E.T.S. DE INGENIERÍA INFORMÁTICA

PROGRAMA Y BOLETÍN DE PROBLEMAS

de

INTRODUCCIÓN
A LA
MATEMÁTICA DISCRETA

para la titulación de

INGENIERÍA INFORMÁTICA

Programa

Tema 1: Aritmética entera.

El conjunto $\mathbf{Z}$ de los números enteros. Definiciones recursivas. Inducción matemática: conjuntos inductivos, el método de inducción. Divisores. Máximo común divisor: algoritmo de Euclides. La identidad de Bezout. Mínimo común múltiplo. Ecuaciones diofánticas lineales. Números primos y factorización. Distribución de primos. Primos de Fermat y Mersenne. Test de primalidad y factorización.

Tema 2: Aritmética modular.

Aritmética modular. Congruencias lineales. Sistemas de congruencias lineales: Teorema Chino del Resto. La aritmética en $\mathbf{Z}_p$: el Pequeño Teorema de Fermat y el Teorema de Wilson. Test de pseudoprimalidad: pseudoprimos y números de Carmichael. Test de Lucas-Lehmer. La función de Euler. Aplicaciones: criptografía RSA.

Tema 3: Técnicas de contar.

El principio de adición. El principio de inclusión y exclusión. Contar en tablas. Funciones, palabras y variaciones: variaciones sin repetición y permutaciones. Números binómicos: combinaciones con repetición y Teorema del binomio.

Tema 4: Recursión.

Recurrencias lineales homogéneas. Recurrencias lineales no homogéneas con coeficientes constantes. Funciones generadoras.

Bibliografía

[1] Anderson, I. *Introducción a la combinatoria*. Ed. Vicens Vives, 1993.

[2] Biggs, N.L. *Matemática discreta*. Ed. Vicens Vives, 1994.

[3] Cobos Gavala, F.J. *Introducción a la Matemática Discreta*. Apuntes disponibles en la dirección:

http://ma1.eii.us.es/docencia/apuntes/Ap_IMD.pdf

[4] Grimaldi, R.P. *Matemáticas discreta y combinatoria*. Ed. Addison-Wesley Iberoamericana, 1989.

[5] Jones, G.A. y Jones, J.M. *Elementary Number Theory*. Springer-Verlag, 1998.

1. Aritmética entera

1.1 Ejercicios resueltos

Ejercicio 1.1 Probar que

$$1+3+\cdots+(2n-1)=n^2 \quad \forall\, n\in \mathbf{Z}^+$$

SOLUCIÓN: Para $n=1$ sólo aparece un sumando, verificándose que $1=1^2$.

Si suponemos que se verifica para n veamos que también se cumple para $n+1$ es decir, que

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

o lo que es lo mismo

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

En efecto:

$$1+\cdots+(2n-1)+(2n+1)=[1+\cdots+(2n-1)]+(2n+1)=$$
$$=n^2+(2n+1)=(n+1)^2$$

Por lo que la igualdad es cierta para cualquier $n\in\mathbf{Z}^+$. ■

Ejercicio 1.2 Probar mediante *inducción completa* que $a_n<\left(\frac{7}{4}\right)^n \ \forall\, n\in\mathbf{Z}^+$ donde (a_n) es la sucesión definida por $\begin{cases} a_1=1,\ a_2=3 \\ a_n=a_{n-1}+a_{n-2} \quad \forall\, n\geq 3 \end{cases}$

SOLUCIÓN: Los dos primeros términos verifican la proposición, ya que

$$a_1=1<\left(\frac{7}{4}\right)^1=\frac{7}{4}=1'75 \quad \text{y} \quad a_2=3<\left(\frac{7}{4}\right)^2=\frac{49}{16}=3'0625$$

por lo que basta probar, haciendo uso del método de inducción completa, que si la proposición es cierta para $n \leq k$ también lo es para $n = k+1$, es decir, que

$$a_n < \left(\frac{7}{4}\right)^n \ \forall\, n \leq k \implies a_{k+1} < \left(\frac{7}{4}\right)^{k+1}$$

Haciendo uso de las hipótesis de inducción tenemos que

$$a_{k+1} = a_k + a_{k-1} < \left(\frac{7}{4}\right)^k + \left(\frac{7}{4}\right)^{k-1} = \left(\frac{7}{4}\right)^{k-1} \cdot \left(\frac{7}{4} + 1\right)$$

Como $\dfrac{7}{4} + 1 = \dfrac{11}{4} = 2'75 < \left(\dfrac{7}{4}\right)^2 = 3'0625$, podemos asegurar que

$$a_{k+1} < \left(\frac{7}{4}\right)^{k-1} \cdot \left(\frac{7}{4} + 1\right) < \left(\frac{7}{4}\right)^{k-1} \cdot \left(\frac{7}{4}\right)^2 = \left(\frac{7}{4}\right)^{k+1}$$

Por lo que $\quad a_n < \left(\dfrac{7}{4}\right)^n \quad \forall\, n \in \mathbf{Z}^+$. ■

Ejercicio 1.3 Hallar la solución general de la ecuación $1485x + 1745y = 15$.

SOLUCIÓN:

$$d = \text{mcd}\,(1485, 1745) = 5 = 1485 \cdot (-47) + 1745 \cdot 40.$$

Como $d = 5$ divide a $c = 15$, la ecuación tiene solución. Además, se tiene que

$$1485 \cdot (-3 \cdot 47) + 1745 \cdot (3 \cdot 40) = 3 \cdot 5 \Longrightarrow 1485 \cdot (-141) + 1745 \cdot (120) = 15$$

por lo que una solución particular de la ecuación es $x_0 = -141$, $y_0 = 120$. La solución general viene dada por

$$\begin{cases} x = x_0 + \dfrac{bn}{d} = -141 + \dfrac{1745n}{5} = -141 + 349n, \\ y = y_0 - \dfrac{an}{d} = 120 - \dfrac{1485n}{5} = 120 - 297n. \end{cases} \qquad \forall\, n \in \mathbf{Z}$$

■

Ejercicio 1.4 Sea $c \in \mathbf{Z}^+$ con $10 \leq c \leq 1000$.

a) Determinar el mínimo valor de c para el que la ecuación $84x + 990y = c$ admite soluciones. Resolverla en dicho caso.

b) ¿Existe algún valor de c (en el rango especificado) para el que dicha ecuación admita soluciones positivas?

SOLUCIÓN:

a) Para que la ecuación tenga solución debe verificarse que mcd $(84, 990) = 6$ divida a c, por lo que el mínimo valor que puede tomar c es 12.

$$84x + 990y = 12 \iff 14x + 165y = 2$$

Si resolvemos la congruencia
$165y \equiv 2 \pmod{14} \iff 11y \equiv 2 \pmod{14} \iff -3y \equiv 2 \pmod{14}$
$\iff 15y \equiv -10 \pmod{14} \iff y \equiv 4 \pmod{14}$
obtenemos que

$$165 \cdot 4 - 2 = \dot{14} = 14 \cdot 47$$

o, lo que es lo mismo, que

$$14 \cdot (-47) + 165 \cdot 4 = 2$$

es decir, una solución particular de la ecuación es $x_0 = -47$ e $y_0 = 4$. Dado que la solución general de la ecuación $ax + by = c$ es

$$x = x_0 + \frac{bn}{d} \qquad y = y_0 - \frac{an}{d} \quad \text{donde} \quad d = \text{mcd}\,(a, b)$$

La solución general de la ecuación $84x + 990y = 12$ es

$$x = -47 + 165\,n \qquad y = 4 - 14\,n \quad \text{con} \quad n \in \mathbf{Z}$$

b) El mínimo valor que puede tomar la expresión $84x + 990y$ cuando x e y toman valores enteros positivos es 1074 (para $x = y = 1$), por lo que el mínimo valor que puede tomar c para que existan soluciones positivas es 1074, que se encuentra fuera del rango $10 \leq c \leq 1000$. Es decir, no existe ningún valor de $c \in \mathbf{Z}^+$ con $10 \leq c \leq 1000$ para el que la ecuación $84x + 990y = c$ admita soluciones enteras y positivas. ■

Ejercicio 1.5 Enviamos por correo dos tipos de paquetes A y B. Por enviar los del tipo A nos cobran 15 céntimos de euro más que por los del tipo B. Sabiendo que hemos enviado más paquetes del tipo B que del tipo A, que en total hemos enviado 12 paquetes y que nos han cobrado un total de 13 euros con 20 céntimos, ¿cuántos hemos enviado de cada tipo y qué nos han cobrado por cada uno?

SOLUCIÓN: Si denotamos por n al número de paquetes del tipo B y por p al precio, en céntimos de euro, que nos cobran por enviar cada uno de ellos, sabemos que los del tipo A serán $12 - n$ y nos cobrarán $p + 15$ céntimos de

euro por su envío.

Nos queda entonces que $pn + (p+15)(12-n) = 1320$ (expresando los precios en céntimos de euro), es decir

$$12p - 15n = 1140 \iff 4p - 5n = 380$$

Dado que mcd $(4,5) = 1 = 4\cdot(-1) - 5\cdot(-1) \implies 4\cdot(-380) - 5\cdot(-380) = 380$, la ecuación tiene como solución particular $n_0 = p_0 = -380$ y la solución general viene dada por

$$\left.\begin{array}{l} p = -380 + 5t \\ n = -380 + 4t \end{array}\right\} \forall\, t \in \mathbf{Z}$$

Como $n > 0$ y $12 - n > 0$ se obtiene que

$$-380 + 4t > 0 \implies t > 95$$

$$12 - (-380 + 4t) > 0 \implies t < 98$$

Las únicas soluciones posibles son, por tanto, $t = 96$ o $t = 97$.

Para $t = 96$ se obtiene que $n = 4$, es decir, se habrían enviado 4 paquetes del tipo B y 8 del tipo A, que contradice el hecho de que se han enviado más paquetes del tipo B que del A.

Para $t = 97$ obtenemos que $n = 8$ y $p = 105$, por lo que se han enviado 8 paquetes del tipo B a 1 euro con 5 céntimos cada uno y 4 del tipo A a 1 euro con 20 céntimos cada uno. ■

Ejercicio 1.6 Hallar todos los puntos enteros del primer octante $(x, y, z \geq 0)$ de la recta determinada por los planos

$$2x + 3y + 5z = 17$$
$$3x + 4y + 4z = 18$$

SOLUCIÓN: Eliminamos una de las incógnitas (por ejemplo la z) multiplicando la primera ecuación por 4, la segunda por 5 y restando; resultando el sistema equivalente al dado

$$2x + 3y + 5z = 17$$
$$7x + 8y = 22$$

La segunda ecuación es una diofántica que, dado que mcd $(7,8) = 1$ divide a 22, admite soluciones enteras.

Como $7 \cdot (-1) + 8 \cdot 1 = 1$ tenemos que $7 \cdot (-22) + 8 \cdot 22 = 22$ y, por tanto, una solución particular viene dada por

$$x_0 = -22 \quad y_0 = 22$$

y la solución general por

$$\begin{cases} x = -22 + 8t \\ y = \quad 22 - 7t \end{cases} \quad \forall\, t \in \mathbf{Z}$$

Al buscar sólo los valores no negativos han de ser

$$\left.\begin{array}{l} x = -22 + 8t \geq 0 \implies t \geq \dfrac{22}{8} = 2.75 \implies t \geq 3 \\ y = \quad 22 - 7t \geq 0 \implies t \leq \dfrac{22}{7} = 3.14 \implies t \leq 3 \end{array}\right\} \implies t = 3$$

obteniéndose que la única solución no negativa es $x = -22 + 8 \cdot 3 = 2$ e $y = 22 - 7 \cdot 3 = 1$, en cuyo caso obtenemos que

$$2x + 3y + 5z = 17 \implies 4 + 3 + 5z = 17 \implies 5z = 10 \implies z = 2$$

y, por tanto, el único punto de coordenadas enteras del primer octante de la recta dada es el $(2, 1, 2)$ ■

Ejercicio 1.7 Se considera la ecuación diofántica lineal $3x + 7y = c$ donde $c \in \mathbf{Z}^+$.

a) Hallar la solución general de la ecuación.

b) ¿Cúal es el mínimo valor que puede tomar c para que la ecuación posea soluciones positivas?

c) ¿A partir de qué valor de c podemos garantizar que la ecuación siempre va a tener soluciones positivas? (Independientemente de que para algún valor anterior también puede admitirla).

d) ¿Entre qué dos valores debe situarse c para poder garantizar la existencia de "dos" soluciones positivas, sin poder garantizar la existencia de una tercera? ¿Podría darse el caso de que para alguno de los valores encontrados tuviese tres soluciones positivas?

e) ¿Cuál es el mínimo valor que puede tomar c para que la ecuación admita soluciones pares (tanto "x" como "y" deben ser pares)? Hallar, para dicho valor de c todas las soluciones pares de la ecuación.

SOLUCIÓN:

a) Dado que mcd $(3, 7) = 1$ divide a c, la ecuación admite solución.

La identidad de Bezout nos dice que $3 \cdot (-2) + 7 \cdot 1 = 1$, por lo que $3 \cdot (-2c) + 7 \cdot c = c$, es decir, una solución particular de la ecuación es $x_0 = -2c$ e $y_0 = c$.

La solución general viene dada por

$$\left.\begin{array}{l} x = -2c + 7t \\ y = c - 3t \end{array}\right\} \quad \forall\, t \in \mathbf{Z}$$

b) La solución positiva más pequeña es $x = y = 1$, en cuyo caso $c = 10$.

c) Para que la ecuación admita soluciones positivas ha de verificarse que

$$\left.\begin{array}{l} x = -2c + 7t > 0 \\ y = c - 3t > 0 \end{array}\right\} \implies \left.\begin{array}{l} t > \dfrac{2c}{7} \\ t < \dfrac{c}{3} \end{array}\right\} \implies t \in \left(\frac{2c}{7}, \frac{c}{3}\right)$$

Teniendo en cuenta que el intervalo es abierto, la amplitud mínima que debe tener para garantizar la existencia de soluciones positivas es un número mayor que 1, por lo que

$$\frac{c}{3} - \frac{2c}{7} = \frac{c}{21} > 1 \implies c > 21$$

Así pues, sólo podemos garantizar que la ecuación siempre va a tener soluciones positivas positivas para valores de c mayores o igual a 22.

d) Si queremos que la ecuación admita dos soluciones positivas, el intervalo $\left(\frac{2c}{7}, \frac{c}{3}\right)$ debe tener una amplitud superior a 2 pero no superior a tres, ya que entonces se garantizarían tres soluciones positivas, es decir,

$$2 < \frac{c}{3} - \frac{2c}{7} = \frac{c}{21} \leq 3 \implies 42 < c \leq 63$$

por lo que el mínimo valor que puede tomar c es 43 y el máximo 63.

