0 \le k \le n-1} c_{n-1-k} c_k \qquad c_0 = 2$$

35. Si se tiene la secuencia $\langle a_n \rangle_{n \ge 0}$, se define la *suavización exponencial* de esa secuencia con parámetro α, donde $0 \le \alpha \le 1$, mediante la recurrencia para $n \ge 0$:

$$s_n = \alpha a_n + (1 - \alpha) s_{n-1} \qquad s_0 = a_0$$

Suponiendo dada la función generatriz ordinaria es $A(x)$ de $\langle a_n \rangle_{n \ge 0}$, encuentre la función generatriz ordinaria $S(x)$ de la secuencia $\langle s_n \rangle_{n \ge 0}$.

36. Explique cómo resolvería las siguientes recurrencias, en las cuales a_n es desconocida y u_n se conoce:

a) $a_{n+2} + a_{n+1} - 3a_n = u_n \qquad a_0 = a_1 = 2$

b) $a_{n+1} = \sum_{0 \le i \le n} a_i u_{n-i} \qquad a_0 = 1$

37. Resuelva las siguientes recurrencias:

a) $a_{k+1} = 3a_k + 2 \quad k \ge 0,\ a_0 = 0$

b) $b_{k+2} = 2b_{k+1} - b_k \quad k \ge 0,\ b_0 = 0,\ b_1 = 1$

c) $c_{k+1} = c_k + \alpha^k \quad k \ge 0,\ c_0 = \beta$

38. Resuelva las siguientes recurrencias usando funciones generatrices exponenciales:

a) $a_{k+1} = 3a_k + 2 \quad k \ge 0,\ a_0 = 0$

b) $b_{k+2} = 2b_{k+1} - b_k \quad k \ge 0,\ b_0 = 0,\ b_1 = 1$

c) $c_{k+1} = c_k + \alpha^k \quad k \ge 0,\ c_0 = \beta$

39. Considere la recurrencia ($n \ge 1$):

$$\begin{aligned} f(1) &= 1 \\ f(2) &= 2 \\ f(3n) &= 3f(n) \\ f(3n+1) &= 2f(n) + f(n+1) \\ f(3n+2) &= f(n) + 2f(n+1) \end{aligned}$$

a) Defina la función generatriz

$$F(z) = \sum_{n \ge 1} f(n) z^{n-1}$$

y encuentre una ecuación que relacione $F(z)$ con $F(z^3)$ multiplicando las ecuaciones de la recurrencia por z^{3n-1}, z^{3n} y z^{3n+1}, respectivamente, y sumando.

b) De la relación anterior puede obtener una ecuación "límite" para $F(z)$ en forma de un producto infinito.

Borrador

c) Por el otro lado, la recurrencia tiene la obvia solución $f(n) = n$. ¿Qué puede concluir? ¿Puede demostrar esto de una forma alternativa?

40. Encuentre una fórmula explícita para los *números de Lucas*, definidos mediante $L_0 = 2$, $L_1 = 1$, y para $n \geq 0$:

$$L_{n+2} = L_{n+1} + L_n$$

41. ¿Cuántas palabras de largo n formadas únicamente por las 5 vocales pueden formarse, si deben contener un número par de vocales fuertes ('a', 'e' y 'o')?

42. El profesor Upham de la Universidad de Miskatonic anda de viaje, y dejó a su ayudante (que es medio lerdo) a cargo de su curso de Recurrenciología. El ayudante entendió mal la materia que le encargó el profesor ver en clase, e insiste en resolver la "recurrencia de BonJovi" la cual comienza $b_0 = 0, b_1 = 1$, y cada elemento sucesivo es la suma de *todos* los elementos anteriores. En su desesperación lo contacta a Ud. como experto de la UTFSM para que le resuelva la recurrencia.

43. En el sánscrito hay dos tipos de sílabas: Sílabas largas (L) y cortas (S). El largo de una sílaba larga es exactamente el doble del largo de una corta. ¿Cuántas palabras de largo n (una sílaba corta cuenta por 1, una larga por 2) pueden crearse, si sólo se consideran los largos de las sílabas?

44. Resuelva las siguientes recurrencias, en las cuales siempre $n \geq 0$:

a) $u_{n+1} - 2u_n = 4^n \qquad u_0 = 1$

b) $u_{n+2} - 3u_{n+1} - 4u_n = 0 \qquad u_0 = 1, u_1 = 3$

c) $u_{n+3} - 6u_{n+2} + 11u_{n+1} - 6u_n = 0 \qquad u_0 = 2, u_1 = 0, u_2 = -2$

d) $u_{n+1} - 2u_n = \alpha^n \qquad \alpha \neq 2, u_0 = 1$

e) Resuelva la recurrencia del ejercicio 44*d* cuando $\alpha = 2$.

45. Considere la secuencia $\langle z_n \rangle_{n \geq 0}$, donde $b \neq 1$:

$$z_{n+1} = \frac{z_n - a}{z_n - b} \qquad z_0 = 1$$

a) Si $\langle u_n \rangle_{n \geq 0}$ se define por:

$$\frac{u_{n+1}}{u_n} = z_n - b$$

Encuentre una recurrencia para los u_n

b) Resuelva la recurrencia anterior

c) Encuentre una expresión para los z_n

46. La secuencia $\langle a_n \rangle_{n \geq 0}$ cumple la recurrencia:

$$a_n = \frac{1}{2} \sum_{0 \leq k \leq n-1} \binom{n-1}{k} a_k a_{n-k-1}$$

Además $a_0 = a_1 = 1$. Muestre cómo atacaría este problema, llegando hasta una ecuación para una función generatriz.

47. Los *números de Euler* pueden definirse mediante la recurrencia:

$$E_n + \sum_{0 \leq k \leq n-1} \binom{n}{k} 2^{n-1-k} E_k = 1$$

Encuentre una función generatriz para ellos.

48. Un rectángulo de $2 \times n$ se llena con piezas de dominó (rectángulos de 2×1). ¿De cuántas maneras diferentes puede hacerse esto?

Borrador

49. Encuentre una ecuación para una función generatriz de la secuencia $\langle u_n \rangle_{n\geq 0}$, que satisface la recurrencia:

$$3u_{n+2} - u_n = 6n^2 \qquad u_0 = 1,\ u_1 = 2$$

Explique cómo puede obtener la secuencia explícitamente partiendo del resultado anterior.

50. *a)* $a_n = 5a_{n-1} - 6a_{n-2} \quad a_0 = 0,\ a_1 = 1$
b) $b_{n+1} = b_n + 6b_{n-1} \quad b_0 = b_1 = 1$
c) $c_n = c_{n-1} + n \quad c_0 = 0$

51. En el conocido juego de Torres de Hanoi de debe mover una torre de n discos de la pila 1 a la pila 3, usando como intermedio una pila 2 inicialmente vacía. Los discos deben estar siempre en orden de tamaño decreciente en las pilas. Interesa saber cuántas movidas se requieren para llevar a cabo esta tarea.

52. Dé una ecuación para la función generatriz ordinaria $U(x)$ de la secuencia definida mediante:

$$u_n = 5u_{n-1} - 6u_{n-2} \quad \text{para } n \geq 2 \qquad u_0 = 1,\ u_1 = 3$$

53. Determine el valor de la suma siguiente, donde F_n son los números de Fibonacci:

$$S_n = \sum_{0\leq k\leq n} \binom{n}{k} F_k$$

54. Derive una ecuación para la función generatriz del número de secuencias de n enteros entre 0 y k que no tienen dos 0 seguidos.

