E.T.S. DE INGENIERÍA INFORMÁTICA

Apuntes de

INTRODUCCIÓN A LA MATEMÁTICA DISCRETA

para la titulación de

INGENIERÍA INFORMÁTICA

Fco. Javier Cobos Gavala

Contenido

1. Aritmética entera

Dado que se supone que el alumno está familiarizado con las operaciones definidas en el conjunto **Z** de los números enteros, definiremos este conjunto a través de una *axiomática*, es decir, a través de las propiedades que cumplen sus elementos en relación con las operaciones en él definidas.

1.1 El conjunto Z de los números enteros

El conjunto, que denotaremos por **Z**, de números enteros es un conjunto de números en el que se han definido dos leyes de composición u operaciones, entre sus elementos, que verifican la siguiente lista de *axiomas*:

Propiedades de la suma y el producto

Axioma 1 *La suma y el producto son leyes de composición internas.*

$$\forall a, b \in \mathbf{Z} \Rightarrow a + b \in \mathbf{Z}, \quad ab \in \mathbf{Z}$$

Axioma 2 *Ambas leyes son asociativas.*

$$\forall a, b, c \in \mathbf{Z} \Rightarrow a + (b + c) = (a + b) + c = a + b + c \quad a(bc) = (ab)c = abc$$

Axioma 3 *Existen elementos neutro 0 y unidad 1* tales que:

$$\forall a \in \mathbf{Z} \Rightarrow a + 0 = 0 + a = a \quad a \cdot 1 = 1 \cdot a = a$$

Axioma 4 *Existen elementos opuestos.* Es decir:

$$\forall a \in \mathbf{Z} \quad \exists \ -a \in \mathbf{Z} \ : \ a + (-a) = -a + a = 0$$

Axioma 5 *Ambas leyes son conmutativas.*

$$\forall a, b \in \mathbf{Z} \Rightarrow a + b = b + a \quad ab = ba$$

Axioma 6 *El producto es distributivo respecto de la suma.*

$$\forall a, b, c \in \mathbf{Z} \Rightarrow a(b + c) = ab + ac$$

La relación de orden

En el conjunto $\mathbf{Z}$ de los números enteros se define la *relación de orden* "$\leq$", la cual cumple los siguientes propiedades:

Axioma 7 *Propiedad reflexiva*: $\forall a \in \mathbf{Z} \Longrightarrow a \leq a.$

Axioma 8 *Propiedad antisimétrica*: $\left.\begin{array}{l} a \leq b \\ b \leq a \end{array}\right\} \Longrightarrow a = b.$

Axioma 9 *Propiedad transitiva*: $\left.\begin{array}{l} a \leq b \\ b \leq c \end{array}\right\} \Longrightarrow a \leq c.$

Definición 1.1 *Sea $S \subset \mathbf{Z}$ un subconjunto de $\mathbf{Z}$. Se dice que $c \in \mathbf{Z}$ es una cota inferior del conjunto S si $c \leq a$ cualquiera que sea el elemento $a \in S$. Si además $c \in S$, recibe el nombre de primer elemento. Análogamente, se dice que $d \in \mathbf{Z}$ es una cota superior del conjunto S si $a \leq d$ cualquiera que sea el elemento $a \in S$. Si además $d \in S$, recibe el nombre de último elemento.*

Decimos *una* y no *la* cota inferior (superior) ya que cualquier número $c' \in \mathbf{Z}$ ($d' \in \mathbf{Z}$) con $c' < c$ ($d' > d$) también será una cota inferior (superior) de S.

Teniendo en cuenta la definición anterior, el conjunto $\mathbf{Z}$ de los números enteros verifica:

Axioma 10 [Buena ordenación]

> *Todo subconjunto de $\mathbf{Z}$ no vacío y acotado inferiormente (superiormente) posee un primer (último) elemento.*

Axioma 11

$$\begin{cases} a \leq b \ \text{ y } \ c > 0 \Longrightarrow & ac \leq bc \\ a \leq b \Longrightarrow & a + c \leq b + c \end{cases}$$

Teorema 1.1 [Propiedad cancelativa del producto]

$$\text{Si} \quad a \neq 0 \quad \text{y} \quad ab = ac \implies b = c$$

Demostración. Es fácil probar que si $a \cdot b = 0$ con $a \neq 0$ entonces es $b = 0$ y, a partir de ahí, que

$$ab = ac \implies a(b-c) = 0 \text{ y por ser } a \neq 0 \implies b - c = 0$$

es decir, que si $ab = ac$ y $a \neq 0$ es $b = c$. ■

Para un tratamiento formal del tema sería necesario probar que este conjunto de axiomas define a un único conjunto numérico que coincide con el conjunto **Z** definido intuitivamente. Aquí prescindiremos de la demostración de la existencia y unicidad de este conjunto debido a que desbordaría las necesidades de este curso de Introducción a la Matemática Discreta.

1.2 Inducción matemática

En cualquier ciencia experimental, la inducción es el proceso de obtener un resultado general a partir del análisis de casos particulares. De esta forma, observando la caída de una serie de cuerpos pesados se induce que *cualquier* cuerpo más pesado que el aire cae por la acción de la gravedad. Este hecho se considerará válido mientras no se encuentre un cuerpo más pesado que el aire que no caiga.

En Matemáticas se utiliza un proceso equivalente pero con la diferencia de que el resultado inducido es necesario *probar* que siempre se va a cumplir.

1.2.1 Definiciones recursivas

Muchas veces nos habremos encontrado con expresiones del tipo

$$S_n = 1 + 3 + 5 + \cdots + (2n-1) \quad \text{con} \quad n \in \mathbf{N} \tag{1.1}$$

pero *¿cómo interpretar los puntos suspensivos?*

La respuesta es que nos hacen ver que estamos dando una definición *recursiva* de S_n. Es decir, estamos definiendo

$$S_1 = 1 \quad \text{y} \quad S_n = S_{n-1} + (2n-1) \quad \text{siempre que } n \in \mathbf{N}$$

De esta manera, para definir el valor de S_n debemos utilizar el de S_{n-1}. En otras palabras, estamos utilizando la función en su propia definición. Evidentemente, si para calcular el transformado de un elemento n necesitamos conocer el del elemento anterior $n-1$, tendremos que conocer cuál es el transformado del primer elemento para, a partir de él, calcular todos los demás.

Obsérvese que, como consecuencia del axioma de buena ordenación, podemos definir funciones de $\mathbf{N}$ en otro conjunto cualquiera de forma recursiva, ya que cualquiera que sea el conjunto de originales $C \subseteq \mathbf{N}$ por ser un subconjunto de $\mathbf{Z}$ y estar acotado inferiormente (ya que $\mathbf{N}$ lo está por 0), posee un primer elemento y, por tanto, a partir de ese elemento podemos definir todos los posteriores. No ocurriría así si tratáramos de definir una función $f : \mathbf{Z} \to Y$ de forma recursiva ya que al dar $f(n)$ en función de $f(n-1)$ y no estar $\mathbf{Z}$ acotado inferiormente, no tendríamos un primer elemento a partir del cual obtener todos los restantes.

Debido a que las funciones de $\mathbf{N}$ en otro conjunto numérico como pueden ser $\mathbf{R}$ o $\mathbf{C}$ reciben el nombre de *sucesiones* y se suelen denotar por u_n en vez de por $u(n)$, utilizaremos dicha notación.

En nuestro ejemplo tenemos que

$$S_1 = 1 \quad S_2 = 4 \quad S_3 = 9 \quad \ldots$$

Si consideramos el polinomio $P(n) = n^3 - 5n^2 + 11n - 6$ vemos que:

$$P(1) = 1 = S_1 \quad P(2) = 4 = S_2 \quad \text{y} \quad P(3) = 9 = S_3$$

sin embargo, no podemos asegurar que $S_n = P(n) \quad \forall n \in \mathbf{N}$. Para poder garantizarlo tendríamos que probar que se verifica para *cualquier* elemento $n \in \mathbf{N}$. Para probar que no es cierto bastará con encontrar un contraejemplo, es decir, un caso para el que no se verifique la igualdad. En nuestro caso $P(4) = 22$ mientras que $S_4 = 16$, es decir $P(4) \neq S_4$ por lo que podemos asegurar que la igualdad no es cierta.

Vemos entonces que una igualdad de este tipo no puede probarse estudiando casos particulares, ya que para 1, 2 y 3 sí era cierto, pero para 4 no lo es. En general puede que lo hayamos comprobado para una gran cantidad de elementos y sin embargo, falle en cualquier momento. De aquí, la necesidad de *probar* que va a cumplirse cualquiera que sea el elemento que se tome.

1.2.2 Conjuntos inductivos

Definición 1.2 [Conjunto inductivo]

Un conjunto S se dice que es inductivo si verifica las condiciones:

$$\begin{cases} 1 \in S \\ x \in S \implies x+1 \in S \end{cases}$$

Teorema 1.2 *Si $S \subseteq \mathbf{N}$ es un conjunto inductivo, entonces $S = \mathbf{N}$.*

Demostración. Si $S \neq \mathbf{N}$, sea S^* el complementario de S en $\mathbf{N}$.

Como $S^* \subseteq \mathbf{N} \subset \mathbf{Z}$ y está acotado inferiormente (ya que $\mathbf{N}$ lo está), por el axioma de buena ordenación de los números enteros, sabemos que S^* posee un primer elemento que denotaremos por a.

Por tratarse del *primer* elemento, $a-1 \notin S^*$, por lo que $a-1 \in S$ y como por hipótesis S era inductivo, $(a-1)+1 = a \in S$ en contra de que a era un elemento de S^*.

Por tanto, ha de ser necesariamente $S^* = \emptyset$ o lo que es lo mismo, $S = \mathbf{N}$. ■

1.2.3 El método de inducción

Teorema 1.3 [Método de inducción simple]

Sea P_n una proposición matemática. Si se verifican:

$$\begin{cases} P_1 \text{ es verdadera} \\ P_k \text{ verdadera} \implies P_{k+1} \text{ también lo es,} \end{cases}$$

entonces, P_n es verdadera para cualquier $n \in \mathbf{N}$.

Demostración. Sea $S = \{n \in \mathbf{N} \ : \ P_n \text{ es cierta}\}$.

Las hipótesis del teorema nos dicen que:

$$\left.\begin{array}{l} 1 \in S \\ k \in S \implies k+1 \in S \end{array}\right\} \implies S \text{ es inductivo} \implies S = \mathbf{N}$$

La propiedad P_n es cierta $\forall\, n \in \mathbf{N}$. ■

Ejemplo 1.1 Si nos fijamos en la sucesión definida en (1.1) observamos que

$$S_1 = 1 = 1^2 \quad S_2 = 4 = 2^2 \quad S_3 = 9 = 3^2 \quad S_4 = 16 = 4^2$$

En un primer paso, la inducción nos conduce a pensar en la posibilidad de que $S_n = n^2$. Es ahora cuando debemos aplicar formalmente el método de inducción matemática.

Hemos comprobado ya que se verifica para $n = 1$. Además, supongamos que $S_n = n^2$ y veamos si entonces es $S_{n+1} = (n+1)^2$. En efecto:

$$S_{n+1} = S_n + [2(n+1) - 1] = n^2 + 2n + 1 = (n+1)^2$$

Al haber probado la veracidad para $n = 1$ y que es cierto para $n + 1$ si lo es para n, hemos probado que es cierta para cualquier natural n.

Es ahora cuando podemos asegurar que $S_n = n^2 \ \ \forall n \in \mathbf{N}$. □

Una variante del método de inducción matemática es el denominado *método de inducción completa*.

Teorema 1.4 [Método de inducción completa]

Sea P_n una proposición matemática. Si se verifican:

$$\begin{cases} P_1, P_2, \ldots, P_r \text{ son verdaderas} \\ P_1,\ P_2, \ldots, P_k, \text{ con } k \geq r, \text{ verdaderas} \implies P_{k+1} \text{ también lo es} \end{cases}$$

entonces, P_n es verdadera para cualquier $n \in \mathbf{N}$.

1.3 Múltiplos y Divisores

Comenzaremos esta sección estudiando el *algoritmo de divisibilidad* que establece el siguiente teorema:

Teorema 1.5 [Algoritmo de la divisibilidad]

Si a y b son enteros con $b > 0$, existe un único par de enteros q y r tales que

$$a = qb + r \qquad con \qquad 0 \leq r < b.$$

Demostración.

a) Existencia:

Sea $S = \{a - nb \mid n \in \mathbf{Z}\} = \{a,\ a \pm b,\ a \pm 2b,\ \dots\}$. Este conjunto de enteros contiene elementos no negativos (por ejemplo, para $n = -|a|$), por lo que $S \cap \mathbf{N}$ es un subconjunto no vacío de $\mathbf{N}$ y, por tanto, de $\mathbf{Z}$. El principio de buena ordenación de los números enteros nos asegura la existencia de un primer elemento que será de la forma $r = a - qb \geq 0$ para algún entero q. Se tiene, por tanto, que $a = qb + r$ con $r \geq 0$. Si $r \geq b$, S contendría al elemento no negativo $a - (q+1)b = r - b < r$ que contradice el hecho de que r es el primer elemento de $S \cap \mathbf{N}$. Por tanto, $r < b$.

b) Unicidad

Supongamos que $a = qb + r = q'b + r'$ con $0 \leq r < b$ y $0 \leq r' < b$. Entonces $r - r' = (q' - q)b$. Si $q \neq q'$, es $|q' - q| \geq 1$, por lo que $|r - r'| \geq |b| = b$ lo que imposibilita el hecho de que r y r' estén ambos entre 0 y $b-1$ inclusive. Por tanto, ha de ser $q = q'$ y de ahí que también sea $r = r'$, lo que prueba la unicidad. ■

Ejemplo 1.2

a) Si $a = 9$ y $b = 4$, como $9 = 2 \times 4 + 1$ con $0 \leq 1 < 4$, se tiene que $q = 2$ y $r = 1$.

b) Si $a = -9$ y $b = 4$, como $-9 = -3 \times 4 + 3$ con $0 \leq 3 < 4$, se tiene que $q = -3$ y $r = 3$. □

Si consideramos ahora el caso $b < 0$, dado que $-b > 0$, el Teorema 1.5 nos garantiza la existencia de los enteros q^* y r tales que $a = q^*(-b) + r$ con $0 \leq r < -b$, y haciendo $q^* = -q$ se obtiene que $a = qb + r$. La prueba de la unicidad es similar a la anterior.

Teniendo en cuenta este resultado y el del Teorema 1.5, podemos establecer el siguiente corolario:

Corolario 1.6 *Si a y b son dos enteros con $b \neq 0$, existe un único par de enteros q y r tales que*

$$a = qb + r \qquad con \qquad 0 \leq r < |b|$$

Definición 1.3 *Con la notación del Teorema 1.5 el entero q recibe el nombre de cociente entero o simplemente cociente y el también entero r el de resto. Si dividimos por b obtenemos que*

$$\frac{a}{b} = q + \frac{r}{b} \qquad con \qquad 0 \leq \frac{r}{b} < 1$$

por lo que q es el mayor entero no superior a a/b, recibe el nombre de suelo de a/b y se representa por $\left\lfloor \frac{a}{b} \right\rfloor$.

De forma análoga, al menor entero no inferior al cociente a/b lo denotamos por $\left\lceil \frac{a}{b} \right\rceil$ y recibe el nombre de techo de a/b.

$$Suelo\ de\ \frac{a}{b} \iff \left\lfloor \frac{a}{b} \right\rfloor\ mayor\ entero\ no\ superior\ a\ \frac{a}{b}$$

$$Techo\ de\ \frac{a}{b} \iff \left\lceil \frac{a}{b} \right\rceil\ menor\ entero\ no\ inferior\ a\ \frac{a}{b}$$

Ejemplo 1.3 Vamos a probar, como una aplicación, que si n es un cuadrado perfecto, al dividirlo entre 4 sólo puede darnos como resto 0 ó 1.

Sea $n = a^2$. El Teorema 1.5 (con $b = 4$) nos dice que $a = 4q + r$ con $r = 0,\ 1,\ 2$ ó 3, por lo que $n = a^2 = (4q + r)^2 = 16q^2 + 8qr + r^2$.

a) Si $r = 0$ obtenemos que $n = 4(4q^2) + 0 \implies$ el resto es 0,
b) si $r = 1$ que $n = 4(4q^2 + 2q) + 1 \implies$ el resto es 1,
c) si $r = 2$ que $n = 4(4q^2 + 4q + 1) + 0 \implies$ el resto es 0,
d) y si $r = 3$ que $n = 4(4q^2 + 6q + 2) + 1 \implies$ el resto es 1.

En cualquiera de los casos, el resto es siempre 0 ó 1. □

Definición 1.4 *Si a y b son enteros y $a = qb$ para algún entero q, diremos que b divide a a, que b es un divisor (o factor) de a, o que a es múltiplo. Si b no divide a a lo denotaremos por $b \nmid a$.*

$$b \mid a \iff b\ divide\ a\ a$$
$$b \nmid a \iff b\ no\ divide\ a\ a$$
$$a = \bullet\, b \iff a\ es\ múltiplo\ de\ b$$

Ejemplo 1.4 Los factores o divisores de 6 son $\pm 1,\ \pm 2,\ \pm 3$ y ± 6. □

Obsérvese que cualquier entero divide a 0 (ya que $0 = 0 \cdot b$ para cualquiera que sea $b \in \mathbf{Z}$), 1 divide a cualquier entero y cualquier entero se divide a si mismo.

A partir de ahora, cuando hablemos de los divisores de un número nos referiremos a sus divisores positivos.

Definición 1.5 *Dado un entero n, se denominan divisores propios a sus divisores distintos de 1 y del propio n, a los cuales se les denomina divisores impropios del número.*

Teorema 1.7 [Propiedades de la divisibilidad]

a) $a \mid b$ *y* $b \mid c \implies a \mid c$.

b) $a \mid b$ *y* $c \mid d \implies ac \mid bd$.

c) $m \neq 0 \implies a \mid b$ *si, y sólo si,* $ma \mid mb$.

d) $d \mid a$ *y* $a \neq 0 \implies |d| \leq |a|$.

e) Si c divide a $a_1, a_2, \ldots, a_k \implies c$ divide a $a_1u_1 + a_2u_2 + \cdots + a_ku_k$ cualesquiera que sean los enteros $u_1, u_2, \ldots, u_k$.

f) $a \mid b$ *y* $b \mid a$ *si, y sólo si,* $a = \pm b$.

Demostración.

a)

$$\left.\begin{array}{l} a \mid b \implies b = aq_1 \quad \text{con} \quad q_1 \in \mathbf{Z} \\ b \mid c \implies c = bq_2 \quad \text{con} \quad q_2 \in \mathbf{Z} \end{array}\right\} \implies$$

$$c = aq_1q_2 = aq \quad \text{con} \quad q = q_1q_2 \in \mathbf{Z} \implies a \mid c.$$

b)

$$\left.\begin{array}{l} a \mid b \implies b = aq_1 \quad \text{con} \quad q_1 \in \mathbf{Z} \\ c \mid d \implies d = cq_2 \quad \text{con} \quad q_2 \in \mathbf{Z} \end{array}\right\} \implies$$

$$bd = acq_1q_2 = acq \quad \text{con} \quad q = q_1q_2 \in \mathbf{Z} \implies ac \mid bd.$$

c) $\Rightarrow$

$$\left.\begin{array}{l} a \,|\, b \implies b = aq \quad \text{con} \quad q \in \mathbf{Z} \\ m \neq 0 \end{array}\right\} \implies$$

$$mb = maq \quad \text{con} \quad ma \neq 0 \implies ma \,|\, mb.$$

$\Leftarrow$

$$ma \,|\, mb \implies mb = maq \quad \text{con} \quad q \in \mathbf{Z}$$

al ser $m \neq 0$ por la propiedad cancelativa de los enteros tenemos que $b = aq$ con $q \in \mathbf{Z}$, por lo que $a \,|\, b$.

d) Si $d \,|\, a$ tenemos que $a = dq$ con $q \in \mathbf{Z}$ y $q \neq 0$ (en caso contrario sería $a = 0$ en contra de nuestra hipótesis). Se tiene por tanto que $|q| \geq 1$, por lo que

$$a = dq \implies |a| = |d| \cdot |q| \geq |d| \cdot 1 = |d|$$

o, lo que es lo mismo, que $|d| \leq |a|$.

e) Si $c \,|\, a_i$ se tiene que $a_i = q_i c$ para algunos enteros q_i (i=1,2,...,k). Entonces $a_1u_1 + a_2u_2 + \cdots + a_ku_k = q_1cu_1 + q_2cu_2 + \cdots + q_kcu_k = (q_1u_1 + q_2u_2 + \cdots + q_ku_k)c$ y dado que $q_1u_1 + q_2u_2 + \cdots + q_ku_k$ es un entero (ya que $q_i \in \mathbf{Z}$ y $u_i \in \mathbf{Z}$) se tiene que $c \,|\, (a_1u_1 + a_2u_2 + \cdots + a_ku_k)$.

f) Si $a = \pm b$ se tiene que $b = qa$ y $a = q'b$ donde $q = q' = \pm 1$, por lo que $a \,|\, b$ y $b \,|\, a$.

Recíprocamente, si $a \,|\, b$ y $b \,|\, a$ es $b = qa$ y $a = q'b$ con $q, q' \in \mathbf{Z}$.

Si $b = 0$, de la segunda igualdad se obtiene que $a = 0$, por lo que $a = \pm b$. Podemos suponer, por tanto, que $b \neq 0$.

Utilizando ambas expresiones, obtenemos que $b = qq'b$ y como $b \neq 0$ es $qq' = 1$, por lo que $q, q' = \pm 1$ (Teorema 1.7–(d)) y $a = \pm b$. ■

La forma más usual del Teorema 1.7–(e) es el caso $k = 2$, que recordamos a continuación con una notación más simple.

Corolario 1.8 *Si c es un divisor de a y de b, divide a $au + bv$ cualesquiera que sean los enteros u y v.*

1.3.1 Máximo común divisor

Si $d \,|\, a$ y $d \,|\, b$ decimos que d es un *divisor común* o *factor común* de a y b; por ejemplo, 1 es un divisor común a cualquier par de enteros a y b.

Teorema 1.9 [Máximo común divisor]

Dados dos enteros a y b, no ambos nulos, se denomina máximo común divisor de a y b, y se denota por $\text{mcd}\,(a,b)$*, al mayor de sus divisores comunes, que existe y es único.*

$$\begin{cases} d \,|\, a \quad y \quad d \,|\, b \quad \text{(por ser } d \text{ un divisor común).} \\ \\ \text{Si } c \,|\, a \text{ y } c \,|\, b \Longrightarrow c \leq d \text{ (pues } d \text{ es el mayor divisor común de } a \text{ y } b\text{).} \end{cases}$$

Demostración.

- Existencia: Sean

$$\begin{aligned} D_a &= \{\text{divisores positivos de } a\} \implies \text{a } \textit{cota superior de } D_a \\ D_b &= \{\text{divisores positivos de } b\} \implies \text{b } \textit{cota superior de } D_b \end{aligned}$$

  El conjunto $D_{ab} = D_a \cap D_b$ de los divisores comunes de a y b verifica que

$$\begin{aligned} &D_{ab} \subseteq \mathbf{Z} \\ &D_{ab} \neq \emptyset \quad \text{ya que} \begin{cases} 1 \in D_a \\ 1 \in D_b \end{cases} \\ &D_{ab} \quad \text{está acotado superiormente por estarlo } D_a \text{ y } D_b \end{aligned}$$

  El principio de buena ordenación nos garantiza la existencia de un último elemento, es decir, del mcd (a,b)

- Unicidad: Supongamos que existiesen dos d y d'.

$$\left.\begin{aligned} d \,|\, a,\ d \,|\, b \quad &\text{y al ser } d' = \text{mcd}\,(a,b) \implies d \leq d' \\ d' \,|\, a,\ d' \,|\, b \quad &\text{y al ser } d \ = \text{mcd}\,(a,b) \implies d' \leq d \end{aligned}\right\} \implies d = d'$$

■

El caso $a = b = 0$ debe ser excluido ya que como cualquier entero divide a 0, el conjunto $D_{00} = \mathbf{Z}$ no está acotado superiormente.

Teorema 1.10 [Propiedades del máximo común divisor]

- $\text{mcd}\,(a,b) = \text{mcd}\,(b,a) = \text{mcd}\,(-a,b) = \text{mcd}\,(a,-b) = \text{mcd}\,(-a,-b)$
- $\text{mcd}\,(a,a) = \text{mcd}\,(a,0) = a$

Calcularemos siempre $\text{mcd}\,(a,b)$ *con* $a > b > 0$

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

Demostración. Las dos primeras son triviales. Para la tercera sean

$$\begin{cases} d = \text{mcd}\,(a_1,\ldots,a_k), \\ d_{12} = \text{mcd}\,(a_1,a_2), \\ D = \text{mcd}\,(d_{12},a_3,\ldots,a_k). \end{cases}$$

Se trata de probar que $D = d$, y para ello, es necesario ver que

a) D divide a $a_1,\ldots,a_k$
b) si c divide a $a_1,\ldots,a_k \Longrightarrow c \leq D$

En efecto:

a) $D \,|\, d_{12},a_3,\ldots,a_k$ y como $d_{12} \,|\, a_1,a_2$ se tiene que $D \,|\, a_1,\ldots,a_k$.

b) Si $c \,|\, a_1,\ldots,a_k$ se tiene que $\begin{cases} c \,|\, a_1,a_2 \Longrightarrow c \,|\, d_{12} \\ c \,|\, a_3,\ldots,a_k \end{cases} \Longrightarrow c \leq D.$ ∎

1.3.2 Algoritmo de Euclides

Una forma de encontrar el máximo común divisor de a y b consiste simplemente en construir las listas de todos los divisores positivos de a y todos los de b para buscar el mayor entero que aparece en ambas, pero evidentemente no es práctica. Existe un método eficiente, para calcular el máximo común divisor, llamado *algoritmo de Euclides* (publicado en el libro VII de los *Elementos* de Euclides alrededor del año 300 a.C.).

Lema 1.11 *Dados dos enteros* a *y* b *se verifica que* $\text{mcd}\,(a,b) = \text{mcd}\,(b,r)$ *cualesquiera que sean los enteros* q *y* r *verificando que* $a = bq + r$.

Demostración. Por el Corolario 1.8 cualquier divisor común de b y de r también divide a $qb + r = a$; de manera análoga, como $r = a - qb$, obtenemos que cualquier divisor común de a y b también divide a r. Por tanto, las parejas (a, b) y (b, r) poseen los mismos divisores comunes lo que nos lleva a que comparten el máximo común divisor. ■

Algoritmo de Euclides

Sean a y b dos enteros (no ambos nulos) y tratemos de calcular $d = \text{mcd}\,(a, b)$ donde podemos suponer que $a > b > 0$. Utilizando el algoritmo de la divisibilidad (Teorema 1.5) obtenemos

$$a = q_1 b + r_1 \qquad \text{con} \qquad 0 \leq r_1 < b.$$

Dividendo ahora b entre r_1 se obtiene

$$b = q_2 r_1 + r_2 \qquad \text{con} \qquad 0 \leq r_2 < r_1.$$

Repitiendo el proceso obtenemos una sucesión de restos (r_i) con

$$b > r_1 > r_2 > \cdots > r_k > \cdots \geq 0$$

Al tratarse de una sucesión de enteros positivos estrictamente decreciente, llegará un momento en el que necesariamente sea $r_n = 0$ y en ese punto finalizamos el proceso.

$$\text{mcd}\,(a, b) = \text{mcd}\,(b, r_1) = \cdots = \text{mcd}\,(r_{n-2}, r_{n-1}) = \text{mcd}\,(r_{n-1}, 0) = r_{n-1}$$

Ejemplo 1.5 Para calcular el mcd $(112, 70)$ obtenemos

$$\text{mcd}\,(112, 70) \overset{112=70+42}{=} \text{mcd}\,(70, 42) \overset{70=42+28}{=} \text{mcd}\,(42, 28) \overset{42=28+14}{=} \text{mcd}\,(28, 14) \overset{28=2\cdot 14+0}{=} \text{mcd}\,(14, 0) = 14 \qquad \square$$

Este algoritmo para el cálculo del máximo común divisor de dos enteros positivos a y b (con $a > b > 0$) recibe el nombre de *Algoritmo de Euclides* y puede escribirse como sigue:

P1 Leer a y b

P2 r = resto de dividir a entre b

P3 si $r = 0$ entonces el mcd $(a, b) = b$. FIN

P4 si no $a = b$, $b = r$

P5 ir al Paso 2

Ejemplo 1.6 Para calcular $d = \text{mcd}\,(1492, 1066)$ obtenemos

$$1492 = 1 \times 1066 + 426$$
$$1066 = 2 \times 426 + 214$$
$$426 = 1 \times 214 + 212$$
$$214 = 1 \times 212 + 2$$
$$212 = 106 \times 2 + 0$$

a	b	r
1492	1066	426
1066	426	214
426	214	212
214	212	2
212	**2**	**0**

por lo que $\text{mcd}\,(1492, 1066) = 2$ □

Algoritmo del mínimo resto

Aunque el algoritmo de Euclides no es mejorable, en cuanto al *orden del algoritmo*, sí se puede mejorar, en algunos casos, en el número de divisiones.

Si en alguna de las divisiones efectuadas obtenemos

$$r_{k-1} = q \cdot r_k + r_{k+1} \quad 0 \le r_{k+1} < r_k \quad r_{k+1} > \frac{r_k}{2}$$

podemos hacer la división por exceso para obtener

$$r_{k-1} = (q+1) \cdot r_k + (r_{k+1} - r_k) \quad r_{k+1} - r_k < 0$$

$$\text{mcd}\,(r_{k-1}, r_k) = \text{mcd}\,(r_k, r'_{k+1}) \quad \text{con} \quad r'_{k+1} = r_k - r_{k+1} < r_{k+1}$$

por lo que aceleraremos la convergencia a cero de la sucesión de restos.

El resto r'_{k+1} se conoce como *mínimo resto* ya que de todos los restos posibles de la división de r_{k-1} entre r_k (olvidándonos del resto no negativo menor que el divisor) es el que tiene menor valor absoluto.