Es evidente que en un intervalo de amplitud mayor que 2 y menor que tres, existen, al menos, dos valores enteros, pero no quiere decir que no pueda haber tres, por lo que podría darse el caso de tres soluciones positivas.

Así, por ejemplo, para $c = 52$ el intervalo $\left(\frac{2c}{7}, \frac{c}{3}\right) = (14'8571, 17'3333)$ tiene de amplitud $2'4762$, pero en dicho intervalo hay tres valores enteros, el 15, el 16 y el 17.

e) Basta con hacer $x = 2x'$ e $y = 2y'$ para que el problema se reduzca a buscar cuándo va ha tener solución la ecuación

$$3(2x') + 7(2y') = c \iff 6x' + 14y' = c$$

Dado que mcd $(6, 14) = 2$, para que la ecuación admita solución, c ha de ser par, por lo que el mínimo valor que puede tomar es 2.

En ese caso, la ecuación se convierte en $6x' + 14y' = 2$ equivalente a $3x' + 7y' = 1$ cuya solución general (véase el primer apartado para $c = 1$) es

$$\begin{aligned} x' &= -2 + 7t \\ y' &= 1 - 3t \end{aligned}$$

por lo que las soluciones pares de la ecuación $3x + 7y = 2$ viene dadas por

$$\left.\begin{aligned} x = 2x' &= -4 + 14t \\ y = 2y' &= 2 - 6t \end{aligned}\right\} \quad \forall\, t \in \mathbf{Z}$$

■

Ejercicio 1.8 Probar que el polinomio $P(x) = x^2 + x + 1$ es irreducible. ¿Se pude aplicar, en este caso, el criterio de Eisenstein?

SOLUCIÓN: En este caso, no existe ningún primo que divida al término independiente, por lo que no se puede aplicar el criterio de Eisenstein. Sin embargo, como las raíces del polinomio son complejas, no puede descomponerse en producto de polinomios de primer grado con coeficientes enteros, por lo que es irreducible. ■

1.2 Ejercicios propuestos

Ejercicio 1.9 Utilizar el método de inducción para probar que para cualquier entero $n \geq 2$ se verifica que $2^n > n + 1$.

Ejercicio 1.10

a) Hacer una tabla de valores de $S_n = 1^3 + 2^3 + \cdots + n^3$ para $1 \leq n \leq 6$.

b) Inducir de la tabla una fórmula para S_n. *Sol*: $S_n = \dfrac{n^2(n+1)^2}{4}$.

c) Demostrar por inducción matemática la validez de la fórmula anterior. Si no se consigue, repetir la etapa b.

Ejercicio 1.11 Se considera la sucesión definida por $a_1 = 1$ y $a_n = a_{n-1} + n$ para $n \geq 2$.

a) Hacer uso del método de inducción para probar que $a_n + a_{n-1} = n^2$ cualquiera que sea el entero $n \geq 2$.

b) Determinar la fórmula explícita del término general de la sucesión (a_n). *Sol*: $a_n = \dfrac{n^2+n}{2}$.

Ejercicio 1.12 Demostrar por inducción que si u_n es la sucesión definida por:

$$u_1 = 3,\ u_2 = 5,\ u_n = 3u_{n-1} - 2u_{n-2} \quad \forall\, n \geq 3$$

entonces, $u_n = 2^n + 1 \ \ \forall\, n \in \mathbf{Z}^+$.

Ejercicio 1.13 Dada la sucesión de Fibonacci definida por

$$\begin{cases} f_1 = 1, \quad f_2 = 1 \\ f_n = f_{n-1} + f_{n-2} \quad \forall\, n \geq 3 \end{cases}$$

probar, por inducción en n, que f_{3n} es par cualquiera que sea $n \in \mathbf{Z}^+$.

Ejercicio 1.14 Dada la sucesión de Fibonacci definida por

$$\begin{cases} f_1 = 1, \quad f_2 = 1 \\ f_n = f_{n-1} + f_{n-2} \quad \forall\, n \geq 3 \end{cases}$$

probar, por inducción en n, que

$$\forall\, n \in \mathbf{Z}^+ \quad \text{es} \quad f_1 + f_3 + f_5 + \cdots + f_{2n-1} = f_{2n}$$

Ejercicio 1.15 Dada la sucesión de Fibonacci definida por

$$\begin{cases} f_1 = 1, \quad f_2 = 1 \\ f_n = f_{n-1} + f_{n-2} \quad \forall\, n \geq 3 \end{cases}$$

probar, por inducción en n, que $\displaystyle\sum_{i=1}^{n} f_i \cdot (f_i - 1) = (f_n - 1)(f_{n+1} - 1) \ \ \forall\, n \geq 1$.

Ejercicio 1.16 Se considera la sucesión de Fibonacci definida por

$$\begin{cases} f_0 = 0, \ f_1 = 1 \\ f_n = f_{n-1} + f_{n-2} \quad \forall\, n \geq 2 \end{cases}$$

a) Probar, por inducción en n, que si

$$F = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \implies F^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix} \quad \forall\, n \in \mathbf{Z}^+$$

b) Haciendo uso de la propiedad anterior, probar que $f_{n+1}f_{n-1} = f_n^2 + (-1)^n$ cualquiera que sea $n \in \mathbf{Z}^+$.

Ejercicio 1.17 ¿Si a divide a b, y c divide a d, debe $a + c$ dividir a $b + d$? Justifica la respuesta. *Sol*: Falso.

Ejercicio 1.18 Probar o encontrar un contraejemplo a las siguientes implicaciones

a) $a^3 \,|\, b^2 \implies a \,|\, b$ *Sol* : Cierta. b) $a^2 \,|\, b^3 \implies a \,|\, b$ *Sol* : Falsa.

Ejercicio 1.19 Expresar mcd $(1485, 1745)$ de la forma $1485u + 1745v$.
Sol: mcd $(1745, 1485) = 1745 \cdot 40 + 1485 \cdot (-47)$

Ejercicio 1.20 Probar que $c \,|\, a$ y $c \,|\, b$ si, y sólo si, $c \,|$ mcd (a, b).

Ejercicio 1.21 Probar que se verifica la igualdad

$$\text{mcd}\,(a_1, \ldots, a_k) = \text{mcd}\,(\text{mcd}\,(a_1, a_2), a_3, \ldots, a_k)$$

y que si $a_1, a_2, \ldots, a_k$ son enteros no nulos, existen enteros $u_1, \ldots, u_k$ para los que mcd $(a_1, \ldots, a_k) = a_1u_1 + \cdots + a_ku_k$.

Encontrar dicha expresión cuando $k = 3$ con $a_1 = 1092$, $a_2 = 1155$ y $a_3 = 2002$.
Sol: $u_1 = -1710$, $u_2 = 1615$ y $u_3 = 1$.

Ejercicio 1.22 Hallar mcd $(910, 780, 286, 195)$. *Sol*: 13.

Ejercicio 1.23 Probar que c es un múltiplo común de a y b si, y sólo si, es un múltiplo de $m = \text{mcm}\,(a, b)$.

Ejercicio 1.24 ¿Tiene soluciones enteras la ecuación $12x + 21y = 46$? Justifíquese la respuesta. *Sol*: No.

Ejercicio 1.25 Encontrar todas las soluciones positivas de la ecuación diofántica lineal $5x + 12y = 71$. *Sol*: $x = 7,\ y = 3$.

Ejercicio 1.26 Si $a_1, \ldots, a_k$ y c son números enteros, ¿cuándo tiene soluciones enteras $x_1, \ldots, x_k$ la ecuación diofántica $a_1x_1 + \cdots + a_kx_k = c$? Justifica la respuesta. *Sol*: Cuando el mcd $(a_1, \ldots, a_k)$ divide a c.

Ejercicio 1.27 Una determinada empresa desea emitir un anuncio por 2 cadenas de televisión con el objetivo de que sea visto diariamente por 910 personas. Al realizar un estudio de audiencia de las dos cadenas se sabe que cada vez que se emite en la primera cadena CTV1 va a ser visto por 325 personas, mientras que en la segunda CTV2 sólo será visto por 26. ¿Cuántas veces al día debe emitirse en cada una de las cadenas para cubrir el objetivo previsto de las, exactamente, 910 personas teniendo en cuenta que CTV1 cobra 600 euros cada vez que lo emite y CTV2 sólo cobra 60?

Sol: 2 veces al día por CTV1 y 10 por CTV2.

Ejercicio 1.28 Un coleccionista de obras de arte ha adquirido varios cuadros y dibujos de un artista moderno. Las pinturas le han costado 649 euros cada una y los dibujos se los han dejado a 132 euros cada uno. Cuando el coleccionista llega a su casa, no recuerda si el coste total de las obras de arte ha sido de 2716 o 2761 euros.

a) ¿Cuánto les han costado exactamente? *Sol*: 2761 euros.

b) ¿Cuántos cuadros y cuantos dibujos ha comprado? *Sol*: 1 cuadro y 16 dibujos.

Ejercicio 1.29 La unidad monetaria de Interia es el "*interio*" existiendo únicamente billetes de 18, 20 y 45 interios.

a) Probar que se puede realizar una compra por cualquier cantidad entera.

b) ¿Cómo podría pagarse 1 interio? ¿es única la solución? Justifica la respuesta.

Ejercicio 1.30 La compañía Cabitele nos cobra por llamar desde una de sus cabinas 50 céntimos de euro el minuto por una llamada a Madrid y 1 euro

con 20 céntimos si es a París. No contabiliza fracciones, es decir, por 1 minuto y 1 segundo nos cobra 2 minutos.

Si la cabina no devuelve cambio pero podemos (sin colgar) volver a marcar otro teléfono mientras exista crédito, ¿se pueden consumir 10 euros sin perder dinero y sin que se nos corte la llamada teniendo en cuenta que queremos hablar necesariamente con dos personas, una que se encuentra en Madrid y otra que se encuentra en Paris? ¿Cuántos minutos podremos hablar con cada una de ellas? ¿Existe más de una solución?

Sol: 8 minutos con Madrid y 5 con París solución única.

Ejercicio 1.31 Determinar el valor del mcd $(1066, 1492)$ y mcd $(1485, 1745)$ mediante el *algoritmo del mínimo resto* y comparar el número de pasos requeridos por este algoritmo con los que se requieren con el algoritmo de Euclides.

Sol: Euclides 5 y mínimo resto 4. Euclides 6 y mínimo resto 5.

Ejercicio 1.32 Probar que si p es primo y $p \mid a^k$, entonces $p \mid a$ y, por tanto, $p^k \mid a^k$; ¿es también válido si p es compuesto? *Sol*: Si p es compuesto no es válido.

Ejercicio 1.33 Aplicar el criterio de Eisenstein para probar que el polinomio $P(x) = x^3 - 4x + 2$ es irreducible. *Sol*: Se verifica el criterio para $p = 2$.

Ejercicio 1.34 ¿Cuáles de las siguientes proposiciones son verdaderas y cuáles falsas, donde a y b son enteros positivos y p primo? En cada caso, dar una demostración o un contraejemplo.

a) Si mcd $(a, p^2) = p$ entonces mcd $(a^2, p^2) = p^2$. *Sol*: V.

b) Si mcd $(a, p^2) = p$ y mcd $(b, p^2) = p^2$ entonces mcd $(ab, p^4) = p^3$. *Sol*: F.

c) Si mcd $(a, p^2) = p$ y mcd $(b, p^2) = p$ entonces mcd $(ab, p^4) = p^2$. *Sol*: V.

d) Si mcd $(a, p^2) = p$ entonces mcd $(a + p, p^2) = p$. *Sol*: F.

Ejercicio 1.35 Probar que si $a \geq 2$ y $a^m + 1$ es primo (como por ejemplo $37 = 6^2 + 1$), entonces a es par y m es una potencia de 2.

Ejercicio 1.36 Usar la criba de Eratóstenes para hallar todos los primos menores que 100.

Ejercicio 1.37 ¿Para qué primos p es también primo p^2+1?

Ejercicio 1.38 Probar que si $p > 1$ y p divide a $(p-1)!+1$, entonces p es primo.

Ejercicio 1.39 Se consideran los números de Fermat $F_n = 2^{2^n}+1$. Probar, mediante inducción en n, que

$$F_0 F_1 \cdots F_{n-1} = F_n - 2. \quad \forall\, n \geq 1$$

Ejercicio 1.40 Sean p y q dos números primos con $p > q$ y tales que $p \cdot q + 1$ también es primo. Probar, razonadamente, las siguientes afirmaciones:

a) q ha de ser, necesariamente, 2.

b) Si $p \neq 3$ entonces $p+1$ es múltiplo de 6.

c) Si $p \neq 3$, p no puede ser un primo de Mersenne.

d) Probar que los números F_n de Fermat verifican la recurrencia

$$\begin{cases} F_0 = 3 \\ F_n = (F_{n-1}-1)^2 + 1 \quad \forall\, n \geq 1 \end{cases}$$

y hacer uso de dicha propiedad para probar que si $n \geq 3$ entonces F_n termina en 7.

e) Si $p \neq 3$ y $p \neq 5$, p no puede ser un primo de Fermat.

Ejercicio 1.41 Demostrar que todo número primo mayor que 3 es de la forma $6n+1$ o $6n+5$.

Ejercicio 1.42 Probar que si $n, q \geq 1$, el número de múltiplos de q entre $1, 2, \ldots, n$ es $\lfloor n/q \rfloor$. Utilizar este resultado para probar que si p es primo y $p^e \,||\, n!$, entonces

$$e = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \cdots.$$

¿En cuántos ceros termina la expresión decimal de 1000!? *Sol*: 249.

Ejercicio 1.43 Contestar *razonadamente* a las siguientes cuestiones independientes.

a) ¿Es cierto que dos números enteros positivos y consecutivos son siempre primos entre sí? ¿y dos impares consecutivos?

b) Se dice que dos números primos son *gemelos* si son impares consecutivos, por ejemplo 3 y 5, 5 y 7, 11 y 13, etc. ¿Es posible encontrar tres números impares consecutivos (además de 3, 5 y 7) de forma que los tres sean primos?

c) ¿Puede hacerse la diferencia entre dos números primos consecutivos tan grande como se quiera (mayor que cualquier entero positivo n por grande que éste sea)?

2. Aritmética modular

2.1 Ejercicios resueltos

Ejercicio 2.1 Probar, mediante congruencias, que $3^{2n+5} + 2^{4n+1}$ es divisible por 7 cualquiera que sea el entero $n \geq 1$.