55. Resuelva las siguientes:

a) Dé una ecuación para la función generatriz ordinaria de la secuencia $\langle a_n \rangle_{n\geq 0}$ definida por la recurrencia:

$$a_n = a_{n-1} + 2a_{n-2} + 2n - 4 + (-1)^n \qquad a_0 = 3,\ a_1 = 8$$

b) La secuencia $\langle a_n \rangle_{n\geq 0}$ tiene función generatriz ordinaria:

$$A(z) = \frac{1}{2} \cdot \frac{1}{1+z} + \frac{29}{2} \cdot \frac{1}{1-z} - \frac{6}{(1-z)^2} + \frac{2}{(1-z)^3}$$

Dé una fórmula explícita para a_n.

56. En un *árbol binario balanceado* las alturas de los subárboles derecho e izquierdo difieren a lo más en 1. Derive una recurrencia para el número mínimo de nodos t_n en un árbol balanceado de altura n.

57. Encuentre una recurrencia para el número s_n de subconjuntos de $\{1, \ldots, n\}$ en que no hay dos elementos contiguos. Los primeros valores son $s_0 = 1$ (cumple el conjunto vacío únicamente), $s_1 = 2$ (cumplen el conjunto vacío y ese elemento solo), $s_2 = 3$ (cumplen el conjunto vacío y cada elemento por sí solo), ... Resuelva esta recurrencia.
Pista: Considere los subconjuntos que contienen a n y los que no lo contienen.

58. Considere las palabras formados por $\{a, b, c\}$ de largo n. Encuentre recurrencias para el número de palabras de largo n que tienen un número par de a, u_n, y el número de palabras que tienen un número impar de a, v_n.

59. Para palabras como en el problema 58, encuentre una expresión para el número de palabras que tienen dos a en posiciones pares.

60. Sean las secuencias U_n y V_n definidas por las recurrencias:

$$U_n = 2V_{n-1} + U_{n-2} \qquad U_0 = 1,\ U_1 = 0$$
$$V_n = U_{n-1} + V_{n-2} \qquad V_0 = 0,\ V_1 = 1$$

Usando la técnica vista en clases esto lleva a un sistema de ecuaciones para las funciones generatrices $u(z)$ y $v(z)$, y de allí a las funciones generatrices. Obtenga fórmulas explícitas para los elementos de las secuencias.

Borrador

61. Encuentre una ecuación para la función generatriz de la secuencia definida por

$$u_{n+1} = \sum_{0 \le k \le n} a^{n-k} u_k \qquad u_0 = 1$$

62. Encuentre una ecuación para la función generatriz de la secuencia definida por

$$v_{n+2} = 3v_{n+1} - 2v_n + 5 \cdot 7^n \qquad v_0 = 1,\ v_1 = 2$$

63. Resuelva la recurrencia:

$$u_{n+1} = a \sum_{0 \le k \le n} u_k \qquad u_0 = 1$$

64. Considere la recurrencia:

$$(n^2 + 2)v_{n+2} - 5v_n = 2^n - 5n^3 \qquad v_0 = 1, v_1 = 3$$

Encuentre una ecuación para la función generatriz:

$$V(z) = \sum_{n \ge 0} v_n z^n$$

65. Resuelva las siguientes:

a) Dé una ecuación para la función generatriz ordinaria de la secuencia $\langle a_n \rangle_{n \ge 0}$ definida por la recurrencia:

$$a_{n+2} - a_n = 6n \qquad a_0 = 3, a_1 = 8$$

b) La secuencia $\langle a_n \rangle_{n \ge 0}$ tiene función generatriz ordinaria:

$$A(z) = \frac{37}{4(1-z)} - \frac{7}{4(1+z)} - \frac{15}{2(1-z)^2} + \frac{3}{(1-z)^3}$$

Dé una fórmula explícita para a_n.

66. Un modelo crudo del algoritmo de factorización ρ de Pollard es considerar que se distribuyen los $n+1$ valores 0 a n en ciclos de árboles binarios con al menos un nodo. Describa esta estructura simbólicamente mediante un sistema de ecuaciones, y encuentre un sistema de ecuaciones para las funciones generatrices del caso.

67. Resuelva la recurrencia:

$$c_{n+1,k+1} = c_{n+1,k} + c_{n,k+1} \qquad c_{i,0} = c_{0,i} = 1 \quad \text{para todo } i \ge 0$$

68. Halle una ecuación para la función generatriz ordinaria $A(z)$ de la secuencia $\langle a_n \rangle_{n \ge 0}$ definida por la recurrencia:

$$a_{n+3} - 2a_{n+1} + a_n = n3^n - 5^{-n} + 1 \qquad a_0 = 1,\ a_1 = 2,\ a_2 = 4$$

69. Sea $\mathcal{B}_n$ el conjunto de palabras de largo n que pueden formarse con las letras a, b y c, de forma que nunca hayan tres letras consecutivas diferentes (o sea, de cada tres letras al menos dos son iguales). Halle una recurrencia para $|\mathcal{B}_n|$.

70. Resuelva:

$$(n+1)y_n = 2ny_{n-1} + n$$

con la condición inicial $y_0 = 4$.

Borrador

71. Resuelva:

$$a_n = \binom{n}{2} + 3a_{n-1}$$

si $a_0 = 1$.

72. Resuelva la recurrencia:

$$a_{n+2} = 9a_{n+1} - 18a_n$$

donde $a_0 = 1$, $a_1 = 3$.

73. Resolver la recurrencia:

$$n^2 a_n - 5(n-1)^2 a_n + 2 = 0$$

donde $a_0 = 0$.

74. Resolver la recurrencia:

$$x_{n+2} + x_{n+1} + x_n = 0$$

con $x_0 = x_1 = 1$.

75. Resolver la recurrencia:

$$g_n = 12g_{n-2} - 16g_{n-3} + 6 \cdot 2^n + 25n$$

con $g_0 = 23$, $g_1 = 37$, $g_2 = 42$.

76. Resolver la recurrencia:

$$f(1) = 1$$
$$f(2) = 2$$
$$f(n) = 5f(n/2) - 4f(n/4)$$

77. Hallar el límite:

$$\lim_{n\to\infty} a_n$$

si $a_0 = 1$, $a_1 = m$ y

$$a_{n+2} = \frac{2a_{n+1}a_n}{a_{n+1} + a_n}$$

78. Considere la secuencia definida mediante $u_0 = 2$ y:

$$u_{n+1} = s_n^2 - s_n$$
$$s_n = \sum_{0 \le k \le n} u_k$$

Encuentre una cota superior para u_n.

79. Una máquina vendedora de estampillas acepta monedas de un dólar, billetes de un dólar y billetes de cinco dólares. Plantee una recurrencia para el número de maneras de ingresar n dólares, si el orden en que se ingresa el dinero importa.

80. Resolver la recurrencia:

$$A(h, 0) = 1$$
$$A(h, h) = c^h$$
$$A(h, r) = A(h-1, r) + (c-1)A(h, r-1)$$

Borrador

81. Hallar la función generatriz de los términos de la secuencia definida por:

$$aa_n = 2(a_{n-1} + a_{n-2}) \qquad a_0 = 1, a_1 = 2$$

82. Determine el número de secuencias de $\{0, 1, 2\}$ tales que nunca queda un símbolo solo.

83. Calcular el número de secuencias de largo n de $\{0, 1, 2, 3\}$ que tengan un número par de 0 y de 1.

84. Resolver la recurrencia:

$$t(n) = t\left(\frac{n}{4}\right) + \sqrt{n} + n^2 + n^2 \log_8 n$$

85. Halle el número de secuencias de $\{0, 1\}$ de largo n que tienen dos unos consecutivos.

86. Hallar el número de secuencias de $\{0, 1, 2\}$ de largo n que no contienen 00 ni 01 y que no terminen en 0.

87. Determine el número de secuencias binarias de largo n que comienzan en 1 que representan números divisibles por tres.