Dicho algoritmo se puede escribir de la forma

```
P1   Leer a y b
P2   r = resto de dividir a entre b
P3   si r = 0 entonces el mcd (a, b) = b.  FIN
P4   r > b/2 entonces r = b − r
P5   si no a = b , b = r
P6   ir al Paso 2
```

Ejemplo 1.7 Sigamos ambos algoritmos para los enteros 21 y 13.

Euclides

a	b	r
21	13	8
13	8	5
8	5	3
5	3	2
3	2	1
2	1	0

6 divisiones

Mínimo resto

a	b	r	r
21	13	~~8~~	5
13	5	~~3~~	2
3	2	1	
2	1	0	

4 divisiones

□

1.3.3 La identidad de Bezout

Si nos fijamos en el Ejemplo 1.5 observamos que:

$$14 = 42-28 = (112-70)-(70-42) = 112-2\cdot 70+42 = 112-2\cdot 70+(112-70) \Rightarrow$$

$$14 = 2 \cdot 112 - 3 \cdot 70$$

¿Es siempre posible expresar $\text{mcd}\,(a,b)$ *como combinación lineal de* a *y* b*?*

Teorema 1.12 [Identidad de Bezout]

Si a *y* b *son enteros (no ambos nulos) existen enteros* u *y* v *tales que*

$$\text{mcd}\,(a,b) = au + bv.$$

Los enteros u *y* v *no son únicos.*

Demostración. Haremos uso de las ecuaciones que utilizamos en la aplicación del algoritmo de Euclides para calcular $d = \text{mcd}\,(a,b)$ como el último resto no nulo r_{n-1}. La penúltima ecuación, escrita de la forma

$$r_{n-1} = r_{n-3} - q_{n-1}r_{n-2},$$

expresa d como una combinación lineal de r_{n-3} y r_{n-2}.

Utilizamos ahora la ecuación anterior, en la forma

$$r_{n-2} = r_{n-4} - q_{n-2}r_{n-3},$$

para eliminar r_{n-2} y expresar d como combinación lineal de r_{n-4} y r_{n-3}.

Retrocediendo podemos ir eliminando sucesivamente $r_{n-3}, r_{n-4}, \ldots$ hasta obtener d como combinación lineal de a y b. ■

Ejemplo 1.8 En el Ejemplo 1.6 utilizamos el algoritmo de Euclides para calcular $d = \text{mcd}\,(1492, 1066)$. Observando las divisiones realizadas en dicho ejemplo obtenemos:

$$\left.\begin{aligned} d = 2 &= 214 - 1 \cdot 212 = 214 - 1 \cdot (426 - 1 \cdot 214) \\ &= -1 \cdot 426 + 2 \cdot 214 = -1 \cdot 426 + 2 \cdot (1066 - 2 \cdot 426) \\ &= 2 \cdot 1066 - 5 \cdot 426 = 2 \cdot 1066 - 5 \cdot (1492 - 1 \cdot 1066) \\ &= -5 \cdot 1492 + 7 \cdot 1066 = -5 \cdot a + 7 \cdot b \end{aligned}\right\} \Rightarrow \begin{cases} u = -5 \\ v = 7 \end{cases}$$

El hecho de que $528 \cdot 1492 - 739 \cdot 1066 = 2$ prueba que los valores que hemos encontrado para u y v no son únicos.
Más adelante, en el Teorema 1.19 veremos cómo se determinan todos los posibles valores de u y v. □

Algoritmo extendido de Euclides

Una mejora del algoritmo de Euclides y conocida como *Algoritmo extendido de Euclides* permite, no sólo calcular $d = \text{mcd}\,(a, b)$, sino que nos proporciona una pareja de enteros u y v tales que $d = au + bv$.

P1	Leer a y b
P2	$u' = 1,\ v = 1,\ u = 0,\ v' = 0,\ c = a,\ d = b$
P3	$q = \left\lfloor \frac{c}{d} \right\rfloor,\ r = c - d \cdot q$
P4	si $r = 0$ entonces FIN $(d = au + bv)$
P5	si no $c = d,\ d = r$
	$t = u',\ u' = u,\ u = t - qu,$
	$t = v',\ v' = v,\ v = t - qv,$
P6	ir al Paso 3

Ejemplo 1.9 La siguiente tabla nos da los valores que toman en cada paso las diferentes variables del algoritmo extendido de Euclides para el cálculo del

máximo común divisor de los números $a = 1769$ y $b = 551$.

u'	u	v'	v	c	d	q	r
1	0	0	1	1769	551	3	116
0	1	1	-3	551	116	4	87
1	-4	-3	13	116	87	1	29
-4	**5**	13	**-16**	87	**29**	3	0

$$29 = 5 \cdot 1769 - 16 \cdot 551$$

□

Al igual que hemos generalizado el algoritmo de Euclides para el caso de k enteros, podemos generalizar la identidad de Bezout.

Teorema 1.13 *Dados los enteros $a_1, a_2, \ldots, a_k$ (no todos nulos) existen enteros $u_1, u_2, \ldots, u_k$ tales que*

$$\text{mcd}\,(a_1, a_2, \ldots, a_k) = u_1a_1 + u_2a_2 + \cdots + u_ka_k$$

Definición 1.6 [Números coprimos]

Dos enteros a y b se dicen coprimos, primos relativos o primos entre sí si $\text{mcd}\,(a, b) = 1$. *Se denota por $a \perp b$.*

En el caso de un conjunto de k enteros se tiene:

- $a_1, a_2, \ldots, a_k$ *coprimos* $\iff \text{mcd}\,(a_1, a_2, \ldots, a_k) = 1$
- $a_1, a_2, \ldots, a_k$ *mutuamente coprimos* $\iff \text{mcd}\,(a_i, a_j) = 1 \quad \forall\, i \neq j$

Teorema 1.14 [Propiedades de los números coprimos]

a) Mutuamente coprimos $\underset{\not\Longleftarrow}{\Longrightarrow}$ *coprimos*

b) $a \perp b \iff \exists\, x, y \in \mathbf{Z}$ *tales que* $ax + by = 1$

c) $a \perp b$, $a \mid c$ *y* $b \mid c \implies ab \mid c$

d) $a \perp b$ *y* $a \mid bc \implies a \mid c$

Demostración.

a) Si $a_1, a_2, \ldots, a_k$ son mutuamente coprimos mcd $(a_1, a_2) = 1$

$$\text{mcd}\,(a_1, a_2, \ldots, a_k) = \text{mcd}\,(1, a_3, \ldots, a_k) = 1 \implies \text{coprimos}$$

Sin embargo 6, 10 y 15 son coprimos ya que mcd $(6, 10, 15) = 1$ pero no mutuamente coprimos, pues mcd $(6, 10) = 2 \neq 1$.

b) Si $a \perp b$ es mcd $(a, b) = 1$ y por la identidad de Bezout sabemos que existen enteros x, y tales que $ax + by = \text{mcd}\,(a, b) = 1$.

Recíprocamente, dado que $d = \text{mcd}\,(a, b)$ divide a a y a b podemos expresar $a = a'd$ y $b = b'd$ con a' y b' enteros, por lo que si existen $x, y \in \mathbf{Z}$ tales que $ax + by = 1$,

$$a'dx + b'dy = 1 \;\Rightarrow\; d(a'x + b'y) = 1 \;\text{ con }\; a'x + b'y \in \mathbf{Z} \;\Rightarrow\; d \,|\, 1 \;\Rightarrow\; d = 1$$

es decir $a \perp b$.

c) $$\left.\begin{array}{l} a \,|\, c \implies c = ae \;\text{ con }\; e \in \mathbf{Z} \\ b \,|\, c \implies c = bf \;\text{ con }\; f \in \mathbf{Z} \end{array}\right\}$$

Además, por ser $a \perp b$, existen $x, y \in \mathbf{Z}$ tales que $ax + by = 1$. Multiplicando por c obtenemos

$$c = cax + cby = (bf)ax + (ae)by = ab(fx + ey) \implies ab \,|\, c.$$

d) $a \perp b \implies \exists\, x, y \in \mathbf{Z}$ tales que $ax + by = 1 \implies c = acx + bcy$.

Por otra parte, $a \,|\, bc \implies bc = at$ con $t \in \mathbf{Z}$ y por tanto

$$c = acx + aty = a(cx + ty) \;\text{ con }\; cx + ty \in \mathbf{Z} \implies a \,|\, c. \qquad \blacksquare$$

Teorema 1.15 *Sean a y b dos enteros (no ambos nulos) cuyo máximo común divisor es d. Entonces un entero c puede escribirse de la forma $ax + by$ para algunos enteros x e y si, y sólo si, c es múltiplo de d. En particular, d es el menor entero de la forma $ax + by$ $(x, y \in \mathbf{Z})$.*

Demostración. Si $c = ax + by$ con $x, y \in \mathbf{Z}$ como d divide a a y a b

$$c = a'dx + b'dy \;\text{ con }\; a', b' \in \mathbf{Z} \implies d \,|\, c$$

Recíprocamente, si $c = de$ para algún entero e, escribiendo la identidad de Bezout $d = au + bv$ se tiene que $c = aue + bve = ax + by$, donde $x = ue$ e $y = ve$ son ambos enteros.

Por tanto, los enteros de la forma $ax + by$ $(x, y \in \mathbf{Z})$ son los múltiplo de d, y el menor entero positivo de esta forma es el menor múltiplo positivo de d, es decir, el propio d. ■

Corolario 1.16 *Si* mcd $(a, b) = d$*, para cualquier entero* $m > 0$

$$\text{mcd}\,(ma, mb) = md \qquad\qquad \text{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Demostración. Por el Teorema 1.15, mcd (ma, mb) es el menor valor de $max + mby = m(ax + by)$ donde $x, y \in \mathbf{Z}$, dado que d es el menor valor positivo de $ax + by$, se tiene que mcd $(ma, mb) = md$.

Escribiendo $d = au + bv$ y dividiendo por d se tiene que

$$\frac{a}{d}u + \frac{b}{d}v = 1 \implies \frac{a}{d} \text{ es primo con } \frac{b}{d}.$$ ■

1.3.4 Mínimo común múltiplo

Si $a = \overset{\bullet}{m}$ y $b = \overset{\bullet}{m}$ decimos que m es un *múltiplo común* de a y b; por ejemplo, ab es un múltiplo común al par de enteros a y b.

Teorema 1.17 [Mínimo común múltiplo]

Dados dos enteros a *y* b*, se denomina mínimo común múltiplo de* a *y* b *y se denota por* mcm (a, b) *al menor de sus múltiplos comunes positivos, que existe y es único.*

$$\begin{cases} a = \overset{\bullet}{m} \;\; y \;\; b = \overset{\bullet}{m} \;\; \text{(por ser } m \text{ un múltiplo común).} \\ \text{Si } c = \overset{\bullet}{a} \text{ y } c = \overset{\bullet}{b} \;\Rightarrow\; c \geq m \;(m \text{ es el menor múltiplo común de } a \text{ y } b). \end{cases}$$

Demostración.

- Existencia: Sean

$$M_a = \{\text{múltiplos positivos de } a\} \implies \text{a } \textit{cota inferior de } M_a$$
$$M_b = \{\text{múltiplos positivos de } b\} \implies \text{b } \textit{cota inferior de } M_b$$

El conjunto $M_{ab} = M_a \cap M_b$ de los múltiplos comunes de a y b verifica que

$$M_{ab} \subseteq \mathbf{Z}$$

$$M_{ab} \neq \emptyset \text{ ya que } \begin{cases} ab \in M_a \\ ab \in M_b \end{cases}$$

M_{ab} está acotado inferiormente por estarlo M_a y M_b

El principio de buena ordenación nos garantiza la existencia de un primer elemento, es decir, del mcm (a, b)

- UNICIDAD: Supongamos que existiesen dos m y m'.

$$\left.\begin{array}{l} m = \overset{\bullet}{a},\ m = \overset{\bullet}{b} \text{ y al ser } m' = \text{mcm}\,(a,b) \implies m \geq m' \\ m' = \overset{\bullet}{a},\ m' = \overset{\bullet}{b} \text{ y al ser } m = \text{mcm}\,(a,b) \implies m' \geq m \end{array}\right\} \Rightarrow m = m'$$

■

Teorema 1.18 *Sean a y b dos enteros positivos y sean d y m su* mcd *y su* mcm *respectivamente. Se verifica entonces que*

$$dm = ab.$$

Demostración. No supone restricción alguna el suponer $a, b > 0$.

Sean $a' = a/d$ y $b' = b/d$ y consideremos

$$\frac{ab}{d} = \frac{da' \cdot db'}{d} = da'b'.$$

Evidentemente $da'b'$ es positivo, por lo que debemos probar que es igual a m probando que satisface las condiciones de la definición de mcm (a, b).

En primer lugar,

$$da'b' = (da')b' = ab' \qquad \text{y} \qquad da'b' = (db')a' = ba';$$

por lo que $da'b' = \overset{\bullet}{a}$ y $da'b' = \overset{\bullet}{b}$, es decir, se satisface la primera condición.

En segundo lugar, supongamos que $c = \overset{\bullet}{a}$ y $c = \overset{\bullet}{b}$ con $c > 0$; debemos probar que $c \geq da'b'$.

La identidad de Bezout nos dice que existen enteros u y v tales que $d = au + bv$, por lo que

$$\frac{c}{da'b'} = \frac{cd}{(da')(db')} = \frac{cd}{ab} = \frac{c(au+bv)}{ab} = \frac{c}{b}u + \frac{c}{a}v \in \mathbf{Z} \text{ por ser } \begin{cases} c = \overset{\bullet}{a} \\ c = \overset{\bullet}{b} \end{cases}$$

es decir, $da'b' \,|\, c$ y por tanto (véase el apartado (d)del Teorema 1.7) se tiene que $da'b' \leq c$ como queríamos probar.

$$da'b' = m \iff da'db' = dm \iff ab = dm$$ ■

Podemos utilizar el Teorema 1.18 para encontrar el mcm (a, b) de una forma eficiente utilizando el algoritmo de Euclides para encontrar $d = \text{mcd}\,(a, b)$ y calcular posteriormente $m = ab/d$.

Ejemplo 1.10 Dado que $\text{mcd}\,(1492, 1066) = 2$ se tiene que

$$\text{mcm}\,(1492, 1066) = (1492 \times 1066)/2 = 795236.$$ □

1.4 Ecuaciones diofánticas lineales

En este curso trataremos algunas *ecuaciones diofánticas* (llamadas así desde el siglo tercero por el matemático de Alejandría, Diophantos): estas son ecuaciones en una o varias variables, para las que nos interesan sólo sus soluciones enteras. Unas de las más simples son las *ecuaciones diofánticas lineales* $a_1x_1 + \cdots + a_nx_n = b$; utilizaremos algunas de las ideas anteriores para encontrar las soluciones enteras $x_1, \ldots, x_n$ de estas ecuaciones. El siguiente resultado lo dio a conocer el matemático indio Brahmagupta alrededor del año 628:

Teorema 1.19 *Sean a, b y c tres enteros con a y b no ambos nulos, y sea $d = \text{mcd}\,(a, b)$. La ecuación*

$$ax + by = c$$

admite soluciones enteras si, y sólo si, c es múltiplo de d, en cuyo caso existen infinitas. Estas son los pares

$$x = x_0 + \frac{bn}{d}, \quad y = y_0 - \frac{an}{d} \qquad (n \in \mathbf{Z})$$

donde x_0, y_0 es una solución particular.

Demostración. El hecho de existir solución si, y sólo si, $d \,|\, c$ es sólo una consecuencia del Teorema 1.15 Para la segunda parte del teorema, sea x_0, y_0 una solución particular, es decir

$$ax_0 + by_0 = c.$$

Si ponemos

$$x = x_0 + \frac{bn}{d}, \quad y = y_0 - \frac{an}{d}$$

donde n es un entero, se tiene que

$$ax + by = a\left(x_0 + \frac{bn}{d}\right) + b\left(y_0 - \frac{an}{d}\right) = ax_0 + by_0 = c,$$

por lo que x, y también es solución. (Obsérvese que x e y son enteros debido a que d divide a a y a b). Se obtienen así infinitas soluciones para los diferentes valores de n.

Para probar que sólo existen estas soluciones, sea x, y una solución tal que $ax + by = c$. Como $ax + by = c = ax_0 + by_0$ se tiene

$$a(x - x_0) + b(y - y_0) = 0,$$

y dividiendo por d

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0). \tag{1.2}$$

Como a y b no son ambos nulos, podemos suponer que $b \neq 0$ (en caso contrario intercambiamos los papeles de a y b en el resto de la demostración). Como b/d divide a ambos miembros de (1.2) y, por el Corolario 1.16, es primo con a/d, debe dividir a $(x - x_0)$. De este modo, $x - x_0 = bn/d$ para algún entero n, es decir

$$x = x_0 + \frac{bn}{d}.$$

Sustituyendo este resultado en (1.2) se tiene

$$-\frac{b}{d}(y - y_0) = \frac{a}{d}(x - x_0) = \frac{a}{d}\frac{bn}{d},$$

donde dividiendo por b/d (que es no nulo) obtenemos

$$y = y_0 - \frac{an}{d}.$$

■

De este modo, podemos encontrar las soluciones de cualquier ecuación diofántica lineal $ax + by = c$ por el siguiente método:

(1) Calcular $d = \text{mcd}\,(a, b)$ por el algoritmo extendido de Euclides.

(2) Comprobar si d divide a c: si no lo divide, no existen soluciones y paramos aquí. Si lo divide, escribimos $c = de$.

(3) Si $d \,|\, c$ el par $(x_0, y_0) = (ue, ve)$ es una solución particular de $ax+by = c$.

(4) Utilizamos ahora el Teorema 1.19 para encontrar la solución general x, y de la ecuación.

Ejemplo 1.11 Consideremos la ecuación

$$1492x + 1066y = -4,$$

en la que $a = 1492$, $b = 1066$ y $c = -4$.

$d = \text{mcd}\,(1492, 162) = 2 \,|\, -4 \implies$ La ecuación admite soluciones enteras.

$2 = -5\cdot 1492 + 7\cdot 1066 \implies 10\cdot 1492 - 14\cdot 1066 = -4 \implies (x_0, y_0) = (10, -14)$

La solución general viene dada por

$$\left.\begin{aligned} x &= 10 + \frac{1066}{2}\, n = 10 + 533\, n \\ y &= -14 - \frac{1492}{2}\, n = -14 - 746\, n \end{aligned}\right\} \quad \forall\, n \in \mathbf{Z}$$

□

1.5 Números primos y factorización

El principal resultado que veremos en lo que resta del capítulo es el Teorema Fundamental de la Aritmética, el cual garantiza que cualquier entero $n > 1$ puede ser descompuesto, de forma única, como producto de primos. Esto permite reducir muchos problemas teórico-numéricos a cuestiones sobre números primos, por lo que dedicamos parte de este capítulo al estudio de esta importante clase de números enteros. El segundo resultado importante es el teorema de Euclides sobre la existencia de infinitos números primos. Además de existir infinitos números primos, estos se distribuyen de forma totalmente irregular entre los enteros y hemos incluido algunos resultados que nos permiten predecir dónde pueden encontrarse números primos o dónde aparecen frecuentemente: algunos de estos resultados, como el Teorema de los Números Primos, tienen bastante dificultad, y están tratados sin demostración.

Definición 1.7 [Números primos y compuestos]

- *Un entero $p > 1$ se dice que es primo si sus únicos divisores son 1 y p.*

  Nótese que 1 no es primo. El número primo más pequeño es el 2, y todos los demás $3, 5, 7, 11, \ldots$ son impares.

- *Un entero $n > 1$ se dice que es compuesto si admite divisores propios, es decir, si existen $a, b \in \mathbf{Z}$ con $1 < a, b < n$ tales que $n = ab$.*

Teorema 1.20 [Propiedades de los números primos]

Sea p un número primo.

a) Si $a \in \mathbf{Z} \implies p \mid a$ o $p \perp a$.

b) Si $a, b \in \mathbf{Z}$ y $p \mid ab \implies p \mid a$ o $p \mid b$

c) Si $a_1, \ldots, a_k \in \mathbf{Z}$ y $p \mid a_1 \cdots a_k \implies p \mid a_i$ para algún $i = 1, \ldots, k$

Demostración.

a) Por definición mcd (a, p) es un divisor positivo de p, por lo que, al ser p primo, debe ser 1 ó p.

- Si mcd $(a, p) = p$, como mcd $(a, p) \mid a \implies p \mid a$
- Si mcd $(a, p) = 1 \implies p \perp a$.

b) Supongamos que $p \mid ab$.

Si p no divide a a, el apartado (a) nos dice que mcd $(a, p) = 1$, por lo que $1 = au + pv$ con $u, v \in \mathbf{Z}$ es decir $b = aub + pvb$.

$$\left.\begin{array}{l} p \mid ab \implies p \mid aub \\ p \mid pvb \end{array}\right\} \implies p \mid (aub + pub) = b$$

c) Haremos inducción en $k \geq 2$.

- Si $k = 2$ está probado en el apartado anterior.
- Supongamos ahora que $k > 2$ y que el resultado es cierto para todos los productos de $k - 1$ factores a_i.

  Si denotamos por $a = a_1 \cdots a_{k-1}$ y $b = a_k$ entonces $a_1 \cdots a_k = ab$ y por tanto, $p \mid ab \implies p \mid a$ o $p \mid b$.

– Si $p \mid a = a_1 \cdot a_2 \cdots a_{k-1} \implies p \mid a_i$ para algún $i = 1, 2, \ldots, a_{k-1}$ por hipótesis de inducción.
– Si $p \mid b \implies p \mid a_k$

En cualquiera de los casos $p \mid a_i$ para algún i, como se pretendía probar. ■

Las propiedades anteriores fallan si p no es primo.

Ejemplo 1.12 Sean $p = 4$ (no primo), $a = 6$ y $b = 10$.

- Ni 4 divide a 6 ni 4 es primo con 6.
- 4 divide a $6 \cdot 10 = 60$ y ni 4 divide a 6 ni 4 divide a 10. □

Como una aplicación del Teorema 1.20–(b) consideremos el conjunto de los polinomios con coeficientes enteros.

Definición 1.8 [Polinomios reducibles e irreducibles]

Un polinomio $P(x)$ (con coeficientes enteros), es reducible si $P(x) = Q(x)R(x)$, donde $Q(x)$ y $R(x)$ son polinomios no constantes con coeficientes enteros. En caso contrario, $P(x)$ es irreducible.

Teorema 1.21 [Criterio de Eisenstein]

Si $P(x) = a_0 + a_1 x + \cdots + a_n x^n$ con $a_i \in \mathbf{Z}$ $\forall\, i = 0, 1, \ldots, n$, p es un primo tal que divide a $a_0, a_1, \ldots, a_{n-1}$ pero no a a_n y p^2 no divide a a_0, entonces $P(x)$ es irreducible.

Demostración. Para probarlo supongamos que $P(x)$ es reducible, es decir,

$$P(x) = Q(x)R(x) \text{ con } \begin{cases} Q(x) = b_0 + b_1 x + \cdots + b_s x^s & s \geq 1 \\ R(x) = c_0 + c_1 x + \cdots + c_t x^t & t \geq 1 \end{cases}$$

Como $a_0 = b_0 c_0$ es divisible por p pero no por p^2, uno y sólo uno entre b_0 y c_0 es divisible por p; trasponiendo $Q(x)$ y $R(x)$ si fuese necesario podemos asumir que p divide a b_0 pero no a c_0.

Además, p no divide a b_s, ya que en caso contrario dividiría a $a_n = b_s c_t$; por

tanto, existe $i \leq s$ tal que p divide a $b_0, b_1, \ldots, b_{i-1}$ pero no a b_i.

Además, $a_i = b_0c_i + b_1c_{i-1} + \cdots + b_{i-1}c_1 + b_ic_0$, con

$$p \text{ divisor de } \begin{cases} a_i \quad \text{ya que} \quad i \leq s = n - t < n \\ \text{y de} \\ b_0c_i + \cdots + b_{i-1}c_1 \end{cases}$$

por lo que $p \,|\, b_ic_0 \implies \begin{cases} p \,|\, b_i \\ \text{o} \\ p \,|\, c_0 \end{cases}$ lo cual es una contradicción, por lo que $P(x)$ debe ser irreducible. ■

Ejemplo 1.13 El polinomio $f(x) = x^3 - 4x + 2$ es irreducible, ya que satisface el criterio de Eisenstein para $p = 2$.

2 es un primo tal que $2 \,|\, a_1 = -4$, $2 \,|\, a_2 = 2$, $2 \not| a_0 = 1$ y $2^2 \not| a_2 = 0$ □

El siguiente resultado, conocido como *Teorema Fundamental de la Aritmética* explica la importancia de los números primos: ellos son los bloques básicos con los que se construye el edificio de los números enteros.

Teorema 1.22 [Teorema Fundamental de la Aritmética]

Cada entero $n > 1$ admite una descomposición en factores primos

$$n = p_1^{e_1} \cdots p_k^{e_k},$$

donde $p_1, \ldots, p_k$ son primos distintos y $e_1, \ldots, e_k$ son enteros positivos; esta factorización es única, independientemente de las permutaciones de sus factores.

(Por ejemplo, 200 admite la descomposición en factores primos $2^3 \cdot 5^2$ o, alternativamente, $5^2 \cdot 2^3$ si permutamos sus factores, pero no admite ninguna otra factorización posible.)

Demostración. Utilizaremos, en primer lugar, el principio de inducción completa para probar la existencia de la descomposición en factores primos.

Como hemos asumido que $n > 1$, comenzaremos la inducción por $n = 2$.

Como siempre, este caso es fácil de probar: la requerida factorización es $n = 2^1$.

Asumamos ahora que $n > 2$ y que cualquier entero estrictamente contenido entre 1 y n admite una descomposición en factores primos.

Si n es primo entonces $n = n^1$ es la factorización buscada, por lo que podemos asumir que n es compuesto, $n = ab$ con $1 < a, b < n$.

Por la hipótesis de inducción, a y b admiten descomposiciones en factores primos, por lo que sustituyendo estas en la ecuación $n = ab$ y asociando las potencias de cada factor primo p_i, obtenemos una descomposición en factores primos de n.

Para probar que es única, supongamos que n admite las factorizaciones

$$n = p_1^{e_1} \cdots p_k^{e_k} = q_1^{f_1} \cdots q_l^{f_l},$$

donde $p_1, \ldots, p_k$ y $q_1, \ldots, q_l$ son dos conjuntos diferentes de primos, y los exponentes e_i y f_j son todos positivos.

La primera factorización prueba que $p_1 \,|\, n$, por lo que teniendo en cuenta la segunda $p_1 \,|\, q_j$ para algún $j = 1, \ldots, l$. Permutando el orden de los factores primos de la segunda factorización, podemos asumir que $j = 1$, es decir, que $p_1 \,|\, q_1$. Como q_1 es primo, se sigue que $p_1 = q_1$, por lo que cancelando dicho factor primo de ambas factorizaciones obtenemos que

$$p_1^{e_1 - 1} p_2^{e_2} \cdots p_k^{e_k} = q_1^{f_1 - 1} q_2^{f_2} \cdots q_l^{f_l}.$$

Reiterando este razonamiento, vamos emparejando primos en ambas factorizaciones y cancelándolos hasta que eliminemos todos los primos de una de las factorizaciones. Si una de ellas se elimina antes que la otra, el resto de la factorización que nos queda es una factorización de 1 como producto de primos p_i o q_j, lo cual es imposible ya que $p_i, q_j > 1$. Se tiene entonces que ambas factorizaciones se cancelan simultáneamente, por lo que debemos cancelar cada copia e_i de cada factor primo p_i con el mismo número f_i de copias de q_i; es decir, $k = l$, cada $p_i = q_i$ (salvo permutación de los factores) y cada $e_i = f_i$, por lo que la descomposición en factores primos de un entero n es única. ■

El Teorema 1.22 nos permite usar la factorización para el cálculo de productos, cocientes, potencias, máximos divisores comunes y mínimos múltiplos comunes.

Supongamos que los enteros a y b admiten las factorizaciones

$$a = p_1^{e_1} \cdots p_k^{e_k} \quad \text{y} \quad b = p_1^{f_1} \cdots p_k^{f_k}$$

(donde cada $e_i, f_i \geq 0$ permitiendo la posibilidad de que algún primo p_i pueda dividir a uno de los enteros a o b pero no a ambos). Tenemos entonces que

$$\begin{aligned} ab &= p_1^{e_1+f_1} \cdots p_k^{e_k+f_k}, \\ a/b &= p_1^{e_1-f_1} \cdots p_k^{e_k-f_k} \quad (\text{si } b \,|\, a), \\ a^m &= p_1^{me_1} \cdots p_k^{me_k}, \\ \text{mcd}\,(a,b) &= p_1^{\text{mín}(e_1,f_1)} \cdots p_k^{\text{mín}(e_k,f_k)}, \\ \text{mcm}\,(a,b) &= p_1^{\text{máx}(e_1,f_1)} \cdots p_k^{\text{máx}(e_k,f_k)}. \end{aligned}$$

donde $\text{mín}(e,f)$ y $\text{máx}(e,f)$ representan al mínimo y al máximo de e y f respectivamente. Desafortunadamente, realizar la factorización de un entero grande requiere *demasiado tiempo*.

La siguiente notación se utiliza muy a menudo: si p es primo, escribimos $p^e \,||\, n$ para indicar que p^e es la mayor potencia de p que divide a n, es decir, p^e divide a n pero p^{e+1} no.

Por ejemplo, $2^3 \,||\, 200$, $5^2 \,||\, 200$ y $p^0 \,||\, 200$ para cualquier primo $p \neq 2, 5$.

El anterior resultado prueba que si $p^e \,||\, a$ y $p^f \,||\, b$ entonces $p^{e+f} \,||\, ab$, $p^{e-f} \,||\, a/b$ (si $b \,|\, a$), $p^{me} \,||\, a^m$, etc.

1.5.1 Distribución de primos

El Teorema de Euclides de la existencia de infinitos números primos es una de los más antiguos y atractivos en matemáticas. En este libro daremos algunas demostraciones diferentes de este resultado, muy diferentes en el estilo, para ilustrar algunas importantes técnicas en teoría de números. (Es conveniente, y en absoluto una pérdida de tiempo, dar diferentes demostraciones de un mismo resultado, ya que uno puede adaptar dichas demostraciones para dar diferentes generalizaciones). Nuestra primera demostración (la más simple) se encuentra en el Libro IX de los *Elementos* de Euclides.