SOLUCIÓN: Trabajando módulo 7 se tiene que

$$3^{2n+5} + 2^{4n+1} = 3^5 \cdot 3^{2n} + 2 \cdot 2^{4n} = 243 \cdot 9^n + 2 \cdot 16^n \equiv 5 \cdot 2^n + 2 \cdot 2^n = 7 \cdot 2^n \equiv 0$$

es decir, 7 divide a $3^{2n+5} + 2^{4n+1}$. ■

Ejercicio 2.2

a) Probar que el número inmediatamente posterior a cualquier potencia de 5 es múltiplo de 2 pero no de 4.

b) Probar, por inducción en n, que si denotamos por $p^m \parallel N$ a la **mayor** potencia del primo p que divide a N (así, por ejemplo, $2^3 \parallel 40$ ya que $2^3 = 8$ es un divisor de 40 pero $2^4 = 16$ no lo es), se verifica que $2^{n+2} \parallel 5^{2^n} - 1$ para cualquier $n \in \mathbf{Z}^+$.
Indicación: recuérdese que $a^{2k} - 1 = (a^k - 1)(a^k + 1)$.

SOLUCIÓN:

a) $\left.\begin{array}{l} 5 \equiv 1 \pmod 2 \\ 5 \equiv 1 \pmod 4 \end{array}\right\} \Longrightarrow$ para cualquier $n \in \mathbf{Z}^+$ es $\left\{\begin{array}{l} 5^n \equiv 1 \pmod 2 \\ 5^n \equiv 1 \pmod 4 \end{array}\right.$, por lo que $\left\{\begin{array}{l} 5^n + 1 \equiv 0 \pmod 2 \\ 5^n + 1 \equiv 2 \pmod 4 \end{array}\right.$ es decir, el numero inmediatamente posterior a cualquier potencia de 5 es divisible por 2 pero no por 4.

b) Para $n = 1$ se tiene que $2^3 = 2^{1+2} \parallel 5^{2^1} - 1 = 24$.
Supongámoslo cierto para n y vamos a probarlo para $n+1$. Debemos probar que

$$2^{(n+1)+2} = 2^{n+3} \parallel 5^{2^{n+1}} - 1 = 5^{2\cdot 2^n} - 1 = (5^{2^n} - 1)(5^{2^n} + 1).$$

Dado que por hipótesis de inducción es $2^{n+2} \parallel 5^{2^n} - 1$ y además $2^1 \parallel 5^{2^n} + 1$, ya que se trata del número inmediatamente posterior a una potencia de 5, se deduce que $2^{n+3} \parallel 5^{2^{n+1}} - 1$, lo que prueba el resultado. ■

Ejercicio 2.3 Sean a, b y c tres enteros positivos tales que $a \mid b$. Si al dividir c entre a obtenemos un resto r y al dividir c entre b un resto s, ¿qué resto se obtiene de la división de s entre a?

a) Razonar el ejercicio haciendo uso del algoritmo de la divisibilidad y no de congruencias.

b) Repetirlo haciendo uso de congruencias y no del algoritmo de la divisibilidad.

SOLUCIÓN:

a) Sabemos que

$$\begin{array}{llllll} c = a \cdot q_1 + r & \text{con} & q_1 \in \mathbf{Z} & \text{y} & 0 \leq r < a \\ c = b \cdot q_2 + s & \text{con} & q_2 \in \mathbf{Z} & \text{y} & 0 \leq s < b \end{array}$$

por lo que

$$a \cdot q_1 + r = b \cdot q_2 + s \implies a \cdot q_1 - b \cdot q_2 = s - r$$

como $a \mid b$ podemos expresar b de la forma $b = a \cdot b'$ con $b' \in \mathbf{Z}$ y, por tanto

$$s - r = a \cdot q_1 - a \cdot b' \cdot q_2 = a \cdot (q_1 - b' \cdot q_2) = a \cdot q \quad \text{con} \quad q = q_1 - b' \cdot q_2 \in \mathbf{Z}$$

es decir, $s = a \cdot q + r$ con $0 \leq r < a$, por lo que el resto de dividir s entre a es también r.

b) Sabemos que $\begin{cases} c \equiv r \pmod{a} \\ c \equiv s \pmod{b} \end{cases}$

De la segunda ecuación tenemos que $c = s + bt$ con $t \in \mathbf{Z}$, que llevada a la primera nos da

$$s + bt \equiv r \pmod{a}$$

como, por otra parte $a \mid b$ se tiene que $b \equiv 0 \pmod{a}$, por lo que la ecuación anterior se reduce a

$$s \equiv r \pmod{a}$$

es decir, el resto de dividir s entre a es r. (Obsérvese que $0 \leq r < a$ por tratarse del resto de la división de c entre a). ■

Ejercicio 2.4 ¿Puede conocerse un entero positivo sabiendo que es menor que 100 y conociendo los restos de sus divisiones entre 3, 5 y 7?

SOLUCIÓN: Basta con resolver el sistema de congruencias

$$x \equiv a \pmod{3} \quad x \equiv b \pmod{5} \quad x \equiv c \pmod{7}$$

que tiene solución única en $\mathbf{Z}_{105}$.
Procediendo como en los ejercicios anteriores, la solución general viene dada por $x = -35a + 21b + 15c + 105t$ con $t \in \mathbf{Z}$. De entre todas las soluciones nos quedaremos con la que se encuentra en el rango $1 \leq x \leq 100$. Así, por ejemplo, si los restos son 2, 2 y 5 respectivamente, $x = -70+42+75+105t = 47+105t$, por lo que el número buscado es 47. ■

Ejercicio 2.5 Dado el sistema:

$$\begin{cases} x \equiv 4 \pmod{8} \\ x \equiv a \pmod{6} \\ x \equiv -1 \pmod{15} \end{cases}$$

a) Determinar todos los posibles valores del parámetro $a \in \mathbf{Z}$ que hacen que el sistema tenga solución.

b) Probar que la solución del sistema, en caso de tener solución, es independiente del parámetro a.

c) Resolver el sistema en los casos en que tiene solución.

SOLUCIÓN:

a) Las condiciones que se deben cumplir para que el sistema tenga solución son:

$$\text{mcd}\,(8,6) = 2 \mid (4-a) \Longrightarrow 2 \mid a \Longrightarrow a \equiv 0 \pmod{2}$$
$$\text{mcd}\,(6,15) = 3 \mid (a+1) \Longrightarrow a+1 \equiv 0 \pmod{3} \Longrightarrow a \equiv 2 \pmod{3}$$

De la segunda ecuación se obtiene que $a = 2 + 3u$, que llevada a la primera nos da $2 + 3u \equiv 0 \pmod 2 \iff u \equiv 0 \pmod 2$, es decir, $u = 2t$.
La solución del sistema vendrá dada por $a = 2+3(2t) = 2+6t$ cualquiera que sea $t \in \mathbf{Z}$. Así pues, el sistema tiene solución siempre que $a = 2+6t$ con $t \in \mathbf{Z}$.

b) Teniendo en cuenta que, para cualquier valor de parámetro $a = 2+6t$ que hace que el sistema tenga solución, la segunda ecuación se convierte en $x \equiv 2 + 6t \pmod 6$ que es equivalente a $x \equiv 2 \pmod 6$, dicha solución es independiente del valor del parámetro $a = 2 + 6t$.

c) El sistema ha quedado de la forma

$$x \equiv 4 \pmod 8 \quad x \equiv 2 \pmod 6 \quad x \equiv -1 \pmod{15}$$

equivalente a

$$\begin{array}{lll} x \equiv 4 \pmod{2^3} & x \equiv 2 \pmod 2 & x \equiv -1 \pmod 3 \\ & x \equiv 2 \pmod 3 & x \equiv -1 \pmod 5 \end{array}$$

y como sabemos que tiene solución, vuelve a ser equivalente a

$$x \equiv 4 \pmod{2^3} \quad x \equiv 2 \pmod 3 \quad x \equiv -1 \pmod 5$$

o lo que es lo mismo

$$x \equiv 4 \pmod 8 \quad x \equiv 2 \pmod 3 \quad x \equiv 4 \pmod 5$$

De la primera se obtiene que $x = 4 + 8u$, que llevada a la tercera nos queda

$$4 + 8u \equiv 4 \pmod 5 \iff 3u \equiv 0 \pmod 5 \iff u \equiv 0 \pmod 5$$

es decir, $u = 5v \implies x = 4 + 8(5v) = 4 + 40v$.

Obligando ahora a que cumpla la segunda:

$$4 + 40v \equiv 2 \pmod 3 \iff v \equiv 1 \pmod 3$$

de donde $v = 1 + 3t$ y, por tanto $x = 4 + 40(1 + 3t) = 44 + 120t$.

La solución es, por tanto $x = 44 + 120t$ cualquiera que sea $t \in \mathbf{Z}$. ■

Ejercicio 2.6 Determinar los dígitos x e y del número $n = 59x7y8$ sabiendo que es divisible por 123.

SOLUCIÓN: Al ser divisible por 123 sabemos que

$$59x7y8 \equiv 0 \pmod{123} \implies 590708 + 1000x + 10y \equiv 0 \pmod{123}$$

es decir

$$62 + 16x + 10y \equiv 0 \pmod{123} \iff 31 + 8x + 5y \equiv 0 \pmod{123}$$

ya que 2 es primo con 123.

Por otra parte, dado que $0 \leq x, y \leq 9$ sabemos que

$$31 \leq 31 + 8x + 5y \leq 148$$

Como el único múltiplo de 123 que existe en dicho intervalo es el propio 123, se tiene que

$$31 + 8x + 5y = 123 \iff 8x + 5y = 92$$

Al ser mcd $(8, 5) = 1 = 8 \cdot 2 + 5 \cdot (-3)$, la ecuación tiene solución, siendo una solución particular

$$x_0 = 2 \cdot 92 = 184 \quad \text{y} \quad y_0 = -3 \cdot 92 = -276$$

La solución general viene dada por

$$\left.\begin{array}{l} x = 184 + 5t \\ y = -276 - 8t \end{array}\right\} \quad \forall\, t \in \mathbf{Z}$$

Como $0 \leq y \leq 9$ se tiene que

$$0 \leq -276 - 8t \leq 9 \iff 276 \leq -8t \leq 285$$

es decir

$$34'5 \leq -t \leq 35'625 \iff -35'625 \leq t \leq -34'5$$

siendo -35 el único número entero de dicho intervalo, por lo que $t = -35$, obteniéndose que

$$x = 9, \quad y = 4 \quad \text{y} \quad n = 599748 = 123 \cdot 4876$$

■

Ejercicio 2.7 Juan saca a pasear a su perro cada 6 horas y Pedro cada 10. Si Juan lo ha sacado a las 8 de la mañana y Pedro a las 12,

a) ¿Cuál es la última hora de la mañana a la que puede sacar su perro Luis si quiere sacarlo cada 15 horas y no coincidir nunca ni con Juan ni con Pedro?

b) ¿A qué hora de la tarde debería sacarlo si quisiera coincidir con ambos? y ¿cuándo coincidirían?

SOLUCIÓN:

a) Los datos que nos dan para Juan y Pedro se traducen en

$$\begin{array}{rcl} x \equiv 8 \pmod 6 & \iff & x \equiv 2 \pmod 6 \\ x \equiv 12 \pmod{10} & \iff & x \equiv 2 \pmod{10} \end{array}$$

La ecuación para Luis es $x \equiv a \pmod{15}$ y debe resultar incompatible con las dos anteriores.

Para ser incompatible con la de Juan $\text{mcd}\,(15, 6) = 3$ no debe dividir a $a-2$ y para ser incompatible con la de Pedro, $\text{mcd}\,(15, 10) = 5$ tampoco debe dividir a $a - 2$.

Si lo sacase a las 12 ($a = 12$) no resultaría incompatible con la de Pedro y si lo hiciese a las 11 no lo sería con la de Juan, por lo que la última hora de la mañana a la que deberá sacar al perro son las 10 ya que 3 no divide a $10 - 2 = 8$ y 5 tampoco divide a 8, por lo que nunca coincidiría ni con Juan ni con Pedro.

b) Para que con $12 < a \leq 24$ resulte que $a - 2$ sea divisible por 3 y por 5 ha de ser $a - 2 = 15$ es decir, $a = 17$, por lo que si lo saca a las 5 de la tarde habrá un momento en el que coincidan los tres.

El sistema quedaría entonces

$$\left.\begin{array}{rcl} x \equiv 8 \pmod 6 & \iff & x \equiv 2 \pmod 6 \\ x \equiv 12 \pmod{10} & \iff & x \equiv 2 \pmod{10} \\ x \equiv 17 \pmod{15} & \iff & x \equiv 2 \pmod{15} \end{array}\right\} \implies x \equiv 2 \pmod{30}$$

por lo que coincidirían, por primera vez a las 32 horas, es decir, mañana a las 8 de la mañana y volverían a hacerlo cada 30 horas. ■

Ejercicio 2.8 Para todo $n \in \mathbf{N}$, sea $A_n = 2^n + 4^n + 8^n$.

a) Probar que si $n \equiv m \pmod 3$ entonces $A_n \equiv A_m \pmod 7$.

b) Probar, sin hallar su expresión decimal, que el número cuya expresión en binario viene dada por 1000100010000, es divisible entre 7.

SOLUCIÓN:

a) Supongamos, sin pérdida de generalidad que $m > n$. Si $n \equiv m \pmod 3$ es $m = n + 3p$ con $p \in \mathbf{N}$. Entonces:

$$\begin{aligned} A_m - A_n &= 2^{n+3p} + 4^{n+3p} + 8^{n+3p} - 2^n - 4^n - 8^n = \\ &= 2^n(8^p - 1) + 4^n(8^{2p} - 1) + 8^n(8^{3p} - 1) \end{aligned}$$

Como $x^p - 1$ es divisible entre $x - 1$ cualquiera que sea $p \in \mathbf{N}$,

$$8^p - 1,\ 8^{2p} - 1 \text{ y } 8^{3p} - 1 \text{ son divisibles entre } 8 - 1 = 7$$

por lo que $A_m - A_n = \dot{7}$ y por tanto $A_n \equiv A_m \pmod 7$.

b) El número cuya expresión en binario es 1000100010000 es en sistema decimal $2^4 + 2^8 + 2^{12} = 2^4 + 4^4 + 8^4 = A_4$ y como $4 \equiv 1 \pmod 3$ se verifica que $A_4 \equiv A_1 \pmod 7$.

Como $A_1 = 2 + 4 + 8 = 14 = \dot{7}$, se verifica que A_4 es divisible por 7. ■

Ejercicio 2.9 Hallar tres números primos p_1, p_2 y p_3, con

$$5 < p_1 < p_2 < p_3 < 37$$

tales que $n = p_1 \cdot p_2 \cdot p_3$ y $m = 37 \cdot p_1 \cdot p_2 \cdot p_3$ sean números de Carmichael.