Borrador

14. Aplicaciones a probabilidades

1. Una *distribución discreta de probabilidad* $\mathscr{P} = \langle p_n \rangle_{n\geq 0}$ cumple $0 \leq p_n \leq 1$ y $\sum_n p_n = 1$. Su *función generatriz de probabilidad* es

$$P(z) = \sum_{n\geq 0} p_n z^n$$

El *valor esperado* de una función $g(n)$ para la distribución $\langle p_n \rangle_{n\geq 0}$ se define como

$$E(g) = \sum_{n\geq 0} p_n g(n)$$

a) Si $g(n)$ es un polinomio, explique cómo calcular $E(g)$ a partir de $P(z)$.

La distribución de Poisson con parámetro λ da el número de eventos en un intervalo de tamaño t como

$$p_n = \frac{(\lambda t)^n}{n!} e^{-\lambda t}$$

b) Demuestre que esta es una distribución de probabilidad discreta.

c) Encuentre la *media* $\mu = E(n)$ y *varianza* $\sigma^2 = E((n-\mu)^2)$ para el número de eventos en un intervalo t si la distribución es Poisson con parámetro λ.

Borrador

15. Aplicaciones combinatorias

1. Hermenegildo es aficionado a las carreras de caballos, pero tiene mala suerte. Apuesta al orden en que llegarán a la meta los 10 caballos de una carrera, y ninguno llega en la posición que predice Hermenegildo. ¿Cuántos órdenes de llegada dan este triste resultado? ¿Qué tan mala es la suerte de Hermenegildo (vale decir, qué tan probable es este resultado, suponiendo que todos los órdenes de llegada son igualmente probables)?

2. Evalúe la siguiente suma:

$$\sum_{0 \leq k \leq n} \begin{bmatrix} n \\ k \end{bmatrix}$$

3. En el restaurante de Eddinton se sirve una ensalada de frutas legendaria. Desde su fundación la receta se mantiene igual. Se toman frutillas en medias docenas, un número impar de manzanas, entre dos y siete plátanos. Opcionalmente se agrega una naranja. Se pide calcular cuántos postres distintos se pueden hacer con un total de n frutas.

4. Se tienen 10 000 pelotas rojas idénticas, 10 000 pelotas amarillas idénticas y 10 000 pelotas verdes idénticas. ¿De cuántas maneras se pueden elegir 2 013 pelotas si el número de pelotas rojas es par o el de pelotas amarillas es impar?

5. ¿Cuántos números de 4 dígitos hay cuyos dígitos están en orden creciente?

6. ¿De cuántas maneras se pueden elegir tres números entre 1 y $2n$ de forma que estén en progresión aritmética?

Borrador

16. Método simbólico

1. Javiera tiene 8 especias diferentes en su cocina, las que guarda en un pequeño estante de tres repisas. ¿De cuántas formas diferentes puede disponer sus especias, si caben a lo más 5 especias en cada repisa, y Javiera considera que el estante se ve mal si hay repisas vacías? ¿Si el orden en cada repisa no importara, cuántas alternativas hay? Resuelva estos problemas mediante funciones generatrices.

2. ¿De cuántas maneras se pueden distribuir i manzanas y j naranjas entre n niños? Use funciones generatrices para este problema.

3. Los microorganimos del planeta Xyzzy tienen un genoma formado por un número de ciclos. Dos biólogos discuten acaloradamente si esto da más o menos posibilidades que un único cromosoma lineal. Determine quién tiene la razón.

4. La contabilidad inca se llevaba en *quipus*; cordeles con nudos (hay m tipos de nudos) en orden, se ata un número variable de cordeles a un cordel horizontal. Halle la función generatriz que cuenta el número de quipu de n nudos.

5. Derive una ecuación para la función generatriz del número de secuencias de enteros entre 0 y k de largo n que no tienen dos 0 seguidos.

6. Encuentre el número de secuencias binarias de largo n que:
   (a) No contienen 00 (b) No contienen 01

7. Un *árbol binario rotulado de tamaño* n es un árbol binario de n nodos, numerados de 1 a n. Considerándolo como un nodo raíz (rotulado con uno cualquiera de los n números) un subárbol izquierdo de k nodos y un subárbol derecho con los restantes $n-k-1$ rótulos encuentre el número b_n de árboles binarios rotulados de tamaño n.

8. Un *arbusto* es un único nodo, o un nodo conectado a más de un arbusto (el orden de subarbustos importa). Halle la función generatriz $A(z)$ del número a_n de arbustos de n nodos por el método simbólico. Obtenga una expresión para a_n en forma de una suma.

9. El código Morse representa caracteres mediante una secuencia de largo variable de puntos ($\cdot$) y rayas ($-$), separadas por espacios. Por ejemplo, la representación del famoso SOS es $\cdots \quad --- \quad \cdots$, mientras MORSE es $-- \quad --- \quad \cdot-\cdot \quad \cdots \quad \cdot$. El estándar dice que un punto dura una unidad de tiempo y una raya tres. Explique cómo calcularía la duración de la secuencia más larga requerida si se desean representar n símbolos distintos.

10. En el código Morse se transmiten símbolos como secuencias de puntos ($\cdot$) y rayas ($-$). El estándar dice que una raya dura exactamente 3 veces lo que dura un punto. Encuentre una función generatriz para el número m_k de secuencias de duración k.

11. Un *3-árbol* es vacío, o consta de un nodo raíz y cero o tres 3-árboles hijos en orden. Use el método simbólico para hallar una ecuación para la función generatriz del número de 3-árboles con n nodos.

12. Un *árbol 1-2* se define como un nodo (su raíz) y cero, uno o dos árboles 1-2 descendientes (sólo importa el orden). Encuentre la función generatriz del número de árboles 1-2 con n nodos.

13. Una *combinación* del natural n es representarlo como una suma de naturales. Por ejemplo, hay 8 combinaciones de 4:

    $$4 = 3+1 = 2+2 = 2+1+1 = 1+3 = 1+2+1 = 1+1+2 = 1+1+1+1$$

    Se anota $c(n)$ para el número de combinaciones de n.

    Es natural representar por ejemplo 4 como ||||. Use el método simbólico para obtener una expresión explícita para $c(n)$.

14. Pueden definirse árboles binarios diciendo que o constan de un único *nodo externo* o que tienen un *nodo interno* (la raíz) que tiene un subárbol binario izquierdo y uno derecho. Describa la clase de árboles binarios, fijándose solo en los nodos externos, mediante el método simbólico, y obtenga el número de árboles binarios con n nodos externos.

Borrador

17. Principio de Inclusión y Exclusión

1. Encuentre el número de permutaciones de las 26 letras del alfabeto inglés que no contengan *ayer*, *ola*, *grande*, *barco*.

2. En términos de la notación que usamos para el Principio de Inclusión-Exclusión, encuentre la función generatriz para el número de objetos que tienen a lo más r propiedades:

$$M_r = \sum_{0 \leq k \leq r} e_k$$

3. ¿Cuántos números telefónicos de 10 dígitos contienen todos los dígitos impares?