Teorema 1.23 [Teorema de Euclides]

Existen infinitos números primos.

Demostración. Lo demostraremos por reducción al absurdo: suponemos que sólo existe un número finito de primos y llegamos a una contradicción, por lo que debe existir una cantidad infinita de ellos.

Supongamos que sólo existen los primos $p_1, p_2, \ldots, p_k$. Sea

$$m = p_1 p_2 \cdots p_k + 1.$$

Como m es un entero mayor que 1, el Teorema Fundamental de la Aritmética (Teorema 1.22) implica que es divisible por algún primo p (incluyendo la posibilidad de que $m = p$).

Según nuestra hipótesis, el primo p ha de ser uno de los primos $p_1, p_2, \ldots, p_k$, por lo que p divide al producto $p_1 p_2 \cdots p_k$.

Como p divide a m y a $p_1 p_2 \cdots p_k$ debe dividir a $m - p_1 p_2 \cdots p_k = 1$, lo cual es imposible.

Deducimos de aquí que nuestra hipótesis es falsa, por lo que deben existir infinitos números primos. ■

Para cualquier número real $x > 0$, sea $\pi(x)$ el número de primos $p \leq x$; así, por ejemplo, $\pi(1) = 0$, $\pi(2) = \pi(2\frac{1}{2}) = 1$, y $\pi(10) = 4$.

Teorema 1.24 [Teorema de los números primos]

$\pi(x)$ viene dado, aproximadamente, por la función

$$\operatorname{li} x = \int_2^x \frac{dt}{\ln t},$$

o, equivalentemente, por $x/\ln x$, en el sentido de que

$$\frac{\pi(x)}{x/\ln x} \to 1 \quad \textit{como} \quad x \to \infty.$$

Este resultado fué conjeturado por Gauus en 1793 y probado finalmente por Hadamard y Vallé Poussin en 1896.

Se puede interpretar el Teorema de los Números primos como un reflejo de que la proporción $\pi(x)/\lfloor x \rfloor$ de primos entre los enteros positivos $i \leq x$ es aproximadamente $1/\ln x$ para grandes x. Como $1/\ln x \to 0$ cuando $x \to \infty$, esto prueba que los primos son menos frecuentes entre grandes enteros que entre enteros pequeños. Por ejemplo, existen 168 primos entre 1 y 1000, 135 entre 1001 y 2000, 127 entre 2001 y 3000, y así sucesivamente.

Podemos usar el método de la demostración del Teorema 1.23 para probar que ciertos conjuntos de enteros contienen infinitos números primos, como en el siguiente teorema.

Cualquier entero impar debe dar de resto 1 ó 3 cuando lo dividimos por 4, por lo que deben tener la forma $4q+1$ ó $4q+3$ para algún entero q. Como $(4s+1)(4t+1) = 4(4st+s+t)+1$, el producto de dos enteros de la forma $4q+1$ tiene también la misma forma y, por inducción, el producto de cualquier número de enteros de esta forma.

Teorema 1.25 *Existen infinitos números primos de la forma $4q+3$.*

Demostración. Lo demostraremos por reducción al absurdo.

Supongamos que sólo existe un número finito de primos de esta forma, que denotaremos por $p_1, \ldots, p_k$. Sea $m = 4p_1 \cdots p_k - 1$, por lo que m también es de la forma $4q+3$ (con $q = p_1 \cdots p_k - 1$). Como m es impar, también debe serlo cualquier primo p que divida a m, por lo que p debe tener la forma $4q+1$ ó $4q+3$ para algún q. Si todos los primos p que dividen a m son de la forma $4q+1$ entonces m debe tener también esa forma, lo cual es falso. Por tanto, m debe ser divisible, al menos, por un primo p de la forma $4q+3$. Según nuestra hipótesis, debe ser $p = p_i$ para algún i, por lo que p divide a $4p_1 \cdots p_k - m = 1$, lo cual es imposible. Esta contradicción prueba el resultado. ■

Este resultado es un caso particular de un teorema general demostrado por Dirichlet en 1837 sobre números primos en progresión aritmética.

Teorema 1.26 *Si a y b son enteros primos entre sí, existen infinitos números primos de la forma $aq+b$.*

A pesar de los resultados anteriores probando la existencia de conjuntos infinitos de primos, es difícil dar ejemplos explícitos de tales conjuntos infinitos ya que los números primos aparecen con mucha irregularidad dentro de los enteros.

El intervalo entre primos consecutivos puede ser arbitrariamente grande.

$$\left.\begin{array}{l} (n+1)!+2 \\ (n+1)!+3 \\ \quad\vdots \\ (n+1)!+(n+1) \end{array}\right\} \text{ son } n \text{ números compuestos consecutivos}$$

por lo que el primo inmediatamente anterior a $(n+1)!+2$ y el inmediatamente posterior a $(n+1)!+(n+1)$ son dos primos consecutivos que distan entre sí más de n.

Como extremo opuesto, aparte del intervalo 1 entre los primos 2 y 3, el menor intervalo posible es 2 entre las parejas p y $p+2$ denominadas *primos gemelos*.

Existen bastantes ejemplos de primos gemelos, como 3 y 5 ó 41 y 43, lo que puede dar pie a la conjetura de la existencia de infinitas parejas de primos gemelos, pero nadie ha sido capaz de probarlo todavía.

1.5.2 Primos de Fermat y Mersenne

Para encontrar ejemplos específicos de primos, parece razonable observar los enteros de la forma $2^m \pm 1$, ya que muchos primos pequeños, tales como $3, 5, 7, 17, 31, \ldots$, tienen esa forma.

Lema 1.27 *Si 2^m+1 es primo, entonces $m = 2^n$ para algún entero $n \geq 0$.*

Demostración. Probaremos el recíproco, es decir, si m no es una potencia de 2, entonces 2^m+1 no es primo.

Si m no es una potencia de 2 es de la forma $2^n q$ para algún $q > 1$ impar.

Como $(t+1) \mid (t^q+1)$ y además es un factor propio, ya que $q > 1$, poniendo $t = x^{2^n}$ observamos que $x^{2^n}+1$ es un factor propio de $(x^{2^n})^p + 1 = x^m + 1$.

Haciendo $x = 2$ vemos que $2^{2^n}+1$ es un factor propio de 2^m+1 por lo que éste último no puede ser primo. ■

Definición 1.9 [Números de Fermat]

Los números de la forma $F_n = 2^{2^n}+1$ se denominan números de Fermat y aquellos que son primos se denominan primos de Fermat.

Fermat conjeturó que F_n es primo para cualquier $n \geq 0$.

$$F_0 = 3 \quad F_1 = 5 \quad F_2 = 17 \quad F_3 = 257 \quad \text{y} \quad F_4 = 65537$$

son realmente primos pero en 1732 Euler probó la no primalidad de

$$F_5 = 2^{2^5}+1 = 4294967297 = 641 \times 6700417$$

Los números de Fermat han sido estudiados exhaustivamente, con frecuencia con la ayuda de ordenadores, pero no ha sido encontrado ningún otro primo de Fermat. Es concebible que existan mas números primos de Fermat (presumiblemente infinitos) aunque no hayan sido encontrados todavía, pero la evidencia no es convincente.

Estos primos son importantes en geometría: en 1801 Gauss probó que un polígono regular de k lados puede ser dibujado con regla y compás si, y sólo si, $k = 2^e p_1 \cdots p_r$ donde $p_1, \ldots, p_r$ son distintos primos de Fermat.

Aunque sólo algunos de los números de Fermat sean primos, el siguiente resultado muestra que sus divisores abarcan un conjunto infinito de primos.

Lema 1.28 *Los números F_n de Fermat son mutuamente coprimos.*

Demostración. Sea $d = \text{mcd}\,(F_m, F_n)$ con $n = m + k$ y $k > 0$.

$$(x+1)\,|\,(x^{2^k}-1) \implies (2^{2^m}+1)\,|\,((2^{2^m})^{2^k}-1) \implies F_m\,|\,(F_n-2)$$

$$\left.\begin{array}{c} d\,|\,F_n \\ d\,|\,F_m\,|\,(F_n-2) \;\Rightarrow\; d\,|\,(F_n-2) \end{array}\right\} \Rightarrow\; d\,|\,[F_n-(F_n-2)] = 2 \;\Rightarrow\; \left\{\begin{array}{c} d=1 \\ \text{o} \\ d=2 \end{array}\right.$$

Dado que todos los números de Fermat son impares $d \neq 2$, por lo que necesariamente es $d = 1 \implies F_m \perp F_n$. ∎

Esto nos proporciona otra demostración del Teorema 1.23, ya que se deduce del Lema 1.28 que cualquier conjunto infinito de números de Fermat debe contener infinitos factores primos diferentes.

Teorema 1.29 *Si $m > 1$ y $a^m - 1$ es primo, entonces $a = 2$ y m es primo.*

Demostración. Dado que $(a-1)\,|\,(a^m-1)$, si $a \neq 2$ es $a - 1 > 1$ y por tanto un divisor propio de $a^m - 1$, es decir $a^m - 1$ no sería primo, por lo que necesariamente ha de ser $a = 2$.

Veamos ahora, para el caso $a = 2$, que si m no es primo entonces $2^m - 1$ tampoco lo es.

Si m no es primo, existen enteros n y q con $1 < n, q < m$ tales que $m = nq$.

Dado que $(2^n - 1) \mid ((2^n)^q - 1) = 2^m - 1$ con $2^n - 1 > 1$ el número $2^m - 1$ posee divisores propios y por tanto es compuesto.

Por lo que para que $a^m - 1$ sea primo han de ser $a = 2$ y m primo. ■

Definición 1.10 [Números de Mersenne]

Los enteros de la forma $2^p - 1$, con p primo, se denominan números de Mersenne y se denotan por M_p. Aquellos que son primos se conocen como primos de Mersenne.

Los primeros números de Mersenne son

$$M_2 = 3 \quad M_3 = 7 \quad M_5 = 31 \quad M_7 = 127$$

los cuales son primos, pero $M_{11} = 2047 = 23 \times 89$ es compuesto.

Desde que Mersenne los estudiara en 1644 han sido encontrados 46 primos de Mersenne. El último fue dado a conocer por Hans-Michael Elvenich el 6 de septiembre de 2008, aunque el mayor de los conocidos se descubrió (con número de orden 45) en UCLA el 23 de agosto de 2008; se trata del número $M_{43112609} = 2^{43112609} - 1$ el cual tiene 12.978.189 dígitos. En el tema siguiente veremos un test determinista de primalidad eficiente para números de Mersenne.

Como en el caso de los números primos de Fermat, no se conoce si existen infinitos primos de Mersenne. Existe un resultado similar al Lema 1.28, por el que los números de Mersenne son mutuamente coprimos.

1.5.3 Test de primalidad y factorización

Existen dos problemas prácticos en relación a la teoría que hemos considerado en este capítulo:

- *¿Cómo se determina cuando es primo un número entero n?*
- *¿Cómo se descompone en factores primos un número entero dado n?*

En relación al primero de los problemas, conocido como *test de primalidad*, tenemos:

Lema 1.30 *Un entero $n > 1$ es compuesto si, y sólo si, es divisible por algún primo $p \leq \sqrt{n}$.*

Demostración.

- Si n es divisible por algún primo p con $1 < p \leq \sqrt{n} < n$ entonces es compuesto.

- Recíprocamente, si n es compuesto, es $n = ab$ con $1 < a, b < n$; al menos uno de los dos (a ó b) ha de ser menor o igual que $\sqrt{n}$ (de lo contrario, $ab > n$) y dicho factor ha de ser o bien un primo menor que $\sqrt{n}$ o bien divisible por algún primo $p \leq \sqrt{n}$, el cual también divide a n. ■

Evidentemente es necesario el conocimiento previo de la lista de todos los primos menores que $\sqrt{n}$ y el método más efectivo para construirla es el denominado *Criba de Eratóstenes*.

Criba de Eratóstenes

Se trata de una forma sistemática de construir la lista de los números primos existentes hasta un entero dado N.

Se escribe, en primer lugar, la lista de enteros $2, 3, \ldots, N$ en orden creciente. Subrayamos el 2 (que es primo) y eliminamos todos los múltiplos de 2 tales como $4, 6, 8, \ldots$ (por ser compuestos).

El primer entero, posterior a 2, que no ha sido eliminado es 3: este es primo, por lo que lo subrayamos y eliminamos todos sus múltiplos $6, 9, 12, \ldots$.

En la siguiente etapa subrayamos 5 y eliminamos todos sus múltiplos.

Continuamos de esta forma hasta que todos los elementos de la lista hayan sido o bien subrayados o bien eliminados.

En cada etapa, el primer entero que no ha sido eliminado debe ser primo, ya que de lo contrario habría resultado eliminado por ser múltiplo de alguno de los primos anteriores, por lo que sólo los primos aparecerán subrayados y, recíprocamente, todos los primos de la lista aparecerán subrayados, por lo que al finalizar el proceso, tendremos la lista de todos los primos $p \leq N$.

De hecho, podemos detener el proceso cuando eliminamos todos los múltiplos

de los primos $p \leq \sqrt{N}$, ya que el Lema 1.30 implica que todos los elementos no eliminados de la lista en ese momento, han de ser primos.

Este método es efectivo para enteros pequeños, ya que no hay que considerar demasiados números primos p, pero cuando n se hace grande se necesita demasiado tiempo: por el Teorema de los Números Primos, el número de primos $p \leq \sqrt{n}$ viene dado por

$$\pi(\sqrt{n}) \simeq \frac{\sqrt{n}}{\ln(\sqrt{n})} = \frac{2\sqrt{n}}{\ln n}.$$

En criptografía (estudio de los códigos secretos), se utilizan con regularidad enteros con algunos cientos de dígitos decimales; si, por ejemplo, $n \simeq 10^{100}$, este método requiere testar alrededor de $8 \cdot 10^{47}$ números primos y hasta las más avanzadas supercomputadoras tardarían un tiempo mayor que el estimado para la edad del universo (alrededor de 15000 millones de años) en realizar dicha tarea.

Afortunadamente, existen otros algoritmos alternativos (utilizando algunas sofisticadas teorías de números), para testar la primalidad de muchos enteros grandes, más eficientes. Algunos de estos test rápidos son algoritmos probabilísticos, tales como el de Solovay-Strassen, el cual siempre detecta si un número entero es primo, pero puede declarar, incorrectamente, como primo un número compuesto; esto puede parecer un defecto desastroso, pero de hecho, la probabilidad de que esto ocurra es muy pequeña (tan pequeña como la probabilidad de un error computacional debido a un fallo de la máquina), por lo que, en la práctica, resulta ser muy seguro. Para detalles sobre test de primalidad y criptografía, ver Koblitz (1994) y Kranakis (1986).

El segundo problema, el de la *factorización* es mucho más complejo que el del test de primalidad. (No puede ser más fácil ya que la factorización requiere, en primer lugar, conocer que el número es compuesto). En teoría, podemos realizar la factorización de un entero n estudiando su divisibilidad por los primos $2, 3, 5 \ldots$ hasta encontrar un primer factor primo p; reemplazando n por n/p y repitiendo el proceso, buscamos el primer factor de n/p; de esta forma obtenemos todos los factores de n con sus multiplicidades. Este algoritmo no es, en absoluto, efectivo para números grandes, ya que si n es grande, nos encontramos con los mismos problemas que en el test de primalidad, pues existen demasiados primos por los que probar. Existen métodos más sutiles para la factorización, pero hasta ahora, el mejor de los algoritmos conocidos

no puede, en la práctica, factorizar enteros de varios cientos de dígitos (aunque nadie ha probado aún que nunca pueda encontrarse un algoritmo eficiente).

1.6 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

$$\left\{ \begin{array}{l} x = -22 + 8t \\ \\ y = \quad 22 - 7t \end{array} \right. \quad \forall\, t \in \mathbf{Z}$$

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 $\text{mcd}\,(3,7) = 1$ 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

$$x' = -2 + 7t$$

$$y' = 1 - 3t$$

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

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

■

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. ■

1.7 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

En este capítulo estudiaremos la aritmética modular, es decir, la aritmética de las clases de congruencias, la cual simplifica los problemas teórico-numéricos sustituyendo cada entero por el resto de dividirlo entre un entero positivo fijo n. Esto produce el efecto de sustituir el conjunto infinito $\mathbf{Z}$ de números enteros por un conjunto $\mathbf{Z}_n$ que sólo contiene n elementos. Encontraremos que se pueden sumar, restar y multiplicar los elementos de $\mathbf{Z}_n$ (igual que en $\mathbf{Z}$), aunque encontramos algunas dificultades en la división. De este modo, $\mathbf{Z}_n$ hereda mucha de las propiedades de $\mathbf{Z}$, pero al tratarse de un conjunto finito es más fácil trabajar con ellos. Después de un minucioso estudio de las ecuaciones lineales en congruencias (análogas en $\mathbf{Z}_n$ a la ecuación $ax = b$), consideraremos sistemas lineales de congruencias, que es donde el Teorema Chino de los restos y sus generalizaciones juegan un importante papel.

2.1 Números congruentes

Muchos problemas en los que se requieren enteros muy grandes pueden simplificarse con una técnica denominada *aritmética modular*, en la que se utilizan congruencias en vez de ecuaciones. La idea básica es elegir un determinado entero n (dependiendo del problema), llamado *módulo* y sustituir cualquier entero por el resto de su división entre n. En general, los restos son pequeños y, por tanto, es fácil trabajar con ellos. Antes de entrar en la teoría general, veamos dos ejemplos sencillos.

Ejemplo 2.1 Si contamos 100 días a partir de hoy, ¿en qué día de la semana caerá? Podemos resolver esta cuestión cogiendo un calendario y contando 100 días, pero un método más sencillo es utilizar el hecho de que los días de la semana se repiten en ciclos de 7. Como $100 = 14 \times 7 + 2$, dentro de 100 días será el mismo día de la semana que dentro de dos días y ésto es fácil de

determinar. Aquí hemos tomado $n = 7$ y hemos reemplazado 100 por el resto de su división entre 7, es decir, por 2. □

Ejemplo 2.2 ¿Es 22051946 un cuadrado perfecto? Esto se puede resolver calculando $\sqrt{22051946}$ y viendo si se obtiene un número entero, o alternativamente, elevando al cuadrado varios enteros y ver si puede obtenerse 22051946, pero es mucho más sencillo ver que este número no puede ser un cuadrado perfecto. En el Capítulo 1 (Ejemplo 1.3) se probó que un cuadrado perfecto debe dar de resto 0 ó 1 cuando se divide por 4. Para trabajar sólo con dos dígitos podemos ver que

$$22051946 = 220519 \times 100 + 46 = 220519 \times 25 \times 4 + 46$$

nos da el mismo resto que 46, y como $46 = 11 \times 4 + 2$, el resto es 2. Se sigue de ahí que 22051946 no es un cuadrado perfecto. (Naturalmente, si el resto hubiese sido 0 ó 1, no podríamos afirmar que se trata de un cuadrado y deberíamos utilizar otro método para comprobarlo). En este caso $n = 4$ y reemplazamos 22051946 primero por 46 y más tarde por 2. □

Definición 2.1 [Números congruentes]

Sea n un entero positivo y sean a y b dos enteros cualesquiera. Se dice que a es congruente con b módulo n y lo denotamos por $a \equiv b \pmod{n}$ si a y b dan el mismo resto cuando se dividen entre n.

$$\left.\begin{array}{ll} a = q\,n + r & 0 \leq r < n \\ b = q'n + r' & 0 \leq r' < n \end{array}\right\} \quad a \equiv b \pmod{n} \iff r = r'$$

Ejemplo 2.3

$100 \equiv 2 \pmod{7}$ en el Ejemplo 2.1

$22051946 \equiv 46 \equiv 2 \pmod{4}$ en el Ejemplo 2.2 □

Lema 2.1 [Caracterización de los números congruentes]

Para cualquier entero dado $n \geq 1$

$$a \equiv b \pmod{n} \iff n|(a - b)$$

Demostración.

$$\left.\begin{array}{ll} a = q\,n + r & 0 \le r < n \\ b = q'n + r' & 0 \le r' < n \end{array}\right\} \Rightarrow\ a-b = (q-q')n+(r-r')\ \text{ con }\ -n < r-r' < n$$

- $a \equiv b \pmod{n} \implies r = r' \implies a - b = (q - q')n \implies n \,|\, (a - b)$
- $n \,|\, (a - b) \implies n \,|\, [(a - b) - (q - q')n] = r - r'$ y dado que el único múltiplo de n en el intervalo $(-n, n)$ es el cero,

$$r - r' = 0 \implies r = r' \implies a \equiv b \pmod{n}$$ ■

El siguiente resultado recoge algunas observaciones triviales, pero de uso muy frecuente, en las congruencias:

Lema 2.2 [Relación de equivalencia]

Para cualquier entero fijo $n \ge 1$ se verifican las propiedades:

a) Reflexiva: $a \equiv a \pmod{n}$ *para cualquier entero* a

b) Simétrica: $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$

c) Transitiva: $\left.\begin{array}{l} a \equiv b \pmod{n} \\ b \equiv c \pmod{n} \end{array}\right\} \implies a \equiv c \pmod{n}.$

Demostración.

a) $n \,|\, (a - a) \quad \forall\, a \in \mathbf{Z} \iff a \equiv a \pmod{n} \ \forall\, a \in \mathbf{Z}$

b) $n \,|\, (a - b) \implies n \,|\, (b - a) \iff a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$

c) $\left.\begin{array}{l} n \,|\, (a - b) \\ n \,|\, (b - c) \end{array}\right\} \implies n \,|\, [(a - b) + (b - c)] = a - c \iff$

$$\left.\begin{array}{l} a \equiv b \pmod{n} \\ b \equiv c \pmod{n} \end{array}\right\} \implies a \equiv c \pmod{n}$$

Estas tres propiedades definen una *relación de equivalencia*, por lo que para cada entero n, la congruencia módulo n es una relación de equivalencia en $\mathbf{Z}$.

Al igual que una relación de orden "ordena un conjunto", una relación de equivalencia lo divide en subconjuntos disjuntos denominados *clases de equivalencia* de tal forma que cada una de las clases contiene a todos los elementos que están relacionados entre sí.

Definición 2.2 [Clases de equivalencia]

En nuestro caso, cada elemento $a \in \mathbf{Z}$ define la clase de equivalencia

$$[a] = \{x \in \mathbf{Z} \ : \ x \equiv a \pmod{n}\} = \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}$$

quedando $\mathbf{Z}$ dividido en las n clases de equivalencia correspondientes a los n posibles restos de dividir un entero entre n

$$[0],\ [1],\ [2],\ \ldots,\ [n-1] \quad \textit{ya que} \quad a \equiv b \pmod{n} \iff [a] = [b]$$

Ejemplo 2.4 Para $n = 2$ el conjunto $\mathbf{Z}$ queda dividido en las clases $[0]$ y $[1]$ que se corresponden con los números pares y los impares respectivamente. □

Definición 2.3 [Enteros módulo n]

Para cada $n \geq 1$, el conjunto de las n clases de congruencia módulo n lo denotamos por $\mathbf{Z}_n$ y se conoce como el conjunto de los enteros módulo n.

$$\mathbf{Z}_n = \{0,\ 1,\ 2,\ \ldots,\ n-1\}$$

donde los elementos $a \in \mathbf{Z}_n$ representan a sus respectivas clases de equivalencia módulo n.

Nuestra próxima meta es estudiar cómo operar con las clases de congruencia, de tal forma que $\mathbf{Z}_n$ sea un conjunto numérico con propiedades similares a las de $\mathbf{Z}$. Haremos uso de la suma, la resta y el producto en $\mathbf{Z}$ para definir las correspondientes operaciones con las clases de congruencias en $\mathbf{Z}_n$.

2.2 La aritmética en $\mathbf{Z}_n$

Si a y b son elementos de $\mathbf{Z}_n$ (es decir, representan a las clases de equivalencia $[a]$ y $[b]$ módulo n respectivamente), definimos su suma, diferencia y producto como las clases

$$\begin{aligned} [a]+[b] &= [a+b] \\ [a]-[b] &= [a-b] \\ [a][b] &= [ab] \end{aligned}$$

Antes de continuar debemos probar que las tres operaciones están bien definidas, en el sentido de que los resultados que se obtienen dependan sólo de las clases $[a]$ y $[b]$, y no de los elementos a y b en particular que se hayan tomado como representantes de la clase.

Ejemplo 2.5 Consideremos el conjunto $\mathbf{Z}_2 = \{0, 1\}$ donde $0 = [0]_2$ representa a cualquier entero par y $1 = [1]_2$ a cualquier número impar.

Decir en $\mathbf{Z}_2$ que

$$1 + 1 = [1] + [1] = [1 + 1] = [2] = [0] = 0$$

equivale a decir que la suma de dos números impares es par, pero independientemente de los números impares que se hayan sumado. □

Con más precisión, debemos probar que si trabajando módulo n

$$\left.\begin{array}{l} [a]=[a'] \\ [b]=[b'] \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcl} [a+b] &=& [a'+b'] \\ [a-b] &=& [a'-b'] \\ [ab] &=& [a'b'] \end{array}\right.$$

Lema 2.3 *Para cualquier entero* $n \geq 1$, *si* $a' \equiv a \pmod{n}$ *y* $b' \equiv b \pmod{n}$, *entonces* $a' + b' \equiv a + b$, $a' - b' \equiv a - b$ *y* $a'b' \equiv ab$.

Demostración.

$$[a] = [a'] \iff a \equiv a' \pmod{n} \implies a' = a + kn \text{ para algún } k \in \mathbf{Z}$$

$$[b] = [b'] \iff b \equiv b' \pmod{n} \implies b' = b + ln \text{ para algún } l \in \mathbf{Z}$$

- $a' + b' = a + kn + b + ln = (a + b) + (k + l)n \implies$

$$a + b \equiv a' + b' \pmod{n} \implies [a + b] = [a' + b']$$

- $a' - b' = a + kn - b - ln = (a - b) + (k - l)n \implies$

$$a - b \equiv a' - b' \pmod{n} \implies [a - b] = [a' - b']$$

- $a'b' = (a + kn)(b + ln) = ab + (al + bk + kln)n \implies$

$$ab \equiv a'b' \pmod{n} \implies [ab] = [a'b']$$

entonces

$$a' \pm b' = (a \pm b) + (k \pm l)n \equiv a \pm b$$
$$a'b' = ab + (al + bk + kln)n \equiv ab$$ ■

Se deduce de aquí que la suma, la resta y el producto de pares de clases de congruencia en $\mathbf{Z}_n$ están bien definidas.

Si repetimos las definiciones de suma y producto podemos definir, para cualquier entero $k \geq 2$ sumas finitas, productos y potencias de clases en $\mathbf{Z}_n$ por

$$\begin{aligned} [a_1] + [a_2] + \cdots + [a_k] &= [a_1 + a_2 + \cdots + a_k] \\ [a_1][a_2] \cdots [a_k] &= [a_1 a_2 \cdots a_k] \\ [a]^k &= [a^k] \end{aligned}$$

El motivo de hacer énfasis en probar que las operaciones aritméticas en $\mathbf{Z}_n$ están bien definidas se hace evidente si intentamos definir la exponencial de clases en $\mathbf{Z}_n$. Podemos definir

$$[a]^{[b]} = [a^b],$$

limitándonos a los valores no negativos de b con el fin de que a^b sea entero.

Si fijamos $n = 3$ se tiene, por ejemplo, que

$$[2]^{[1]} = [2^1] = [2]$$

desafortunadamente, $[1] = [4]$ en $\mathbf{Z}_3$ y nuestra definición nos dice que

$$[2]^{[4]} = [2^4] = [16] = [1] \neq [2]$$

por lo que se obtienen diferentes clases de congruencia para $[a]^{[b]}$ para diferentes representantes b y b' de la misma clase $[b]$.

Limitamos, por tanto, la aritmética en $\mathbf{Z}_n$ a las operaciones bien definidas, tales como la suma, la resta, el producto, la potencia y más adelante veremos que también puede definirse una forma restringida de división.

Dado que las operaciones definidas no dependen de los representantes elegidos podremos utilizar un representante u otro dependiendo del problema que queramos resolver.

Ejemplo 2.6 Calculemos resto de la división de 28×33 entre 35.

$$\left.\begin{array}{l} 28 \equiv -7 \pmod{35} \\ 33 \equiv -2 \pmod{35} \end{array}\right\} \implies 28 \times 33 \equiv (-7) \times (-2) \equiv 14 \pmod{35}$$

Es decir, el resto de la división es 14.

Obsérvese que en $\mathbf{Z}_{35}$ hemos tomado como representantes de las clases 28 y 33 a los enteros -7 y -2 ya que el producto es independiente de los representantes que se tomen. □

Propiedades de la suma y el producto

- Internas:$\forall x, y \in \mathbf{Z}_n \implies x + y,\ xy \in \mathbf{Z}_n$.
- Asociativas: $\forall x, y, z \in \mathbf{Z}_n \implies x+(y+z) = (x+y)+z\ \ x(yz) = (xy)z$.
- Conmutativas: $\forall x, y \in \mathbf{Z}_n \implies x + y = y + x, \quad xy = yx$.
- Distributiva: $\forall x, y, z \in \mathbf{Z}_n \implies x(y + z) = xy + xz$.
- Elementos neutro y unidad: $\exists\ 0, 1 \in \mathbf{Z}_n$ *tales que* $\forall x \in \mathbf{Z}_n \implies$

$$x + 0 = 0 + x = x \quad \text{y} \quad x \cdot 1 = 1 \cdot x = x$$

- Elementos opuestos: $\forall x \in \mathbf{Z}_n$ *existe un único elemento, que denotaremos por* $-x \in \mathbf{Z}_n$ *tal que* $x + (-x) = (-x) + x = 0$.
- Divisores de cero: *Un elemento no nulo de* $\mathbf{Z}_n$ *tal que su producto por otro elemento también no nulo produce un resultado nulo se dice que es un divisor de cero.*

Así, por ejemplo, en $\mathbf{Z}_4$ 2 es divisor de cero ya que $2 \cdot 2 = 0$.