SOLUCIÓN: Al ser $p_1 < p_2 < p_3 < 37$ ambos números son libres de cuadrados, por lo que serán de Carmichael si

$$\begin{aligned} &n \equiv 1 \pmod{(p_1 - 1)} \\ &n \equiv 1 \pmod{(p_2 - 1)} \\ &n \equiv 1 \pmod{(p_3 - 1)} \\ &m = 37n \equiv 1 \pmod{(p_1 - 1)} \\ &m = 37n \equiv 1 \pmod{(p_2 - 1)} \\ &m = 37n \equiv 1 \pmod{(p_3 - 1)} \\ &m = 37n \equiv 1 \pmod{36} \end{aligned}$$

$$\left.\begin{aligned} &n \equiv 1 \pmod{(p_1 - 1)} \\ &m = 37n \equiv 1 \pmod{(p_1 - 1)} \end{aligned}\right\} \implies 37 \equiv 1 \pmod{(p_1 - 1)} \implies p_1 - 1 \,|\, 36$$

$$\left.\begin{aligned} &n \equiv 1 \pmod{(p_2 - 1)} \\ &m = 37n \equiv 1 \pmod{(p_2 - 1)} \end{aligned}\right\} \implies 37 \equiv 1 \pmod{(p_2 - 1)} \implies p_2 - 1 \,|\, 36$$

$$\left.\begin{aligned} &n \equiv 1 \pmod{(p_3 - 1)} \\ &m = 37n \equiv 1 \pmod{(p_3 - 1)} \end{aligned}\right\} \implies 37 \equiv 1 \pmod{(p_3 - 1)} \implies p_3 - 1 \,|\, 36$$

Los divisores de 36 son: 1, 2, 3, 4, 6, 9, 12, 18 y 36 por lo que los posibles valores de p_i son 2, 3, 4, 5, 7, 10, 13, 19 y 37. Al tratarse de primos mayores que 5 y menores que 37, sólo nos queda la posibilidad de que

$$p_1 = 7, \quad p_2 = 13 \quad \text{y} \quad p_3 = 19$$

es decir:

$$n = 7 \cdot 13 \cdot 19 = 1729 \quad \text{y} \quad m = 7 \cdot 13 \cdot 19 \cdot 37 = 63973.$$

Es fácil comprobar que también se verifica la última ecuación (no utilizada)

$$37n = 37 \cdot 1729 \equiv 1729 \equiv 1 \pmod{36}.$$ ■

Ejercicio 2.10 ¿Para qué valores de n es $\phi(n) \equiv 2 \pmod 4$?

SOLUCIÓN: Sabemos que

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \Longrightarrow \phi(n) = p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1) \cdots (p_k - 1).$$

Dado que $\phi(n)$ es par y no es múltiplo de 4, sólo pueden darse una de las siguientes posibilidades:

a) Si n es par $\Rightarrow$
$$\begin{cases} \text{Si } n = 2^\alpha & \Rightarrow \phi(n) = 2^{\alpha-1} \Rightarrow \alpha = 2 \Rightarrow n = 2^2 = 4 \\ \text{Si } n = 2^\alpha p^\beta & \Rightarrow \phi(n) = 2^{\alpha-1} p^{\beta-1}(p-1) \\ & \Rightarrow \alpha = 1,\ p - 1 \equiv 2 \pmod 4 \\ & \Rightarrow n = 2 \cdot p^\beta \text{ con } p \text{ primo tal que p=4a+3} \end{cases}$$

b) Si n es impar $n = p^\alpha$ con p primo tal que $p = 4a + 3$. ■

2.2 Ejercicios propuestos

Ejercicio 2.11 Sin realizar los productos, calcular los restos de dividir:

a) 28×33 entre 35. *Sol*: 14.

b) 15×59 entre 75. *Sol*: 60.

c) 3^8 entre 13. *Sol*: 9.

d) 5^{28574} entre 17. *Sol*: 15.

e) 35^{346} entre 41. *Sol*: 2.

Ejercicio 2.12 Sin hacer uso de una calculadora, encontrar el resto de dividir:

a) 34×17 entre 29. *Sol*: 27.

b) 19×14 entre 23. *Sol*: 13.

c) 5^{10} entre 19. *Sol*: 5.

d) $1! + 2! + 3! + \cdots + 10!$ entre 10. *Sol*: 3.

Ejercicio 2.13 Probar que los siguientes polinomios no tienen raíces enteras:

a) $x^3 - x + 1$

b) $x^3 + x^2 - x + 1$

c) $x^3 + x^2 - x + 3$

d) $x^5 - x^2 + x - 3$.

Ejercicio 2.14 Hallar la solución general de la congruencia $12x \equiv 9 \pmod{15}$. *Sol*: $x = 2 + 5\,t \ \forall\, t \in \mathbf{Z}$.

Ejercicio 2.15 Para cada una de las siguientes congruencias, decidir cuáles tienen solución y cuáles no, encontrando la solución general.

a) $3x \equiv 5 \pmod{7}$. *Sol*: $x = 4 + 7\,t \ \ \forall\, t \in \mathbf{Z}$.

b) $12x \equiv 15 \pmod{22}$. *Sol*: Carece de soluciones enteras.

c) $19x \equiv 42 \pmod{50}$. *Sol*: $x = 10 + 50\,t \ \ \forall\, t \in \mathbf{Z}$.

d) $18x \equiv 42 \pmod{50}$. *Sol*: $x = 19 + 25\,t \ \ \forall\, t \in \mathbf{Z}$.

Ejercicio 2.16

a) Probar que si a es una "unidad" de Z_n entonces mcd $(a, n) = 1$.

b) Probar que si $a^m \equiv 1 \pmod{n}$ con $m \in \mathbf{Z}$ y $m \geq 2$, entonces

$$\text{mcd}\,(a, n) = 1.$$

c) Si a no es una unidad de Z_{26} y $a^{10} \equiv 10 \pmod{26}$, ¿cuánto puede valer el mcd $(a, 26)$? *Sol*: 2.

Ejercicio 2.17 Si $x \equiv 2 \pmod 3$ y $x \equiv 3 \pmod 5$, ¿cuánto es $x \bmod 15$? *Sol*: 8.

Ejercicio 2.18 Resolver el sistema de congruencias

$$x \equiv 1 \pmod 4, \quad x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5.$$

Sol: $x = 53 + 60\,t \ \ \forall\, t \in \mathbf{Z}$.

Ejercicio 2.19 Resolver el sistema de congruencias

$$x \equiv 2 \pmod 7, \quad x \equiv 7 \pmod 9, \quad x \equiv 3 \pmod 4.$$

Sol: $x = 79 + 252\,t \ \ \forall\, t \in \mathbf{Z}$.

Ejercicio 2.20 Resolver el sistema de congruencias

$$3x \equiv 6 \pmod{12}, \quad 2x \equiv 5 \pmod 7, \quad 3x \equiv 1 \pmod 5.$$

Sol: $x = 62 + 140\,t \ \ \forall\, t \in \mathbf{Z}$.

Ejercicio 2.21 Resolver la congruencia $91x \equiv 419 \pmod{440}$.

Sol: $x = 169 + 440\,t \ \ \forall\, t \in \mathbf{Z}$. (Transformarla en un sistema).

Ejercicio 2.22 Hallar la solución general de la congruencia

$$54\,x \equiv 342 \pmod{23400}.$$

Sol: $x = 873 + 1300\,t \ \ \forall\, t \in \mathbf{Z}$. (Transformarla en un sistema).

Ejercicio 2.23 Determinar cuáles de los siguientes sistemas de congruencias tienen solución y, en caso de tenerla, encontrar la solución general:

a) $x \equiv 1 \pmod 6, \quad x \equiv 5 \pmod{14}, \quad x \equiv 4 \pmod{21}$.

Sol: No tiene solución.

b) $x \equiv 1 \pmod 6, \quad x \equiv 5 \pmod{14}, \quad x \equiv -2 \pmod{21}$.

Sol: $x = 19 + 42\,t \ \ \forall\, t \in \mathbf{Z}$.

c) $x \equiv 13 \pmod{40}, \quad x \equiv 5 \pmod{44}, \quad x \equiv 38 \pmod{275}$.

Sol: $x = 1413 + 2200\,t \ \ \forall\, t \in \mathbf{Z}$.

Ejercicio 2.24 Resolver el sistema de congruencias:

$$x \equiv 1 \pmod 4, \quad x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5.$$

Sol: $x = 53 + 60\,t \quad \forall\, t \in \mathbf{Z}$.

Ejercicio 2.25 Hallar el valor de n sabiendo que se trata del menor múltiplo de 4, no inferior a 250, que da de resto 4 tanto si lo dividimos entre 6 como si lo hacemos entre 9. *Sol*: 256.

Ejercicio 2.26 Siete ladrones tratan de repartir, entre ellos y a partes iguales, un botín de lingotes de oro. Desafortunadamente, sobran seis lingotes y en la pelea que se desata muere uno de ellos. Como al hacer de nuevo el reparto sobran dos lingotes, vuelven a pelear y muere otro. En el siguiente reparto vuelve a sobrar una barra y sólo después de que muera otro es posible repartirlas por igual. ¿Cuál es el mínimo número de barras para que esto ocurra? *Sol*: 356.

Ejercicio 2.27 Una banda de 20 piratas trata de repartirse un botín de entre 5000 y 10000 monedas de oro. Al intentar hacer un reparto equitativo les sobran 15 monedas que se disputan entre ellos y como consecuencia de la pelea muere uno de los piratas. Deciden hacer de nuevo un reparto equitativo pero les vuelven a sobrar 15 monedas. En una nueva disputa vuelve a morir otro de los piratas y al volver a efectuar el reparto les sobran 3 monedas.

a) Calcular el número de monedas del botín. *Sol*: 7995.

b) Si la historia continúa, es decir, siempre que sobren monedas se organiza una reyerta y muere uno de los piratas, ¿cuántos quedarán vivos cuando en el reparto no sobre ninguna moneda? La respuesta no tendrá validez si se calcula eliminando sucesivamente piratas hasta dar con la solución. *Sol*: 15.

Ejercicio 2.28 Se dispone de una cantidad par de monedas. Si formamos montones de 17 monedas cada uno nos sobran 8 monedas, mientras que si, con la mitad de las monedas iniciales, se forman montones de 7 nos sobran 3. Calcular la cantidad de monedas de que se disponía sabiendo que su número era inferior a 600. En caso de existir más de una solución ¿existe alguna de ellas para la que $7^N \bmod 31 = p$ donde N representa la solución buscada y p un número primo? ¿Es ahora única la solución?

Sol: 76, 314 o 552. Sólo el 76 cumple la condición.

Ejercicio 2.29 Laura trabaja cuatro días seguidos y descansa al quinto. María trabaja dos y descansa al tercero.

a) Si sólo se ven cuando ambas descansan y hay Luna llena (la Luna tiene un período de 28 días) ¿cuándo volverán a verse si María descansó ayer, Laura lo hará pasado mañana y hace diez días que hubo Luna llena? *Sol*: Dentro de 242 días.

b) Hasta esa fecha, ¿cuántos días habrán descansado ambas pero no se habrán visto por falta de Luna llena? *Sol*: 16 veces.

Ejercicio 2.30

a) Resolver el sistema de congruencias $\begin{cases} 3x \equiv 2 \pmod 7 \\ 21x \equiv 15 \pmod{30} \\ 6x \equiv 5 \pmod{25} \end{cases}$

Sol: $x = 255 + 350\,t \quad \forall\, t \in \mathbf{Z}$.

b) Probar que si x es una solución cualquiera del sistema anterior, existen enteros α y β tales que $x\alpha + 28\beta = 1$.

Sol: Probar que cualquier solución es prima con 28 y aplicar Bezout.

Ejercicio 2.31 Altea miró a Gaia, su superior, y dijo: creo que sólo falta un mes para producirse la próxima conjunción de Cuzco, Inca y Machu Picchu y aún alcanzaremos a ver la siguiente antes de que nos releven.

Sí, gracias –contestó Gaia–. Para su interior pensó cuán equivocado estaba Altea. Se encontraban desde hacía 36 años y 26 meses siderales (recuérdese que el año sideral tenía 60 meses siderales, cada uno de 60 días estándares, los cuales, a su vez, tenían 60 horas cada una de 60 minutos) en una base espacial en el sistema solar de Manco Cápac, a más de un millón de parsecs de casa.

El sistema de Manco Cápac disponía de un sol mas bien pequeño y tres planetas: Cuzco, que se alineó con la base por primera vez 0.2 años después de llegar ellos y que volvería a hacerlo cada 15 meses; Inca que se alineó, por primera vez, con la base a los 3 meses de su llegada y que volvería a hacerlo cada 840 días y finalmente, Machu Picchu, cuya primera alineación la observaron a los 0.15 años de su estancia en la base y que tiene un período de 11 meses.

Ahora hacía escasamente 36 años y medio que habían llegado y, oficialmente, le quedaban aún otros 63 años y medio de servicio en la base, lo que les permitiría ver las dos conjunciones que preveía Altea.

Pero Altea y él mismo habían bajado un peldaño en la escala social; ahora Altea era de la antepenúltima generación y Gaia de la penúltima y sus contactos en la capital, el planeta Imperia, les habían indicado que probablemente todos ellos fueran relevados por los de la última generación.

... ¡Relevado! ¿Y después qué? ¿Era nostalgia lo que sentía? ¿Acaso asomaba una lágrima de su ojo izquierdo? No lo creía posible, pues él era Gaia aunque, en realidad, su verdadero nombre era C3PO, un robot de última ... , perdón, de penúltima generación.

a) Justificar que encontrar cuándo habrá conjunción de los tres planetas equivale a resolver el sistema de congruencias

$$x \equiv 12 \pmod{15} \quad x \equiv 3 \pmod{14} \quad x \equiv 9 \pmod{11}$$

Nota: trabajar en meses siderales.

b) Resolver el sistema para justificar la veracidad de la predicción de Altea de que sólo falta un mes para la conjunción de los tres planetas.
Sol: $x = 2187 + 2310\,t \quad \forall\, t \in \mathbf{Z}$

c) ¿Cuánto tiempo debería tardar el relevo para poder observar la segunda conjunción de los planetas prevista por Altea? *Sol*: 38 años y 31 meses.

d) ¿Cuándo volverán a alinearse, sola y exclusivamente, Inca y Machu Picchu? *Sol*: 2 años y 35 meses.

Ejercicio 2.32 Se han lanzado, en un ordenador, tres procesos que periódicamente acceden a un recurso compartido. Si dos de ellos acceden de forma simultanea no hay problemas, pero si lo hacen los tres se producirá un bloqueo. Considerando los datos de la siguiente tabla, se pide:

Proceso	accede por primera vez al recurso	accede cada
1	10:00 horas	5 minutos
2	10:02 horas	12 minutos
3	c minutos después de las 10 horas	4 minutos

a) Llamando x al número de minutos transcurridos desde las 10:00 horas hasta la ocurrencia de un bloqueo, razonar que x debe verificar el sistema de congruencias

$$x \equiv 0 \pmod{5} \quad x \equiv 2 \pmod{12} \quad x \equiv c \pmod{4}$$

b) Demostrar que se producirá un bloqueo si, y sólo si, $c \equiv 2 \pmod{4}$.

c) Si $c = 6$, encontrar la hora del primer bloqueo que se producirá entre las 10:00 y las 11:00 horas. ¿Y para $c = 10$?
Sol: 10:50 horas en ambos casos.

