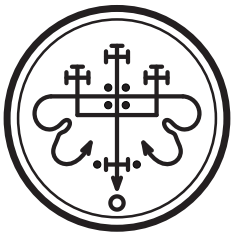
Problemas Propuestos
Fundamentos de Informática I

Horst H.~von Brand

17 de marzo de 2015



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 $A \smallsetminus B$ 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.

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 $\mathscr{U}$. 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. *a*) Defina una función $f : \mathbb{N} \to \mathbb{N}$ que es uno a uno, pero no sobre
   b) Defina una función $g : \mathbb{N} \to \mathbb{N}$ que es sobre, pero no uno a uno

7. ¿Es simétrica la composición de dos relaciones simétricas?

8. ¿Es una relación simétrica y transitiva necesariamente reflexiva?

9. 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 $(x-u)^2 + (y-v)^2 \leq 1$.

10. 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

11. Considere una relación simétrica R. ¿Qué puede decir sobre su transpuesta R^{-1}?

12. Considere dos relaciones transitivas R_1 y R_2. ¿Qué puede decir sobre su composición $R_2 \circ R_1$?

13. Una función es un caso particular de relación. ¿La transpuesta de una función es siempre una función?

14. 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 $x - y \in \mathbb{Z}$

15. Estudie las propiedades de las relaciones definidas en la lista que sigue, sobre los conjuntos que se indica.

    a) $\mathscr{R}_1$ definida sobre $\mathbb{R}$ por $x \; \mathscr{R}_1 \; y$ si y sólo si $\cos x = \sin y$
    b) $\mathscr{R}_2$ definida sobre $\mathbb{R} \times \mathbb{R}$ por $(u,v) \; \mathscr{R}_2 \; (x,y)$ si y sólo si $(x-u, y-v) \in \mathbb{Z} \times \mathbb{Z}$
    c) $\mathscr{R}_3$ definida sobre $[1,500] \times [1,500]$ por $(u,v) \; \mathscr{R}_3 \; (x,y)$ si y sólo si $uy = xv$ (los rangos son de números enteros)

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.

4. Demostraciones

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

   Pista: En este rango $\sin x \ge 0$ y $\cos x \ge 0$. 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:

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

8. Demuestre por inducción que:

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

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:

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

11. Demuestre por inducción que:

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

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

13. Demostrar que para $n \ge 2$ 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 $n \ge 0$. Demostrar que $T_n < 2^n$.

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 $a_2 x^2 + a_1 x + a_0$ con coeficientes enteros que tiene $\sqrt[3]{2}$ como raíz.

Pista: Considere $x^3 - 2 = (a_2 x^2 + a_1 x + a_0)(b_1 x + b_0)$

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:

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

33. Demuestre que:

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

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

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

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

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

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

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

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

37. Demuestre por inducción sobre n que:

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

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 $n \ge 1$. Demuestre además que $u_{n+1} > u_n$.

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

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 $\mathbb{Z}[\tau] = \{a + b\tau : a, b \in \mathbb{Z}\}$ 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?

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

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

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 $C = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. 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 $\{a \cdot x : x \in A \text{ y } x \neq 0\}$, 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 $\phi : R[x] \to R$ 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 $\mathbb{Z}_3$.

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 $\mathbb{Z}_2$?

6. Teoría de números

1. Demuestre que el conjunto de los subconjuntos de $\mathscr{U}$, $2^{\mathscr{U}}$ 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 $c \in \mathbb{Z}$.

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 $1 \le i \le n-1$ 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 $\mathbb{Z}_{144}$

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 $I = \{ax + by + cz\colon\ x, y, z \in \mathbb{Z}\}$. 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.

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 $\gcd(a^2, b^2) = \big(\gcd(a,b)\big)^2$

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 $1 \le a, b, c < m$ tales que $ac \equiv bc \pmod{m}$, pero $a \not\equiv b \pmod{m}$.

64. ¿Cuánto es $\phi(360)$?

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:

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:

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

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:

$$\sum_{1 \leq k \leq 9} k d_k \bmod 11$$

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)?

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 $(x_i, f(x_i) \pmod{p})$. Demuestre que sólo si al menos k participantes cooperan es posible determinar el secreto s.

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 $0 \le x < p$, y calcula $h = r^x \bmod p$. Su clave pública es (p, r, h). Si Bob desea comunicarle m a ella, con $0 \le m < p$, elige y al azar en el rango $0 \le y < p$ 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 mód 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, $1 \le k \le p-1$. 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).

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 $\{a_1^{n_1} a_2^{n_2} \ldots a_k^{n_k}\}$? ¿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 $1 \le a_1 \le a_2 \le \ldots \le a_k \le n$. **Pista:** Use las variables auxiliares $x_1 = a_1 - 1$, $x_2 = a_2 - a_1$, $\ldots$, $x_{k+1} = n - a_k$.

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?

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?

    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:

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

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?

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?

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:

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

¿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`?

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?