La existencia de divisores de cero hace que, en $\mathbf{Z}_n$, *no se verifique la propiedad cancelativa del producto*.

Ejemplo 2.7 Si confeccionamos las tablas de la suma y el producto en $\mathbf{Z}_4$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

observamos que $2 \cdot 1 = 2 \cdot 3$ y esto no implica la igualdad de 1 y 3, es decir, en $\mathbf{Z}_4$ no se verifica la propiedad cancelativa del producto. □

A la vista de la tabla del producto en $\mathbf{Z}_4$ nos damos cuenta de que aunque el producto no tiene elemento inverso, existen elementos que sí lo tienen, por ejemplo el 3 ($3 \times 3 = 1$, es decir 3 es autoinverso). Cabe entonces hacerse la siguiente pregunta

¿cuándo va a tener inverso un elemento de $\mathbf{Z}_n$?

Definición 2.4 UNIDADES DE $\mathbf{Z}_n$

Un elemento r de $\mathbf{Z}_n$ decimos que es una unidad si es inversible, es decir, si existe otro elemento $s \in \mathbf{Z}_n$ tal que $sr = rs = 1$.

Teorema 2.4 *El inverso de un elemento unidad es único.*

Demostración. Supongamos que existan dos elementos inversos de r, s y s' y probemos que $s = s'$. En efecto:

$$s = s \cdot 1 = s(rs') = (sr)s' = 1 \cdot s' = s'.$$ ■

Teorema 2.5 *Un elemento $r \in \mathbf{Z}_n$ es inversible si, y sólo si, r y n son primos entre si, es decir, si* $\operatorname{mcd}(n, r) = 1$.

$$r \text{ unidad de } \mathbf{Z}_n \iff r \perp n$$

Demostración.

Si r es una unidad, existe $r^{-1} \in \mathbf{Z}_n$ tal que

$$rr^{-1} = 1 \implies rr^{-1} \equiv 1 \pmod{n} \implies rr^{-1} - 1 = kn \quad \text{con} \quad k \in \mathbf{Z}$$

$$rr^{-1} - kn = 1 \quad \text{véase el Teorema 1.14–(b)} \implies r \perp n$$

Si $r \perp n$, existen enteros a y b tales que (véase el Teorema 1.14–(b))

$$ar + bm = 1 \implies ar - 1 = -bn = \overset{\bullet}{n} \implies ar \equiv 1 \pmod{n}$$

o lo que es lo mismo, $ar = 1 \implies r$ es una unidad de $\mathbf{Z}_n$. ■

El algoritmo extendido de Euclides nos proporciona el inverso de los elementos unitarios de $\mathbf{Z}_n$.

Ejemplo 2.8 Las unidades de $\mathbf{Z}_8$ son $1, 3, 5$ y 7, en efecto:

$$1 \cdot 1 = 1 \qquad 3 \cdot 3 = 1 \qquad 5 \cdot 5 = 1 \qquad 7 \cdot 7 = 1$$

por lo que cada una de estas unidades es su propio inverso.

En $\mathbf{Z}_9$ las unidades son $1, 2, 4, 5, 7$ y 8

$$1 \cdot 1 = 1 \qquad 2 \cdot 5 = 1 \qquad 4 \cdot 7 = 1 \qquad 8 \cdot 8 = 1$$ □

La estructura de $[\mathbf{Z}_n, +, \cdot]$

- Si n es compuesto $n = ab$ con $1 < a, b < n$ por lo que en $\mathbf{Z}_n$ las clases definidas por dichos elementos verificarán que $ab = 0$ es decir, $\mathbf{Z}_n$ posee divisores de cero y la estructura de $[\mathbf{Z}_n, +, \cdot]$ es de un *anillo con divisores de cero*.

- Si p es primo, cualquier elemento no nulo de $\mathbf{Z}_p = \{0, 1, \ldots, p-1\}$ es primo con p y posee inverso, por lo que todos los elementos no nulos de $\mathbf{Z}_p$ tienen inverso, resultando que $[\mathbf{Z}_p, +, \cdot]$ tiene estructura de *cuerpo*.

Teorema 2.6 *Los únicos elementos autoinversos de* $\mathbf{Z}_p$ *con* p *primo son* 1 *y* $p - 1$.

Demostración. Si s es autoinverso en $\mathbf{Z}_p$

$$s^2 \equiv 1 \pmod{p} \implies s^2 - 1 = (s-1)(s+1) \equiv 0 \pmod{p}.$$

Al ser p primo, $\mathbf{Z}_p$ no tiene divisores de 0, por lo que se ha de verificar que

$$\begin{cases} s-1 \equiv 0 \pmod{p} \implies s \equiv 1 \pmod{p} \implies s = 1 \text{ en } \mathbf{Z}_p \\ s+1 \equiv 0 \pmod{p} \implies s \equiv -1 \pmod{p} \implies s = p-1 \text{ en } \mathbf{Z}_p \end{cases}$$

Recíprocamente, 1 y $n-1$ son siempre autoinversos en $\mathbf{Z}_n$, ya que

$$\begin{cases} 1 \cdot 1 \equiv 1 \pmod{n} \\ (n-1)\cdot(n-1) = n^2 - 2n + 1 \equiv 1 \pmod{n} \end{cases}$$

en particular, en $\mathbf{Z}_p$.

En el caso $p = 2$ los elementos 1 y $2 - 1 = 1$ coinciden, existiendo un único autoinverso en $\mathbf{Z}_2$. Obsérvese, no obstante, que el único elemento no nulo de $\mathbf{Z}_2$ es el 1.

2.3 Criterios de divisibilidad

Teorema 2.7 *Sea $P(x)$ un polinomio con coeficientes enteros y sea $n \geq 1$.*

$$a \equiv b \pmod{n} \implies P(a) \equiv P(b) \pmod{n}$$

Demostración. Sea $P(x) = a_0 + a_1 x + \cdots + a_k x^k$ con $c_i \in \mathbf{Z}\ \forall\, i = 1, 2, \ldots, k$

$$P(a) = a_0 + a_1 a + \cdots + a_k a^k \qquad P(b) = a_0 + a_1 b + \cdots + a_k b^k$$

$$a \equiv b \implies a^i \equiv b^i \implies c_i a^i \equiv c_i b^i\ \forall\, i = 1, 2, \ldots k \implies P(a) \equiv P(b) \pmod{n}$$

■

Una aplicación directa del teorema anterior es la obtención de *criterios de divisibilidad*.

Sea $N = a_n a_{n-1} \ldots a_1 a_0$ con $0 \leq a_i \leq 9$ la expresión decimal de un entero N.

$$N = a_n 10^n + \cdots a_1 10 + a_0 = P(10) \quad \text{con} \quad P(x) = a_n x^n + \cdots a_1 x + a_0$$

Criterio de divisibilidad por 3

$$10 \equiv 1 \pmod 3 \implies N = P(10) \equiv P(1) = \sum_{i=0}^{n} a_i \pmod 3$$

Un número es divisible por 3 si, y sólo si, lo es el número formado por la suma de sus cifras.

Criterio de divisibilidad por 9

$$10 \equiv 1 \pmod 9 \implies N = P(10) \equiv P(1) = \sum_{i=0}^{n} a_i \pmod 9$$

Un número es divisible por 9 si, y sólo si, lo es el número formado por la suma de sus cifras.

Criterio de divisibilidad por 11

$$10 \equiv -1 \pmod{11} \implies N \equiv P(-1) = a_0 - a_1 + \cdots + (-1)^n a_n \pmod{11}$$

Un número es divisible por 11 si, y sólo si, lo es número resultante de sumar las cifras que ocupan lugar par y restarle la suma de las cifras que ocupan lugar impar.

Otra aplicación del Teorema 2.7 nos permite detectar si un polinomio entero puede tener raíces enteras.

Teorema 2.8 *Sea $P(x)$ un polinomio con coeficientes enteros. Dado que*

$$\left.\begin{array}{c} P(\overline{x}) = 0 \quad con \quad \overline{x} \in \mathbf{Z} \\ \overline{x} \equiv a \pmod n \end{array}\right\} \implies P(a) \equiv 0 \pmod n$$

Si para algún $n > 1$ se verifica que $P(a) \not\equiv 0 \pmod n \ \ \forall\, a \in \mathbf{Z}_n$, el polinomio carece de raíces enteras.

Ejemplo 2.9 Para $n = 4$ el polinomio $P(x) = x^5 - x^2 + x - 3$ verifica que

$$\left.\begin{array}{l} P(0) = -3 \equiv 1 \neq 0 \pmod 4 \\ P(1) = -2 \equiv 2 \neq 0 \pmod 4 \\ P(2) = 27 \equiv 3 \neq 0 \pmod 4 \\ P(3) = 234 \equiv 2 \neq 0 \pmod 4 \end{array}\right\} \implies P(x) \text{ carece de raíces enteras}$$

□

Como n divide a m si, y sólo si, $m \equiv 0 \pmod{n}$, se sigue que los problemas sobre divisibilidad son equivalentes a los problemas sobre congruencias y, estos últimos son, a veces, más fáciles de resolver. Una típica ilustración de ello es la siguiente:

Ejemplo 2.10 Probar, mediante congruencias, que $3^{2n+5} + 2^{4n+1}$ es divisible por 7 cualquiera que sea el entero $n \geq 1$.

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 $3^{2n+5} + 2^{4n+1}$ □

El polinomio $P(x) = x^2 + x + 41$ tiene la propiedad de que $P(x)$ es primo para $x = -40, -39, \ldots, 38, 39$ (sin embargo no lo es para $x = -41$ o $x = 40$). Esto motiva a uno a preguntarse:

¿existen polinomios tales que $P(x)$ sea primo para cualquier valor de x?

Teorema 2.9 *No existen polinomios no constantes $P(x)$, con coeficientes enteros, tales que $P(x)$ sea primo para cualquier entero x.*

Demostración. Supongamos que $P(x)$ es primo para cualquier entero x y que no es constante.

Si elegimos un entero a, entonces $P(a)$ es un primo p.

Para cada $b \equiv a \pmod{p}$ se sabe que $P(b) \equiv P(a) \pmod{p}$, por lo que $P(b) \equiv 0 \pmod{p}$ y, por tanto, p divide a $P(b)$.

Por nuestra hipótesis, $P(b)$ es primo, por lo que $P(b) = p$.

Como existen infinitos enteros $b \equiv a \pmod{p}$, el polinomio $Q(x) = P(x) - p$ tiene infinitas raíces.

Sin embargo, esto no es posible: teniendo grado $d \geq 1$, $Q(x)$ puede tener, a lo sumo, d raíces, por lo que tales polinomios $P(x)$ no existen. ■

2.4 Congruencias lineales

Volvemos ahora a la cuestión de la división de clases de congruencias, pospuesta anteriormente en este capítulo. Con el fin de dar sentido al cociente $[a]/[b]$

de dos clases de congruencias $[a], [b] \in \mathbf{Z}_n$, tenemos que considerar la solución de la *congruencia lineal* $ax \equiv b \pmod{n}$. Nótese que si x es una solución, y $x' \equiv x$, entonces $ax' \equiv ax \equiv b$ y, por tanto, x' también es una solución; por lo que las soluciones (en caso de existir) las constituyen clases de congruencia. Como $ax \equiv b \pmod{n}$ si, y sólo si, $ax - b$ es múltiplo de n, se tiene que x es una solución de la congruencia lineal si, y sólo si, existe un entero y tal que x e y satisfacen la ecuación diofántica $ax + ny = b$. Nosotros estudiamos esta ecuación (con un pequeño cambio de notación) en el Capítulo 1, de donde cambiando el Teorema 1.19 al lenguaje de las congruencias, se tiene:

Teorema 2.10 *Si $d = \text{mcd}\,(a, n)$, entonces la congruencia lineal*

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

tiene solución si, y sólo si, d divide a b. Si d divide a b y x_0 es una solución, la solución general viene dada por

$$x = x_0 + \frac{nt}{d}$$

donde $t \in \mathbf{Z}$: en particular, las soluciones forman, exactamente, d clases de congruencias módulo n, con representantes:

$$x = x_0,\ x_0 + \frac{n}{d},\ x_0 + \frac{2n}{d}, \cdots\ x_0 + \frac{(d-1)n}{d}$$

(De hecho, la ecuación $x = x_0 + t(n/d)$ prueba que las soluciones forman un *única* clase de congruencia $[x_0] \pmod{n/d}$, pero dado que el problema se plantea en términos de congruencias módulo n, está generalizado (y es frecuente) expresar las soluciones en esos mismos términos.)

Demostración. Independientemente de un pequeño cambio de notación (n y b son reemplazadas por b y c), la única parte de este teorema que no es una traslación directa del Teorema 1.19 es el apartado sobre las clases de congruencias. Para probarlo, obsérvese que

$$x_0 + \frac{nt}{d} \equiv x_0 + \frac{nt'}{d} \pmod{n}$$

si, y sólo si, n divide a $n(t - t')/d$, es decir, si, y sólo si, d divide a $t - t'$, por lo que las clases de congruencia de las soluciones módulo n se obtienen haciendo que t recorra un conjunto completo de restos módulo d tales como $0, 1, \ldots, d - 1$. ■

Ejemplo 2.11 Consideremos la congruencia

$$10x \equiv 3 \pmod{12}.$$

Aquí $a = 10$, $b = 3$ y $n = 12$, por lo que $d = \text{mcd}\,(10, 12) = 2$; como no divide a 3, no existen soluciones. (Esto puede verse directamente: los elementos de la clase de congruencia [3] en $\mathbf{Z}_{12}$ son todos impares, mientras que cualquier elemento de $[10][x]$ es par.) □

Ejemplo 2.12 Consideremos ahora la congruencia

$$10x \equiv 6 \pmod{12}.$$

Al igual que antes, $d = 2$ y ahora sí divide a $b = 6$, por lo que existen dos clases de soluciones. Podemos tomar $x_0 = 3$ como solución particular para expresar la solución general de la forma

$$x = x_0 + \frac{nt}{d} = 3 + \frac{12t}{2} = 3 + 6t$$

donde $t \in \mathbf{Z}$. Estas soluciones constituyen dos clases de congruencia [3] y [9] módulo 12, cuyos representantes $x_0 = 3$ y $x_0 + (n/d) = 9$; constituyen la única clase de congruencia [3] módulo 6. □

Corolario 2.11 *Si* $\text{mcd}\,(a, n) = 1$ *las soluciones* x *de la congruencia lineal* $ax \equiv b \pmod{n}$ *constituyen una única clase de congruencia módulo* n*.*

Demostración. Hacer $d = 1$ en el Teorema 2.10. ■

Esto nos lleva a que si a y n son primos entre sí, para cada b existe una única clase $[x]$ tal que $[a][x] = [b]$ en $\mathbf{Z}_n$; podemos considerar que la clase $[x]$ es la clase cociente $[b]/[a]$ obtenida dividiendo $[b]$ entre $[a]$ en $\mathbf{Z}_n$. Si $d = \text{mcd}\,(a, n) > 1$ existen, sin embargo, más de una clase $[x]$ (cuando d divide a b), o ninguna (cuando d no divide a b), por lo que no podemos definir, en este caso, la clase cociente $[b]/[a]$.

Ejemplo 2.13 Consideremos la congruencia

$$7x \equiv 3 \pmod{12}.$$

Aquí $a = 7$ y $n = 12$ por lo que, al ser primos entre sí, sólo existe una clase solución; esta es la clase $[x] = [9]$, ya que $7 \times 9 = 63 \equiv 3 \pmod{12}$. □

En los Ejemplos 2.11, 2.12 y 2.13 se tiene $n = 12$. Cuando n es pequeño, es factible encontrar soluciones a la congruencia $ax \equiv b \pmod{n}$ por inspección: se puede calcular ax para cada uno de los n elementos x de un conjunto completo de restos módulo n y ver cuáles de esos productos son congruentes con b. Sin embargo, cuando n es grande es necesario encontrar un método más eficiente para resolver congruencias lineales. Daremos un método para ello, basado en el Teorema 2.10, pero primero necesitamos algunos resultados previos que ayudan a simplificar el problema.

Lema 2.12 [Propiedades de las congruencias lineales]

a) Sea m un divisor de a, b y n y sean $a' = a/m$, $b' = b/m$ y $n' = n/m$;

$$ax \equiv b \pmod{n} \iff a'x \equiv b' \pmod{n'}.$$

b) Sean a y n primos entre sí, m un divisor de a y b y sean $a' = a/m$ y $b' = b/m$;

$$ax \equiv b \pmod{n} \iff a'x \equiv b' \pmod{n}.$$

Demostración.

a) $ax \equiv b \pmod{n} \iff ax - b = qn$ para algún entero q; dividiendo por m se tiene

$$a'x - b' = qn' \iff a'x \equiv b' \pmod{n'}$$

b) $ax \equiv b \pmod{n} \iff ax - b = qn$ para algún entero q; dividiendo por m se tiene

$$a'x - b' = qn/m \iff m \mid qn$$

Como m es un divisor de a, el cual es primo con n, m también es primo con n y, según el Teorema 1.14–(d), $m \mid q$.

Se tiene entonces que $a'x - b' = (q/m)n$ es un múltiplo de n, por lo que $a'x \equiv b' \pmod{n}$.

Recíprocamente, si $a'x \equiv b' \pmod{n}$ se tiene que $a'x - b' = q'n$ para algún entero q', por lo que multiplicando por m obtenemos

$$ax - b = mq'n \iff ax \equiv b \pmod{n}$$

■

Obsérvese que en (a), donde m es un divisor de a, b y n, dividimos los tres enteros por m, mientras que en (b), donde m es divisor de a y b, dividimos sólo estos dos enteros entre m, dejando n inalterado.

Daremos ahora un método para resolver la congruencia $ax \equiv b \pmod{n}$.

Cálculo de una solución particular

Vamos a desarrollar un proceso para tratar de eliminar el coeficiente a de la congruencia, ya que en ese caso nos quedaría

$$x \equiv b \pmod{n} \iff x = b + n\,t \quad \forall\, t \in \mathbf{Z}$$

$$10x \equiv 6 \pmod{14}$$

Paso 1 Calculamos $d = \text{mcd}\,(a, n)$ y vemos si $d \,|\, b$. En caso contrario, no existen soluciones y paramos. Si lo divide, vamos al paso 2.

$$d = \text{mcd}\,(10, 12) = 2 \,|\, 6 = b \implies \textit{la congruencia admite soluciones}$$

Paso 2 Como d divide de a, b y n,

$$ax \equiv b \pmod{n} \implies a'x \equiv b' \pmod{n'} \text{ con } a' \perp n' \quad \textit{Si } a' = 1, \textit{ FIN}$$

$$10x \equiv 6 \pmod{12} \iff 5x \equiv 3 \pmod{6} \text{ con } 5 \perp 6$$

Paso 3 Calculamos $d' = \text{mcd}\,(a', b')$ y llamando $a'' = a'/d'$ y $b'' = b'/d'$

$$a'x \equiv b' \pmod{n'} \implies a''x \equiv b'' \pmod{n'} \quad \textit{Si } a'' = 1, \textit{ FIN}$$

$$\text{mcd}\,(5, 3) = 1 \implies 5x \equiv 3 \pmod{6}$$

Paso 4 Observando que

$$b'' \equiv b'' \pm n' \equiv b'' \pm 2n' \equiv \cdots \pmod{n'}$$

podemos sumar o restar al término independiente múltiplos del módulo con vistas a que la aplicación del paso 3 reduzca en módulo el coeficiente de la congruencia.

$$5x \equiv 3 \pmod{6} \Rightarrow \begin{cases} 5x \equiv 3 + 1 \cdot 6 = 9 \pmod{6} \\ 5x \equiv 3 + 2 \cdot 6 = 15 \pmod{6} \Rightarrow x \equiv 3 \pmod{6} \end{cases}$$

Se ha eliminado el coeficiente, FIN. $x = 3 + 6\,t \quad \forall\, t \in \mathbf{Z}$.

Otra alternativa consiste en multiplicar la congruencia (no el módulo) por algún número primo con el módulo (inverso del paso 2) para que, el coeficiente se reduzca en función del módulo.

$5 \perp 6 \Rightarrow 5 \cdot 5x \equiv 5 \cdot 3 \pmod 6 \Rightarrow 25x \equiv 15 \pmod 6 \Rightarrow x \equiv 3 \pmod 6$

Se ha eliminado el coeficiente, FIN. $x = 3 + 6\,t \quad \forall\, t \in \mathbf{Z}$.

Si lo que queremos es un algoritmo programable debemos convertirla en la ecuación diofántica equivalente $ax - nt = b$ y hallar la solución general para la variable x mediante el Algoritmo Extendido de Euclides (AEE).

Así pues, el algoritmo que programaríamos sería el siguiente, que tiene por entradas los enteros a, b y n:

```
1   Calcular d = mcd (a, n)
2   Si b ≢ 0 (mod d)
        retornar No tiene solución
        si no, a = a/d, b = b/d, n = n/d
            Aplicar el AEE al par (a, n) → u · a + v · n = 1
            Retorna x = u · b mod n
```

Ejemplo 2.14 Consideremos la congruencia $4x \equiv 13 \pmod{47}$.

dado que $\text{mcd}\,(4, 47) = 1 \mid 13$ la congruencia admite soluciones.

Al ser $d = 1$ el primer paso nos deja la congruencia invariante.

Al ser también $\text{mcd}\,(4, 13) = 1$ el segundo paso tampoco modifica la ecuación.

Teniendo en cuenta que $12 \perp 47$ podemos multiplicar la congruencia por 12 dejando inalterado al módulo

$$48x \equiv 156 \pmod{47} \iff x \equiv 15 \pmod{47}$$

Es decir, $x = 15 + 47\,t \quad \forall\, t \in \mathbf{Z}$. □

2.5 Sistemas de congruencias lineales

Un *sistema de congruencias lineales* es un sistema de la forma

$$\begin{aligned} a_1x &\equiv b_1 \pmod{n_1} \\ a_2x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ a_kx &\equiv b_k \pmod{n_k} \end{aligned}$$

Es decir, se trata de un sistema de k ecuaciones pero con una sola incógnita.

Para que el sistema tenga solución deberán tenerla cada una de las ecuaciones del sistema, lo que equivale a decir que se pueden eliminar todos los coeficientes a_i, ya que eliminado a_i está resuelta la ecuación i-ésima.

Una vez eliminados todos los coeficientes a_i lo único que sabemos es que todas las ecuaciones tienen solución, pero desconocemos si existe alguna solución común a todas ellas.

Es evidente que a la hora de resolver un sistema lo primero que habrá que hacer es ver si cada ecuación tiene solución (en caso contrario el sistema no puede tenerla) y una vez comprobado (una vez eliminados todos los coeficientes a_i) tratar de ver si existe alguna solución común a todas las ecuaciones, es decir, tratar de ver si *el sistema* tiene solución.

La primera parte, eliminar los coeficientes a_i, ya sabemos hacerlo, se trata de resolver las k congruencias lineales, por lo que el estudio de la existencia de soluciones de un sistema lo haremos sobre un sistema que ya tiene resueltas todas sus congruencias, es decir, partiremos de un sistema de la forma

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

2.5.1 Teorema chino de los restos

En el siglo IV a.C. el matemático chino Sun Tsu Suan-Ching estudió problemas como el de encontrar un número que genere los restos 2, 3 y 2 al dividirlo por 3,

5 y 7 respectivamente. Esto equivale a encontrar un x tal que las congruencias

$$x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 2 \pmod 7$$

se satisfagan simultáneamente. Obsérvese que si x_0 es una solución, también lo es $x = x_0 + (3\times 5\times 7)t$ para cualquier entero t, por lo que la solución constituye una clase de congruencia módulo 105. En este caso, las soluciones constituyen una *única* clase de congruencia, pero en otros casos pueden constituir varias clases o incluso no existir. Por ejemplo, el sistema de congruencias lineales

$$x \equiv 3 \pmod 9, \quad x \equiv 2 \pmod 6$$

carece de soluciones, ya que si $x \equiv 3 \pmod 9$ entonces 3 es un divisor de x, mientras que si $x \equiv 2 \pmod 6$, 3 no puede ser un divisor de x. El problema consiste en que los módulos 9 y 6 tienen el factor 3 común, por tanto, ambas congruencias tienen implicaciones sobre las clases de congruencia módulo 3, y en este caso particular, ambas implicaciones son mutuamente inconsistentes. Para evitar este tipo de problema, nos limitaremos, en principio, a los casos en los que los módulos son mutuamente primos entre sí. Afortunadamente, el siguiente resultado, conocido como *teorema Chino de los restos*, soluciona este tipo de problemas.

Teorema 2.13 [Teorema Chino de los restos]

Sean $n_1, n_2, \ldots, n_k$ enteros positivos tales que $\operatorname{mcd}(n_i, n_j) = 1$ siempre que $i \neq j$, y sean $a_1, a_2, \ldots, a_k$ enteros cualesquiera. Entonces, las soluciones del sistema de congruencias lineales

$$x \equiv a_1 \pmod{n_1}, \quad x \equiv a_2 \pmod{n_2}, \quad \ldots \quad x \equiv a_k \pmod{n_k}$$

constituyen una única clase de congruencia módulo n, donde $n = n_1 n_2 \cdots n_k$.

(Este resultado tiene aplicaciones en muchas áreas, incluyendo la astronomía: si k eventos ocurren regularmente, con períodos $n_1, \ldots, n_k$ y con el i-ésimo evento ocurriendo en los tiempos $x = a_i, a_i + n_i, a_i + 2n_i, \ldots$, los k eventos ocurren simultáneamente cada x tiempo, donde $x \equiv a_i \pmod{n_i}$ para todo i; el teorema prueba que si los períodos n_i son mutuamente primos entre sí, cada coincidencia ocurre con período n. La conjunción de los planetas y los eclipses son ejemplos de tales eventos regulares, y el pronosticarlos fue la motivación original de este teorema).

Demostración. Construyamos las constantes

$$c_i = \frac{n}{n_i} = n_1 \cdots n_{i-1} n_{i+1} \cdots n_k \quad \text{para cada } i = 1, \ldots, k$$

Dado que $n_i \perp n_j$ si $i \neq j$ se sabe que $n_i \perp c_i \ \ \forall\, i = 1, 2, \ldots, k$.

El Corolario 2.11 implica, además, que para cada i, la congruencia

$$c_i x \equiv 1 \pmod{n_i}$$

tiene una única clase d_i de soluciones módulo n_i.

Podemos exigir ahora que el entero

$$x_0 = a_1 c_1 d_1 + a_2 c_2 d_2 + \cdots + a_k c_k d_k$$

satisfaga simultáneamente las congruencias dadas, esto es, $x_0 \equiv a_i \pmod{n_i}$ para cada i.

Como cualquier $c_j \ \ (j \neq i)$ es divisible por $n_i \implies a_j c_j d_j \equiv 0 \pmod{n_i}$ y por tanto

$$x_0 \equiv a_i c_i d_i \pmod{n_i} \ \ \forall\, i = 1, 2, \ldots, k$$

Como además $c_i d_i \equiv 1 \pmod{n_i}$ (por construcción de los d_i) se tiene

$$x_0 \equiv a_i \pmod{n_i} \ \ \forall\, i = 1, 2, \ldots, k$$

es decir, x_0 es una solución particular del sistema y se sigue inmediatamente que toda la clase de congruencia $[x_0]$ módulo n está compuesta de soluciones.

Para ver que esta clase es única, supongamos que x es una solución; entonces $x \equiv a_i \pmod{n_i}$ para todo $i = 1, 2, \ldots, k$.

$$\left.\begin{array}{l} x \equiv a_i \pmod{n_i} \\ x_0 \equiv a_i \pmod{n_i} \end{array}\right\} \implies x \equiv x_0 \pmod{n_i} \implies n_i \,|\, (x - x_0) \ \ \forall\, i = 1, 2, \ldots, k$$

Como $n_1, \ldots, n_k$ son mutuamente primos entre sí, su producto n también divide a $x - x_0$, por lo que $x \equiv x_0 \pmod{n}$.

En otras palabras, la solución general viene dada por

$$x = x_0 + n\,t \ \ \forall\, t \in \mathbf{Z} \quad \text{con} \quad n = n_1 \cdot n_2 \cdots n_k$$

■

Lema 2.14 *Consideremos la descomposición de n en factores primos*

$$n = p_1^{e_1} \cdots p_k^{e_k},$$

donde $p_1, \ldots, p_k$ son primos diferentes. Para cualesquiera enteros a y b

$$a \equiv b \pmod{n} \iff a \equiv b \pmod{p_i^{e_i}} \ \ \textit{para cada} \ \ i = 1, \ldots, k$$

Demostración. Sea $n = p_1^{e_1} \cdots p_k^{e_k}$.

$$n_i = p_i^{e_i} \quad i = 1, \ldots, k \implies \begin{cases} n_i \perp n_j \text{ si } i \neq j \\ n = n_1\, n_2 \cdots n_k \end{cases}$$

El Teorema Chino de los restos implica además que las soluciones del sistema de congruencias $x \equiv b \pmod{n_i}$ $1 \leq i \leq k$ constituyen una única clase de congruencia módulo n.

Dado que b es claramente una solución del sistema

$$x \equiv b \pmod{n} \iff x \equiv b \pmod{p_i^{e_i}} \quad i = 1, \ldots, k$$

En particular, para $x = a$

$$a \equiv b \pmod{n} \iff a \equiv b \pmod{p_i^{e_i}} \quad i = 1, \ldots, k$$ ■

Ejemplo 2.15 Vamos a resolver la congruencia $91x \equiv 419 \pmod{440}$.