4. Aplique el principio de inclusión-exclusión para encontrar $\phi(n)$ si $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$ con los p_i primos diferentes y $k_i \geq 1$.

5. Se dice que una función $f : A \to B$ es *sobre* si para cada $b \in B$ hay al menos un $a \in A$ tal que $f(a) = b$. Use el principio de inclusión-exclusión para determinar el número de tales funciones (tomando $A = \{1, 2, \ldots, n\}$ y $B = \{1, 2, \ldots, m\}$, conviene definir que una función tiene la propiedad i si no hay a con $f(a) = i$). Deje su resultado expresado como una sumatoria.

6. Use el principio de inclusión y exclusión para expresar en forma de una suma el número de matrices 0-1 de $m \times n$ sin filas ni columnas sólo ceros.

7. Use el principio de inclusión y exclusión para determinar el número de manos de poker (13 valores de 4 pintas) con todas las pintas. Deje su resultado expresado como una sumatoria.

8. Un número se define como *famoso en base b* si tiene a lo más b dígitos y su i-ésimo dígito en base b es i. Por ejemplo, 9213 es famoso en base 10, ya que su segundo dígito es 2. Explique cómo puede calcularse cuántos números famosos de largo b hay para cada base b.

9. ¿Cuántas palabras de largo n formadas únicamente por las 5 vocales pueden formarse, si deben contener un número par de vocales fuertes ('a', 'e' y 'o')?

10. Use el principio de inclusión y exclusión para determinar el número de funciones sobre $f\colon X \to Y$, donde $|X| \geq |Y|$.
Pista: Considere que la función $g\colon X \to Y$ tiene la propiedad i si no hay $x \in X$ tal que $g(x) = i$.

11. Considere palabras de largo n formadas por símbolos tomados entre $\{a, b, c, d, e, f\}$. ¿Cuántas de ellas tienen a lo más tres símbolos distintos? ¿Cuántas tienen exactamente tres símbolos diferentes?

12. En la Universidad de Miskatonic hay 67 estudiantes en el curso del profesor Warren Rice. De ellos, 47 leen francés, 35 leen alemán, y 23 leen ambos lenguajes. ¿Cuántos no leen ninguno de los dos? Si además hay 20 estudiantes que leen ruso, 12 de los cuales leen francés, y 11 de ellos leen alemán, y 5 leen los tres lenguajes, determine cuántos estudiantes no leen ninguna de las tres lenguas.

13. En una sala hay 18 estudiantes, de los cuales 7 estudian matemáticas, 10 estudian ciencia, y 10 programación. Además, 3 estudian matemáticas y ciencias, 4 estudian matemáticas y programación, y 5 estudian ciencias y programación. Sabemos que uno estudia los tres temas. ¿Cuántos de los presentes no estudian ninguno de los temas?

14. En el bar "El Tufo" el único que no toma es el barman. Su hobby es mantener una estadística de cuántos asistentes toman cada tipo de bebida, entre aguardiente *Bigote de Tigre*, ron *Siete Tiritones* y tequila *Los Tres Cuates*. Cierto día un borrachín particularmente odioso le borró parte de sus anotaciones, quedándole sólo que 2 habían tomado de los tres tragos; recordaba que 4 habían tomado al menos aguardiente y ron, y que a 5 les sirvió ron y tequila. En total se sirvieron 16 aguardientes, 10 ron y 14 tequilas esa noche. Sabiendo que ese día fueron 26 los visitantes del tugurio, y que ninguno tomó dos veces de la misma bebida, determine a cuántos sirvió sólo aguardiente y tequila.

Borrador

15. En Gales pareciera ser que los nombres de las localidades siguen la regla que no pueden contener más de dos vocales. Suponiendo el alfabeto inglés (26 letras, 5 de las cuales son vocales), ¿cuántos nombres de localidades galesas de n letras pueden formarse?

16. Considere palabras de largo n formadas por las letras a, b, c, d, e, f.

    a) ¿Cuántas tienen al menos 3 letras distintas?

    b) ¿Cuántas están formadas por exactamente 4 letras diferentes?

    c) ¿Cuántas tienen un número par de vocales?

17. Indique el número de soluciones enteras de la ecuación:

    $$x_1 + x_2 + x_3 = 11$$

    si $0 \leq x_1 \leq 3$, $0 \leq x_2 \leq 4$ y $0 \leq x_3 \leq 6$.

18. En el curso Estructura de Datos (este semestre es chico, de sólo 2 054 alumnos) se hace una encuesta sobre los lenguajes que cada estudiante sabe. 1 786 dicen saber Python, 999 saben Java, 345 cursaron C. Hay 876 que dicen dominar Java y Python, 231 Java y C, 290 C y Python y hay 189 que se dicen expertos en los tres. ¿Cuántos dicen manejar a lo menos dos lenguajes diferentes? ¿Cuántos no saben ninguno de estos lenguajes?

19. Usando el principio de inclusión y exclusión, calcule de cuántas maneras distintas se pueden escoger 7 cartas de una baraja inglesa de 52 cartas de modo que contenga al menos una carta de cada pinta (corazón, diamante, trébol, pica).

20. Una función $f\colon \mathcal{A} \to \mathcal{B}$ es *sobreyectiva* si para cada $b \in \mathcal{B}$ hay al menos un $a \in \mathcal{A}$ tal que $f(a) = b$. Use el principio de inclusión-exclusión para determinar el número de tales funciones si $|\mathcal{A}| = m$ y $|\mathcal{B}| = n$.

21. En el picnic anual de la Universidad de Miskatonic los 65 empleados se reparten la organización. De ellos 21 traen hot dogs, 35 traen pollo frito, 28 traen ensaladas, 32 traen postres, 13 traen hot dogs y pollo frito, 10 traen hot dogs y ensaladas, 9 traen hot dogs y postres, 12 traen pollo frito y ensalada, 17 traen pollo frito y postres, 14 traen ensalada y postre, 4 traen hot dogs, pollo frito y ensalada, 6 traen hot dogs, pollo frito y postre, 5 traen hot dogs, ensaladas y postre. 7 traen pollo frito, ensaladas y postre, y 2 traen los cuatro items.

    a) Quienes no traen comida deben preparar todo y ordenar luego. ¿Cuántos hacen estas tareas?

    b) ¿Cuántos sólo traen hot dogs?

    c) ¿Cuántos traen exactamente un item?

22. Usando el principio de inclusión y exclusión, derive una expresión para el número de funciones sobreyectivas de $[m]$ a $[n]$.

Borrador

18. Fórmula de inversión de Lagrange

1. Suponga que la función $u(t)$ se define mediante:

   $$u = te^u$$

   Encuentre los coeficientes de la serie de potencias de $u(t)^{1/2}$

2. Considere árboles m-arios, que son vacíos, o constan de una raíz y m subárboles m-arios en orden (el caso $m = 2$ son los árboles binarios tradicionales). Encuentre el número de árboles m-arios de n nodos.

Borrador

19. Grafos

1. Tres casas A, B y C deben ser conectadas a los servicios de agua, electricidad y gas (a, e, g).

   a) Describa este grafo mediante listas de adyacencia

   b) Dibuje este grafo. ¿Es posible dibujarlo sin que se crucen arcos?

2. Considere el grafo completo K_n. ¿Cuántos vértices y cuántos arcos tiene? ¿Para qué valores de n es posible dibujarlo sin que los arcos se crucen?