Ejercicio 2.33

a) ¿Es posible encontrar algún entero positivo n tal que

$$a^2 \mid n \quad (a+1)^2 \mid (n+1) \quad \text{y} \quad (a+2)^2 \mid (n+2)$$

a.1) Siendo a un entero positivo par? *Sol*: No.

a.2) Siendo a "cualquier" entero positivo impar? *Sol*: Sí.

b) Hallar el menor entero positivo n, que verifica dichas condiciones, para el caso $a = 3$. *Sol*: 2223.

Ejercicio 2.34 Encontrar **todas** las soluciones comprendidas entre 1000 y 2000 del sistema

$$\begin{cases} 2x & \equiv & 4 & (\text{mod } 10) \\ 7x & \equiv & 19 & (\text{mod } 24) \\ 2x & \equiv & -1 & (\text{mod } 45) \end{cases}$$

Sean m la menor y M la mayor de las soluciones encontradas. ¿Se puede asegurar si son primos o compuestos sabiendo que $2^m \equiv 2 \pmod{m}$ y que $2^M \equiv 1048 \pmod{M}$? Justifica las respuestas.

Sol: $1237 - 1597 - 1957$. 1957 podemos asegurar que es compuesto, pero 1237 no podemos asegurar que sea primo.

Ejercicio 2.35

a) Considérese un polinomio $P(x)$ con coeficientes enteros y sea n un entero positivo. Probar que si $a \equiv b \pmod{n}$ entonces $P(a) \equiv P(b) \pmod{n}$.

b) Del apartado anterior se deduce que si $n \in \mathbf{Z}$ es una raíz de $P(x)$ y $n \equiv r \pmod{m}$ (para un determinado $m \in \mathbf{Z}^+$) entonces $P(r) \equiv P(n) = 0 \pmod{m}$.

Utilizar dicha propiedad para probar que cualquiera que sea el polinomio $P(x)$ que tome los valores que se dan en la siguiente tabla, carece de raíces enteras. ¿Se deduce de ello que el polinomio es irreducible?

x	0	1	2	3	4	5
$P(x)$	3	-2	-73	-204	-221	338

Sol: No se deduce.

c) El polinomio de menor grado que satisface los valores de la tabla anterior es

$$P(x) = x^5 - 3x^4 - 6x^3 - 9x^2 + 12x + 3.$$

Aplicar el criterio de Eisenstein para probar que se trata de un polinomio irreducible. ¿Se deduce de ello que el polinomio carece de raíces enteras? *Sol*: Sí se deduce.

Ejercicio 2.36 Probar que 1729 y 2821 son números de Carmichael.

Ejercicio 2.37 Encontrar un número de Carmichael de la forma $7 \cdot 23 \cdot p$, donde p es primo. *Sol*: 6601.

Ejercicio 2.38 Encontrar dos números de Carmichael de la forma $13 \cdot 61 \cdot p$ donde p es primo. *Sol*: 29341 y 314821.

Ejercicio 2.39 Probar que no existe ningún número de Carmichael de la forma $n = 55 \cdot m$ siendo m un número libre de cuadrados y primo con 55.

Ejercicio 2.40

Un número n se dice que es de Carmichael si, siendo compuesto, $a^n \equiv a \pmod{n}$ cualquiera que sea el entero a.

a) Utilizar la definición para probar que 561 es de Carmichael.

Un entero $n = p_1 p_2 \cdots p_k$ con $k > 1$ y $p_i \neq p_j$ si $i \neq j$ es de Carmichael si, y sólo si, $(p_i - 1) \mid (n - 1) \;\; \forall\, i = 1, 2, \ldots k$.

b) Probar que no existe ningún número de Carmichael de la forma $21p$ siendo p un número primo.

c) Probar que el único número de Carmichael de la forma $33p$, con p primo, es 561.

Ejercicio 2.41 Sean a y b dos enteros positivos.

a) Probar que si a es primo con b y ambos dividen a c entonces $a \cdot b$ también divide a c. ¿Sería cierto si a y b no fuesen coprimos? Justifica la respuesta.

b) Probar que si a es impar entonces $a^2 - 1$ es divisible por 8.

c) Probar que si $a \perp 240$ entonces 240 divide a $a^4 - 1$.

Ejercicio 2.42 Probar que si p es un primo impar, entonces

a) $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}$

b) $1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod{p}$

Ejercicio 2.43

a) Un entero $n = p_1 \cdot p_2 \cdots p_k$ con $k > 1$ es de Carmichael si, y sólo si, es libre de cuadrados y $p_i - 1$ divide a $n-1$ cualquiera que sea $i = 1, 2, \ldots k$.

Probar que cualquier número de Carmichael es el producto de, al menos, tres primos diferentes.

b) Un entero n se dice que es pseudoprimo para la base a si, siendo compuesto, verifica que $a^n \equiv a \pmod{n}$.

Probar, haciendo uso del teorema de Fermat, que si n es el entero resultante del producto de dos primos gemelos (impares consecutivos), no puede ser pseudoprimo para la base 2.

Ejercicio 2.44

a) Hallar dos números primos p y q (con $p < q$) tales que $91 \cdot p$ y $91 \cdot q$ sean ambos números de Carmichael. *Sol*: 19 y 31.

b) Aplicar el test de base 2 al número $n = p \cdot q$ para determinar si se trata, o no, de un pseudoprimo. *Sol*: No lo es.

c) Sin calcular su valor, determinar en qué cifra termina el número $p^q - q^p$. *Sol*: Termina en 8.

Ejercicio 2.45

a) Probar que todos los números de Carmichael son impares.

b) Sabiendo que el número de divisores del entero $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ viene dado por $s = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdots (\alpha_k + 1)$, probar que si N es de Carmichael entonces s divide a $\phi(N)$.

c) Determinar todos los enteros de la forma $n = 2^\alpha \cdot 3^\beta \cdot p^\gamma$ sabiendo que α, β y γ son enteros positivos, que p es un primo distinto de 2 y de 3 y que $\phi(n) = 432$. *Sol*: $1308 - 1314 - 1332 - 1368 - 1404 - 1512 - 1620$.

Ejercicio 2.46 Sean p, p_1, p_2 y p_3 números primos tales que $p_1 < p_2 < p_3$ y $p = p_1^2 + p_2^2 + p_3^2$. Probar que

a) p_1 no puede ser 2.

b) p_1 ha de ser necesariamente igual a 3.

c) Si $p = 419$ ¿cuánto pueden valer p_2 y p_3? En caso de existir más de una solución, ¿existe alguna para la que el número $n = p_1 \cdot p_2 \cdot p_3$ sea de Carmichael?

Sol: $3 \times 7 \times 19$ no es de Carmichael. $3 \times 11 \times 17$ sí lo es.

Ejercicio 2.47

a) Hacer uso de congruencias para probar que la condición necesaria y suficiente para que un número sea divisible por 4 es que lo sea el número formado por sus dos últimas cifras.

b) ¿Existe algún número de Carmichael terminado en 15? En caso afirmativo, hallar el menor de ellos. *Sol*: No.

c) ¿Existe algún múltiplo positivo de 91 terminado en 15?

En caso afirmativo, hallar todos los comprendidos entre 10000 y 30000. *Sol*: 15015 y 24115.

Ejercicio 2.48 Encontrar todos los valores de n para los que $\phi(n) = 16$.

Sol: $17 - 32 - 34 - 40 - 48 - 60$.

Ejercicio 2.49

a) Encontrar todos los valores de n para los que $\phi(n) = n/2$.

Sol: 2^α con $\alpha \neq 0$.

b) Encontrar todos los valores de n para los que $\phi(n) = n/3$.

Sol: $2^\alpha \cdot 3^\beta$ con $\alpha, beta \neq 0$.

Ejercicio 2.50 Utilizar un código lineal con clave (3,0) en $\mathbf{Z}_{28}$ para cifrar la cadena de caracteres "HOLA A TODOS". *Sol*: WSHC CGSLSD.

Ejercicio 2.51 Tomando $r = 1,\ n = 29,\ e = 5$, cifrar y descifrar el mensaje "CODIFICAME". *Sol*: $11 - 23 - 09 - 05 - 04 - 05 - 11 - 01 - 06 - 22$

Ejercicio 2.52 Utilizando el alfabeto {␣, E, M, N, O, P, R, S} y numerando sus elementos del 0 al 7 respectivamente, descifrar el mensaje **061 − 026 − 091−014−035−094−021** sabiendo que fue cifrado mediante un código RSA con $r = 2$ y que la clave es $(n, e) = (101, 67)$. *Sol*: NO␣ME␣ESPERES␣.

Ejercicio 2.53 Utilizando el alfabeto {␣, A, B, C, D, E} y numerando sus elementos del 0 al 5 respectivamente. Si tomamos, para un código RSA, la clave $(n, e) = (12, 5)$ con $r = 2$ se pide:

a) Cifrar el mensaje **BECA**.

b) Descifrar el mensaje cifrado en el apartado anterior.

c) ¿Qué es lo que falla? Justifica la respuesta.

Ejercicio 2.54 Utilizando el alfabeto {␣, A, D, E, I, L, N, O, R, U} y numerando sus elementos del 0 al 9 respectivamente, descifrar el mensaje

$$\mathbf{798 - 012 - 450 - 847 - 822}$$

sabiendo que fue cifrado mediante un código RSA con $r = 3$ y clave $(n, e) = (1009, 605)$. *Sol*: LEONARD ␣ EULER ␣ ␣.

Ejercicio 2.55 Utilizando el alfabeto {␣, A, B, C, D, E, I, Ñ, O, S, T } y numerando sus elementos del 0 al 10 respectivamente, se pide:

a) Si queremos cifrar mensajes mediante RSA tomando $r = 2$ (dividiendo el texto en grupos de dos letras) ¿es correcta la clave $(n, e) = (1213, 485)$? Justifica la respuesta. *Sol*: Es correcta.

b) Teniendo en cuenta que se ha utilizado dicha clave, descifrar el mensaje

$$466 - 1117 - 952 - 533 - 295 - 359$$

Sol: AÑO␣BISIESTO.

3. Técnicas de contar

3.1 Ejercicios resueltos

Ejercicio 3.1 Sea C un conjunto de 5 enteros positivos no superiores a 9. Demostrar que existen, al menos, dos subconjuntos de C cuyos elementos suman lo mismo.

SOLUCIÓN: Subconjuntos de *un* elemento existen $\binom{5}{1} = 5$, los cuales pueden ser todos diferentes.

Entre subconjuntos de *uno* o *dos* elementos existen

$$\binom{5}{1} + \binom{5}{2} = 5 + 10 = 15$$

Lo mínimo que pueden sumar sus elementos es 1 y lo máximo $9 + 8 = 17$, por lo que todos pueden producir sumas diferentes.

Entre subconjuntos de *uno, dos* o *tres* elementos existen

$$\binom{5}{1} + \binom{5}{2} + \binom{5}{3} = 5 + 10 + 10 = 25$$

La suma de sus elementos está comprendida entre 1 y $9 + 8 + 7 = 24$, por lo que el *principio de distribución* nos dice que debe haber, al menos, dos de ellos cuyos elementos sumen lo mismo. ■

Ejercicio 3.2 Probar que en cualquier grupo de 6 personas, o hay 3 que se conocen entre sí o hay 3 que son mutuamente desconocidos.

SOLUCIÓN: Etiquetemos a una persona x y clasifiquemos a las cinco restantes en dos grupos, A los que conocen a x y B los que desconocen a x.

Al haber cinco personas y dos grupos, el *principio de distribución* nos dice que debe haber, necesariamente, un grupo que contenga, al menos, a tres personas.

a) Sea A el conjunto que contiene, al menos, a tres personas. Si éstas son mutuamente desconocidas ya tenemos el resultado deseado. Si no fuese así es que, al menos, dos de ellas se conocen y como las dos conocen a x hemos encontrado a tres mutuamente conocidas.

b) Si el que contiene, al menos, a tres personas es el conjunto B de las que desconocen a x razonamos de forma similar al caso anterior, es decir, si las tres personas se conocen entre sí ya tenemos el resultado deseado, mientras que si, al menos una pareja se desconocen, al desconocer también a x tenemos tres personas mutuamente desconocidas. ■

Ejercicio 3.3 Sea p un número primo mayor que 3 y α, β dos enteros positivos. Si la descomposición en factores primos de un número n es $n = 2^\alpha \cdot 3^\alpha \cdot p^\beta$, se pide:

a) Hallar n sabiendo que $\phi(n) = 216$, siendo ϕ la función de Euler.

b) En el caso de existir más de una solución del apartado anterior, elegir dos de ellas, n_1 y n_2 y hallar $\phi(|n_1 - n_2|)$ utilizando el principio de inclusión y exclusión.

SOLUCIÓN:

a) $\phi(n) = 2^\alpha 3^\alpha p^\beta \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{p}\right) = 2^\alpha 3^{\alpha-1} p^{\beta-1}(p-1)$

Como $\phi(n) = 216 = 2^3 3^3$, ha de ser $\beta = 1$ y $p - 1 = 2^{3-\alpha} 3^{3-\alpha+1}$ y al ser $p - 1$ par (p es primo distinto de 2) α sólo puede ser 1 ó 2.

- Si $\alpha = 1$, $p - 1 = 2^2 \cdot 3^3 = 108 \Longrightarrow p = 109$ y $n = 2 \cdot 3 \cdot 109 = 654$.
- Si $\alpha = 2$, $p - 1 = 2 \cdot 3^2 = 18 \Longrightarrow p = 19$ y $n = 2^2 \cdot 3^2 \cdot 19 = 684$.

b) Como sólo existen dos soluciones, tomamos $n_1 = 684$ y $n_2 = 654$, por lo que $|n_1 - n_2| = |684 - 654| = 30$.
Se trata entonces de calcular $\phi(30) = \phi(2 \cdot 3 \cdot 5)$.
Sean D, T y C los conjuntos de números $1 \leq n \leq 30$ que son múltiplos de 2, de 3 o de 5 respectivamente.

$$\begin{array}{lll} |D| = 15 & |D \cap T| = 5 & |D \cap T \cap C| = 1 \\ |T| = 10 & |D \cap C| = 3 & \\ |C| = 6 & |T \cap C| = 2 & \end{array}$$

Por lo que los números enteros no superiores a 30 que no son primos con 30 son:

$$|D \cup T \cup C| = 15 + 10 + 6 - (5 + 3 + 2) + 1 = 22$$

Por tanto, $\phi(30) = 30 - |D \cup T \cup C| = 30 - 22 = 8$. ■

Ejercicio 3.4 ¿De cuántas maneras se pueden ordenar las letras de la palabra XSIAON de modo que las palabras ASI y NO nunca aparezcan?