Al ser $\text{mcd}\,(91, 440) = 1$ tiene solución y, por ser $440 = 2^3 \cdot 5 \cdot 11$, la congruencia es equivalente al sistema

$$\begin{cases} 91x \equiv 419 \pmod 8 \\ 91x \equiv 419 \pmod 5 \\ 91x \equiv 419 \pmod{11} \end{cases} \iff \begin{cases} 3x \equiv 3 \pmod 8 \\ x \equiv 4 \pmod 5 \\ 3x \equiv 1 \pmod{11} \end{cases} \iff \begin{cases} x \equiv 1 \pmod 8 \\ x \equiv 4 \pmod 5 \\ x \equiv 4 \pmod{11} \end{cases}$$

Sistema, este último, en el que

$$a_1 = 1, \quad a_2 = 4, \quad a_3 = 4, \quad n_1 = 8, \quad n_2 = 5, \quad n_3 = 11, \quad n = n_1 \cdot n_2 \cdot n_3 = 440$$

$$c_1 = \frac{n}{n_1} = 55 \quad c_2 = \frac{n}{n_2} = 88 \quad c_3 = \frac{n}{n_3} = 40$$

$$c_1 d_1 \equiv 1 \pmod{n_1} \Rightarrow 55 d_1 \equiv 1 \pmod 8 \Rightarrow d_1 \equiv 7 \pmod 8 \Rightarrow d_1 = 7$$

$$c_2 d_2 \equiv 1 \pmod{n_2} \Rightarrow 88 d_2 \equiv 1 \pmod 5 \Rightarrow d_2 \equiv 2 \pmod 5 \Rightarrow d_2 = 2$$

$$c_3 d_3 \equiv 1 \pmod{n_3} \Rightarrow 40 d_3 \equiv 1 \pmod{11} \Rightarrow d_3 \equiv 8 \pmod{11} \Rightarrow d_3 = 8$$

$$x_0 = a_1 c_1 d_1 + a_2 c_2 d_2 + a_3 c_3 d_3 = 1 \cdot 55 \cdot 7 + 4 \cdot 88 \cdot 2 + 4 \cdot 40 \cdot 8 = 2369$$

por lo que la solución general viene dada por la de la congruencia

$$x \equiv 2369 \pmod{440} \iff x \equiv 169 \pmod{440}$$

$$x = 169 + 440\, t \quad \forall\, t \in \mathbf{Z}$$ □

Veamos ahora un segundo método de resolución de sistemas de congruencias lineales, el cual es menos directo pero más intuitivo.

Método de resolución de sistemas de congruencias lineales

Comenzamos buscando la solución de una de las congruencias. Usualmente se comienza por la congruencia que tiene mayor módulo. Para el sistema

$$x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 2 \pmod 7$$

comenzamos por $x \equiv 2 \pmod 7$; la cual tiene, obviamente, la solución

$$x = 2 + 7u \quad \forall\, u \in \mathbf{Z}$$

Obligamos ahora a que dicha solución verifique la siguiente congruencia

$$2 + 7u \equiv 3 \pmod 5 \implies 2u \equiv 1 \pmod 5 \implies u \equiv 3 \pmod 5 \implies$$

$$u = 3 + 5v \quad \forall\, v \in \mathbf{Z}$$

por lo que

$$x = 2 + 7u = 2 + 7(3 + 5v) = 23 + 35v \quad \forall\, v \in \mathbf{Z}$$

verificará simultáneamente ambas congruencias.

Llevando este resultado a la tercera

$$23 + 35v \equiv 2 \pmod 3 \implies 2v \equiv 0 \pmod 3 \implies v \equiv 0 \pmod 3 \implies$$

$$v = 3t \quad \forall\, t \in \mathbf{Z} \implies x = 23 + 35(3\,t) = 23 + 105\,t \quad \forall\, t \in \mathbf{Z}$$

La solución general del sistema viene dada por

$$x = 23 + 105\,t \quad \forall\, t \in \mathbf{Z}$$

2.5.2 Teorema chino de los restos generalizado

Nuestro resultado final, obtenido por Yih-Hing en el siglo VII, generaliza el Teorema Chino de los restos al caso en el que los módulos no son primos entre sí.

Teorema 2.15 [Teorema Chino de los restos generalizado]

Consideremos los enteros positivos $n_1, n_2, \ldots, n_k$ y sean $a_1, a_2, \ldots, a_k$ enteros cualesquiera. El sistema de congruencias

$$x \equiv a_1 \pmod{n_1}, \quad \ldots \quad , \quad x \equiv a_k \pmod{n_k}$$

admiten solución si, y sólo si, $\text{mcd}\,(n_i, n_j)$ *divide a* $a_i - a_j$ *para cualesquiera* $i \neq j$.

Cuando se verifica esta condición, la solución general constituye una única clase de congruencia módulo n, donde n es el mínimo común múltiplo de $n_1, \ldots, n_k$.

Demostración.

- Si existe solución

$$x_0 \equiv a_i \pmod{n_i} \implies n_i | (x_0 - a_i) \quad \forall\, i = 1, 2, \ldots, k$$

Para cada par $i \neq j$ sea $n_{ij} = \text{mcd}\,(n_i, n_j)$

$$\left.\begin{array}{l} n_{ij} \,|\, n_i \;\Rightarrow\; n_{ij} \,|\, (x_0 - a_i) \\ n_{ij} \,|\, n_j \;\Rightarrow\; n_{ij} \,|\, (x_0 - a_j) \end{array}\right\} \Rightarrow\; n_{ij} \,|\, [(x_0 - a_i) - (x_0 - a_j)] = a_i - a_j$$

Si x es una solución cualquiera se verifica para cada $i = 1,\ 2,\ \ldots,\ k$

$$\left.\begin{array}{l} x \equiv a_i \pmod{n_i} \\ x_0 \equiv a_i \pmod{n_i} \end{array}\right\} \implies x \equiv x_0 \pmod{n_i} \implies$$

$$n_i \,|\, (x - x_0) \quad \forall\, i = 1,\ 2,\ \ldots,\ k \implies$$

$$\left.\begin{array}{l} x - x_0 = \overset{\bullet}{n}_i \\ 1 \leq i \leq k \end{array}\right\} \implies x - x_0 = \overset{\bullet}{n} \;\text{ con }\; n = \text{mcm}\,(n_1, \ldots, n_k) \implies$$

$$x \equiv x_0 \pmod{n}$$

- Si $n_{ij} \,|\, (a_i - a_j) \;\; \forall\, i \neq j$

  Sabemos que $x \equiv a \pmod{n}$ con $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, es decir

$$\begin{cases} x \equiv a \pmod{p_1^{\alpha_1}} \\ x \equiv a \pmod{p_2^{\alpha_2}} \\ \vdots \\ x \equiv a \pmod{p_s^{\alpha_s}} \end{cases}$$

  Por lo que podemos reemplazar cada ecuación por un sistema equivalente en el que los módulos son todos potencias de primos no necesariamente distintos.

  Por otra parte, si hemos obtenido dos ecuaciones de la forma

$$\left.\begin{array}{l} x \equiv a_i \pmod{p^e} \;\text{ obtenida a partir de } x \equiv a_i \pmod{n_i} \\ x \equiv a_j \pmod{p^f} \;\; f \leq e \text{ obtenida a partir de } x \equiv a_j \pmod{n_j} \end{array}\right\} \Rightarrow$$

$$\left.\begin{array}{l} p^f \,|\, n_j \\ p^f \,|\, p^e \,|\, n_i \end{array}\right\} \implies p^f \,|\, n_{ij} \,|\, (a_i - a_j) \implies a_i \equiv a_j \pmod{p^f}$$

$$x \equiv a_i \pmod{p^e} \implies x \equiv a_i \pmod{p^f} \implies x \equiv a_j \pmod{p^f}$$

  Esto significa que podemos eliminar todas las congruencias para este primo, con la única excepción de la congruencia $x \equiv a_i \pmod{p^e}$ en la que interviene la mayor potencia de p, ya que esta última congruencia implica las demás.

  Si hacemos esto con cada primo p, nos quedamos con un sistema de congruencias de la forma $x \equiv a_i \pmod{p^e}$ involucrando a los distintos primos p y dado que los módulos p^e son mutuamente primos entre sí, el Teorema Chino de los restos implica que las congruencias tienen una solución común, la cual es, automáticamente, una solución del sistema original. ■

Ejemplo 2.16 Consideremos las congruencias

$$x \equiv 11 \pmod{36}, \quad x \equiv 7 \pmod{40}, \quad x \equiv 32 \pmod{75}.$$

$$\left.\begin{array}{l} \text{mcd}\,(36,40) = 4 \,|\, (a_1 - a_2) = \quad 4 \\ \text{mcd}\,(36,75) = 3 \,|\, (a_1 - a_3) = -21 \\ \text{mcd}\,(40,75) = 5 \,|\, (a_2 - a_3) = -25 \end{array}\right\} \Longrightarrow \textit{El sistema tiene solución}$$

$$\left\{\begin{array}{l} x \equiv 11 \pmod{2^2 \cdot 3^2} \iff \left\{\begin{array}{l} x \equiv 11 \pmod{2^2} \iff x \equiv 3 \pmod{2^2} \\ x \equiv 11 \pmod{3^2} \iff x \equiv 2 \pmod{3^2} \end{array}\right. \\ x \equiv 7 \pmod{2^3 \cdot 5} \iff \left\{\begin{array}{l} x \equiv 7 \pmod{2^3} \iff x \equiv 7 \pmod{2^3} \\ x \equiv 7 \pmod{5} \iff x \equiv 2 \pmod{5} \end{array}\right. \\ x \equiv 32 \pmod{3 \cdot 5^2} \iff \left\{\begin{array}{l} x \equiv 32 \pmod{3} \iff x \equiv 2 \pmod{3} \\ x \equiv 32 \pmod{5^2} \iff x \equiv 7 \pmod{5^2} \end{array}\right. \end{array}\right.$$

De este conjunto de seis congruencias en las que los módulos son potencias de los primos 2, 3 y 5, seleccionamos las que involucran a la *mayor potencia de cada primo* para quedarnos con el sistema

$$x \equiv 2 \pmod{9}, \quad x \equiv 7 \pmod{8}, \quad x \equiv 7 \pmod{25}$$

cuyos módulos son mutuamente primos entre sí, y podemos aplicarle los métodos anteriores, basados en el Teorema Chino de los restos, para encontrar la solución general

$$x \equiv 407 \pmod{1800}$$

□

Al igual que ocurría con la resolución de una congruencia lineal, el método descrito anteriormente para la resolución de un sistema de congruencias es muy útil cuando se resuelve un sistema *a mano* pero no es algoritmizable. Si lo que queremos es un algoritmo que podamos programar en un ordenador nos basamos en la demostración del Teorema 2.13 una vez resuelta cada una de las ecuaciones del sistema. Es decir:

P1 Resolver cada ecuación $a_i x \equiv b_i \pmod{n_i}$ del sistema para convertirlo en uno del tipo $x \equiv a_i \pmod{n_i}$

Si alguna carece de solución el sistema no la tiene.

P2 Comprobar que $\text{mcd}\,(n_i, n_j)$ divide a $a_i - a_j$

Si falla algún caso, el sistema no tiene solución.

P3 Descomponer cada ecuación en un sistema.

P4 Eliminar las ecuaciones que no son necesarias.

P5 Calcular n (producto de los módulos resultantes),

$c_i = n/n_i$ y d_i soluciones de las ecuaciones

$$c_i x \equiv 1 \pmod{n_i}$$

P6 El sistema es equivalente a la congruencia

$$x \equiv \sum_i a_i c_i d_i \pmod{n}$$

Obsérvese que el primer paso (resolver cada una de las ecuaciones) y el cálculo de los d_i se realiza, según se vio en el algoritmo de resolución de congruencias lineales, mediante el Algoritmo Extendido de Euclides.

2.6 El Pequeño Teorema de Fermat

El siguiente resultado se conoce como *Pequeño teorema de Fermat*, aunque también se debe a Leibniz y la primera publicación de su demostración se debe a Euler.

Teorema 2.16 [Pequeño teorema de Fermat] *Si p es primo y $a \perp p$, $a^{p-1} \equiv 1 \pmod{p}$.*

Demostración. Por ser p primo, el conjunto de las unidades de $\mathbf{Z}_p$ resulta ser $U_p = \{1, 2, \ldots, p-1\}$ y dado que $a \perp p$, a posee inverso $a^{-1} \in \mathbf{Z}_p$.

El conjunto $aU_p = \{a, 2a, \ldots, (p-1)a\}$ tiene todos sus elementos diferentes:

$$ai = aj \text{ con } i \neq j \implies a^{-1}ai = a^{-1}aj \implies i = j \implies \textit{contradicción}$$

Además, dado que sus elementos son producto de dos unidades de $\mathbf{Z}_p$ todos son unidades de $\mathbf{Z}_p$ y, por tanto $U_p = aU_p$, por lo que en $\mathbf{Z}_p$

$$1 \cdot 2 \cdots (p-1) = a \cdot 2a \cdots (p-1)a \implies 1 = a^{p-1}$$

Es decir, $a^{p-1} \equiv 1 \pmod{p}$. ■

Corolario 2.17 *Si p es primo, para cualquier entero a se verifica que*

$$a^p \equiv a \pmod{p}.$$

Demostración.

- Si $a \perp p$, el Pequeño teorema de Fermat nos dice que $a^{p-1} \equiv 1 \pmod{p}$, y multiplicando por a se obtiene el resultado, $a^p \equiv a \pmod{p}$.
- Si $a \not\perp p$ entonces $a = \overset{\bullet}{p}$, por lo que $a^p \equiv a \equiv 0 \pmod{p}$. ■

Este resultado nos permite reducir el exponente de a módulo p en el caso de que a no sea primo con p, o lo que es lo mismo, si $a \not\equiv 0 \pmod{p}$.

Ejemplo 2.17 Encontrar el resto de la división de 2^{68} entre 19.

Como 19 es primo y 2 es primo con 19, podemos aplicar el Pequeño teorema de Fermat con $p = 19$ y $a = 2$ por lo que $2^{18} \equiv 1 \pmod{19}$. Dado que $68 = 18 \times 3 + 14$, se tiene

$$2^{68} = (2^{18})^3 \times 2^{14} \equiv 1^3 \times 2^{14} = 2^{14} \pmod{19}.$$

Como $2^4 = 16 \equiv -3 \pmod{19}$, podemos escribir $14 = 4 \times 3 + 2$ y deducir que

$$2^{14} = (2^4)^3 \times 2^2 \equiv (-3)^3 \times 2^2 \equiv -27 \times 4 \equiv -8 \times 4 \equiv -32 \equiv 6 \pmod{19}$$

por lo que el resto de la división es 6. □

Ejemplo 2.18 Vamos a probar que $a^{25} - a$ es divisible entre 30 cualquiera que sea el entero a.

En este caso es más apropiado el Corolario 2.17, ya que incluye a cualquier entero, sin necesidad de que sea primo con p.

Factorizando 30 vemos que es suficiente probar que $a^{25} - a$ es divisible por los primos 2, 3 y 5. Vamos a verlo, en primer lugar para $p = 5$.

Aplicando el Corolario 2.17 dos veces tenemos:

$$a^{25} = (a^5)^5 \equiv a^5 \equiv a \pmod 5$$

por lo que 5 divide a $a^{25} - a$ cualquiera que sea el entero a.

Análogamente, $a^3 \equiv a \pmod 3$, por lo que

$$a^{25} = (a^3)^8 a \equiv a^8 a = a^9 = (a^3)^3 \equiv a^3 \equiv a \pmod 3$$

es decir, 3 divide a $a^{25} - a$ cualquiera que sea el entero a.

Para $p = 2$ un razonamiento más directo es ver que $a^{25} - a$ siempre es par, pero para continuar con el mismo método que en los casos anteriores, podemos usar $a^2 \equiv a \pmod 2$ de donde se deduce (de una forma más laboriosa) que

$$a^{25} = (a^2)^{12} a \equiv a^{12} a = (a^2)^6 a \equiv a^6 a = (a^2)^3 a$$

$$\equiv a^3 a = a^4 = (a^2)^2 \equiv a^2 \equiv a \pmod 2.$$

□

2.7 La función de Euler

Una de las funciones más importantes en teoría de números es la *función de Euler* $\phi(n)$, la cual nos proporciona el número de unidades de $\mathbf{Z}_n$. Veremos cómo evaluar esta función, estudiaremos sus propiedades básicas, y veremos cómo puede aplicarse a varios problemas, tales como el cálculo de grandes potencias y el cifrado de mensajes secretos.

Un importante resultado de este capítulo ha sido el Pequeño Teorema de Fermat: si p es primo, $a^{p-1} \equiv 1 \pmod p$ para cualquier entero a primo con p.

Nos gustaría encontrar un resultado similar para módulos compuestos, pero si reemplazamos p por un entero compuesto n, la congruencia resultante $a^{n-1} \equiv 1 \pmod n$ en general no es cierta.

Si $d = \text{mcd}\,(a, n) > 1$ cualquier potencia positiva de a es divisible por d, por lo que no puede ser congruente con 1 módulo n. Esto nos sugiere que debemos restringirnos a los enteros a que sean primos con n.

Aun entonces, la congruencia puede fallar: por ejemplo, si $n = 4$ y $a = 3$, $a^{n-1} = 27 \not\equiv 1 \pmod 4$.

Necesitamos un exponente diferente $e(n)$ tal que $a^{e(n)} \equiv 1 \pmod n$ para todo entero a primo con n.

La función más sencilla que tiene esta propiedad nos devuelve a la función de Euler $\phi(n)$, objeto de esta sección, y una de las más importantes funciones en teoría de números.

Definición 2.5 [Función de Euler]

Se denomina función de Euler a la función $\phi : \mathbf{N} \to \mathbf{N}$ *que asocia a cada* $n \in \mathbf{N}$ *el número de unidades de* $\mathbf{Z}_n$*, es decir:* $\phi(n) = |U_n|$

La siguiente tabla nos da el valor de la función de Euler para los primeros enteros

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Propiedades de la función de Euler

- $\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1) = p^e\left(1 - \frac{1}{p}\right)$.

  $$\mathbf{Z}_{p^e} = \{1, 2, \ldots, p^e\} \text{ contiene } \frac{p^e}{p} = p^{e-1} \text{ múltiplos de } p$$

  por lo que el resto, $p^e - p^{e-1}$ son primos con p es decir, unidades de $\mathbf{Z}_{p^e}$

  $$\phi(p^e) = |U_{p^e}| = p^e - p^{e-1} = p^{e-1}(p-1) = p^e\left(1 - \frac{1}{p}\right).$$

- $m \perp n \implies \phi(mn) = \phi(m)\phi(n)$.

  Podemos suponer que $m, n > 1$, pues en caso contrario el resultado es

trivial, ya que $\phi(1) = 1$. Coloquemos los mn enteros $1, 2, \ldots, mn$, en una matriz de n filas por m columnas, de la siguiente forma:

$$\begin{array}{llll} 1 & 2 & 3 & \cdots \; m \\ m+1 & m+2 & m+3 & \cdots \; 2m \\ \vdots & \vdots & \vdots & \ddots \; \vdots \\ (n-1)m+1 & (n-1)m+2 & (n-1)m+3 & \cdots \; nm \end{array}$$

Estos enteros i forman un conjunto completo de restos módulo mn, por lo que $\phi(mn)$ representa el número de ellos que son primos con mn, o lo que es lo mismo, los que verifican que mcd $(i, m) =$ mcd $(i, n) = 1$.

Los enteros de una columna dada son todos congruentes módulo m, y las m columnas representan a las m clases de congruencia módulo m; por tanto, exactamente $\phi(m)$ columnas están constituidas por enteros i primos con m y las demás columnas están constituidas por enteros con mcd $(i, m) > 1$.

Cada columna de enteros primos con m tiene la forma $c, m + c, 2m + c, \ldots, (n-1)m + c$ para algún c,; por lo que constituye un conjunto completo de restos módulo n, ya que $A = \{0, 1, 2, \ldots, n-1\}$ lo es y mcd $(m, n) = 1$.

Dicha columna contiene además $\phi(n)$ enteros primos con n, por lo que las $\phi(m)$ columnas contienen $\phi(m)\phi(n)$ enteros i primos con m y con n. Por tanto, $\phi(mn) = \phi(m)\phi(n)$ como queríamos probar.

- $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k} \implies$

$$\phi(n) = \prod_{i=1}^{k} (p_i^{e_i} - p_i^{e_i - 1}) = \prod_{i=1}^{k} p_i^{e_i - 1}(p_i - 1) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Es consecuencia directa de las dos propiedades anteriores.

- $d =$ mcd $(n, m) \implies \phi(mn)\phi(d) = \phi(m)\phi(n)d$.

$$\left.\begin{array}{l} m = p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_s^{\beta_s} \\ n = p_1^{\gamma_1} \cdots p_k^{\gamma_k} r_1^{\delta_1} \cdots r_t^{\delta_t} \end{array}\right\} \implies d = p_1^{\mu_1} \cdots p_k^{\mu_k} \quad \mu_i = \min_{i=1,\ldots,k} (\alpha_i, \gamma_i)$$

$$\phi(m) = m\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)\prod_{j=1}^{s}\left(1-\frac{1}{q_j}\right)$$
$$\phi(n) = n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)\prod_{l=1}^{t}\left(1-\frac{1}{r_l}\right)$$
$$\phi(d) = d\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$$
$$\phi(mn) = mn\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)\prod_{j=1}^{s}\left(1-\frac{1}{q_j}\right)\prod_{l=1}^{t}\left(1-\frac{1}{r_l}\right)$$
$$\phi(mn)\phi(d) = mnd\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)^2\prod_{j=1}^{s}\left(1-\frac{1}{q_j}\right)\prod_{l=1}^{t}\left(1-\frac{1}{r_l}\right)$$
$$\phi(m)\phi(n)d = mnd\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)^2\prod_{j=1}^{s}\left(1-\frac{1}{q_j}\right)\prod_{l=1}^{t}\left(1-\frac{1}{r_l}\right)$$
$$\phi(mn)\phi(d) = \phi(m)\phi(n)d$$

Ejemplo 2.19 $\phi(60) = \phi(2^2\cdot 3\cdot 5) = 60\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 16.$ □

En 1760, Euler probó la siguiente generalización del Pequeño Teorema de Fermat y que se conoce como *teorema de Euler*.

Teorema 2.18 [Teorema de Euler]

Si $a \perp n$ se verifica que $a^{\phi(n)} \equiv 1 \pmod{n}$.

Demostración.

$$\phi(n) = |U_n| \implies U_n = \{u_1, u_2, \ldots, u_{\phi(n)}\}$$

$$aU_n = \{au_1, au_2, \ldots, au_{\phi(n)}\} \text{ posee } \phi(n) \text{ elementos diferentes}$$

ya que al ser $a \perp n \implies a$ posee inverso en $\mathbf{Z}_n \implies$

$$au_i = au_j \text{ con } i \neq j \implies a^{-1}au_i = a^{-1}au_j \implies i = j \text{ } \textit{contradicción}$$

Además, dado que sus elementos son producto de dos unidades de $\mathbf{Z}_n$ todos son unidades de $\mathbf{Z}_n$ y trabajando en $\mathbf{Z}_n$

$$U_n = aU_n \implies u_1\cdot u_2\cdots u_{\phi(n)} = au_1\cdot au_2\cdots au_{\phi(n)} \implies 1 = a^{\phi(n)}$$

es decir, $a^{\phi(n)} \equiv 1 \pmod{n}$. ■

El Pequeño Teorema de Fermat es un caso especial de este resultado: si n es un primo $\phi(n) = n - 1$ y, por tanto, $a^{n-1} \equiv 1 \pmod{n}$.

Ejemplo 2.20 Encontrar el resto de la división de 23^{65} entre 60.

Dado que 23 es primo con 60, el teorema de Euler nos dice que

$$23^{\phi(60)} = 23^{16} \equiv 1 \pmod{60}$$

$$23^{65} = 23^{16 \cdot 4 + 1} = (23^{16})^4 \cdot 23 \equiv 1^4 \cdot 23 = 23 \pmod{60}$$

por lo que el resto buscado es 23. □

2.8 Test de primalidad

Vimos en el Capítulo 1 que una forma de determinar si un entero positivo n es primo consiste en ir probando si es divisible por cada uno de los primos existentes hasta su raíz cuadrada. Vimos también que para un entero n (suficientemente grande) el número de primos $p \leq \sqrt{n}$ viene dado por

$$\pi(\sqrt{n}) \simeq \frac{\sqrt{n}}{\ln(\sqrt{n})} = \frac{2\sqrt{n}}{\ln n}.$$

es decir, para saber si un entero de 14 dígitos es primo haría falta probar si es divisible por los, aproximadamente, 620000 primos anteriores a su raíz cuadrada.

Teniendo en cuenta que pretendemos trabajar con números de una gran cantidad de dígitos se comprende enseguida que el método no es eficiente, por lo que debemos encontrar otros métodos para determinar si un entero n (suficientemente grande) es primo o compuesto.

Los únicos métodos deterministas son el estudiado anteriormente (probar si es divisible por alguno de los primos existentes hasta su raíz cuadrada) que hemos visto que no es eficiente y, por tanto no es aplicable, y el que se conoce como *test de Wilson* que establece el siguiente teorema debido a Wilson pero que fue probado, por primera vez, por Lagrange en 1770.

Teorema 2.19 [Teorema de Wilson]

Un entero positivo p es primo si, y sólo si, $(p-1)! + 1 \equiv 0 \pmod{p}$.

Demostración.

a) Condición suficiente

$$(p-1)!+1 \equiv 0 \pmod{p} \implies p \text{ es primo}$$

Supongamos que p fuese compuesto, es decir, que $p = a \cdot b$ con $a, b \in \mathbf{Z}^+$ y $1 < a, b < p$.

La condición $(p-1)!+1 \equiv 0 \pmod{p}$ equivale a que p divide a $(p-1)!+1$.

$$\left.\begin{array}{l} a \text{ divide a } p \\ \\ p \text{ divide a } (p-1)!+1 \end{array}\right\} \implies a \text{ divide a } (p-1)!+1$$

por $a \leq p-1$, a es uno de los factores de $(p-1)!$ por lo que

$$\left.\begin{array}{l} a \,|\, (p-1)!+1 \\ \\ a \,|\, (p-1)! \end{array}\right\} \implies a \,|\, 1 \implies a = 1$$

pero eso contradice el hecho de que $1 < a < p$, por lo que p no puede ser compuesto y, por tanto, es primo.

b) Condición necesaria

$$\text{Si } p \text{ es primo} \implies (p-1)!+1 \equiv 0 \pmod{p}$$

Los únicos elementos autoinversos de $\mathbf{Z}_p$ son el 1 y el $p-1$ (véase el Teorema 2.6).

Por ser p un número primo impar, todos los elementos no nulos de $\mathbf{Z}_p$ son inversibles y como los únicos elementos que coinciden con su propio inverso son 1 y $p-1$, todos los demás podemos agruparlos por parejas (un elemento y su inverso). De ahí se deduce que

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-2) \cdot (p-1) \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$$

ya que los demás se elementos se han cancelado dos a dos, por lo que $(p-1)!+1 \equiv 0 \pmod{p}$. ■

Ejemplo 2.21 Podemos asegurar que 13 es primo ya que

$$(13-1)!+1 = 12!+1 = 479001601 = 36846277 \cdot 13 \equiv 0 \pmod{13} \qquad \square$$

El test de Wilson no es aplicable ya que el factorial de un entero suficientemente grande requiere tal número de operaciones que cualquier ordenador superaría, en tiempo, a la edad del Universo.

Nos encontramos, por tanto, que *no existe ningún método determinista que pueda realizarse de manera efectiva*.

Todos los métodos que se aplican en la práctica son métodos probabilísticos, es decir, métodos que no nos pueden asegurar que un entero n sea primo aunque sí pueden garantizarnos una probabilidad alta de que lo sea.

Todos los test que veremos a continuación si detectan que n es compuesto, nos garantizan que lo es, y sólo cuando no pueden detectar si es compuesto nos dirán que *posiblemente* pueda ser primo, aunque con una probabilidad alta. Esa probabilidad depende del test que estemos aplicando.

2.9 Pseudoprimalidad

En teoría, el Teorema de Wilson resuelve el problema del test de primalidad considerado en el Capítulo 1. Sin embargo, la dificultad de computar factoriales hace que el test sea muy ineficaz, incluso para enteros pequeños. En muchos casos podemos mejorarlo utilizando contrarrecíproco del corolario del pequeño teorema de Fermat. Este test resulta mucho más fácil de aplicar, ya que en aritmética modular, las grandes potencias pueden calcularse mucho más fácilmente que los factoriales, como pronto probaremos. Esto es, particularmente cierto, cuando se dispone de un ordenador o, simplemente, de una calculadora. Aunque nos limitaremos a ver ejemplos con enteros pequeños que pueden tratarse a mano, resulta un buen ejercicio escribir programas que extiendan las técnicas a enteros mucho mayores.

2.9.1 Test de pseudoprimalidad de Fermat

Proposición 2.20 [Test de pseudoprimalidad de Fermat]

Sea n un entero positivo. Si existe un entero a para el que $a^n \not\equiv a \pmod{n}$, podemos asegurar que n es compuesto.

Demostración. Si n fuese primo, el corolario del pequeño teorema de Fermat nos garantizaría que $a^n \equiv a \pmod{n}$, por lo que n no puede ser primo. ■

Los chinos utilizaban este test para $a = 2$ y conjeturaron hace 25 siglos que el recíproco también era cierto, se decir, que si n superaba el test para $a = 2$, entonces n era considerado primo. Esto resultó ser falso, pero hasta 1819 no se encontró un contraejemplo: existen números n que siendo compuestos verifican $2^n \equiv 2 \pmod{n}$, es decir, que superan el test de pseudoprimalidad de Fermat para la base 2 y sin embargo no son primos. A dichos enteros los denominamos *pseudoprimos*: parecen que son primos, pero de hecho son compuestos.

Definición 2.6 [Pseudoprimos]

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

Ejemplo 2.22 El número $341 = 11 \cdot 31$ es compuesto. Sin embargo, al ser compuesto y verificar que $2^{341} \equiv 2 \pmod{341}$, resulta ser un pseudoprimo para la base 2. □

Si el número de pseudoprimos para una determinada base a *fuese finito* bastaría aplicar el test de pseudoprimalidad de Fermat en dicha base a un determinado entero n para decidir:

- Si $a^n \not\equiv a \pmod{n}$ el número es compuesto.
- Si $a^n \equiv a \pmod{n}$ el número o es compuesto o es pseudoprimo para dicha base. Mirando si figura en la lista de los pseudoprimos para dicha base podríamos decidir si se trata de un primo o de un número compuesto.