3. Dibuje los grafos dados por:

   a) $V = \{a, b, c, d, e\}$, $E = \{ab, ac, ad, de, ce, be\}$

   b) $V = \{1, 2, 3, 4\}$, $E = \{12, 13, 24, 23\}$

4. Halle los componentes conexos del grafo descrito por la matriz de adyacencia:

$$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

5. Demuestre que si un par de vértices de un grafo están conectados por un camino, están conectados por un camino simple.

6. Sea $G = (V, A)$ un grafo, $|V| = n$ y $|E| = m$. Demuestre que:

   a) $m \leq \frac{n(n-1)}{2}$

   b) Si G es un grafo bipartito, entonces $m \leq \frac{n^2}{4}$

7. Si G tiene vértices $v_1, v_2, \ldots, v_n$, la secuencia $(d(v_1), d(v_2), \ldots, d(v_n))$ es denominada la *secuencia de grados de G*.

   a) ¿Existe un multigrafo con secuencia de grados 3, 3, 3, 3, 5, 6, 6, 6, 6?

   b) ¿Existe un multigrafo con secuencia de grados 1, 1, 3, 3, 3, 3, 5, 6, 8, 9?

   c) ¿Existe un grafo (simple) con las secuencias de grados anteriores?

8. Definimos el *doble* de un grafo $G = (V, E)$ como tomar dos copias del grafo y conectar entre sí vértices correspondientes. Demuestre que si G es bipartito, lo es su doble.

9. Un *k-cubo* (Q_k) es un grafo (simple) cuyos vértices son k-tuplas ordenadas de 0 y 1, tal que dos vértices son adyacentes si y sólo si difieren en exactamente una coordenada.

   a) Dibuje Q_1, Q_2, Q_3 y Q_4

   b) ¿Cuál es el número de vértices y aristas de cada uno de esos grafos?

   c) Demuestre que Q_k es un grafo bipartito

10. Demuestre que todo árbol es un grafo bipartito. ¿Cuáles son los valores posibles de $\chi(T)$, si T es un árbol?

11. El grafo de ciclo C_n es un ciclo de n elementos. El grafo de rueda W_{n+1} es un C_n, cuyos vértices están conectados a un $n+1$-ésimo vértice.

    a) Encuentre una relación entre los polinomios $P(W_n, \lambda)$ y $P(C_n, \lambda)$ (Considere lo que pasa si se pinta el "eje" de algún color)

    b) Encuentre y resuelva una recurrencia para $P(C_n, \lambda)$

    c) ¿Cuánto valen $\chi(C_n)$ y $\chi(W_n)$?

12. El *grafo de estrella* E_n es un centro conectado a n puntas. La figura 1 muestra E_7. Encuentre el polinomio cromático $P(E_n, \lambda)$.

Borrador

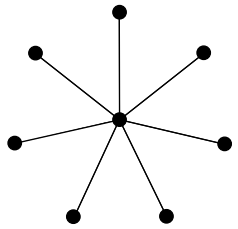


Figura 1: El grafo E_7

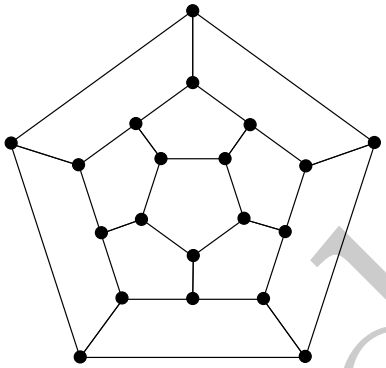


Figura 2: Grafo del dodecaedro

13. Demuestre que en un grafo con al menos dos vértices siempre hay al menos dos vértices con el mismo grado.
14. El grafo de la figura 2 es el que corresponde a uno de los sólidos platónicos, el dodecaedro.
    a) Encuentre el grafo dual a este.
    b) ¿Cuál es el número cromático de este grafo?
    c) ¿Es este un grafo bipartito?
15. Respecto del grafo de la figura 3:

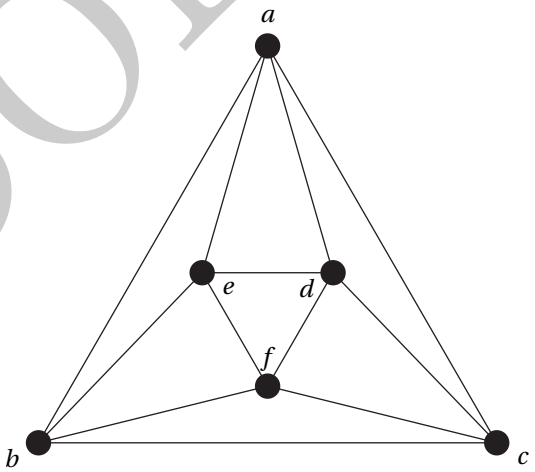


Figura 3: Un grafo

    a) ¿Cuál es su número cromático?
    b) ¿Cuál es su índice cromático?
    c) ¿Tiene un camino o circuito de Euler (pasa por cada arco exactamente una vez)?

Borrador

d) ¿Tiene un circuito de Hamilton (pasa por cada vértice exactamente una vez)?

16. El grafo de rueda W_{n+1} se obtiene de C_n (definido en el problema 11) conectando todos sus vértices con un nuevo vértice (el "eje" de la rueda). ¿Cuánto son $\chi(C_n)$ y $\chi(W_n)$?

17. Encuentre $P(W_n, \lambda)$, donde el grafo W_n se define en el problema 16.

18. Demuestre que el polinomio cromático $P(G, \lambda)$ de un grafo $G = (V, E)$ con $n = |V|$ vértices es de grado n, y que el coeficiente de λ^n es 1.

19. Un grafo G se dice *autocomplementario* si es isomorfo a $\overline{G}$. Demuestre que los grafos autocomplementarios son conexos.

20. Se define el *grafo bipartito completo* $K_{m,n}$ formado por dos grupos de m y n vértices con conexiones entre cada vértice de un grupo y el otro, y ninguna conexión al interior de cada grupo.

    a) ¿Cuándo es regular $K_{m,n}$?

    b) ¿Para qué valores de m y n hay un camino o circuito de Euler de $K_{m,n}$?

    c) ¿Cuáles de los $K_{m,n}$ tienen un ciclo Hamiltoniano?

21. Demuestre que un grafo cuyas componentes conexas son todas caminos simples es bipartito. ¿Bajo qué condiciones hay un matching completo en este tipo de grafos?

    Pista: ¿Qué ocurre si el camino comienza y termina en X?

22. En redes de actividades en la cual la actividad (u, v) toma tiempo $\omega(u, v)$ calculamos el instante más temprano en que puede ocurrir el evento v mediante $E(v) = \max_u\{E(u)+\omega(u, v)\}$. Indique en qué orden debe efectuarse este cálculo, y explique el porqué.

23. Dado un grafo $G = (V, E)$, explique cómo puede determinar si es un árbol usando los algoritmos vistos en clase.

24. Un estudiante completamente confundido programa el algoritmo de Kruskal de forma de siempre agregar el arco de *mayor* costo. ¿Que obtiene como resultado? Justifique su aseveración.

25. En el algoritmo para hallar un camino alternante cuando se construye un *matching* máximo en un grafo bipartito no se usa búsqueda en profundidad sino a lo ancho. Explique porqué.

26. ¿Bajo qué condiciones hay un matching completo en un grafo bipartito? Explique cuidadosamente su notación.

27. Dados una red de flujos $D = (V, A)$, con fuente s y sumidero t, capacidades $c\colon A \to \mathbb{R}$; un flujo $f\colon A \to \mathbb{R}$ en la red y dos cortes (S, T) y (S', T'). Demuestre que el valor neto del flujo f a través de los dos cortes es el mismo.