SOLUCIÓN: El número total de ordenaciones es de $n = 6! = 720$.

El número de las que llevan la palabra ASI es $4! = 24$, pues basta con considerar la palabra ASI como una sola letra del grupo X(ASI)ON.

Razonando de igual manera, se obtiene que las que llevan la palabra NO son $5! = 120$.

Las que llevan simultáneamente ASI y NO vienen dadas por $3! = 6$ (considérese ASI como una letra y NO como otra).

El número de las que llevan ASI o NO viene dado, aplicando el *principio de inclusión y exclusión* por $120 + 24 - 6 = 138$.

El número de ordenaciones pedidas es por tanto $720 - 138 = 582$. ■

Ejercicio 3.5 Considérese el polinomio $\Psi_p(x) = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$ con p primo. En este ejercicio tratamos de probar que dicho polinomio es irreducible.

a) Pruébese que no se puede aplicar el criterio de Eisenstein para verificar que $\Psi_p(x)$ es irreducible.

b) Justifíquese que para probar la irreducibilidad de $\Psi_p(x)$ es suficiente probar la del polinomio $f(x) = \Psi_p(x+1)$.

c) Probar que

$$f(x) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{p-1} x^{p-2} + \cdots + \binom{p}{2} x + \binom{p}{1}.$$

d) Probar que existe un primo que divide a todos los coeficientes de $f(x)$ excepto al de mayor grado (x^{p-1}) y que el cuadrado de dicho primo no divide al término independiente, por lo que $f(x)$ es irreducible.

e) Dar un ejemplo de un número n *no primo* tal que $\Psi_n(x)$ no sea irreducible.

SOLUCIÓN:

a) No puede aplicarse el criterio de Eisenstein ya que no existe ningún primo que divida a todos los coeficientes, excepto al del término de mayor grado, y tal que su cuadrado no divida al término independiente.

b) Basta con observar que

$$f(x) = g(x)h(x) \Longrightarrow \Psi_p(x) = f(x-1) = g(x-1)h(x-1).$$

Recíprocamente,

$$\Psi_p(x) = \varphi(x)\mu(x) \Longrightarrow f(x) = \Psi_p(x+1) = \varphi(x+1)\mu(x+1).$$

Es decir, si $f(x)$ es reducible, también lo es $\Psi_p(x)$ y viceversa.

c) Como $\Psi_p(x) = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1 = \dfrac{x^p - 1}{x - 1}$, se tiene que

$$f(x) = \Psi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{(x+1)^p - 1}{x}$$

basta entonces con hacer el desarrollo del binomio del numerador para obtener la expresión

$$f(x) = x^{p-1} + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{2}x + \binom{p}{1}.$$

d) Al ser p primo y $\binom{p}{i}$ entero, p es un divisor de $\binom{p}{i}$ cualquiera que sea $1 \leq i \leq p-1$, es decir, p divide a todos los coeficientes excepto al del término de mayor grado. Dado que, además, el término independiente es p, p^2 no divide a dicho término, por lo que el polinomio $f(x)$ y, por tanto, $\Psi_p(x)$ es irreducible.

e) Basta tomar $p = 4$ para obtener $\Psi_4 = x^3 + x^2 + x + 1 = (x+1)(x^2+1)$, por lo que $\Psi_4(x)$ no es irreducible. ■

Ejercicio 3.6 Una empresa posee seis ordenadores y los quiere colocar en red. Si cada ordenador debe conectase con otros dos, y sólo con otros dos, ¿cuánto tiempo tardarán en estudiar todas las configuraciones posibles, para encontrar la más adecuada, si emplean dos minutos en analizar cada una de ellas por separado?

SOLUCIÓN: Numeramos los ordenadores del 1 al 6. Si ordenamos sus números en una determinada posición, por ejemplo

$$1 - 2 - 3 - 4 - 5 - 6$$

y decimos que cada ordenador está conectado a los dos adyacentes (los extremos están conectados entre sí) observamos que el número total de configuraciones vendrá dado por las permutaciones de 5 (el 1 siempre lo ponemos en primer lugar) es decir, existen $5! = 120$ configuraciones diferentes, por lo que se tardaría un total de $120 \cdot 2 = 240$ minutos en estudiarlas todas. En otras palabras, tardarían 4 horas en encontrar la configuración más adecuada. ■

Ejercicio 3.7 Por un canal de comunicación, se va a transmitir un mensaje usando 12 símbolos diferentes. Además de estos 12 símbolos, el transmisor también enviará un total de 45 espacios en blanco entre los símbolos, con tres espacios como mínimo entre cada par de símbolos consecutivos ¿de cuántas formas se puede mandar el mensaje?

SOLUCIÓN: Existen $12!$ formas de ordenar los 12 símbolos diferentes y, en cada una de ellas, existen 11 lugares entre ellos. El hecho de que tengan que transmitirse un mínimo de tres espacios en blanco entre cada dos símbolos consecutivos, hace que tengamos asignados a priori la situación de 33 espacios en blanco, quedándonos sólo 12 para distribuir entre las 11 posiciones posibles. Se trata entonces de una combinación con repetición de 11 elementos tomados de 12 en 12, es decir $\binom{12+11-1}{12} = \binom{22}{12}$ posibilidades para cada una de las $12!$ formas de transmitir los símbolos, por lo que el mensaje puede enviarse de

$$12! \cdot \binom{22}{12} = 22 \cdot 21 \cdot 20 \cdot 19 \cdot 18 \cdot 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 = 309744468633600$$

formas diferentes. ■

Ejercicio 3.8 Dados 12 números primos diferentes $p_1, \ldots, p_{12}$, consideremos los conjuntos

$$P = \{p_i p_j p_k \,:\, 1 \leq i < j < k \leq 12\} \quad \text{y} \quad P' = \{p_i p_j p_k \,:\, 1 \leq i \leq j \leq k \leq 12\}$$

a) Determinar el número de elementos de los conjuntos P y P'.

b) Probar que existen, al menos, tres elementos de P cuyas dos últimas cifras coinciden.

c) Sabiendo que el número de divisores del entero $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ viene dado por $N = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$, determinar el número de elementos del conjunto P' que tienen exactamente 6 divisores.

SOLUCIÓN:

a) Teniendo en cuenta que $1 \leq i < j < k \leq 12$, los tres primos de la factorización de cada elemento de P son distintos, por lo que basta con elegir tres primos distintos de los 12 de los que disponemos y multiplicarlos.

Se tiene, por tanto, que $|P| = \binom{12}{3} = \dfrac{12 \cdot 11 \cdot 10}{3 \cdot 2 \cdot 1} = 220$.

Los elementos del conjunto P' se obtienen de forma análoga, sólo que ahora los tres primos de la factorización de cada uno de sus elementos pueden repetirse, por lo que $|P'|$ vendrá dado por las combinaciones con repetición de 12 elementos elegidos de tres en tres, es decir:

$$|P'| = \binom{12+3-1}{3} = \binom{14}{3} = \frac{14 \cdot 13 \cdot 12}{3 \cdot 2 \cdot 1} = 364.$$

b) Si los clasificamos los elementos de P según sus terminaciones

$$A_{00}, A_{01}, A_{02}, \ldots, A_{99}$$

dado que $2 \cdot 100 < 220$, el *principio de distribución* nos dice que, al menos, uno de los conjuntos debe contener un mínimo de tres elementos.

En otras palabras: existen, al menos, tres elementos de P cuyas dos últimas cifras coinciden.

c) Para que un elemento de P' tenga exactamente 6 divisores ha de ser de la forma

$$p_i p_i p_j = p_i^2 p_j \quad \text{con} \quad i < j \quad \text{ó} \quad p_i p_j p_j = p_i p_j^2 \quad \text{con} \quad i < j$$

Sólo podemos elegir, por tanto, dos primos diferentes de entre los doce de los que disponemos y formar con ellos uno de los dos tipos posibles, es decir, existirán

$$\binom{12}{2} = \frac{12 \cdot 11}{2 \cdot 1} = 66$$

del tipo $p_i^2 p_j$ con $i < j$ y otros 66 del tipo $p_i p_j^2$ con $i < j$, por lo que existe un total de 132 elementos de P' con exactamente 6 divisores. ■

3.2 Ejercicios propuestos

Ejercicio 3.9 Se recibe de Secretaría la siguiente información: cada alumno de una determinada titulación está matriculado en cuatro de las siete asignaturas que se ofertan, las listas de alumnos por asignaturas están constituidas por 52, 30, 30, 20, 25, 12 y 18 alumnos respectivamente. ¿A qué conclusión nos lleva dicha información?
Sol: Los datos no son correctos. (Aplicar el método de *contar en tablas*).

Ejercicio 3.10 En una clase de música con 73 alumnos hay 52 que tocan el piano, 25 el violín, 20 la flauta, 17 tocan piano y violín, 12 piano y flauta, 7 violín y flauta y sólo hay 1 que toque los tres instrumentos. ¿Hay algún alumno que no toque ninguno de los tres instrumentos? *Sol*: 11.

Ejercicio 3.11 Una multinacional tiene 10000 empleados de los cuales 5600 hablan inglés, 4400 francés y 2200 castellano. Se sabe que cualquiera de ellos habla, al menos, uno de los tres idiomas, que 1600 hablan inglés y francés, 200 francés y castellano y 100 hablan los tres idiomas. Si el director general habla inglés y castellano, ¿con cuantos empleados puede comunicarse sin necesidad de intérprete? ¿Cuántos empleados hablan únicamente castellano?
Sol: $7300 - 1600$.

Ejercicio 3.12 Hallar cuántos enteros hay en el rango $1 \leq n \leq 1000$ que no son divisibles ni por 2 ni por 3 ni por 5. *Sol*: 266.

Ejercicio 3.13 ¿Cuántas cadenas de 8 bits comienzan por 101 o tienen el cuarto bit igual a 1? *Sol*: 144.

Ejercicio 3.14 Usar el principio de inclusión y exclusión para encontrar el valor de $\phi(60)$. *Sol*: 16.

Ejercicio 3.15

a) Utilizar el principio de inclusión y exclusión para hallar cuántos enteros positivos y menores que 10000 son primos con 3780. *Sol*: 2285.

b) Utilizar la función de Euler para hallar cuántos de ellos son mayores que 3780. *Sol*: 1421.

Ejercicio 3.16 ¿Cuántos números de teléfono de 5 dígitos tienen un dígito que aparece más de una vez? *Sol*: 69760.

Ejercicio 3.17 ¿Cuántos números pares mayores que 1000000 y menores que 5000000 pueden escribirse con las cifras del número $p - q$ donde $p > q$ son los dos primos resultantes de la factorización del número $n = 10088821$ sabiendo que $\phi(n) = 10082272$? *Sol*: 1024.

Ejercicio 3.18

a) Hallar el menor número $a > 800$ tal que si lo dividimos por 21, si $7a$ lo dividimos por 15 o si $2a$ lo dividimos por 5, obtenemos siempre un resto igual a 4. *Sol*: 802.

b) Determinar el número b de formas en que podemos ordenar las letras de la palabra EXAMEN teniendo en cuanta que las dos letras E no pueden ir juntas. *Sol*: 240.

c) Haciendo uso del principio de inclusión y exclusión calcular $\phi(682)$.
Sol: 300.

Ejercicio 3.19 ¿Cuántas palabras de longitud 3 (sin repetir signos) pueden escribirse con un alfabeto de 256 letras teniendo en cuenta que dos determinados signos (por ejemplo, las letras "a" y "b") no figuren nunca juntos (consecutivos)? *Sol*: 16.580.104.

Ejercicio 3.20

a) Probar que si p es primo, $\binom{p}{i}$ con $1 \leq i \leq p-1$ es un múltiplo de p. Encontrar un contraejemplo para el caso en que p no sea primo.

b) ¿Se puede probar directamente, por inducción matemática, que una propiedad es cierta para cualquier $n \in \mathbf{Z}$? Justifíquese la respuesta.

c) Demostrar que cualquiera que sea $n \in \mathbf{Z}$, se verifica que

$$P(n) = \frac{n^7}{7} + \frac{n^3}{3} + \frac{11n}{21} \in \mathbf{Z}.$$

Ejercicio 3.21 Probar las igualdades:

$$\text{a)} \quad \binom{r}{k} = \frac{r}{k}\binom{r-1}{k-1} \qquad \text{b)} \quad r\binom{r-1}{k} = (r-k)\binom{r}{k}$$

Ejercicio 3.22 Probar la identidad:

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

Sol: Aplicar inducción en n.

Ejercicio 3.23

a) Probar que si n es un entero positivo, entonces

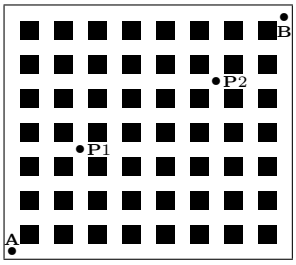
$$\binom{2(n+1)}{n+1} = 2 \cdot \frac{2n+1}{n+1} \cdot \binom{2n}{n}.$$

b) Probar por inducción sobre n que para todo $n \geq 2$ se verifica que

$$2^n < \binom{2n}{n} < 4^n.$$

Ejercicio 3.24 Sabiendo que si p es primo y $p^e \,||\, n!$ entonces $e = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \cdots$, hallar el máximo común divisor de $\binom{100}{50}$ y 4032.
Sol: 72.

Ejercicio 3.25 La cuadrícula de la figura representa las calles de una pequeña ciudad.



a) Qué características debe tener un camino de A a B de forma que no exista otro más corto que él? *Sol*: Utilizar sólo las direcciones norte y este.

b) ¿Cuántos caminos distintos puede seguir un ladrón que roba una joyería situada en la esquina A para ir a su casa, situada en la esquina B, teniendo que cuenta que pretende ir por uno de los caminos más cortos y que debe evitar pasar por las esquinas $P1$ y $P2$ en las que se encuentran las dos comisarías de policía de la ciudad? *Sol*: 2463.

Ejercicio 3.26

a) Los padres de una familia de 3 hijos deciden repartir semanalmente entre ellos 32 euros para sus gastos. Si desean dar un número entero de euros, no menor de 4, a cada hijo –salvo al mayor, al que desean darle no menos de 10– ¿de cuántas maneras distintas pueden hacer la asignación semanal? *Sol*: 120.

b) Si además, desean darle no más de 10 euros a los dos más pequeños, ni más de 15 al mayor, ¿de cuántas formas diferentes pueden hacer ahora la asignación? *Sol*: 10.

c) Si además de las restricciones del primer apartado, no quieren que los dos pequeños tengan la misma asignación, ¿cuál sería ahora en número de asignaciones posibles? *Sol*: 112.