Desgraciadamente, esto no es posible ya que:

Teorema 2.21 *Existen infinitos pseudoprimos para cualquier base a.*

Demostración. Haremos la demostración para la base 2.

Vamos a probar que si n es pseudoprimo para la base 2, $2^n - 1$ también lo

es. Como $2^n - 1 > n$, partiendo de $n = 341$ podremos entonces generar una sucesión infinita de pseudoprimos para dicha base.

Si n es pseudoprimo, es compuesto, $n = rs$ con $1 < r, s < n$ y dado que

$$(x-1) \,|\, (x^s - 1) \implies (2^r - 1) \,|\, ((2^r)^s - 1) = 2^n - 1 \;\text{ con }\; 2^r - 1 > 1$$

$2^n - 1$ también es compuesto.

Debemos probar ahora que $2^{2^n-1} \equiv 2 \pmod{2^n - 1}$.

Como n es pseudoprimo para la base 2

$$2^n \equiv 2 \pmod{n} \implies 2^n = nk + 2 \;\text{ para algún entero }\; k \geq 1$$

Dado que $(2^n - 1) \,|\, ((2^n)^k - 1) = 2^{nk} - 1$, se obtiene que

$$2^{nk} \equiv 1 \pmod{2^n - 1} \iff 2^{nk+1} \equiv 2 \pmod{2^n - 1}$$

Teniendo en cuenta que $nk + 1 = 2^n - 1$

$$2^{2^n-1} \equiv 2 \pmod{2^n - 1}$$

por lo que 2^{2^n-1} es pseudoprimo para la base 2. ■

Otra posible estrategia cuando $a^n \equiv a \pmod{n}$ es cambiar de base.

Ejemplo 2.23

- $2^{341} \equiv 2 \pmod{341}$. No sabemos si 341 es primo o pseudoprimo para la base 2. Es decir, no sabemos si es primo o compuesto.
- $3^{341} \equiv 168 \neq 3 \pmod{341}$. Podemos asegurar que es compuesto. □

Obsérvese que si n supera el test para bases a y b (posiblemente iguales)

$$\left.\begin{array}{l} a^n \equiv a \pmod{n} \\ b^n \equiv b \pmod{n} \end{array}\right\} \implies (ab)^n \equiv ab \pmod{n}$$

es decir, también supera el test para la base ab, no aportando nada nuevo la aplicación de este test, por lo que parece sensato restringir los valores de las bases a los sucesivos números primos.

Al estudiar el test de Wilson, dijimos que no era aplicable ya que el cálculo de $(n-1)!$ requiere, para valores grandes de n un número de operaciones que

en un ordenador puede superar la edad del Universo. Así para un número de 100 dígitos $n \approx 10^{100}$ se deberían realizar 10^{100} productos y un ordenador que realizase un billón de operaciones por segundo requeriría aproximadamente $3 \cdot 10^{78}$ siglos en realizarlos.

Al aplicar el test de pseudoprimalidad de Fermat es necesario calcular a^n por lo que multiplicando a por a sucesivamente serían necesarias $n-1$ operaciones, las mismas que requiere el cálculo de $(n-1)!$ Por lo que nuestro ordenador tardaría $3 \cdot 10^{78}$ siglos en realizar los cálculos cuando n es un número de 100 dígitos.

Veamos cómo puede reducirse el número de operaciones en el cálculo de grandes potencias.

Algoritmo de cálculo de grandes potencias

Supongamos que queremos calcular a^n. Por ejemplo n^{19}.

- Expresamos n en notación binaria. $19 \to 10011$.
- Intercalamos una C entre cada dos cifras. $1C0C0C1C1$.
- Eliminamos los ceros. $1CCC1C1$.
- Sustituimos los unos por la letra M. $MCCCMCM$.

Comenzando ahora por 1 y siguiendo la secuencia obtenida en la que M representa multiplicar por n y C elevar al cuadrado vamos obteniendo:

$$1 \xrightarrow{\text{M}} a \xrightarrow{\text{C}} a^2 \xrightarrow{\text{C}} a^4 \xrightarrow{\text{C}} a^8 \xrightarrow{\text{M}} a^9 \xrightarrow{\text{C}} a^{18} \xrightarrow{\text{M}} a^{19}$$

Este algoritmo nos asegura que, para cualquier entero positivo n, el número de multiplicaciones que requiere el cálculo de a^n es, como máximo, el doble del número de dígitos de la expresión binaria de n, es decir, como máximo $2 \cdot (1 + \lfloor \log_2 n \rfloor)$.

Para un número de 100 dígitos $n \approx 10^{100}$ habría que hacer, en el peor de los casos

$$2 \cdot (1 + \lfloor \log_2 10^{100} \rfloor) = 666$$

operaciones y nuestro ordenador que realiza un billón de operaciones por segundo tardaría menos de una milmillonésima de segundo en realizarlas, frente a los $3 \cdot 10^{78}$ siglos que tardaría multiplicando a por a sucesivamente.

Podemos por tanto asegurar que el test de pseudoprimalidad de Fermat es fácilmente aplicable.

Hemos visto que si para una determinada base el test no puede asegurarnos si nuestro número es primo o compuesto, podemos cambiar de base. Así, por ejemplo, si la base 2 no nos determina cómo es el número, cambiamos a la base 3 y así sucesivamente (utilizando siempre números primos como base).

Es evidente que al aumentar el número de bases para las que $a^n \equiv a \pmod{n}$ mayor probabilidad tendremos de que nuestro número n sea primo.

¿Sería una buena estrategia seguir probando bases hasta encontrar alguna en la que, si el número es compuesto, se detecte como compuesto?

La respuesta evidentemente es que no.

Definición 2.7 [Números de Carmichael]

Se denominan números de Carmichael a aquellos números que siendo compuestos superan los test de pseudoprimalidad de Fermat cualquiera que sea la base que se tome.

$$n \text{ de Carmichael} \iff \begin{cases} n \text{ compuesto} \\ a^n \equiv a \pmod{n} \quad \forall\, a \in \mathbf{Z}^+ \end{cases}$$

Los números de Carmichael se dan con mucha menor frecuencia que los primos aunque no son difíciles de construir.

En 1912, Carmichael conjeturó que *existen infinitos*, y fue probado en 1992 por Alford, Granville y Pomerance.

Teorema 2.22 [Caracterización de los números de Carmichael]

Un número compuesto n es de Carmichael si, y sólo si, es libre de cuadrados (un producto de primos distintos) y $p-1$ divide a $n-1$ para cada primo p que divide a n.

Ejemplo 2.24 $561 = 3 \cdot 11 \cdot 17$ es compuesto y libre de cuadrados y además

$$\begin{cases} 3-1= \ 2 \,|\, (561-1) = 560 \\ 11-1 = 10 \,|\, (561-1) = 560 \\ 17-1 = 16 \,|\, (561-1) = 560 \end{cases}$$

por lo que se trata de un número de Carmichael. □

Ejemplo 2.25 Encontrar todos los números de Carmichael de la forma $7 \cdot 13 \cdot p$ donde p sea un primo mayor que 13.

Al ser $p > 13$ sabemos que el número $n = 7 \cdot 13 \cdot p$ es libre de cuadrados.

La otra condición que debe cumplir es que 6, 12 y $p-1$ dividan a $n-1$ es decir:

$$n = 7 \cdot 13 \cdot p \equiv 1 \pmod 6 \qquad \Rightarrow p \equiv 1 \pmod 6$$

$$n = 7 \cdot 13 \cdot p \equiv 1 \pmod{12} \qquad \Rightarrow p \equiv 7 \pmod{12}$$

$$n = 7 \cdot 13 \cdot p \equiv 1 \pmod{(p-1)} \Rightarrow 90 \equiv 0 \pmod{(p-1)} \ \Rightarrow \ (p-1) \,|\, 90$$

Como los divisores de 90 son 1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45 y 90, los posible valores de p son 2, 3, 4, 6, 7, 10, 11, 16, 19, 31, 46 y 91.

Al tratarse de un número primo mayor que 13 sólo nos quedan dos posibilidades o 19 o 31 y dado que ambas verifican las condiciones

$$p \equiv 1 \pmod 6 \quad \text{y} \quad p \equiv 7 \pmod{12}$$

ambas son válidas, por lo que existen dos números de Carmichael con dichas características:

$$7 \cdot 13 \cdot 19 = 1729 \quad \text{y} \quad 7 \cdot 13 \cdot 31 = 2821$$ □

Para tratar de evitar los números de Carmichael al aplicar el test de pseudoprimalidad de Fermat, realizamos el siguiente proceso:

Test de pseudoprimalidad de Fermat

Elegimos al azar una base a del rango $\{2, 3, \ldots, n-1\}$, resultando:

- Si mcd $(a, n) = d > 1$, como d divide a n sabemos que n es compuesto.
- Si mcd $(a, n) = 1$ y $a^{n-1} \not\equiv 1 \pmod{n} \implies n$ es compuesto.

  Obsérvese que al ser $a \perp n$ podemos hacer uso del teorema de Fermat en vez de su corolario.
- Si mcd $(a, n) = 1$ y $a^{n-1} \equiv 1 \pmod{n}$ nos quedaremos con la duda de si se trata de un primo o de un pseudoprimo para la base a.

```
1   Escoger, aleatoriamente una base a ∈ {2, ..., n − 1}

2   Calcular el mcd (a, n)

    Si mcd (a, n) > 1, devolver compuesto

      si no, si a^{n−1} ≢ 1 (mod n), devolver compuesto

        si no, devolver posible primo
```

Obsérvese que al tomar $a \in \{2, \ldots, n-1\}$ existen $n - \phi(n) - 1$ posibilidades de que mcd $(a, n) > 1$ en cuyo caso sabemos que el número n es compuesto y sólo $\phi(n) - 1$ casos en los que mcd $(a, n) = 1$ y sería necesario aplicar realmente el test de pseudoprimalidad, por lo que existen muchas posibilidades de que aun siendo n un número de Carmichael, el test detecte que se trata de un número compuesto.

2.9.2 Test de pseudoprimalidad fuerte

Vamos a ver a continuación un test de pseudoprimalidad, basado en el anterior que trata de evitar los números de Carmichael y reduce a la mitad el número de pseudoprimos para cada base.

Teorema 2.23 [Teorema de Miller-Rabin]

Sea n un número primo impar y escribámoslo de la forma $n = 1 + 2^s \cdot d$ con d impar. La sucesión de Miller-Rabin

$$a^d,\ a^{2d},\ a^{4d}, \ldots,\ a^{2^{s-1}d},\ a^{2^s d} \pmod{n}$$

para cualquier $a \perp n$ finaliza con un 1; además, si $a^d \not\equiv 1 \pmod{n}$ el valor inmediatamente anterior a la primera aparición de un 1 es $n - 1$.

Demostración. La propiedad puede ser reformulada como sigue:

Si n es primo y $n-1 = s^s \cdot d$, la sucesión de Miller-Rabin adopta una de las siguientes formas

$$(1, 1, \ldots, 1) \quad 0 \quad (*, *, \ldots, n-1, 1, \ldots, 1)$$

para cualquier entero $a \perp n$ tal que $1 < a < n$.

Por el teorema de Fermat $a^{2^s d} = a^{n-1} \equiv 1 \pmod{n}$ y, por tanto, la sucesión termina en 1.

$$\left.\begin{array}{c} n \text{ primo} \\ a^{2^s d} = (a^{2^{s-1} d})^2 \equiv 1 \pmod{n} \end{array}\right\} \implies a^{2^{s-1} d} \equiv \pm 1 \pmod{n} \text{ (Teorema 2.6)}$$

es decir, $a^{2^{s-1} d}$ vale 1 o $n-1$, por lo que el término anterior a la aparición de un 1 es $n-1$. ■

Si n es *compuesto* pero cumple las características del Teorema de Miller-Rabin se dice que es un *fuerte pseudoprimo para la base a*. Si n es primo o fuerte pseudoprimo (pero no podemos asegurar cuál de las dos cosas es) diremos que es *probablemente primo*.

Test de pseudoprimalidad fuerte

Sea $n - 1 = 2^s \cdot d$ con d impar y s no negativo, n es probablemente primo si $a^d \equiv 1 \pmod{n}$ o $(a^d)^{2^r} \equiv 1 \pmod{n}$ para algún entero no negativo $r \leq s$. En caso contrario es compuesto.

Proposición 2.24 *Supongamos que testamos un entero impar n para k bases aleatorias. Si n es primo el resultado de los test es siempre correcto. Si n es compuesto, la probabilidad de que n supere los k test es, a lo sumo, $1/4^k$.*

Obsérvese que, probando 100 bases diferentes, la probabilidad de que demos por primo a un número que no lo es, es decir, que el test nos de una respuesta incorrecta, es menor que 10^{-60} siendo superior la probabilidad de que el ordenador produzca errores en el proceso de aplicación del test para esas 100 bases.

Ejemplo 2.26 Sabemos que 561 es pseudoprimo para cualquier base, ya que se trata del menor número de Carmichael, por lo que el test de pseudoprimalidad de Fermat no podría detectar si es primo o compuesto.

Si aplicamos el algoritmo de Miller-Rabin para la base 2 obtenemos que

$$561 - 1 = 560 = 2^4 \cdot 35 \implies s = 4 \quad \text{y} \quad d = 35.$$

$$a_0 = 2^{35} \bmod 561 = 263$$
$$a_1 = 263^2 \bmod 561 = 166$$
$$a_2 = 166^2 \bmod 561 = 67$$
$$a_3 = 67^2 \bmod 561 = 1$$

por lo que al ser $a_3 = 1$ y $a_2 \neq 560$ sabemos que n es compuesto. □

El algoritmo tendría como entrada un entero positivo impar n y vendría dado por:

1 Escoger, aleatoriamente una base $a \in \{2, \ldots, n-1\}$

2 Si $\text{mcd}\,(a, n) \neq 1$ devolver **compuesto**.

3 Si no, factorizar $n - 1 = 2^s \cdot d$ con d impar y $s \geq 1$

4 Calcular

$$a_0 = a^d \bmod n, \quad a_1 = a_0^2 \bmod n, \ldots, \quad a_k = a_{k-1}^2 \bmod n$$

hasta que $k = s$ o bien $a_k = 1$.

5 Si $k = s$ y $a_k \neq 1$ devolver **compuesto**.

si no, si $k = 0$ devolver **primo**.

si no, si $a_{k-1} \neq n - 1$ devolver **compuesto**.

si no, devolver **primo**.

Ejemplo 2.27 Sea $n = 9585921133193329$. Entonces

$$n-1 = 9585921133193328 = 2^4 \cdot 599120070824583 \Rightarrow \begin{cases} s = 4 \\ d = 599120070824583 \end{cases}$$

La sucesión de Miller-Rabin para $a = 3$ (primo con 9585921133193329) es

$$a_0 = 3^{599120070824583} \bmod 9585921133193329 = 423408699973621$$

$$a_1 = 423408699973621^2 \bmod 9585921133193329 = 3197354815636220$$

$$a_2 = 3197354815636220^2 \bmod 9585921133193329 = 1$$

por lo que $k = 2 \neq s$ y dado que $k \neq 0$ y $a_1 \neq 9585921133193328$ el algoritmo habría detectado que se trata de un número compuesto (a pesar de tratarse de un número de Carmichael no detectable mediante el algoritmo de pseudoprimalidad de Fermat). □

2.9.3 Test de primalidad de Lucas

El test de primalidad de Lucas es el más complejo de los que describiremos.

Consideremos la ecuación cuadrática $x^2 - ax + b = 0$. Si denotamos por $D = a^2 - 4b$ a su discriminante y por α y β a sus raíces, se tiene que

$$\alpha = (a + \sqrt{D})/2 \quad \text{y} \quad \beta = (a - \sqrt{D})/2$$

y podemos obtener las siguientes relaciones entre a, b, D, α y β:

$$\alpha + \beta = a, \quad \alpha - \beta = \sqrt{D} \quad \alpha\beta = b$$

Usando estas relaciones donde a, b y D son enteros no negativos. Para cada $k \geq 0$ llamamos

$$U_k(a, b) = \frac{\alpha^k - \beta^k}{\alpha - \beta} \quad k \geq 0$$

Definición 2.8 Sucesión de Lucas

Definimos la sucesión de Lucas $U(a, b)$ *con* $a, b, D \in \mathbf{Z}^+ \cup \{0\}$ *como*

$$U(a, b) = (U_0(a, b), U_1(a, b), U_2(a, b), \ldots) \quad \textit{con} \quad U_k(a, b) = \frac{\alpha^k - \beta^k}{\alpha - \beta} \quad k \geq 0$$

La sucesión de Lucas pueden ser definida de forma recursiva mediante

$$U_0 = 1 \quad U_1 = a \quad U_k(a, b) = aU_{k-1}(a, b) - bU_{k-2}(a, b) \quad \forall\, k \geq 2$$

Podemos aplicar ahora la sucesión de Lucas a los test de primalidad. La idea básica es reemplazar en los test de pseudoprimalidad fuerte a^{n-1} por la sucesión de Lucas.

Definición 2.9 Símbolos de Jacobi

Se definen los símbolos de Jacobi $\left(\frac{a}{n}\right)$ *como*

- *Para un primo* p

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & si\ p \mid a \\ 1 & si\ a \perp p \ \ y \ \ x^2 \equiv a \pmod{p}\ admite\ solución \\ -1 & si\ a \perp p \ \ y \ \ x^2 \equiv a \pmod{p}\ no\ admite\ solución \end{cases}$$

- *Para un número compuesto* $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}$$

Sin embargo, no es necesario factorizar n para calcular $\left(\frac{a}{n}\right)$ ya que los símbolos de Jacobi poseen las siguientes propiedades:

Teorema 2.25 [Propiedades de los símbolos de Jacobi]

1. $\left(\frac{a}{n}\right) \in \{-1, 0, 1\} \quad con \quad \left(\frac{a}{n}\right) = 0 \iff \text{mcd}\,(a, n) \neq 1.$

2. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right) \quad y \quad \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \cdot \left(\frac{a}{n}\right)$

3. *Si* $a \equiv b \pmod{n}$ *entonces* $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$

4. $\left(\frac{1}{n}\right) = 1 \quad y \quad \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = \begin{cases} 1 & si\ n \equiv 1 \pmod{4} \\ -1 & si\ n \equiv 3 \pmod{4} \end{cases}$

5. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} 1 & si\ n \equiv \pm 1 \pmod{8} \\ -1 & si\ n \equiv \pm 3 \pmod{8} \end{cases}$

6. $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}}$

Ejemplo 2.28

$$\begin{aligned}\left(\frac{13}{561}\right) &= \left(\frac{561}{13}\right) && \text{por } 6 \\ &= \left(\frac{2}{13}\right) && \text{por } 3 \quad \text{ya que } 561 \equiv 2 \pmod{13} \\ &= -1 && \text{por } 5 \quad \text{ya que } 13 \equiv -3 \pmod{8}\end{aligned}$$

□

Teorema 2.26 [Teorema de Lucas]

Sean a, b, D, y U_k las descritas anteriormente.
Si p es un primo impar, $\text{mcd}\,(b,p) = 1$ *y* $\left(\frac{D}{p}\right) = -1$, *entonces* $p \,|\, U_{p+1}$.

El contrarrecíproco nos lleva al test de Lucas.

Teorema 2.27 [Test de Lucas]

Sea n un entero positivo impar y sean a, b y D las descritas anteriormente tales que $\text{mcd}\,(b,n) = 1$ *y* $\left(\frac{D}{n}\right) = -1$. *Si n no divide a U_{n+1} es compuesto.*

Ejemplo 2.29

$$\text{Sea} \quad n = 561 \quad \text{y tomemos} \quad \begin{cases} \alpha = 14 \\ \beta = 1 \end{cases} \implies \begin{cases} a = \alpha + \beta = 15 \\ b = \alpha\beta = 14 \\ D = \alpha - \beta = 13 \end{cases}$$

Se verifica entonces que

$$\text{mcd}\,(b,n) = \text{mcd}\,(13, 561) = 1 \quad \text{y} \quad \left(\frac{D}{n}\right) = \left(\frac{13}{561}\right) = -1$$

Así pues, si 561 no divide a U_{562} es decir, si $U_{562} \not\equiv 0 \pmod{561}$, es compuesto.

$$U_{562} = \frac{14^{562} - 1^{562}}{14 - 1} = \frac{14^{562} - 1}{13}$$

$$U_{562} \bmod 561 = (14^{562} \bmod 561 - 1)(13^{-1} \bmod 561) = 195 \cdot 259 \bmod 561 =$$

$$= 15 \neq 0$$

y, por tanto, el número es compuesto. □

CONJETURA

Sea n un entero impar mayor que 1. Si n supera un test de pseudoprimalidad fuerte y el test de Lucas, entonces es primo.

La conjetura anterior es utilizada por Maple V (versión 3 y posteriores) en su función ISPRIME utilizada para detectar si un entero es primo. Sin embargo el test sólo sería exacto si la conjetura anterior fuese cierta. En cualquier caso, sólo podemos garantizar lo siguiente:

Proposición 2.28 *Para cualquier entero positivo elegido al azar, la función* ISPRIME *de* Maple *determina si n es verdaderamente primo con una probabilidad de error inferior a 10^{-15}.*

2.10 Test de Lucas-Lehmer

Para la obtención de números primos muy grandes se utilizan los números de Mersenne ($M_p = 2^p - 1$ con p primo). El siguiente algoritmo nos proporciona un test *determinista* de primalidad eficiente para los números de Mersenne.

Teorema 2.29 *Sea p un primo impar y consideremos la sucesión*

$$S_1 = 4 \quad S_2 \equiv S_1^2 - 2 \bmod M_p \quad \cdots \quad S_{p-1} \equiv S_{p-2}^2 - 2 \bmod M_p.$$

Se verifica entonces que el número de Mersenne M_p es primo si, y sólo si, $S_{p-1} \equiv 0 \pmod{M_p}$.

Ejemplo 2.30 El número de Mersenne $M_7 = 2^7 - 1 = 127$ es primo ya que

$$\begin{aligned}
S_1 &= 4 \\
S_2 &= 4^2 - 2 = 14 \equiv 14 \bmod 127 \\
S_3 &= 14^2 - 2 = 194 \equiv 67 \bmod 127 \\
S_4 &= 67^2 - 2 = 4487 \equiv 42 \bmod 127 \\
S_5 &= 42^2 - 2 = 1762 \equiv 111 \equiv -16 \bmod 127 \\
S_6 &= (-16)^2 - 2 = 254 \equiv 0 \bmod 127
\end{aligned}$$

□

Este test, que resulta en apariencia demasiado largo de realizar (no olvidemos que estamos tratando de encontrar primos muy grandes) es ideal para ordenadores, ya que las congruencias se realizan módulo $2^p - 1$ que en binario son muy fáciles de obtener. Además se ha refinado computacionalmente con el uso de Transformadas Rápidas de Fourier para multiplicar a gran velocidad.

El soporte informático para dichos cálculos fue coordinado por el programa **GIMPS** (Great Internet Mersenne Prime Search), que desde su fundación en 1996 ha obtenido todos los años el "Oscar al mayor número primo" y es mediante el test de Lucas-Lehmer como se probó que $M_{43112609}$ es primo (el mayor número primo conocido con 12.978.189 dígitos).

2.11 Aplicaciones

2.11.1 Dígitos de control

Una de las aplicaciones de la aritmética modular más utilizada en la actualidad es la de los *dígitos de control*.

Número de identificación fiscal: NIF

Es de todos conocido que el NIF (Número de Identificación Fiscal) consiste en el número del DNI (Documento Nacional de Identidad) seguido de una letra que permite conocer si se han cometido errores a la hora de transcribir el número del DNI.

Dicha letra se obtiene reduciendo número del DNI módulo 23 y aplicando al resultado la siguiente tabla

$0 \longrightarrow$ T	$6 \longrightarrow$ Y	$12 \longrightarrow$ N	$18 \longrightarrow$ H
$1 \longrightarrow$ R	$7 \longrightarrow$ F	$13 \longrightarrow$ J	$19 \longrightarrow$ L
$2 \longrightarrow$ W	$8 \longrightarrow$ P	$14 \longrightarrow$ Z	$20 \longrightarrow$ C
$3 \longrightarrow$ A	$9 \longrightarrow$ D	$15 \longrightarrow$ S	$21 \longrightarrow$ K
$4 \longrightarrow$ G	$10 \longrightarrow$ X	$16 \longrightarrow$ Q	$22 \longrightarrow$ E
$5 \longrightarrow$ M	$11 \longrightarrow$ B	$17 \longrightarrow$ V	

Si al transcribir el número del DNI se produce uno de los errores más frecuentes, como puede ser el intercambio de dos dígitos consecutivos (en vez de escribir

28456790V se escribe 28546790V) el resto de sus divisiones entre 23 varía (en el primer caso es 17 que se corresponde con la letra V, pero en el segundo caso el resto es 18 que correspondería a la H), por lo que la letra añadida detecta que ha habido un error en la transcripción.

Otro de los errores más frecuentes es que en la transmisión de los datos se pierda uno de los dígitos. Así, por ejemplo, puede ocurrir que sólo se reciba 28-56790V habiéndose perdido el tercer dígito del DNI. Dado que conocemos que su letra es la V, que se corresponde con 17, sabemos que

$$28000000 + 100000x + 56790 \equiv 17 \pmod{23} \iff 19x \equiv 7 \pmod{23}$$

y resolviendo la congruencia obtenemos que $x = 4$, por lo que el NIF completo es 28456790V, es decir, podemos recuperar el número perdido.

International Standard Book Number: ISBN

El ISBN (International Standard Book Number) es un número de 10 cifras que identifica, de forma única, cualquier libro editado en el mundo. Un organismo internacional (`www.isbn.org`) marca las directrices de este número.

Los diez dígitos están repartidos en cuatro bloques:

a) El primero es un indicativo geográfico. A España le corresponde el 84.

b) El segundo bloque corresponde a la editorial.

c) El tercer bloque corresponde al libro (dentro de la editorial).

d) El último bloque (un dígito) lo constituye un dígito de control que se calcula de la siguiente forma:

   Si el ISBN es $x_1x_2 - x_3x_4x_5x_6 - x_7x_8x_9 - x_{10}$, entonces

   $$x_{10} = x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9 \bmod 11$$

   (si el resultado fuese 10 el dígito de control se sustituye por la letra "X".

   En otras palabras: $x_{10} = \sum_{i=1}^{9} i \cdot x_i \bmod 11$

Así, por ejemplo, el ISBN 84-316-3311-5 corresponde al libro de Matemática Discreta de N.L.Biggs (3311) publicado en España (84), por la editorial Vicens

Vives (316). Su dígito de control viene dado por

$$8 + 2 \cdot 4 + 3 \cdot 3 + 4 \cdot 1 + 5 \cdot 6 + 6 \cdot 3 + 7 \cdot 3 + 8 \cdot 1 + 9 \cdot 1 \bmod 11 = 5.$$

Al igual que ocurre con la letra del NIF, el dígito de control nos permite detectar errores y recuperar un dígito que se haya perdido en una transmisión si se conoce en qué posición se encuentra el dígito perdido.

Número de cuenta corriente

El número de una cuenta corriente consta de 20 dígitos distribuidos de la siguiente forma:

$$\overbrace{1234}^{Entidad} -- \overbrace{5678}^{Oficina} -- \underbrace{00}_{Dígitos\ de\ control} -- \overbrace{0123456789}^{N^{\underline{o}}\ de\ cuenta}$$

Los dos dígitos de control vigilan de forma independiente las dos partes del número; el primer dígito controla la entidad y la oficina, mientras que el segundo controla el número de la cuenta. Dichos dígitos se calculan de la siguiente forma:

a) Si la entidad y la oficina vienen determinadas por ABCD-EFGH el primer dígito de control viene dado por

$$7A + 3B + 6C + 1D + 2E + 4F + 8G + 5H \bmod 11$$

con el supuesto de que si el resultado fuese 10, ponemos un 1.

b) El segundo dígito controla el número de cuenta ABCDEFGHIJ y viene determinado por

$$10A + 9B + 7C + 3D + 6E + 1F + 2G + 4H + 8I + 5J \bmod 11$$

y también pondremos un 1 si el resultado es 10.

2.11.2 Criptografía

Vamos a cerrar este capítulo con algunas aplicaciones de la teoría de números a la criptografía. Los códigos secretos han sido utilizados desde la antigüedad para enviar mensajes seguros, por ejemplo en tiempo de guerra o de tensiones

diplomáticas. Hoy día se guarda, con frecuencia, información delicada de naturaleza médica o financiera en los ordenadores, y es importante mantenerla en secreto.

Numeramos las letras del alfabeto (en la práctica, los 256 códigos ASCII)

$$\begin{array}{lllllll} \sqcup = 00 & A = 01 & B = 02 & C = 03 & D = 04 & E = 05 & F = 06 \\ G = 07 & H = 08 & I = 09 & J = 10 & K = 11 & L = 12 & M = 13 \\ N = 14 & \tilde{N} = 15 & O = 16 & P = 17 & Q = 18 & R = 19 & S = 20 \\ T = 21 & U = 22 & V = 23 & W = 24 & X = 25 & Y = 26 & Z = 27 \end{array}$$

Criptografía simétrica

La criptografía simétrica la constituyen los códigos criptográficos que utilizan la misma clave para cifrar y descifrar.

Un ejemplo muy simple de criptografía simétrica es el conocido como *código de Cesar* que consiste en sumar módulo 28 una cantidad fija al número correspondiente a cada letra. Julio Cesar utilizaba la clave $k = 3$. Para descifrar debemos realizar, simplemente, la transformación inversa, restar $k \pmod{28}$.

Ejemplo 2.31 Para cifrar el texto JULIO CESAR convertimos el texto en cifras

$$\text{JULIO CESAR} \implies 10 - 22 - 12 - 9 - 16 - 0 - 3 - 5 - 20 - 1 - 19$$

sumamos 3 (si utilizamos la clave de Cesar) a cada número y obtenemos

$$13 - 25 - 15 - 12 - 19 - 3 - 6 - 8 - 23 - 4 - 22 \implies \text{MXÑLRCFHVDU}$$

Para descifrarlo, volvemos a convertirlo en cifras

$$\text{MXÑLRCFHVDU} \implies 13 - 25 - 15 - 12 - 19 - 3 - 6 - 8 - 23 - 4 - 22$$

le restamos 3 a cada número y obtenemos

$$10 - 22 - 12 - 9 - 16 - 0 - 3 - 5 - 20 - 1 - 19 \implies \text{JULIO CESAR}$$ □

Códigos lineales

Estos códigos generalizan a los de Cesar. En vez de sumar una cantidad fija a cada número lo que realizan es la trasformación lineal

$$n \ \rightarrow \ c = an + b \bmod 28$$

donde el par (a, b) recibe el nombre de *clave* del código.