28. Determine para qué valores de n tiene un circuito hamiltoniano el grafo completo K_n.

29. Demuestre que en un grafo con dos o más vértices hay a lo menos dos vértices con el mismo grado.

30. Dibuje, por separado, todos los grafos no isomorfos que se pueden formar con 1, 2, 3, 4, y 5 vértices.

31. En un grafo dirigido $D = (V, A)$ un vértice puede aparecer como origen de un arco (es la primera componente del arco) o como su destino (es la segunda componente). Así podemos distinguir el *grado de salida* de un vértice, que anotamos $\delta^+(v)$, y el *grado de entrada*, que anotamos $\delta^-(v)$. Formalmente:

$$\delta^+(u) = |\{(u, v)\colon (u, v) \in A\}|$$
$$\delta^-(v) = |\{(u, v)\colon (u, v) \in A\}|$$

    Finalmente entiéndase por *digrafo estricto* un grafo dirigido sin bucles.

    Con esto en mente responda:

Borrador

a) Demuestre que en un grafo dirigido $D = (V, A)$ se cumple

$$\sum_{v \in V} \delta^-(v) = |A| = \sum_{v \in V} \delta^+(v)$$

b) Sea $D = (V, A)$ un digrafo sin ciclos dirigidos. Entonces:

- Demostrar que $\min_{v \in V} \delta^-(v) = 0$.
- Deducir que existe un orden $\{v_1, v_2, v_3, \ldots, v_i\}$ de los vértices del digrafo donde para $1 \leq i \leq |V|$ el arco con cabeza v_i tiene su cola en alguno de $\{v_1, v_2, v_3, \ldots, v_{i-1}\}$.

c) Demuestre que si $D = (V, A)$ es un grafo dirigido estricto con $min_{v \in V}\{\delta^-(v), \delta^+(v)\} = k > 0$, entonces D contiene un ciclo dirigido de largo a lo menos $k + 1$.

32. Sea $N = (V, A)$ una red con flujo máximo conocido. Se le ha dado la tarea de cambiar algo en la red que asegure que la nueva red tendrá un flujo máximo mayor al anterior. Las opciones que tiene para realizar esto son:

    (A) Incrementar la capacidad de un arco existente en 1.

    (B) Agregar un nuevo arco con capacidad 1 entre dos vértices a su elección.

    En base a lo anterior, indique:

    a) ¿Que opción elegiría para garantizar un flujo máximo mayor en la nueva red? Justifique su elección.

    b) ¿Es posible incrementar el flujo máximo en más de 1 con alguna de las opciones anteriores? Justifique su respuesta.

33. ¿Cuántos matchings completos tiene el grafo $K_{m,n}$, dependiendo de los valores de m y n?

34. Calcule el número de *matchings* que tiene el grafo bipartito completo $K_{m,n}$.

35. Sea $D = (V, A)$ un digrafo con capacidad $c : A \to \mathbb{R}$, fuente s y sumidero t. Demuestre formalmente que si $(S_1, \overline{S_1})$ y $(S_2, \overline{S_2})$ son cortes de la red D, entonces lo es $(S_1 \cap S_2, \overline{S_1 \cap S_2})$.

36. Los grafos Q_n pueden describirse mediante vértices que son secuencias de n ceros y unos, y dos vértices están conectados exactamente cuando difieren en una única posición.

    a) Determine su número cromático, $\chi(Q_n)$

    b) Determine el grado de los vértices de este grafo

37. Hallar los valores de n para los que los grafos K_n y W_n admiten un camino euleriano.

38. Se propone organizar una fiesta con 15 invitados, de forma que cada uno de ellos conozca exactamente a 3 de los otros. ¿Le interesa asistir?

39. Sea $G = (V, E)$ un grafo, con $V = \{a, b, c, d, e\}$ y $E = \{\{a, b\}, \{a, c\}, \{a, e\}, \{b, c\}, \{c, d\}, \{d, e\}\}$

    a) Indicar los grados de cada vértice

    b) Hacer una representación gráfica de G

    c) Dar la matriz de adyacencia correspondiente a G

40. Sea $G = (V, E)$ un grafo regular con 15 arcos ($|E| = 15$). Determine cuántos vértices puede tener G.

41. Sea $G = (V, E)$ un grafo con n vértices.

    a) Suponga que G tiene una componente conexa con k vértices. Mostrar que la cantidad total de arcos de G cumple $|E| \leq \binom{k}{2} + \binom{n-k}{2}$

    b) Mostrar que para $1 \leq k < n$ se cumple $\binom{k}{2} + \binom{n-k}{2} \leq \binom{n-1}{2}$

    c) Concluir que si $|E| > \binom{n-1}{2}$ entonces G debe ser conexo

Borrador

42. Definimos el grafo cubo Q_n tomando como vértices las secuencias de n ceros y unos, y conectando pares de vértices si difieren en exactamente una posición.

    a) ¿Cuántos vértices tiene Q_n? ¿Cuántos arcos? b) ¿Es regular Q_n? c) Determine $\chi(Q_n)$

43. Si $G = (V, E)$ es un grafo, su *grafo complementario* $\overline{G} = (V, \overline{E})$ es aquel en el que $\{x, y\}$ es un arco exactamente si $\{x, y\} \notin E$. Demuestre que $\overline{C}_5$ es isomorfo a C_5, pero si $n \neq 5$ $\overline{C}_n$ no es isomorfo a C_n

44. En una provincia hay cinco ciudades. Un ingeniero civil un tanto inexperto debe diseñar un sistema de carreteras de modo que ninguna de las ciudades quede aislada. Muestre a este pobre ingeniero de cuántas maneras es posible hacerlo utilizando el principio de inclusión y exclusión.

45. Para $G = (V, E)$ definimos $p_G(k)$ como el número de maneras de colorear G con k colores. Use el principio de inclusión y exclusión: Ω son las asignaciones de k colores a V, y para $e \in E$ la propiedad P_e es que los dos extremos de e tienen el mismo color.

    a) ¿A qué corresponde $p_G(k)$?

    b) Demuestre que para k colores, cada $N(\supseteq S)$ es un polinomio en k, y también lo son los N_r

    c) Exprese $p_G(k)$ en términos de los resultados anteriores, demostrando que es un polinomio

46. Sea $T_1 = (V, E_1)$ y $T_2 = (V, E_2)$ dos árboles con el mismo conjunto de vértices. Demuestre que el grafo $T_1 \cup T_2 := (V, E_1 \cup E_2)$ se puede colorear usando 4 colores.

47. Demuestre que si un árbol tiene un vértice de grado Δ, tiene al menos Δ hojas.

48. Sea G un grafo, $\overline{G}$ su grafo complementario, n el número de vértices y $\chi(G)$ el número cromático de G. Demuestre:

    a) $\chi(G) \cdot \chi(\overline{G}) \geq n$
    Pista: Sean $\{a_1, a_2, a_3, \ldots, a_n\}$ y $\{b_1, b_2, b_3, \ldots, b_n\}$ coloraciones de G y $\overline{G}$ respectivamente, donde a_i es el color correspondiente al vértice v_i en el grafo G y b_i es el color correspondiente al vértice v_i en el grafo $\overline{G}$. Pruebe que $\{(a_1, b_1), (a_2, b_2), \ldots, (a_n, b_n)\}$ es una coloración de grafo K_n .

    b) $\chi(G) + \chi(\overline{G}) \leq n + 1$
    Pista: Trate el caso extremo en el cual un color se usa en el máximo número de vértices, es decir, el resto de los colores se usa el mínimo

    c) $\chi(G) + \chi(\overline{G}) \geq 2 \cdot \sqrt{n}$
    Pista: Trate el caso extremo en el cual los colores tienen la distribución más uniforme.

    d) Pruebe que si G es un grafo regular de grado k con n vértices entonces

    $$\chi(G) \geq \frac{n}{n-k}$$

    Pista: Halle una partición de los vértices en $\chi(G)$ bloques y determine cuál es el mayor número de vértices posibles en cada bloque.