4. Recursión

4.1 Ejercicios resueltos

Ejercicio 4.1 Los dos primeros términos de una sucesión valen, respectivamente, 1 y 2. Sabiendo que cada término es la media aritmética del anterior con la media aritmética de los dos adyacentes (anterior y posterior), se pide:

a) Hallar una fórmula explícita para los términos de dicha sucesión.

b) Probar, mediante inducción completa, la validez de la fórmula obtenida.

c) Describir un procedimiento para calcular el término 40 realizando, a lo más, 10 operaciones (sumas, restas, multiplicaciones o divisiones).

SOLUCIÓN:

a) Si tomamos tres términos consecutivos a_n, a_{n+1} y a_{n+2} se verifica que

$$a_{n+1} = \frac{a_n + \dfrac{a_n + a_{n+2}}{2}}{2} \implies 4a_{n+1} = 3a_n + a_{n+2}$$

por lo que

$$a_{n+2} = 4a_{n+1} - 3a_n \tag{4.1}$$

La ecuación característica de la RLH es $r^2 - 4r + 3 = 0$ cuyas raíces son 1 y 3. Se tiene por tanto que $a_n = \alpha \cdot 3^n + \beta \cdot 1^n = \alpha \cdot 3^n + \beta$.

$$\left.\begin{array}{lll} a_1 = 1 & \Rightarrow & 1 = 3\alpha + \beta \\ a_2 = 2 & \Rightarrow & 2 = 9\alpha + \beta \end{array}\right\} \Rightarrow \alpha = 1/6 \quad \text{y} \quad \beta = 1/2$$

Se tiene entonces que

$$a_n = \frac{1}{6}\,3^n + \frac{1}{2} = \frac{1}{2}\,(3^{n-1} + 1) \implies a_n = \frac{1}{2}\,(3^{n-1} + 1)$$

b) Para $n = 1$ se tiene que $a_1 = \frac{1}{2}(3^0 + 1) = \frac{1}{2} \cdot 2 = 1$ que es el valor dado para el primer elemento.

Supongamos que la fórmula es cierta para cualquier entero menor o igual a n y probémoslo para $n + 1$.

Dado que (ver 4.1), $a_{n+1} = 4a_n - 3a_{n-1}$ y la fórmula es cierta para a_n y para a_{n-1} se tiene que:

$$a_{n+1} = 4\frac{1}{2}\left(3^{n-1} + 1\right) - 3\frac{1}{2}\left(3^{n-2} + 1\right) = \frac{1}{2}\left(4 \cdot 3^{n-1} + 4 - 3^{n-1} - 3\right) =$$
$$= \frac{1}{2}\left(3 \cdot 3^{n-1} + 1\right) = \frac{1}{2}\left(3^n + 1\right)$$

por lo que la fórmula es cierta para cualquier término de la sucesión.

c) El procedimiento a seguir para calcular el término $a_{40} = \frac{1}{2}(3^{39} + 1)$ es el siguiente:

Núm. de Oper.	1	2	3	4	5	6	7	8	9
Resultado	3^2	3^4	3^8	3^{16}	3^{20}	3^{40}	3^{39}	$3^{39}+1$	$\frac{1}{2}(3^{39}+1)$

por lo que a_{40} puede ser calculado con sólo 9 operaciones. ■

Ejercicio 4.2 Hallar la expresión del término general así como la función generatriz de la sucesión

$$(a_n) = (a, b, a, b, a, b, \ldots)$$

SOLUCIÓN:

a) La sucesión está definida de forma recurrente mediante:

$$\begin{cases} a_0 = a \quad a_1 = b \\ a_n = a_{n-2} \quad \forall\, n \geq 2 \end{cases}$$

por lo que se trata de una RLH de orden 2 con ecuación característica $t^2 = 1$ de raíces 1 y -1 simples.

Su término general es de la forma

$$a_n = A \cdot 1^n + B \cdot (-1)^n = A + B \cdot (-1)^n$$
$$\left.\begin{array}{l} a_0 = a \implies A + B = a \\ a_1 = b \implies A - B = b \end{array}\right\} \implies A = \frac{a+b}{2} \qquad B = \frac{a-b}{2}$$

por lo que

$$a_n = \frac{a+b}{2} + \frac{a-b}{2}(-1)^n \qquad \forall\, n \geq 0$$

b) Si la función generadora es

$$f(x) = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_n x^n + \cdots$$

teniendo en cuenta que $a_n - a_{n-2} = 0$ obtenemos que

$$\begin{array}{rl} f(x) = & a_0 + \ a_1 x + \ a_2 x^2 \ + a_3 x^3 + \cdots + \ a_n x^n + \cdots \\ -x^2 f(x) = & \qquad\qquad -a_0 x^2 \ -a_1 x^3 - \cdots - a_{n-2} x^n - \cdots \\ \hline (1-x^2) f(x) = & a_0 + \ a_1 x + \ 0x^2 \ + \ 0\, x^3 + \cdots \ + \ 0\, x^n + \ \cdots \end{array}$$

$$(1-x^2) f(x) = a + bx \implies f(x) = \frac{a+bx}{1-x^2}$$

■

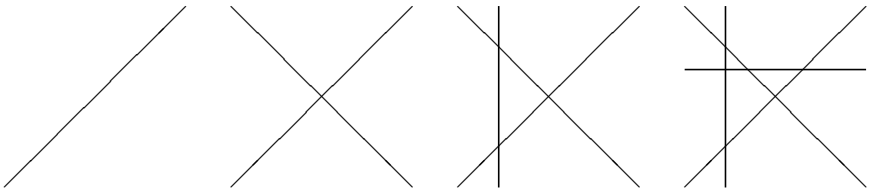
Ejercicio 4.3

a) Se trazan n rectas en el plano de forma que cada una de ellas corta a todas las demás y no existen tres que se intersequen en un mismo punto. Determinar una fórmula explícita para el número u_n de regiones en que dichas rectas dividen al plano.

b) Determinar el número v_n de regiones no acotadas que resultan de la situación del apartado anterior.

SOLUCIÓN:

a) Obsérvese que cada vez que se traza una nueva recta, como ésta corta a las $n-1$ anteriores, debe atravesar n regiones del plano a las cuales divide en dos, es decir, cuando trazamos la recta n-ésima añadimos n regiones.



Esto nos lleva a que

$$u_n = u_{n-1} + n \iff u_{n+1} - u_n = n+1 \qquad \text{con} \quad u_1 = 2$$

La RLH tiene por solución $u_n^{(h)} = A$ y una solución particular de la completa debe ser $u_n^{(p)} = Bn^2 + Cn$. Sustituyendo obtenemos:

$$B[(n+1)^2 - n^2] + C[(n+1) - n] = n+1 \Rightarrow B(2n+1) + C = n+1 \Rightarrow \left\{ \begin{array}{l} B = 1/2 \\ C = 1/2 \end{array} \right.$$

Por tanto, $u_n = \frac{1}{2}(n^2+n) + A$ y como $u_1 = 2$ se obtiene que $A = 1$, por lo que

$$u_n = \frac{1}{2}(n^2+n) + 1 \quad \forall\, n \in \mathbf{Z}^+$$

b) De las regiones que se añaden en cada paso, sólo 2 son no acotadas, por lo que $v_{n+1} - v_n = 2$ para $n \geq 1$ con $v_1 = 2$.

En este caso $v_n^{(h)} = A$ y $v_n^{(p)} = Bn$, por lo que

$$B(n+1) - Bn = 2 \implies B = 2 \implies v_n = 2n + A$$

Como $v_1 = 2$ se obtiene que $A = 0$, por lo que

$$v_n = 2n \quad \forall, n \in \mathbf{Z}^+$$

■

Ejercicio 4.4 Dada la sucesión definida por

$$\begin{aligned} a_0 &= 2 \\ a_1 &= 2+1 = 3 \\ a_2 &= 2+1+2 = 5 \\ a_3 &= 2+1+2+1 = 6 \\ a_4 &= 2+1+2+1+2 = 8 \\ &\vdots \end{aligned}$$

a) Hallar una fórmula explícita de su término general.

b) Encontrar la función generadora de dicha sucesión.

SOLUCIÓN:

a) Basta con darse cuenta que cada vez que saltamos dos lugares en la sucesión hemos añadido un 1 y un 2, o bien, un 2 y un 1, pero en cualquier caso, 3 unidades, por lo que:

$$\begin{cases} a_0 = 2 \\ a_1 = 3 \\ a_{n+2} - a_n = 3 \end{cases}$$

La RLH asociada es $a_{n+2} - a_n = 0$ de ecuación característica $r^2 - 1 = 0$, cuyas raíces son 1 y -1 ambas simples.

La solución general de la RLH asociada es, por tanto

$$a_n^{(h)} = A \cdot 1^n + B \cdot (-1)^n = A + B \cdot (-1)^n$$

El término general de la completa es un polinomio de grado cero (una constante) por lo que deberíamos buscar una solución particular de la completa de la misma forma, pero dado que 1 es una raíz simple de la ecuación característica de la RLH asociada, debemos multiplicarla por n y buscar una solución particular de la forma

$$a_n^{(p)} = Cn$$

Llevándola a la ecuación obtenemos que

$$C(n+2) - Cn = 3 \iff 2C = 3 \implies C = \frac{3}{2}$$

obteniéndose que

$$a_n = a_n^{(h)} + a_n^{(p)} = A + B \cdot (-1)^n + \frac{3}{2}n$$

Imponiendo ahora las condiciones de que $a_0 = 2$ y $a_1 = 3$ se obtiene el sistema

$$\begin{cases} A + B = 2 \\ A - B + \dfrac{3}{2} = 3 \end{cases} \iff \begin{cases} A = 7/4 \\ B = 1/4 \end{cases}$$

de donde

$$a_n = \frac{7}{4} + \frac{1}{4} \cdot (-1)^n + \frac{3}{2}\, n \quad \text{para cualquier entero} \quad n \geq 0$$

b) Sea $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_n x^n + \cdots$ la función generadora.

Teniendo en cuenta que $a_{n+2} - a_n = 3$ cualquiera que sea $n \geq 0$ se tiene que

$$\begin{array}{rl} f(x) = & a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + \ a_n x^n \ + \cdots \\ x^2 f(x) = & \qquad\qquad a_0 x^2 + a_1 x^3 + \cdots + a_{n-2} x^n + \cdots \\ \hline (1-x^2) f(x) = & \ 2 \ + 3x + 3x^2 + \ 3x^3 \ + \cdots + \ 3x^n \ + \cdots \end{array}$$

de donde

$$(1-x^2) f(x) = 2 + 3x\,(1 + x + x^2 + \cdots + x^n + \cdots) = 2 + 3x\,\frac{1}{1-x} = \frac{2+x}{1-x}$$

por lo que la función generadora de la sucesión dada es

$$f(x) = \frac{2+x}{(1-x)(1-x^2)} = \frac{2+x}{1-x-x^2+x^3}$$

■

Ejercicio 4.5 Se considera la sucesión (a_n) para la que

$$\begin{cases} a_0 = 3 \\ a_n - 4a_{n-1} = \begin{cases} 2 & \text{si } n \text{ es par} \\ -8 & \text{si } n \text{ es impar} \end{cases} \end{cases}$$

a) Probar que se verifica que $a_n - 3a_{n-1} - 4a_{n-2} = -6$ para cualquier $n \geq 2$.

b) Calcular su término general.

c) Determinar su función generadora.

SOLUCIÓN:

a) Sabemos que:

$$\left.\begin{array}{ll} \text{Si } n = 2m & a_{2m} - 4a_{2m-1} = 2 \\ \text{Si } n = 2m-1 & a_{2m-1} - 4a_{2m-2} = -8 \end{array}\right\} \Rightarrow a_{2m} - 3a_{2m-1} - 4a_{2m-2} = -6$$

y que

$$\left.\begin{array}{ll} \text{Si } n = 2m & a_{2m} - 4a_{2m-1} = 2 \\ \text{Si } n = 2m+1 & a_{2m+1} - 4a_{2m} = -8 \end{array}\right\} \Rightarrow a_{2m+1} - 3a_{2m} - 4a_{2m-1} = -6$$

por lo que, para cualquier $n \geq 2$, se verifica que

$$a_n - 3a_{n-1} - 4a_{n-2} = -6$$

b) Se trata de una recurrencia lineal no homogénea de orden 2.

La RLH asociada es $a_n - 3a_{n-1} - 4a_{n-2} = 0$ con ecuación característica $t^2 - 3t - 4 = 0$ de raíces -1 y 4, por lo que su término general viene dado por $a_n^{(h)} = A \cdot 4^n + B \cdot (-1)^n$

Al ser una constante el término general de la completa, buscamos una solución particular de la forma $a_n^{(p)} = C$ debiéndose cumplir que

$$C - 3C - 4C = -6 \implies -6C = -6 \implies C = 1$$

resultando que la solución general de la completa es $a_n = a_n^{(h)} + a_n^{(p)}$

$$a_n = A \cdot 4^n + B \cdot (-1)^n + 1$$

Si la n es par $(n = 2m)$ sabemos que $a_{2m} - 4a_{2m-1} = 2$, por lo que

$$A \cdot 4^{2m} + B \cdot (-1)^{2m} + 1 - 4A \cdot 4^{2m-1} - 4B \cdot (-1)^{2m-1} - 4 = 2$$

es decir

$$A \cdot 4^{2m} + B + 1 - A \cdot 4^{2m} + 4B - 4 = 2 \implies 5B - 3 = 2 \implies B = 1$$

por lo que

$$a_n = A \cdot 4^n + (-1)^n + 1$$

y como $a_0 = 3$ debe ser

$$A \cdot 4^0 + (-1)^0 + 1 = 3 \implies A + 1 + 1 = 3 \implies A = 1$$

obteniéndose que

$$a_n = 4^n + (-1)^n + 1 \quad \forall\, n \geq 0$$

c) La función generadora será

$$f(x) = \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} [4^n + (-1)^n + 1]\, x^n = \sum_{n=0}^{\infty} 4^n x^n + \sum_{n=0}^{\infty} (-1)^n x^n + \sum_{n=0}^{\infty} x^n$$

o lo que es lo mismo

$$f(x) = \frac{1}{1-4x} + \frac{1}{1+x} + \frac{1}{1-x} = \frac{3 - 8x - x^2}{1 - 4x - x^2 + 4x^3}$$

■

4.2 Ejercicios propuestos

Ejercicio 4.6 Encontrar una fórmula explícita para los términos de la sucesión definida por:

$$u_0 = 0\ ,\ u_1 = 1\ ,\ u_n = 5u_{n-1} - 6u_{n-2} \quad (n \geq 2)$$

Sol: $u_n = 3^n - 2^n \quad \forall\, n \geq 0$.