Para descifrar se aplica la transformación inversa

$$c \ \rightarrow \ n = a^{-1}(c - b) \bmod 28$$

por lo que hay que tener en cuenta que a debe tener inverso en $\mathbf{Z}_{28}$, es decir, ha de ser primo con 28.

Así pues, para nuestro alfabeto y dado que el número de elementos invertibles (unidades) de $\mathbf{Z}_{28}$ viene dado por $\phi(28) = 12$, existirán $12 \cdot 28 = 336$ claves válidas.

Estos códigos son fáciles de romper. Podemos probar todas las claves válidas hasta obtener un mensaje comprensible.

Ejemplo 2.32 Utilizando la clave $(3, 1)$ obtendríamos:

$$\text{JULIO CESAR} \implies 10 - 22 - 12 - 9 - 16 - 0 - 3 - 5 - 20 - 1 - 19$$

Realizando la transformación

$$n \ \rightarrow \ c = 3n + 1 \bmod 28$$

obtenemos

$$3 - 11 - 9 - 0 - 21 - 1 - 10 - 16 - 5 - 4 - 2 \implies \text{CKI TAJOEDB}$$

Para descifrar, realizamos el proceso inverso:

$$\text{CKI TAJOEDB} \implies 3 - 11 - 9 - 0 - 21 - 1 - 10 - 16 - 5 - 4 - 2$$

Realizamos la transformación

$$c \ \rightarrow \ n = 3^{-1}(c - 1) \bmod 28 = 19(c - 1) \bmod 28$$

para obtener

$$10 - 22 - 12 - 9 - 16 - 0 - 3 - 5 - 20 - 1 - 19 \implies \text{JULIO CESAR} \ \square$$

El principal problema de los códigos simétricos es que para descifrar es necesario conocer la clave con la que se ha cifrado (ya que se utiliza la misma), por lo que *hay que enviar la clave* y puede ser interceptada al igual que el mensaje.

Criptografía asimétrica

La criptografía asimétrica la constituyen los códigos criptográficos que utilizan claves diferentes para cifrar y descifrar.

Esto nos permite que la clave que se usa para cifrar pueda ser *pública* siempre que la clave para descifrar sea *privada*, es decir, conocida *únicamente por el destinatario*, ni siquiera por el *remitente*.

Códigos de clave pública: RSA

Este método fue desarrollado en 1978 por R.L. Rivest, A. Shamir y L. Adleman y es conocido como *sistema criptográfico RSA* (iniciales de sus autores).

Para cifrar un mensaje con un código RSA se reagrupa el texto en bloques de igual longitud, es decir, en grupos de r letras cada uno.

Así, por ejemplo, si el texto es $HOLA\ A\ TODOS$ y elegimos $r = 4$ quedará reagrupado de la forma

$$HOLA - {\sqcup}A{\sqcup}T - ODOS \ \rightarrow\ 08161201 - 00010021 - 16041620$$

A cada uno de estos números lo denominaremos *palabra* y vamos a cifrar palabra a palabra.

La clave pública (n, e)

La clave, que haremos pública, la constituye una pareja de enteros (n, e) elegidos de forma que

- n sea primo con cualquier *posible* palabra de un texto.
  Esta condición se garantiza si cualquier divisor primo de n es mayor que la mayor palabra posible: para $r = 4$, $p_{mín} = 27272727$.

- e debe ser primo con $\phi(n)$.

La clave privada (n, d)

Esta clave está constituida por la pareja (n, d) donde

$$d = e^{-1} \bmod \phi(n)$$

Obsérvese que al haber elegido e primo con $\phi(n)$, e es invertible (es una unidad) en $\mathbf{Z}_{\phi(n)}$, por lo que tenemos garantizada la existencia de d.

El cifrado

Si N es una palabra del texto y (n, e) es la clave pública a utilizar, la palabra cifrada C se obtiene mediante la transformación

$$N \ \rightarrow \ C = N^e \bmod n$$

El descifrado

Si C es una palabra del texto y (n, d) es la clave privada, la palabra descifrada N se obtiene mediante la transformación

$$C \ \rightarrow \ N = C^d \bmod n$$

En otras palabras, se trata de volver a cifrar la palabra cifrada C utilizando ahora la clave privada.

El hecho de ser $d = e^{-1} \bmod \phi(n)$ nos lleva a que $ed + \alpha\phi(n) = 1$ con $\alpha \in \mathbf{Z}$.

Al haber elegido n primo con cualqier posible palabra del texto tenemos asegurado que $N \perp n$ y el teorema de Euler nos dice que $N^{\phi(n)} \equiv 1 \pmod{n}$, es decir, que $N^{\phi(n)} \bmod n = 1$.

$$C^d \bmod n = N^{e \cdot d} \bmod n = N^{e \cdot d}(N^{\phi(n)})^{\alpha} \bmod n = N^{d \cdot e + \alpha\phi(n)} \bmod n =$$
$$= N^1 \bmod n = N$$

La elección de una clave segura

Una clave segura es aquella que garantiza la *privacidad* de la clave privada (n, d).

Dado que los enteros (n, e) son públicos, la seguridad de la clave debe consistir

en la imposibilidad de la determinación del entero d que forma parte de la clave privada.

Teniendo en cuenta que $d = e^{-1} \bmod \phi(n)$ y tanto e como n son públicos, aparentemente nunca podremos tener una clave segura.

Es falso, para la obtención de d es necesario conocer previamente el valor de $\phi(n)$ y para ello *factorizar n*, problema computacionalmente imposible para valores grandes de n.

Un problema muy sencillo es elegir dos primos grandes p y q y multiplicarlos para obtener $n = p \cdot q$. El problema inverso, dado n encontrar p y q es un problema de imposible resolución para n suficientemente grande.

Así pues, si elegimos dos primos p y q de un número de dígitos suficientemente grande nos será muy fácil obtener $n = p \cdot q$ y dado que disponemos de los valores de p y q calcular $\phi(n) = (p-1)(q-1)$ para elegir posteriormente un entero e primo con $\phi(n)$ que junto con el valor de n constituya la clave (n, e) que haremos pública, con la seguridad de que nadie podrá calcular el valor de d, por lo que nadie conocerá nuestra clave privada (n, d).

El proceso

Supongamos que tres personas A, B y C hacen públicas sus respectivas claves (n_A, e_A), (n_B, e_B) y (n_C, e_C).

Si A quiere enviar un mensaje M a B lo cifra con la clave pública (n_B, e_B) del destinatario B.

- Cuando B recibe el mensaje, es capaz de descifrarlo pues conoce su clave privada (n_B, d_B).
- Si C intercepta el mensaje, no puede descifrarlo pues no conoce la clave privada de B (n_B, d_B), ya que para ello necesitaría factorizar n_B y eso no es posible.

La firma

Para evitar que B reciba un mensaje *aparentemente enviado por A* pero de hecho *enviado por C* para tratar de confundirlo, se establece la denominada *firma*.

Dicha firma F se codifica dos veces:

$$F \overset{(n_A,d_A)}{\longrightarrow} F' \overset{(n_B,e_B)}{\longrightarrow} F''$$

A conoce su clave privada (n_A, d_A) y la clave pública de B, (n_B, e_B).

Al recibirlo B, realiza el proceso inverso

$$F'' \overset{(n_B,d_B)}{\longrightarrow} F' \overset{(n_A,e_A)}{\longrightarrow} F$$

B conoce su clave privada (n_B, d_B) y la clave pública de A, (n_A, e_A).

Para que C le enviase un mensaje a B con vistas a que éste pensase que procedía de A sería necesario que C conociera la clave privada (n_A, d_A) de A y eso no es posible.

Ejemplo 2.33 Utilizando el alfabeto castellano y sabiendo que nuestra clave pública es $(7480189, 3)$ nos han enviado, utilizando RSA con $r = 2$, el siguiente mensaje

$$2541003 - 635746 - 4377622 - 5165698 - 1191016 - 5854368$$

Para descifrarlo debemos comenzar por conocer nuestra clave privada (n, d).

$$n = 7480189 = 2729 \cdot 2741 \implies \phi(n) = 2728 \cdot 2740 = 7474720$$

$$d = 3^{-1} \bmod 7474720 = 4983147$$

por lo que nuestra clave privada es $(n, d) = (7480189, 4983147)$.

$$2541003^{4983147} \bmod 7480189 = \ 319$$

$$635746^{4983147} \bmod 7480189 = \ 917$$

$$4377622^{4983147} \bmod 7480189 = 2116$$

$$5165698^{4983147} \bmod 7480189 = \ 719$$

$$1191016^{4983147} \bmod 7480189 = \ 106$$

$$5854368^{4983147} \bmod 7480189 = \ 901$$

Teniendo en cuenta que cada letra del alfabeto necesita de dos dígitos y que $r = 2$, cada palabra descifrada debe contener 4 dígitos. Si no los tiene le

añadimos ceros a la izquierda.

Rompiendo además cada palabra descifrada en sus dos letras obtenemos:

$$03 - 19 - 09 - 17 - 21 - 16 - 07 - 19 - 01 - 06 - 09 - 01$$

es decir: *CRIPTOGRAFIA*. □

2.12 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

$$c = a \cdot q_1 + r \quad \text{con} \quad q_1 \in \mathbf{Z} \quad \text{y} \quad 0 \leq r < a$$
$$c = b \cdot q_2 + s \quad \text{con} \quad q_2 \in \mathbf{Z} \quad \text{y} \quad 0 \leq s < b$$

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:

$$\text{mcd}\,(8,6) = 2 \,|\, (4-a) \Longrightarrow 2 \,|\, a \Longrightarrow a \equiv 0 \pmod 2$$

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

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, $u = 5v \Longrightarrow x = 4+8(5v) = 4+40v$.

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 $\text{mcd}\,(8, 5) = 1 = 8 \cdot 2 + 5 \cdot (-3)$, 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

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

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

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

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:

$$A_m - A_n = 2^{n+3p} + 4^{n+3p} + 8^{n+3p} - 2^n - 4^n - 8^n =$$

$$= 2^n(8^p - 1) + 4^n(8^{2p} - 1) + 8^n(8^{3p} - 1)$$

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

$$n \equiv 1 \pmod{(p_1 - 1)}$$

$$n \equiv 1 \pmod{(p_2 - 1)}$$

$$n \equiv 1 \pmod{(p_3 - 1)}$$

$$m = 37n \equiv 1 \pmod{(p_1 - 1)}$$

$$m = 37n \equiv 1 \pmod{(p_2 - 1)}$$

$$m = 37n \equiv 1 \pmod{(p_3 - 1)}$$

$$m = 37n \equiv 1 \pmod{36}$$

$$\left.\begin{array}{l} n \equiv 1 \pmod{(p_1-1)} \\ m = 37n \equiv 1 \pmod{(p_1-1)} \end{array}\right\} \Longrightarrow 37 \equiv 1 \pmod{(p_1-1)} \Longrightarrow p_1 - 1 \,|\, 36$$

$$\left.\begin{array}{l} n \equiv 1 \pmod{(p_2-1)} \\ m = 37n \equiv 1 \pmod{(p_2-1)} \end{array}\right\} \Longrightarrow 37 \equiv 1 \pmod{(p_2-1)} \Longrightarrow p_2 - 1 \,|\, 36$$

$$\left.\begin{array}{l} n \equiv 1 \pmod{(p_3-1)} \\ m = 37n \equiv 1 \pmod{(p_3-1)} \end{array}\right\} \Longrightarrow 37 \equiv 1 \pmod{(p_3-1)} \Longrightarrow p_3 - 1 \,|\, 36$$

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 $p = 4a + 3$. ■

2.13 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*: $x = 18 + 50\,t \quad \forall\, t \in \mathbf{Z}$.

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

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

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

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

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

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

Ejercicio 2.22 Hallar la solución general de la congruencia

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

Sol: $x = 873 + 1300\,t \quad \forall\, t \in \mathbf{Z}$. (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) $x \equiv 1 \pmod 6$, $x \equiv 5 \pmod{14}$, $x \equiv 4 \pmod{21}$.

Sol: No tiene solución.

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

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

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

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

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 Funciones

El primer contacto que se tiene con una función en la enseñanza primaria es a través de una tabla de valores, de tal forma que a la vista de la tabla

x	1	2	3	4	5	$\cdots$
y	2	4	6	8	10	$\cdots$

se induce la relación $y = 2x$.

La idea de función no es más que la de tratar de asociar a unos elementos, que denominaremos *originales*, otros que llamaremos *imágenes* por medio de un determinado proceso.

Este proceso no ha de ser necesariamente una fórmula matemática sino que puede ser, por ejemplo, dado el nombre de un usuario encontrar su número de abonado en una guía telefónica. Evidentemente, aquí nos interesaremos por aquellos procesos que puedan ser definidos a través de una expresión matemática.

Para que un proceso de este tipo sea considerado una función se han de cumplir dos requisitos lógicos, a saber:

a) A dos entradas iguales han de corresponder dos salidas iguales.

b) Toda entrada ha de tener una salida.

Al conjunto de las posibles entradas lo denominaremos *conjunto original* y al que contiene a todas las posibles salidas lo llamaremos *conjunto final*. Los denotaremos por Xe Y respectivamente.

Definición 3.1 [Función]

Una función $f : X \to Y$ es una aplicación entre los conjuntos X e Y que verifica las siguientes condiciones:

$$\begin{cases} x = y \implies f(x) = f(y) \\ \\ \forall x \in X \Rightarrow \exists\ y \in Y \quad tal\ que \quad y = f(x) \end{cases}$$

Ejemplo 3.1

- $f : \mathbf{N} \to \mathbf{N}$ dada por $f(n) = n^2$ es una función, ya que

  a) $n = m \implies n^2 = m^2$

  b) $\forall n \in \mathbf{N} \implies \exists\ n^2 \in \mathbf{N}$

- $f : \mathbf{Z} \to \mathbf{R}$ dada por $f(x) = +\sqrt{x}$ no es una función ya que, por ejemplo,

  $$-4 \in \mathbf{Z} \quad \text{y} \quad f(-4) = +\sqrt{-4} \notin \mathbf{R}$$

  es decir, no existe $f(-4)$.

- Una función también puede venir definida de forma recursiva:

  $$u(1) = 1 \quad \text{y} \quad \forall n \in \mathbf{N}\ \ u(n+1) = \begin{cases} \frac{1}{2}u(n) & \text{si } u(n) \text{ es par} \\ \\ 5u(n) + 1 & \text{si } u(n) \text{ es impar} \end{cases}$$

  $$u(2) = 6,\ u(3) = 3,\ u(4) = 16,\ u(5) = 8,\ u(6) = 4,\ u(7) = 2,\ \cdots$$

  por lo que se trata de una función, ya que todos los elementos del conjunto original $\mathbf{N}$ tienen un transformado y que además este es único. □

En el ejemplo anterior observamos que $u(1) = u(8) = 1$ es decir, a dos elementos distintos les corresponde un mismo transformado. Parece lógico preguntarse:

¿Qué funciones asocian transformados distintos a originales distintos?

Definición 3.2 [Función inyectiva]

Una función $f : X \to Y$ se dice que es inyectiva si a elementos distintos de X les asocia imágenes distintas en Y. Es decir:

$$f \text{ inyectiva} \iff f(x) = f(y) \implies x = y$$

Ejemplo 3.2

- $f : \mathbf{N} \to \mathbf{N}$ definida por $f(n) = 2n$ es inyectiva, ya que

$$f(n_1) = f(n_2) \Rightarrow 2n_1 = 2n_2 \implies n_1 = n_2.$$

- $f : \mathbf{Z} \to \mathbf{Z}$ dada por $f(x) = x^2$ no es inyectiva, ya que

$$f(-2) = (-2)^2 = (2)^2 = f(2) \quad \text{siendo} \quad -2 \neq 2. \qquad \square$$

Ahora bien, aunque la función $f(n) = 2n$ del ejemplo anterior es inyectiva, es evidente que ningún elemento de $\mathbf{N}$ se transforma mediante f en un natural impar. Es decir, f transforma $\mathbf{N}$ en un subconjunto de $\mathbf{N}$ pero no en *todo* $\mathbf{N}$. Existen elementos del conjunto final que no son transformados de ninguno del conjunto original. Nos preguntamos entonces:

¿Qué funciones transforman el conjunto original en todo el conjunto final?

Definición 3.3 [Función sobreyectiva]

Una función $f : X \to Y$ se dice que es sobreyectiva si cualquier elemento del conjunto final es transformado de alguno del conjunto original.

$$f \text{ sobreyectiva} \iff \forall y \in Y \ \ \exists\, x \in X \ \text{ tal que } \ f(x) = y$$

Ejemplo 3.3 La función $f : \mathbf{R} \to \mathbf{R}^+$ definida por $f(x) = x^2$ es sobreyectiva, ya que

$$\forall\, y \in \mathbf{R}^+ \implies \exists\, x = \sqrt{y} \in \mathbf{R} \ \text{ tal que } \ f(x) = y$$

Sin embargo, no es inyectiva ya que $f(-2) = f(2)$ con $-2 \neq 2$. $\square$

Nos podemos preguntar por último:

¿Qué funciones serán simultáneamente inyectivas y sobreyectivas?

Definición 3.4 [Función biyectiva]

Una función $f : X \to Y$ se dice que es biyectiva, o que se trata de una biyección si es simultáneamente inyectiva y sobreyectiva.

$$f \text{ biyectiva} \iff \begin{cases} f \text{ es inyectiva} & f(x) = f(y) \Rightarrow x = y \\ f \text{ es sobreyectiva} & \forall y \in Y \ \ \exists\, x \in X \ \ \text{tal que} \ \ f(x) = y \end{cases}$$

Ejemplo 3.4 La función $f : \mathbf{Z} \to \mathbf{Z}$ definida por $f(n) = n - 1$ es una biyección. □

Obsérvese que para que se pueda establecer una función biyectiva entre dos conjuntos finitos es necesario que ambos posean el mismo número de elementos, ya que una biyección establece una relación de uno a uno. No ocurre lo mismo entre conjuntos infinitos.

3.1.1 Enumeración

Una aplicación inmediata de las funciones biyectivas es la que nos permite contar los elementos de un conjunto. El hecho de decir que un determinado conjunto X tiene n elementos se debe a que si vamos asignando, comenzando por 1, 2, 3, ..., etc., un número natural a cada elemento del conjunto X, el último número asociado es el de elementos de este posee.

Definición 3.5 [Enumeración]

Si construimos para cada $n \in \mathbf{N}$ el subconjunto $\mathbf{N}_n$ de $\mathbf{N}$ definido por

$$\mathbf{N}_n = \{1,\ 2, \ldots,\ n\}$$

Enumerar los elementos de un conjunto X equivale a establecer una biyección entre $\mathbf{N}_n$ y X.

El número de elementos de un conjunto X viene dado por el valor de n, se le denomina cardinal del conjunto X y se denota por $|X|$.

Al conjunto vacío $\emptyset$ se le asigna el cardinal cero: $|\emptyset| = 0$

3.2 El principio de adición

Al hablar de *enumeración* hemos visto la forma de *contar* los elementos de un conjunto asignando un número natural a cada uno de ellos. Ahora bien, si no disponemos de una lista de sus elementos, sino que el conjunto viene definido a través de unas propiedades, es necesario desarrollar técnicas, diferentes a las ya conocidas, capaces de contar sus elementos.

Definición 3.6 [Conjuntos Unión e Intersección]

- *Dados dos conjuntos A y B, se define el conjunto unión y se denota por $A \cup B$ como el conjunto constituido por todos los elementos que pertenecen a A o a B (o simultáneamente a ambos).*

$$x \in A \cup B \iff \begin{cases} x \in A & \acute{o} \\ x \in B \end{cases}$$

- *Se define el conjunto intersección y se denota por $A \cap B$ como el conjunto de los elementos que pertenecen simultáneamente a ambos conjuntos.*

$$x \in A \cap B \iff \begin{cases} x \in A & y \\ x \in B \end{cases}$$

Si la intersección de dos conjuntos es vacía, diremos que dichos conjuntos son disjuntos.

$$A \text{ y } B \text{ disjuntos} \iff A \cap B = \emptyset$$

Ejemplo 3.5 Si $A = \{1,\ 2,\ 3\}$ y $B = \{2,\ 4,\ 6\}$, tenemos que

$$A \cup B = \{1,\ 2,\ 3,\ 4,\ 6\} \qquad \text{y} \qquad A \cap B = \{2\}$$ □

Lema 3.1 *Si dos conjuntos A y B son disjuntos, se verifica que*

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

Esta propiedad de los conjuntos disjuntos puede ser generalizada como muestra el siguiente teorema.

Teorema 3.2 [Principio de adición]

Si $A_1,\ A_2, \ldots,\ A_n$ *son conjuntos disjuntos dos a dos, es decir*

$$A_i \cap A_j = \emptyset \quad \text{si} \quad i \neq j \quad 1 \leq i, j \leq n$$

se verifica que

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|.$$

Un resultado inmediato del principio de adición es el denominado *principio de distribución* que describimos a continuación.

Teorema 3.3 [Principio de distribución]

Si queremos repartir n *objetos en* m *cajas y* $rm < n$*, al menos una caja ha de recibir más de* r *objetos.*

Demostración. Definamos para $1 \leq i \leq m$ los conjuntos

$$A_i = \{\text{objetos de la caja } i\text{-ésima}\}$$

Evidentemente, ha de verificarse que $|A_1| + |A_2| + \cdots + |A_m| = n$. Ahora bien:

$$|A_1| + |A_2| + \cdots + |A_m| \leq m \cdot \max_i |A_i| \implies n \leq m \cdot \max_i |A_i|$$

Si fuese $\max_i |A_i| \leq r$ tendríamos que $n \leq mr$ contra la hipótesis de que $n > rm$. Por tanto, ha de ser $\max_i |A_i| > r$, es decir, alguna de las cajas ha de recibir más de r objetos. ■

Ejemplo 3.6 Vamos a ver que si A es un conjunto de 101 enteros positivos diferentes, no superiores a 200 y elegidos al azar existen, al menos, dos elementos de A tales que uno divide al otro.

Descompongamos cada elemento $a_i \in A$ de la forma $a_i = 2^\alpha \cdot b$ donde 2^α es la mayor potencia de 2 y b el mayor impar que dividen a a_i.

Así, por ejemplo, $48 = 2^4 \cdot 3$, $122 = 2^1 \cdot 61$ ó $125 = 2^0 \cdot 125$.

Los posibles valores que podemos obtener para b son $\{1, 3, 5, \ldots, 199\}$, por lo que al haber 101 valores de a_i y sólo 100 posibles valores de b, el principio de distribución nos garantiza la existencia de, al menos, dos valores de $a_i = 2^\alpha \cdot b$ y $a_j = 2^\beta \cdot b$ con el mismo valor de b y $\alpha \neq \beta$.

Resulta entonces evidente que si $\alpha < \beta$, a_i divide a a_j. □

3.3 El principio de inclusión y exclusión

Por el principio de adición (3.2) sabemos que si dos conjuntos A y B son disjuntos se verifica que $|A \cup B| = |A| + |B|$. Sin embargo, no sabemos nada sobre el cardinal de la unión cuando los conjuntos no son disjuntos.

Dado que $A \cap B \subset A$ y $A \cap B \subset B$, los elementos de $A \cap B$ se han contado tanto al contar los elementos de A como al hacerlo con los elementos de B, mientras que para contar los de $A \cup B$ sólo debemos hacerlo una vez. Debido a esto no es difícil darse cuenta que se va a verificar que

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

Obsérvese que si $A \cap B = \emptyset \implies |A \cap B| = 0$, en cuyo caso no tenemos otra cosa que el principio de adición.

Para el caso de tres conjuntos se verifica

$$|A \cup B \cup C| = |A \cup (B \cup C)| = |A| + |B \cup C| - |A \cap (B \cup C)| =$$

$$= |A| + |B| + |C| - |B \cap C| - |(A \cap B) \cup (A \cap C)|^{(1)} =$$

$$= |A| + |B| + |C| - |B \cap C| - \{|A \cap B| + |A \cap C| - |A \cap B \cap C|\} =$$

$$= |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$$

Llamando $\alpha_1 = |A| + |B| + |C|$

$$\alpha_2 = |A \cap B| + |A \cap C| + |B \cap C|$$

$$\alpha_3 = |A \cap B \cap C|$$

podemos expresarlo de la forma $|A \cup B \cup C| = \alpha_1 - \alpha_2 + \alpha_3$.

Podemos generalizar este resultado para obtener el siguiente teorema.

Teorema 3.4 [Principio de inclusión y exclusión]

Si $A_1, A_2, \ldots, A_n$ son conjuntos finitos y denotamos por α_i a la suma de los cardinales de las intersecciones de i conjuntos

(1) Debido a la propiedad distributiva de la intersección respecto a la unión de conjuntos. Consúltese cualquier texto elemental de teoría de conjuntos.

$$\alpha_1 = |A_1| + |A_2| + \cdots + |A_n|$$

$$\alpha_2 = |A_1 \cap A_2| + |A_1 \cap A_3| + \cdots + |A_{n-1} \cap A_n|$$

$$\vdots$$

$$\alpha_n = |A_1 \cap A_2 \cap \cdots \cap A_n|$$

se verifica

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \alpha_1 - \alpha_2 + \cdots + (-1)^{n+1}\alpha_n.$$

Demostración. La demostración puede hacerse mediante inducción en el número n de conjuntos A_i. ■

Ejemplo 3.7 En un encuentro de informática hay participantes de España, Francia e Inglaterra. Sabiendo que 9 de ellos hablan francés, otros 9 inglés y otros 9 castellano; que hay 4 que hablan francés e inglés, 3 que hablan francés y castellano, 4 que hablan inglés y castellano y 1 que hablan los tres idiomas, ¿cuántos participantes hay en el encuentro? ¿hay alguno que sólo hable castellano?

Indicando por F, I y C a los conjuntos de participantes que habla francés, inglés y castellano respectivamente, los datos que tenemos son los siguientes:

$$|F| = |I| = |C| = 9,\ |F \cap I| = 4,\ |F \cap C| = 3,\ |I \cap C| = 4,\ |F \cap I \cap C| = 1$$

Teniendo en cuenta que cualquiera de los participantes habla alguno de los tres idiomas, el principio de inclusión y exclusión nos dice que

$$|F \cup I \cup C| = |F| + |I| + |C| - |F \cap I| - |F \cap C| - |I \cap C| + |F \cap I \cap C|$$

$$= 9 + 9 + 9 - 4 - 3 - 4 + 1 = 17$$

por lo que hay 17 participantes de los cuales hablará *sólo castellano* los que no sepan francés ni inglés. Dado que

$$|F \cup I| = |F| + |I| - |F \cap I| = 9 + 9 - 4 = 14$$

hay 14 participantes que hablan francés o inglés por lo que el resto, es decir, 3 sólo saben castellano. □

3.4 Contar en tablas

Definición 3.7 [Conjunto producto cartesiano]

Dados dos conjuntos X e Y, al conjunto de todos los pares ordenados (x, y) donde $x \in X$ e $y \in Y$, se le denomina conjunto producto cartesiano y se le denota por $X \times Y$

$$X \times Y = \{(x, y) \ \ tal\ que \ \ x \in X,\ y \in Y\}$$

verificándose que $|X \times Y| = |X| \times |Y|$.

Ejemplo 3.8 Si $A = \{x_1, x_2, x_3\}$ y $B = \{y_1, y_2\}$, el conjunto producto cartesiano de A por B sería

$$A \times B = \{(x_1, y_1), (x_1, y_2), (x_2, y_1), (x_2, y_2), (x_3, y_1), (x_3, y_2)\}$$

verificándose que $|A| = 3$, $|B| = 2$ y $|A \times B| = |A| \times |B| = 3 \cdot 2 = 6$. □

Definición 3.8 [Tabla]

Un subconjunto T del conjunto producto cartesiano $X \times Y$ recibe el nombre de tabla.

Algunas veces, el problema de contar los elementos de un conjunto que no viene definido a través de una lista para poder enumerarlos, se resuelve mediante el método de *contar en tablas*.

Una técnica para contar los elementos de una tabla es representarla en un cuadro de doble entrada. En una entrada disponemos los elementos de X y en la otra a los elementos de Y y marcamos un punto cuando el par es un elemento de T.

Teorema 3.5 [Contar en tablas]

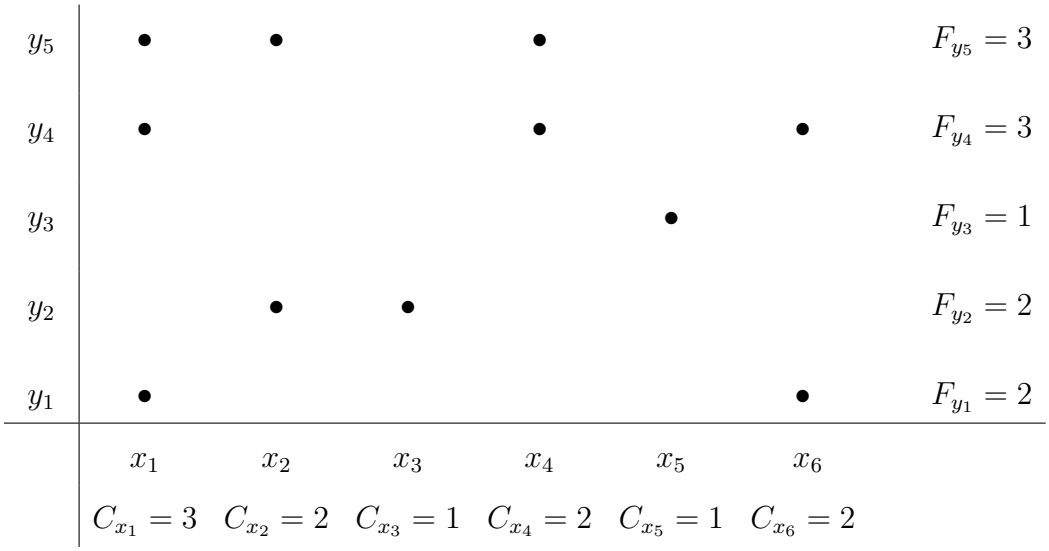
Consideremos una tabla $T \subseteq X \times Y$ y sean

$$F_x = |\{y \in Y \ \ tales\ que \ \ (x, y) \in T\}|$$
$$C_y = |\{x \in X \ \ tales\ que \ \ (x, y) \in T\}|$$

se verifica que

$$\sum_{x \in X} F_x = \sum_{y \in Y} C_y = |T|$$

Ejemplo 3.9 Para la tabla T representada a continuación



se verifica que

$$\sum_{i=1}^{6} C_{x_i} = \sum_{i=1}^{5} F_{y_i} = |T| = 11$$

□

Ejemplo 3.10 De los alumnos de una clase 32 son varones y cada uno de ellos conoce exactamente a 5 compañeras. Si cada alumna conoce exactamente a 8 compañeros, ¿cuántas alumnas hay en la clase?