49. Se define el grafo M_r para $r \geq 2$ como el grafo C_{2r} conectando vértices opuestos: Si los vértices son $0, 1, \ldots, 2r-1$, son arcos $\{0, 1\}$, $\{1, 2\}$, $\ldots$, $\{2r-1, 0\}$; y también $\{0, r\}$, $\{1, r+1\}$, $\ldots$, $\{r-1, 2r-1\}$. Demuestre las siguientes:
    a) $\chi(M_2) = 4$ b) Si $r > 2$ es par, $\chi(M_r) = 3$ c) Si r es impar, $\chi(M_r) = 2$

50. Explique cómo determinar el número cromático y el índice cromático de un árbol.

51. Considere el algoritmo 1. En este algoritmo se usa una estructura de grupos $C(v)$, que para el vértice v retorna el grupo al que pertenece (una representación de un subconjunto de los vértices), y que permite unir dos grupos eficientemente. Responda las siguientes, dependiendo de las características del grafo G:

    a) ¿Cuál es el número de veces en que se unen clases?

    b) ¿Cuántos conjuntos $C(v)$ diferentes resultan? ¿Qué representan?

Borrador

Algoritmo 1: Algoritmo misterioso

function `Misterio`$(G = (V, E))$

for *todo* $v \in V$ **do**
    $C(v) \leftarrow \{v\}$
end
$L \leftarrow E$
while L *no vacía* **do**
    $uv \leftarrow$ extraiga un elemento de L
    if $C(u) \neq C(v)$ **then**
        Una $C(u)$ con $C(v)$
    end
end
return *Número de* $C(v)$ *diferentes*

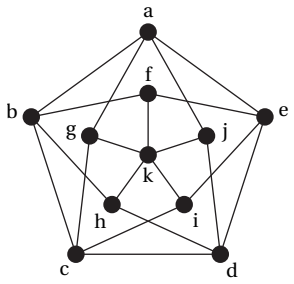


Figura 4: Grafo a colorear

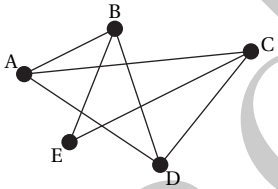


Figura 5: Grafo A

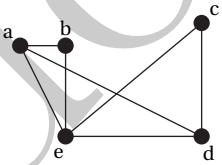


Figura 6: Grafo B

52. Demuestre el equivalente del *handshaking lemma* para digrafos:

$$\sum_{v \in V} \delta^-(v) = \sum_{v \in V} \delta^+(v) = |E|$$

53. Justifique cotas para el número cromático del grafo de la figura 4.

54. ¿Son isomorfos los grafos de las figuras 5 y 6? Justifique, dando un isomorfismo o explicando porqué es imposible.

55. Determine si el grafo de la figura 5 tiene un camino o circuito de Euler.

56. Para $G = (V, E)$ definimos $p_G(k)$ como el número de maneras de colorear G con k colores. Use el principio de inclusión y exclusión: Ω son las asignaciones de k colores a V, y para $e \in E$ la propiedad P_e es que los dos extremos de e tienen el mismo color.

    a) ¿A qué corresponde $p_G(k)$?

    b) Demuestre que para k colores, cada $N(\supseteq S)$ es un polinomio en k, y también lo son los N_r

    c) Exprese $p_G(k)$ en términos de los resultados anteriores, demostrando que es un polinomio

57. Demuestre el equivalente de:

$$\sum_{v \in V} \delta(v) = 2|E|$$

para digrafos:

$$\sum_{v \in V} \delta^-(v) = \sum_{v \in V} \delta^+(v) = |E|$$

Borrador

58. ¿Cuántos *matchings* completos tiene el grafo $K_{m,n}$?

59. Demuestre que si en un grafo bipartito $G = (X \cup Y, E)$ todos los vértices tienen grado al menos dos entonces tiene un *matching* completo.
Pista: ¿Qué son las componentes conexas de un grafo bipartito regular de grado dos?

Borrador

20. Permutaciones

1. Construya la tabla de las operaciones de las permutaciones de cuatro elementos.
2. Dadas las siguientes permutaciones de siete elementos: $\alpha = (1327456)$, $\beta = (7213546)$, $\gamma = (7654321)$, calcule:
   a) $\alpha\beta$
   b) $\beta\alpha$
   c) Verifique que $(\alpha\beta)\gamma = \alpha(\beta\gamma)$
   d) Exprese las permutaciones en forma de ciclos, repita los cálculos anteriores entre ellos, y exprese los resultados como permutaciones
3. Una *inversión* de una permutación τ es un par de elementos $i < j$ tales que $\tau(i) > \tau(j)$.
   a) Si se considera 1 en una permutación de n elementos, claramente nunca puede ser el mayor del par, y no aporta inversiones. Si consideramos 2, puede aportar 0 ó 1 inversiones. El 3 puede aportar 0, 1 ó 2. Siguiendo de esta forma, n aporta entre 0 y $n-1$ inversiones. Si $I_n(x)$ es la función generatriz del número de inversiones en permutaciones de n elementos, demuestre que:
   $$\begin{aligned} I_n(x) &= 1 \cdot (1+x) \cdot \ldots \cdot (1 + x + x^2 + \ldots + x^{n-1}) \\ &= \prod_{1 \le i \le n-1} \sum_{0 \le j \le i} x^j \end{aligned}$$
   b) Encuentre el número promedio de inversiones en permutaciones de n elementos, usando los resultados del problema 5.
4. Una permutación que es su propia inversa se llama *involución*. El número de involuciones de n elementos, I_n, tiene función generatriz exponencial $I(z) = \exp(z + z^2/2)$. Use $zD\log$ para obtener una recurrencia para I_n.
5. Demuestre que dada la secuencia $\{a_n\}_0^\infty$, donde a_n representa el número de elementos que tienen "peso" n, y $A(x) \overset{\text{ops}}{\longleftrightarrow} \{a_n\}_0^\infty$, el "peso promedio" de los a_n dado por:
   $$\mu = \frac{\sum_{n\ge 0} n a_n}{\sum_{n \ge 0} a_n}$$
   (lo que se conoce como la *media* de la secuencia) se puede calcular mediante:
   $$\mu = (\ln A(x))'\big|_{x=1}$$
   Si se define la *varianza* mediante:
   $$\sigma^2 = \frac{\sum_{n\ge 0}(n-\mu)^2 a_n}{\left(\sum_{n\ge 0} a_n\right)^2}$$
   exprese σ^2 en términos de las primeras dos derivadas de $\ln A(x)$ evaluadas en $x = 1$.
6. Una *inversión* de una permutación τ es un par de elementos $i < j$ tales que $\tau(i) > \tau(j)$.
   a) Si se considera 1 en una permutación de n elementos, claramente nunca puede ser el mayor del par, y no aporta inversiones. Si consideramos 2, puede aportar 0 ó 1 inversiones. El 3 puede aportar 0, 1 ó 2. Siguiendo de esta forma, n aporta entre 0 y $n-1$ inversiones. Si $I_n(z)$ es la función generatriz del número de inversiones en permutaciones de n elementos, demuestre que:
   $$\begin{aligned} I_n(z) &= 1 \cdot (1+z) \cdot \ldots \cdot (1 + z + z^2 + \ldots + z^{n-1}) \\ &= \prod_{1 \le i \le n-1} \sum_{0 \le j \le i} z^j \end{aligned}$$
   b) Encuentre el número promedio de inversiones en permutaciones de n elementos, usando los resultados del problema 5.