Ejercicio 4.7 Hallar una fórmula explícita para los términos de la sucesión definida por:

$$u_0 = 1\ ,\ u_1 = 0\ ,\ u_n = 6u_{n-1} - 8u_{n-2} \quad (n \geq 2)$$

Sol: $u_n = 2^{n+1} - 4^n \quad \forall\, n \geq 0$.

Ejercicio 4.8 Hallar una fórmula explícita para los términos de la sucesión definida por:

$$u_0 = 1\ ,\ u_1 = 2\ ,\ u_2 = 3\, u_n = 5u_{n-1} - 8u_{n-2} + 4u_{n-3} \quad (n \geq 3)$$

Sol: $u_n = (2 - \frac{1}{2}n) \cdot 2^n - 1 = (4 - n) \cdot 2^{n-1} - 1 \quad \forall\, n \geq 0$.

Ejercicio 4.9 Hallar una fórmula explícita para el término general de la sucesión definida mediante

$a_0 = 0,\ a_1 = 1,\ a_2 = 3,$ siendo $a_n - a_{n-1} = 4[(a_{n-1} - a_{n-2}) - (a_{n-2} - a_{n-3})]$.

Sol: $u_n = 2^n - 1 \quad \forall\, n \geq 0$.

Ejercicio 4.10 Halar el término general de las sucesiones definidas por:

a) $u_{n+1} - u_n = 2n + 3$ para $n \geq 0$ con $u_0 = 1$.

Sol: $u_n = n^2 + 2n + 1 = (n+1)^2 \quad \forall\, n \geq 0$.

b) $u_{n+1} - u_n = 3n^2 - n$ para $n \geq 0$ con $u_0 = 3$.

Sol: $u_n = n^3 - 2n^2 + n + 3 \quad \forall\, n \geq 0$.

c) $u_{n+1} - 2u_n = 5$ para $n \geq 0$ con $u_0 = 1$.

Sol: $u_n = 6 \cdot 2^n - 5 \quad \forall\, n \geq 0$.

d) $u_{n+1} - 2u_n = 2^n$ para $n \geq 0$ con $u_0 = 1$.

Sol: $u_n = (n+2) \cdot 2^{n-1} \quad \forall\, n \geq 0$.

Ejercicio 4.11 Halar el término general de las sucesiones definidas por:

a) $u_{n+2} + 3u_{n+1} + 2u_n = 3^n \ (n \geq 0)$ con $u_0 = 0$ y $u_1 = 1$.

Sol: $u_n = \dfrac{3}{4}(-1)^n - \dfrac{4}{5}(-2)^n + \dfrac{1}{20} \cdot 3^n \quad \forall\, n \geq 0$.

b) $u_{n+2} + 4u_{n+1} + 4u_n = 7 \ (n \geq 0)$ con $u_0 = 1$ y $u_1 = 2$.

Sol: $u_n = \left(-\dfrac{5}{6}n + \dfrac{2}{9}\right)(-2)^n + \dfrac{7}{9} \quad \forall\, n \geq 0$.

c) $u_{n+2} - 6u_{n+1} + 9u_n = 3 \cdot 2^n + 7 \cdot 3^n \ (n \geq 0)$ con $u_0 = 1$ y $u_1 = 4$.

Sol: $u_n = 3 \cdot 2^n + (\dfrac{7}{18}n^2 + \dfrac{17}{18}n - 2) \cdot 3^n \quad \forall\, n \geq 0$.

Ejercicio 4.12 Calcular el término general de la sucesión definida por

$$\begin{cases} a_0 = 20, \quad a_1 = 22, \quad a_2 = 24 \\ a_n = 4a_{n-1} - 5a_{n-2} + 2a_{n-3} + n \cdot 2^n \end{cases}$$

Sol: $a_n = 10n + 20 + (2n^2 - 6n) \cdot 2^n \quad \forall\, n \geq 0$.

Ejercicio 4.13

a) Determinar una fórmula explícita para el término general de la sucesión u_n definida por la recurrencia lineal y homogénea

$$\begin{aligned} &u_0 = 1\ ,\ u_1 = 6 \\ &u_n = 6u_{n-1} - 9u_{n-2} \quad \forall\ n \geq 2 \end{aligned}$$

Sol: $u_n = (n+1)\cdot 3^n \ \ \forall\, n \geq 0$.

b) Determinar una fórmula explícita para el término general de la sucesión u_n definida por la recurrencia lineal no homogénea

$$\begin{aligned} &u_0 = 1\ ,\ u_1 = 6 \\ &u_n = 4n + 6u_{n-1} - 9u_{n-2} \quad \forall\ n \geq 2 \end{aligned}$$

Sol: $u_n = n + 3 + (\frac{8}{3}n - 2)\cdot 3^n = n + 3 + (8n-6)\cdot 3^{n-1} \ \ \forall\, n \geq 0$.

Ejercicio 4.14

a) Determinar a y b sabiendo que a es el número de enteros positivos, no superiores a 100, que no son divisibles ni por 3 ni por 7 ni por 11 y b el de enteros divisible por 2 y por 9 en el mismo rango. *Sol*: $a = 52$, $b = 5$.

b) Hallar una fórmula explícita para el término general de la sucesión definida por

$$\begin{cases} u_0 = 0,\ u_1 = 10 \\ u_n = au_{n-1} - (130b+1)u_{n-2} \quad \forall n \geq 2, \end{cases}$$

donde a y b son los números obtenidos en el apartado anterior, y utilizar el resultado para probar que cualquier término de la sucesión es divisible por 10. *Sol*: $u_n = 31^n - 21^n \ \ \forall\, n \geq 0$.

Ejercicio 4.15 Encontrar la función generadora de la sucesión

$$a_n = 2^n + 3^n \ \forall\, n \geq 0$$

Sol: $f(x) = \dfrac{2-5x}{1-5x+6x^2}$.

Ejercicio 4.16 Hallar la función generadora de la sucesión definida por

$$\begin{cases} a_0 = 1, \quad a_1 = 2 \\ a_n = 5a_{n-1} - 4a_{n-2} \ \ \forall\, n \geq 2 \end{cases}$$

para, a partir de ella, encontrar una fórmula explícita de su término general.

Sol: $f(x) = \dfrac{1-3x}{1-5x+4x^2}$, $\quad a_n = \dfrac{1}{3}\,4^n + \dfrac{2}{3} \ \ \forall\, n \geq 0$.

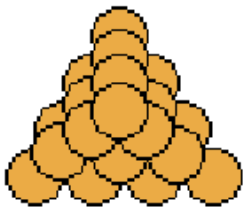
Ejercicio 4.17 Nos regalan tres sellos y decidimos iniciar una colección. El año siguiente, la incrementamos con 8 sellos más (tendríamos entonces 11 sellos). Si cada año compramos un número de sellos igual al doble de los que compramos el año anterior, ¿al cabo de cuántos años habremos superado el millón de sellos? *Sol*: 18.

Ejercicio 4.18

a) Probar, mediante inducción en n, que la suma de los n primeros enteros positivos viene dada por

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

b) En un supermercado quieren apilar las naranjas en una pirámide de base triangular de forma que cada naranja se encuentre en contacto con tres de la capa inferior.



¿cuántas naranjas serán necesarias para formar una pirámide de n capas?

Sol: $\frac{1}{6}n^3 + \frac{1}{2}n^2 + \frac{1}{3}n = \frac{1}{6}n(n+1)(n+2)$.

Ejercicio 4.19 Determinar una fórmula explícita para el término general de la sucesión

$$a_1 = \binom{1}{0}^2,\ a_2 = \binom{1}{0}^2 + \binom{2}{1}^2,\ \cdots,\ a_n = \binom{1}{0}^2 + \binom{2}{1}^2 + \cdots + \binom{n}{n-1}^2,\ \cdots$$

Sol: $a_n = \frac{1}{3}\,n^3 + \frac{1}{2}\,n^2 + \frac{1}{6}\,n \quad \forall\, n \in \mathbf{Z}^+$.

Ejercicio 4.20 La moneda oficial del *País del absurdo* es el Beckett (Bk.), existiendo monedas de 9 y 19 Bk. y billetes de 9, 19, 125 y 232 Bk.

a) ¿Puede cambiarse en monedas alguno de los billetes de más de 100 Bk. existentes? En caso afirmativo, ¿de cuantas formas diferentes puede realizarse el cambio?

Sol: Sólo el de 232 y de forma única.

b) En el último consejo de ministros se ha propuesto emitir nuevos billetes hasta completar una serie de 100 valores diferentes. A instancias del ministro de finanzas, que ha observado que la serie emitida cumple la relación

$$\begin{cases} B_1 = 9 \text{ Bk.} \\ B_2 = 19 \text{ Bk.} \\ B_n + 2B_{n-1} + B_{n-2} - 329n + 816 = 1 \text{ Bk.} \qquad (n \geq 3) \end{cases}$$

se ha decidido que toda la serie debe cumplirla. ¿De qué valor será el último billete de la nueva emisión? *Sol*: 10456 Bk.

Ejercicio 4.21

a) Hallar dos enteros positivos p_1 y p_2 sabiendo que ambos son primos y que $110p_1 + 36p_2 = 4522$.

Sol: 29 y 37.

b) Se considera la sucesión definida por

$$\begin{cases} a_0 = 2, \ a_1 = 5, \ a_2 = 11 \\ a_n = 4a_{n-1} - 5a_{n-2} + 2a_{n-3} - 2 \text{ para } n \geq 3 \end{cases}$$

Calcular una fórmula explícita para a_n y, a partir de ella, determinar el entero $e = a_9 + 2$.

Sol: $a_n = 2^n + n^2 + n + 1 \ \ \forall\, n \geq 0, \ \ e = 605$.

c) Descifrar el mensaje 709–932–214 sabiendo que ha sido cifrado (letra a letra) mediante RSA utilizando la clave (n, e) donde $n = 29 \times 37$ y $e = 605$.

El alfabeto utilizado ha sido el español:

␣	A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12	13

N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26	27

Sol: FIN.

Ejercicio 4.22 La empresa inmobiliaria española *Ladrillitos S.A.* (LASA) decide construir urbanizaciones de lujo en Venezuela y, para ello, crea una filial

Ladrillitos Venezuela S.A. (LAVENSA). Para ello LASA transfiere un millón de euros a LAVENSA y al final del primer año incrementa el capital hasta 8 millones. Las previsiones son que, a partir del segundo año, LAVENSA invierta mensualmente el valor del capital al principio del año anterior y que obtenga unos ingresos por venta de seis veces el valor del capital al inicio del año en curso.

Sea u_n el valor del capital de LAVENSA al final del año n-ésimo.

a) Probar que se verifica la relación de recurrencia

$$\begin{cases} u_0 = 1, \quad u_1 = 8 \\ u_n - 7u_{n-1} + 12u_{n-2} = 0 \quad \forall\, n \geq 2 \end{cases}$$

b) Hallar la función $U(x)$ generadora de u_n. *Sol*: $U(x) = \dfrac{1+x}{1-7x+12x^2}$.

c) Determinar el capital de LAVENSA al final del quinto año de funcionamiento haciendo uso de la función generadora $U(x)$. *Sol*: 4148 millones de euros.

d) Determinar el capital de LAVENSA al final del quinto año de funcionamiento resolviendo la recurrencia (sin hacer uso de la función generadora).

Ejercicio 4.23 Hallar una recurrencia lineal cuyo término general sea

$$a_n = n \cdot 2^{n-1} + 3^{n+1} \;\forall\, n \geq 0$$

¿Cuántos términos iniciales es necesario conocer para que dicha fórmula recurrente defina la sucesión dada cualquiera que sea $n \geq 0$?

Indicación: A la vista de la forma del término general, trata de escribir la ecuación característica de la recurrencia.

Sol: $a_{n+3} = 7a_{n+2} - 16a_{n+1} + 12a_n$. Los tres primeros.

Ejercicio 4.24

a) Probar que las sucesiones definidas por

$$\begin{cases} a_0 = 3, \; a_1 = 12, \; a_2 = 54 \\ a_n = 9a_{n-1} - 24a_{n-2} + 20a_{n-3} \end{cases} \quad \text{y} \quad \begin{cases} b_0 = 3 \\ b_n = 2b_{n-1} + 6 \cdot 5^{n-1} \end{cases}$$

son, exactamente, la misma sucesión. *Sol*: $a_n = b_n = 2^n + 2 \cdot 5^n \quad \forall\, n \geq 0$

b) Calcula su función generadora. *Sol*: $f(x) = \dfrac{3 - 15x + 18x^2}{1 - 9x + 24x^2 - 20x^3}$

Ejercicio 4.25

a) Determinar el término general de la sucesión (a_n) cuya función generadora es

$$f(x) = \frac{2 - 7x + 4x^2}{1 - 7x + 16x^2 - 12x^3}$$

b) Definir la sucesión (a_n) de forma recursiva.

Sol: $a_0 = 2,\ a_1 = 7,\ a_2 = 21,\ a_n = 7a_{n-1} - 16a_{n-2} + 12a_{n-3}\ \forall\, n \geq 3.$

c) Determina, a partir de la definición recursiva, el término general de dicha sucesión.

Sol: $a_n = (n+1) \cdot 2^n + 3^n \quad \forall\, n \geq 0.$

Ejercicio 4.26 Se considera la sucesión $\begin{cases} a_0 = 1,\ a_1 = 9,\ a_2 = 38 \\ a_n = 3a_{n-2} + 2a_{n-3} \quad \forall\, n \geq 3 \end{cases}$

a) Hallar la función generadora de dicha sucesión.

Sol: $f(x) = \dfrac{1 + 9x + 35x^2}{1 - 3x^2 - 2x^3}$.

b) Hacer uso de la función generadora para calcular el término general de la sucesión. *Sol*: $a_n = (9n - \frac{16}{3})(-1)^n + \frac{19}{3} \cdot 2^n \quad \forall\, n \geq 0.$

c) Determinar la fórmula del término general de la sucesión definida por

$$\begin{cases} a_0 = 1,\ a_1 = 9,\ a_2 = 38 \\ a_n = 3a_{n-2} + 2a_{n-3} + 9 \cdot 2^n \quad \forall\, n \geq 3 \end{cases}$$

Sol: $a_n = n(-1)^n + (4n+1)2^n \quad \forall\, n \geq 0.$

Ejercicio 4.27 Dada la sucesión (a_n) con $a_0 = 2$ y $a_1 = 12$ y la función $f : \mathbf{N} \to \mathbf{Z}$ definida de la forma $f(n) = a_{n+1} - 5a_n$, calcular el término general de la sucesión sabiendo que $\dfrac{f(n)}{f(n-1)} = 7 \ \ \forall\, n \in \mathbf{Z}^+$.

a) Planteando una recurrencia para (a_n) y resolviéndola.

b) A través de la función generadora $U(x)$ de la sucesión (a_n).

Sol: $a_n = 5^n + 7^n \quad \forall\, n \geq 0.$