Borrador

21. Teoría de coloreo de Pólya

1. Considere banderas del formato dado por la figura 7, donde cada área tiene color uniforme.

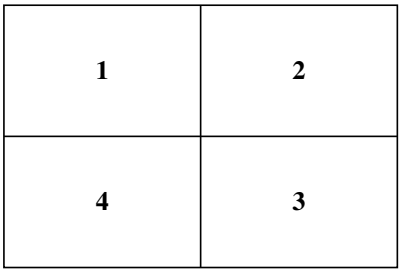


Figura 7: Formato de banderas para pregunta 1

   a) Indique el grupo de simetrías B que resulta de mover esto en el espacio operando sobre las áreas marcadas 1 a 4.

   b) Dé el índice de ciclos del grupo B, $\zeta_B(x_1, x_2, x_3, x_4)$.

   c) Suponiendo dado el índice de ciclos $\zeta_B(x_1, x_2, x_3, x_4)$, explique cómo se calcula el número de banderas esencialmente diferentes si se cuenta con colores rojo, azul y blanco.

   d) Suponiendo dado el índice de ciclos $\zeta_B(x_1, x_2, x_3, x_4)$, y cuatro colores (rojo, azul, verde y blanco), exprese el número de banderas esencialmente distintas que tienen un área de cada color.

2. Para un grupo G de permutaciones de un conjunto X de n elementos se conoce explícitamente el índice de ciclos $\zeta_G(x_1, \ldots, x_n)$. Explique cómo usaría esta información para calcular el número de órbitas de G.

3. Considere el grupo de automorfismos del grafo bipartito $K_{2,3}$.

   a) Describa las operaciones de este grupo mediante sus ciclos. ¿Cuál es el orden del grupo?

   b) Indique las órbitas de los vértices.

   c) ¿Cuál es el número de coloreos esencialmente diferentes si se pueden usar a lo más 3 colores para los vértices?

4. Considere un grupo de permutaciones G que permuta un conjunto X de n elementos. Muestre cómo calcular el número de coloreos esencialmente distintos de X si cada elemento de X tiene un color diferente de los demás, dado el índice de ciclos $\zeta_G(x_1, \ldots, x_n)$. ¿Puede hacerse esto conociendo sólo el orden $|G|$?

5. Considere un grupo de permutaciones G que permuta un conjunto X de n elementos. Muestre cómo calcular el número de coloreos esencialmente distintos de X si cada elemento de X tiene un color diferente de los demás, dado el índice de ciclos $\zeta_G(x_1, \ldots, x_n)$. ¿Puede hacerse esto conociendo sólo el orden $|G|$?

6. Considere árboles binarios completos de altura 2, que se consideran iguales al intercambiar izquierda y derecha

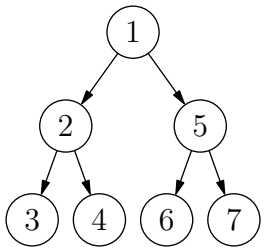


Figura 8: Árboles para la pregunta 6

(como 3 con 4; pero también 2 con 5, que lleva consigo intercambiar 3 con 6 y 4 con 7). Vea la figura 8.

Borrador

a) Determine el índice de ciclos del grupo subyacente, $\zeta_G(x_1, x_2, x_3, x_4, x_5, x_6, x_7)$.

b) En términos de ζ_G, exprese el número de árboles distintos si los nodos se pintan con 2 colores. Explique cómo llega a esta expresión.

c) En términos de ζ_G, exprese el número de árboles distintos que tienen exactamente 3 nodos azules si los nodos se colorean de rojo, azul y verde. Justifique su expresión.

7. Considere una matriz cuadrada de $n \times n$. A esta matriz se le asocia un número, conocido como su *determinante*, que se anota $\det(M)$. Si se intercambian dos filas o columnas de M para dar M', resulta:

$$\det(M') = -\det(M)$$

Podemos considerar entonces como un grupo de permutaciones los reordenamientos de filas y columnas que mantienen el valor de $\det(M)$. En consecuencia, podemos reordenar las columnas según el grupo alternante A_n de permutaciones pares, y hacer lo mismo con las filas, sin cambiar el valor del determinante. Si reordenamos filas y columnas por permutaciones impares ambas, también se mantiene el valor. Sabemos que $|A_n| = n!/2$, y el mismo número de permutaciones impares; con lo que este grupo tiene orden:

$$2 \cdot \frac{n!}{2} \cdot \frac{n!}{2} = \frac{(n!)^2}{2}$$

Obviamente puede ocurrir que dos matrices tengan el mismo determinante aunque no se pueda obtener la una de la otra mediante estas operaciones, pero no nos preocuparemos de ese caso acá.

Para concretar, considere matrices de 2×2, y los casilleros de las mismas identificados como sigue:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

a) Describa el grupo de permutaciones esbozado arriba que mantiene el valor absoluto del determinante en este caso.

b) Encuentre el índice de ciclos del grupo

c) Determine cuántos valores diferentes del determinante pueden obtenerse a lo más con dos valores de los elementos de la matriz.

d) Diga cuántos valores del determinante podrían obtenerse a lo más con dos valores 2 y dos valores 3.

8. Una tribu de hippies artesanos fabrica pulseras formadas alternadamente por tres arcos y tres cuentas, y tienen arcos y cuentas de cinco colores. Para efectos de simetría pueden considerarse las pulseras como triángulos equiláteros en los cuales se colorean los vértices y las aristas.

a) Determine el grupo G de permutaciones relevante, y su índice de ciclos ζ_G.

b) Dado el índice de ciclos anterior, exprese el número de pulseras diferentes que pueden crearse.

c) ¿Cuántas pulseras hay que usan exactamente tres colores?

9. Obtenga el índice de ciclos para el grupo $\mathtt{C}_8$ (rotaciones en el plano de un octágono regular).

10. El dodecaedro regular es un sólido con 12 caras (pentágonos regulares). Tiene 30 aristas y 20 vértices (en cada vértice se encuentran 3 pentágonos). ¿Cuál es el orden del grupo de rotaciones de este sólido en el espacio?

11. Un grupo satánico desea identificar los rangos de sus miembros mediante un distintivo en forma de pentagrama (ver figura 9) coloreando las áreas de color blanco, azul y oro. Debe asegurarse que los distintos rangos sean distinguibles, aún si el distintivo se gira, y les interesa saber cuántos rangos pueden definir. Sus artes no alcanzan a los del Necronomicon, por lo que le solicitan que les haga los cálculos. Explique paso a paso cómo calcularía este valor.

12. Explique en detalle y paso a paso cómo calcularía el número de maneras de colorear los arcos del grafo de la figura 10 con colores azul, rojo y amarillo de forma que cada color aparezca el mismo número de veces.

Borrador

Figura 9: Pentagrama

Borrador

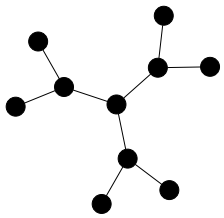


Figura 10: Grafo a colorear arcos