Denotemos por X al conjunto de todos los alumnos, por Y al de las alumnas y sea T la tabla constituida por todos los pares (x, y) definidos por el hecho de que el alumno x conoce a la alumna y.

F_x (número de alumnas que conoce cada alumno) es constante e igual a 5, mientras que C_y (número de alumnos que conoce cada alumna) es también constante e igual a 8.

$$\left.\begin{array}{l} \displaystyle\sum_{x\in X} F_x = 5 + 5 + \overset{(32}{\cdots} + 5 = 5 \cdot 32 = 160 \\ \\ \displaystyle\sum_{y\in Y} C_y = 8 + 8 + \overset{(n}{\cdots} + 8 = 8n \end{array}\right\} \Rightarrow 160 = 8n \implies n = 20$$

es decir, hemos contado las alumnas que hay en la clase sin necesidad de tener una lista de ellas. □

3.5 Funciones, palabras y variaciones

3.5.1 Variaciones

Consideremos las funciones, no necesariamente biyectivas, definidas de $\mathbf{N}_m$ en un conjunto cualquiera X. Los valores que toma una función determina la m-upla $(f(1),\ f(2),\ldots,\ f(m))$ de elementos de X.

Teniendo en cuenta la definición de producto cartesiano

$$X^m = X \times X \times \overset{(m}{\cdots} \times X = \{(x_1,\ x_2,\ldots,\ x_m)\ :\ x_i \in X\ 1 \leq i \leq m\}$$

observamos que a cada función $f : \mathbf{N}_m \to X$ le corresponde un elemento de X^m y viceversa.

Si al conjunto X lo denominamos *alfabeto*, decimos que una *palabra* de longitud m es una función de $\mathbf{N}_m$ en X. Así por ejemplo, si X es el alfabeto, "*casa*" es la palabra definida por $f : \mathbf{N}_4 \to X$ con

$$f(1) = \text{c},\ f(2) = \text{a},\ f(3) = \text{s y } f(4) = \text{a}.$$

Definición 3.9 [Variaciones con repetición]

Al conjunto de todas las palabras de longitud m formadas a partir de un alfabeto de n letras se le denomina conjunto de las variaciones con repetición de n elementos con longitud m.

Teorema 3.6 *Sean X e Y dos conjuntos finitos con $|X| = m$ y $|Y| = n$. Si denotamos por F al conjunto de todas las funciones que pueden ser definidas de X en Y, entonces $|F| = n^m$.*

Demostración. Sea $X = \{x_1,\ x_2,\ldots,\ x_m\}$. Cada elemento $f \in F$ viene determinado por la m-upla $(f(x_1),\ f(x_2),\ldots,\ f(x_m))$ que pertenece al conjunto Y^m, por lo que $|F| = |Y^m| = n^m$. ■

Ejemplo 3.11 Como caso particular, vamos a contar el número de subconjuntos que posee un conjunto cualquiera X de n elementos.

Dado un subconjunto A de X, definimos la función $f_A : X \to \{0, 1\}$ de la forma

$$f_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases}$$

Contar los subconjuntos de X equivale a contar las funciones f_A, por lo que el número de subconjuntos de un conjunto X de n elementos es $2^{|X|} = 2^n$. □

Si consideramos ahora sólo las funciones *inyectivas* que pueden definirse de $\mathbf{N}_m$ en X formaremos palabras que no tienen ninguna letra repetida. Este tipo de palabras recibe el nombre de *variaciones sin repetición* de los elementos de un conjunto X con longitud m.

Teorema 3.7 [VARIACIONES SIN REPETICIÓN]

Si $|X| = n$ el número de variaciones sin repetición de longitud m es

$$n(n-1)(n-2)\cdots(n-m+1) \tag{3.1}$$

Demostración. En efecto, basta tener en cuenta que la m-upla $(1,\ 2, \ldots,\ m)$ se transforma en $(x_1,\ x_2, \ldots,\ x_m)$ mediante una aplicación *inyectiva* f, por lo que $x_i \neq x_j$ si $i \neq j$ y por tanto, x_2 no puede tomar el valor asignado a x_1, x_3 ninguno de los asignados a x_1 ni a x_2 etc. para obtener el resultado. ■

Ejemplo 3.12 ¿Cuántos números de seis cifras pueden escribirse sabiendo que deben comenzar por 1 y no tener cifras repetidas?

Teniendo en cuenta que todos comienzan por 1 basta con escribir las otras cinco cifras del número y que ninguna de estas puede estar repetida ni ser un 1 (que ya está en primera posición), por lo que con las cifras 0, 2, 3, 4, 5, 6, 7, 8 y 9 debemos formar todas las variaciones sin repetición de longitud 5

$$V_{9,5} = 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 = 15120$$

por lo que existen 15120 números con las características pedidas. □

3.5.2 Permutaciones

De igual manera que a las aplicaciones inyectivas de $\mathbf{N}_m$ en X las hemos llamado variaciones sin repetición, a las *funciones biyectivas* las llamaremos *permutaciones*, ya que al ser sobreyectiva la función, lo único que hacemos es permutar el orden de los elementos de X.

Evidentemente, al tratarse de una biyección es inyectiva por lo que su número vendrá dado por la fórmula (3.1) y por ser además sobreyectiva se verifica que $m = n$.

Teorema 3.8 [Permutaciones]

El número de permutaciones de n elementos, que se denota por $n!$ y se lee factorial de n viene dado por

$$n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$$

Ejemplo 3.13 Las letras de la palabra CESA pueden ser permutadas de

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

formas diferentes. □

Supongamos ahora que tratamos de contar el número de formas en que se pueden permutar las letras de la palabra CASA.

Como se trata de permutar las letras, estamos hablando de permutaciones, pero hay que observar que si las letras que se permutan son las dos A-es, la palabra resultante es la misma, por lo que sólo obtendremos la mitad de ordenaciones que el caso de la palabra CESA que tiene las cuatro letras diferentes.

Establecemos de esta forma el concepto de *permutaciones con repetición* en el sentido de que permutamos elementos entre los que existen algunos repetidos.

Teorema 3.9 [Permutaciones con repetición]

El número de permutaciones con repetición de un conjunto de n elementos donde existe un grupo de n_1 elementos repetidos, otro de n_2 elementos etc. viene dado por

$$PR_{n\,;\,n_1,n_2,\ldots,n_k} = \frac{n!}{n_1! \cdot n_2! \cdots n_k!}$$

Ejemplo 3.14 Las letras de la palabra CASA pueden ser permutadas de

$$PR_{4\,;\,2} = \frac{4!}{2} = \frac{4 \cdot 3 \cdot 2 \cdot 1}{2 \cdot 1} = \frac{24}{2} = 12$$

formas diferentes. □

3.6 Números binómicos

3.6.1 Combinaciones

Definición 3.10 [Combinaciones]

Dado un conjunto de n elementos interesa a veces calcular el número de subconjuntos de r elementos que posee. A este número se le denota por $\binom{n}{r}$, *expresión que se lee n sobre r o combinaciones de n elementos tomados de r en r.*

Teorema 3.10 *Sean n y r dos enteros positivos tales que $1 \leq r \leq n$. Se verifica que*

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}.$$

Demostración. Sea X el conjunto de n elementos y etiquetemos un elemento $x \in X$. El conjunto de todos los subconjuntos de r elementos de X podemos separarlo en dos partes disjuntas U y V

$$\left.\begin{array}{l} U = \text{Subconjuntos que contienen a } x. \\ V = \text{Subconjuntos que no contienen a } x. \end{array}\right\} \Longrightarrow \binom{n}{r} = |U| + |V|$$

El conjunto U se obtiene añadiendo el elemento x a todos los subconjuntos de $r-1$ elementos que pueden extraerse de $X - \{x\}$ conjunto, este último, que posee $n-1$ elementos, es decir

$$|U| = \binom{n-1}{r-1}$$

El conjunto V se obtiene de formar todos los subconjuntos de r elementos de $X - \{x\}$, ya que ninguno de los elementos de V contiene a x.

$$|V| = \binom{n-1}{r}$$

Por lo que $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$. ■

Para $r = 0$ se define el número binómico $\binom{n}{0} = 1$.

Evidentemente, si $m > n$ el número binómico $\binom{n}{m} = 0$ ya que un conjunto de n elementos no posee ningún subconjunto de $m > n$ elementos.

Definición 3.11 [Triángulo de Pascal]

El teorema anterior nos permite calcular los números binómicos de forma recursiva construyendo el denominado triángulo de Pascal.

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

Para calcular los valores de los elementos del triángulo basta con observar que los elementos extremos de cada fila son siempre unos y cada elemento interior es la suma de los dos que tiene encima. De esta forma es fácil calcular recursivamente los valores de todos los elementos del triángulo.

$$\begin{array}{ccccccccccc}
 & & & 1 & & & & 1 & & & \\
 & & 1 & & & 2 & & & 1 & & \\
 & 1 & & & 3 & & & 3 & & & 1 \\
\cdots & & \cdots & & & \cdots & & & \cdots & & \cdots
\end{array}$$

Teorema 3.11 [Cálculo de los números binómicos]

Si r y n son enteros positivos tales que $1 \leq r \leq n$ se verifica que

$$\binom{n}{r} = \frac{n(n-1)\cdots(n-r+1)}{r!} = \frac{n!}{r!\,(n-r)!}$$

Demostración. La demostración la haremos por inducción sobre n.

- La fórmula es cierta para $n = 1$ ya que si $n = 1$ ha de ser necesariamente $r = 1$ y $\binom{1}{1} = 1$ ya que un conjunto de un sólo elemento sólo tiene un subconjunto de un elemento.

- Si se verifica para n vamos a probar que también es cierto para $n+1$. En efecto

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

y dado que estamos suponiendo cierta la propiedad para n, tenemos que

$$\begin{aligned}\binom{n+1}{r} &= \frac{n(n-1)\cdots(n-r+2)}{(r-1)!} + \frac{n(n-1)\cdots(n-r+1)}{r!} = \\ &= \frac{n(n-1)\cdots(n-r+2)}{(r-1)!}\left[1 + \frac{n-r+1}{r}\right] = \\ &= \frac{(n+1)n(n-1)\cdots(n-r+2)}{r!}\end{aligned}$$

Si $r = 0$ o $r = n+1$, los valores $\binom{n}{0} = 1$ y $\binom{n}{n+1} = 0$ aseguran la validez de la demostración. ■

Teorema 3.12 *Si p es primo se verifica que p divide a $\binom{p}{i}$ para cualquier i tal que $0 < i < p$.*

Demostración.

$$\binom{p}{i} = \frac{p\cdot(p-1)\cdot(p-2)\cdots(p-i+1)}{i\cdot(i-1)\cdot(i-2)\cdots 2\cdot 1} \in \mathbf{Z}$$

es decir

$$[i\cdot(i-1)\cdot(i-2)\cdots 2\cdot 1] \text{ divide a } [p\cdot(p-1)\cdot(p-2)\cdots(p-i+1)]$$

y como $[i\cdot(i-1)\cdot(i-2)\cdots 2\cdot 1]$ es primo con p, por ser p primo, necesariamente

$$[i\cdot(i-1)\cdot(i-2)\cdots 2\cdot 1] \text{ divide a } [(p-1)\cdot(p-2)\cdots(p-i+1)]$$

por lo que

$$\binom{p}{i} = p\cdot\frac{(p-1)\cdot(p-2)\cdots(p-i+1)}{i\cdot(i-1)\cdot(i-2)\cdots 2\cdot 1} = p\,q \quad \text{con} \quad q\in\mathbf{Z}$$

y, por tanto, p divide a $\binom{p}{i}$. ■

Una propiedad de los números combinatorios que se deduce de manera inmediata nos la muestra el siguiente teorema.

Teorema 3.13 [Números combinatorios complementarios]

Si n y r son dos enteros no negativos, se verifica que

$$\binom{n}{r} = \binom{n}{n-r}$$

Demostración. Basta observar que

$$\binom{n}{n-r} = \frac{n!}{(n-r)!\,[n-(n-r)]!} = \frac{n!}{(n-r)!\,r!} = \binom{n}{r}.$$ ■

3.6.2 Combinaciones con repetición

Supongamos ahora que con las letras a, b y c queremos formar grupos de cuatro letras (no nos importa el orden en que se coloquen). Podemos formar los grupos:

$$aaaa \quad aaab \quad aaac \quad aabb \quad aabc \quad aacc \quad abbb \quad abbc$$
$$abcc \quad accc \quad bbbb \quad bbbc \quad bbcc \quad bccc \quad cccc$$

Es decir, podemos formar, en total, 15 grupos.

A estos grupos se les denomina *combinaciones con repetición* de tres elementos tomados de 4 en 4. En general, de n elementos tomados de r en r.

Teorema 3.14 [Combinaciones con repetición]

El número de combinaciones con repetición de r elementos obtenidos de un conjunto de n objetos viene dado por $\binom{n+r-1}{r}$.

Demostración. Consideremos una caja con $n + (r - 1)$ departamentos y coloquemos un uno en la posición ocupada por un elemento y un cero cuando cambiemos de elemento. Es decir,

$$aabc \implies 110101$$
$$abbc \implies 101101$$

Observamos que a cada grupo de letras le corresponde una secuencia formada por cuatro unos y dos ceros y recíprocamente, a cada secuencia numérica de ese tipo le corresponde uno de los grupos de letras

$$111001 \implies aaac$$
$$001111 \implies cccc$$

Al tener establecida una biyección entre los grupos de letras y las secuencias numéricas y ser ambas finitas debe existir el mismo número de unas que de otras, por lo que remitiremos nuestro problema al de contar las secuencias de seis dígitos con cuatro unos y dos ceros.

Nuestro problema se reduce a encontrar en cuántas posiciones diferentes pueden colocarse los dos ceros. En general, ¿en cuántas posiciones pueden ser colocados los $n + (r-1) - r = n - 1$ ceros?, o lo que es lo mismo, ¿cuántos subconjuntos de $n-1$ elementos posee un conjunto de $n+r-1$ elementos? La respuesta es $\binom{n+r-1}{n-1}$ y dado que $\binom{n}{m} = \binom{n}{n-m}$ podemos decir que $\binom{n+r-1}{n-1} = \binom{n+r-1}{r}$. ■

En nuestro ejemplo es $\binom{3+4-1}{4} = \binom{6}{4} = 15$.

Ejemplo 3.15 Podemos determinar el número de soluciones enteras de la ecuación

$$x_1 + x_2 + x_3 + x_4 = 25 \quad x_i \geq 0 \quad 1 \leq i \leq 4$$

considerando que se han de repartir 25 objetos entre 4 personas.

Para ello alineamos los 25 elementos y los etiquetamos con la persona x_1, x_2, x_3 o x_4 a la que va destinado, es decir, debemos escribir una palabra de 25 letras utilizando las letras x_1, x_2, x_3 y x_4, por lo que el número de soluciones enteras del problema viene dado por las combinaciones con repetición de 4 elementos tomados de 25 en 25, es decir:

$$\binom{25+4-1}{25} = \binom{28}{25} = \binom{28}{3} = 3276.$$

□

Ejemplo 3.16 En el Ejemplo 3.15 determinamos el número $N = 3276$ de soluciones enteras de $x_1 + x_2 + x_3 + x_4 = 25$ donde $x_i \geq 0$ para $1 \leq i \leq 4$.

Si añadimos la restricción $x_i \leq 10$ debemos hacer uso del Principio de Inclusión y Exclusión. Diremos que una solución x_1, x_2, x_3 y x_4 cumple la condición c_i, $1 \leq i \leq 4$ si $x_i > 10$ (o equivalentemente $x_i \geq 11$), por lo que la solución a nuestro problema viene dada por $N(\bar{c_1}\bar{c_2}\bar{c_3}\bar{c_4})$.

Por la naturaleza del problema $N(c_1) = N(c_2) = N(c_3) = N(c_4)$. Para calcular $N(c_i)$ resolvemos el problema

$$x_1 + x_2 + x_3 + x_4 = 25 - 11 = 14 \quad x_i \geq 0 \quad 1 \leq i \leq 4$$

y le añadimos 11 a x_i, por lo que $N(c_i) = \binom{17}{14} = 680$. Para hallar $N(c_i c_j)$ resolvemos el problema

$$x_1 + x_2 + x_3 + x_4 = 25 - 22 = 3 \quad x_i \geq 0 \quad 1 \leq i \leq 4$$

y le añadimos 11 a x_i y otros 11 a x_j, por lo que $N(c_i) = \binom{6}{3} = 20$. Evidentemente, $N(c_i c_j c_k) = N(c_i c_j c_k c_l) = 0$.

$$N(\bar{c_1}\bar{c_2}\bar{c_3}\bar{c_4}) = N - S_1 + S_2 - S_3 + S_4$$

donde

$$S_1 = N(c_1) + N(c_2) + N(c_3) + N(c_4) = \binom{4}{1} N(c_i) = 4 \cdot 680 = 2720$$

$$S_2 = \binom{4}{2} N(c_1 c_j) = 6 \cdot 20 = 120$$

$$S_3 = \binom{4}{3} N(c_i c_j c_k) = 0$$

$$S_4 = \binom{4}{4} N(c_i c_j c_k c_l) = 0$$

por lo que

$$N(\bar{c_1}\bar{c_2}\bar{c_3}\bar{c_4}) = 3276 - 2720 + 120 - 0 + 0 = 676.$$

es decir, sólo existen ahora 676 soluciones a nuestro problema. □

Ejemplo 3.17 El problema de encontrar el número de soluciones enteras de la ecuación

$$x_1 + x_2 + x_3 + x_4 = 25 \quad x_i \geq -2 \quad 1 \leq i \leq 4$$

es equivalente al de resolver

$$x_1 + x_2 + x_3 + x_4 = 33 \quad x_i \geq 0 \quad 1 \leq i \leq 4$$

cuya solución viene dada por

$$\binom{36}{33} = \binom{36}{3} = 7140.$$

□

3.6.3 Teorema del binomio

Sea n un número entero positivo y consideremos la expresión $(a+b)^n$. Esta expresión puede desarrollarse multiplicándola por sí misma n veces. Una forma mucho más rápida para desarrollarla la proporciona el siguiente teorema.

Teorema 3.15 [Teorema del binomio]

El coeficiente del término $a^{n-r}b^r$ del desarrollo de $(a+b)^n$, donde n es un número entero positivo, viene dado por el número binómico $\binom{n}{r}$.

Demostración. Basta observar que para formar el término $a^{n-r}b^n$ del producto

$$(a+b)\cdot(a+b)\overset{(n}{\cdots}(a+b)$$

es necesario formar todos los productos posibles de n factores eligiendo un elemento de cada paréntesis de tal manera que aparezcan $n-r$ *aes* y r *bes* y para ello nos basta con ver de cuántas formas podemos elegir las *bes*. Teniendo en cuenta lo anterior, es evidente que el coeficiente buscado es el número binómico $\binom{n}{r}$. ∎

El desarrollo del binomio nos queda entonces de la forma

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

Ejemplo 3.18 Basándose en el Teorema 3.12 podemos demostrar, por inducción, el corolario del pequeño teorema de Fermat, es decir, que si p es primo se verifica que $p\,|\,a^p-a$ cualquiera que sea el entero a. En efecto:

Para $a=1$ se reduce a probar que $p\,|\,1^p-1=0$ y cualquier entero es divisor de 0.

Si suponemos la propiedad cierta para a tenemos que probarla para $a+1$ es decir, tenemos que probar que $p\,|\,(a+1)^p-(a+1)$. Ahora bien:

$$(a+1)^p-(a+1)=a^p+\binom{p}{1}a^{p-1}+\binom{p}{2}a^{p-2}+\cdots+\binom{p}{p-1}a+1-(a+1)$$

es decir

$$(a+1)^p - (a+1) = (a^p - a) + \left[\binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a \right]$$

donde el primer paréntesis es divisible por p por hipótesis de inducción y el segundo también es divisible por p por serlo todos sus sumandos (Teorema 3.12), por lo que

$$p \,|\, a^p - a \implies p \,|\, (a+1)^p - (a+1)$$

y, por tanto, podemos garantizar que para cualquier entero positivo a y cualquier primo p se verifica que $p \,|\, a^p - a$. □

3.7 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. ■

3.8 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:

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

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

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

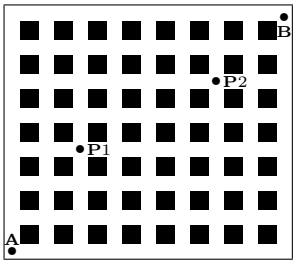
b) Probar por inducción sobre n que para todo $n \geq 2$ se verifica que

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

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

Vimos en el Capítulo 1 que dada una sucesión recurrente, podíamos inducir una expresión para su término general que sólo dependiera de n con el fin de poder calcular un determinado término de la sucesión sin necesidad de calcular *todos* los términos anteriores. Evidentemente, una vez inducida la fórmula era necesario probar que era cierta para cualquier entero positivo, y para ello hacíamos uso del método de inducción.

Dicho proceso tiene el inconveniente de que lo primero que debemos hacer es inducir la fórmula, y eso no es, en general, una tarea fácil, por lo que dedicamos este capítulo a estudiar cómo podemos obtener, de una forma directa, la expresión del término general de una sucesión recurrente.

4.1 Recurrencias lineales homogéneas

Vimos con anterioridad que algunas funciones definidas en $\mathbf{N}$ incluyen a la propia función en su definición. Así, por ejemplo, la función S_n de (1.1) podía ser definida de la forma

$$S_1 = 1 \quad \text{y} \quad S_n = S_{n-1} + (2n-1) \quad \text{siempre que } n \in \mathbf{N}$$

y más tarde vimos como podía expresarse en función del valor de n de la forma $S_n = n^2$.

Esto último nos sugiere que a menudo podemos obtener una ecuación que nos dé el valor de una función definida en forma recursiva en función directa del valor de la variable.

Evidentemente una función recursiva no va a venir siempre expresada, como la del ejemplo anterior, dando u_n en función de u_{n-1} sino que puede venir expresada en función de varios términos anteriores, teniendo en cuenta que habrá

que conocer los valores de tantos términos iniciales como términos anteriores figuren en la definición recursiva, es decir, si definimos $u_n = u_{n-1} + u_{n-2}$ habrá que conocer los valores de u_1 y u_2.

Definición 4.1 [Recurrencias lineales homogéneas]

Una recurrencia en la que un término u_n viene dado en función de los k términos anteriores, $u_{n-1},\ u_{n-2}, \ldots, u_{n-k}$.

$$u_n + a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k} = 0 \quad n \geq k$$

donde $a_1,\ a_2, \ldots,\ a_k$ son constantes conocidas, recibe el nombre de recurrencia lineal homogénea (RLH) de orden k.

Obsérvese que las sucesiones:

$$\begin{aligned} (u_n) &= (1, 3, 4, 7, 11, 18, 29, 47, \ldots) \\ (v_n) &= (2, 5, 7, 12, 19, 31, 50, 81, \ldots) \end{aligned} \tag{4.1}$$

verifican ambas la misma RLH. Cada término es la suma de los dos anteriores

$$u_n = u_{n-1} + u_{n-2} \quad \text{y} \quad v_n = v_{n-1} + v_{n-2}$$

Definición 4.2 [Solución general de una RLH]

Se conoce como solución general de una RLH a una expresión del tipo

$$u_n = F(n\,; A_1, A_2, \ldots, A_k) \quad \textit{con} \quad A_1, A_2, \ldots, A_k \quad \textit{constantes indeterminadas}$$

que verifica cualquier sucesión que satisfaga la RLH.

Definición 4.3 [Condiciones iniciales de una RLH]

Teniendo en cuenta que un término depende de los k términos anteriores es evidente que la solución será única una vez se hayan determinado las constantes $A_1, A_2, \ldots, A_k$ es función de los k primeros términos de la sucesión (u_n).

Los referidos k primeros términos de la sucesión se conocen como condiciones iniciales.

En resumen:

- La RLH de orden k

$$u_n + a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k} = 0 \quad n \geq k$$

  admite infinitas soluciones. Al conjunto de todas ellas se le conoce como *solución general* de la RLH.

- La RLH de orden k

$$u_n + a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k} = 0 \quad n \geq k$$

  junto con las condiciones iniciales

$$u_0 = c_0,\ u_1 = c_1,\ \ldots,\ u_k = c_k$$

  define una única sucesión (u_n).

Definición 4.4 [Ecuación característica de una RLH]

Dada una RLH

$$u_n + a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k} = 0 \quad n \geq k$$

La ecuación

$$t^k + a_1 t^{k-1} + \cdots + a_{k-1} t + a_k = 0$$

se denomina ecuación característica de la RLH.

Teorema 4.1 [RLH: Caso $n = 2$]

Sea (u_n) una sucesión que satisface la RLH

$$u_n + a_1 u_{n-1} + a_2 u_{n-2} = 0 \quad (n \geq 2)$$

con las condiciones iniciales

$$u_0 = c_0,\ u_1 = c_1$$

y sean α y β las raíces de su ecuación característica

$$t^2 + a_1 t + a_2 = 0$$

Si $\alpha \neq \beta$, entonces existen constantes A y B tales que

$$u_n = A\alpha^n + B\beta^n \quad (n \geq 0) \quad \textit{solución general de la RLH}$$

mientras que si $\alpha = \beta$, existen constantes C y D tales que

$$u_n = (Cn + D)\alpha^n \quad (n \geq 0) \quad \textit{solución general de la RLH}$$

Las constantes A y B (o bien C y D según el caso), están determinadas por c_0 y c_1.

Demostración.

a) $\boldsymbol{\alpha \neq \beta}$

Para $n = 0$ y $n = 1$ se obtiene que

$$\left.\begin{array}{l} u_0 = A\alpha^0 + B\beta^0 = A + B = c_0 \\ u_1 = A\alpha^1 + B\beta^1 = A\alpha + B\beta = c_1 \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} A = \dfrac{c_1 - c_0\beta}{\beta - \alpha} \\ B = \dfrac{c_1 - c_0\alpha}{\alpha - \beta} \end{array}\right.$$

Asignando a A y B estos valores, la propiedad $u_n = A\alpha^n + B\beta^n$ se verificará para u_0 y u_1.

Supongamos, por hipótesis de inducción que se verifica hasta $n - 1$ y vamos a probarlo para n.

$$\begin{aligned} u_n = & -(a_1u_{n-1} + a_2u_{n-2}) \\ = & -[a_1(A\alpha^{n-1} + B\beta^{n-1}) + a_2(A\alpha^{n-2} + B\beta^{n-2})] \\ = & -A\alpha^{n-2}(a_1\alpha + a_2) - B\beta^{n-2}(a_1\beta + a_2) \\ = & A\alpha^n + B\beta^n \end{aligned}$$

En el último paso se ha hecho uso de que α y β son raíces de la ecuación característica, por lo que $\alpha^2 + a_1\alpha + a_2 = 0 \implies a_1\alpha + a_2 = -\alpha^2$ y análogamente se obtiene que $a_1\beta + a_2 = -\beta^2$.

Por el principio de inducción tenemos entonces que el resultado es cierto para cualquier $n \geq 0$.

b) $\boldsymbol{\alpha = \beta}$

En este caso, se aplica el mismo método pero utilizando la fórmula correspondiente. ■

Para el caso general de una recurrencia lineal homogénea de orden k se tiene el siguiente teorema.

Teorema 4.2 [RLH: Caso general]

Sea (u_n) una sucesión definida por RLH y sean $\alpha_1,\ \alpha_2, \ldots,\ \alpha_s$ las raíces de la ecuación característica con multiplicidades $m_1,\ m_2, \ldots,\ m_s$ respectivamente. Entonces:

$$u_n = P_1(n)\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_s(n)\alpha_s^n$$

donde para cada $i = 1,\ 2, \ldots,\ s,\ P_i(n)$ es una expresión de la forma

$$A_0 + A_1 n + \cdots + A_{m_i-1} n^{m_i-1}$$

Es decir, los $P_i(n)$ $1 \leq i \leq s$ son polinomios en n de grados no superiores a $m_i - 1$ y que se determinan a partir de las condiciones iniciales, esto es, de los términos iniciales conocidos.

Ejemplo 4.1 : Se denomina *sucesión de Fibonacci* a la definida por:

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

En este caso y dado que la recurrencia viene dada por $f_n - f_{n-1} - f_{n-2} = 0$, la ecuación característica es

$$t^2 - t - 1 = 0$$

cuyas raíces son $\dfrac{1+\sqrt{5}}{2}$ y $\dfrac{1-\sqrt{5}}{2}$, por lo que

$$f_n = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n \tag{4.2}$$

Sustituyendo los valores conocidos para $n = 0$ y $n = 1$ obtenemos

$$\left.\begin{array}{c} A + B = 0 \\ \\ A\left(\dfrac{1+\sqrt{5}}{2}\right) + B\left(\dfrac{1-\sqrt{5}}{2}\right) = 1 \end{array}\right\} \implies A = -B = \frac{1}{\sqrt{5}}$$

obteniéndose la fórmula explícita de la sucesión de Fibonacci

$$f_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right] \quad \forall\, n \geq 0$$

Obsérvese que la fórmula dada en (4.2) *solución general de la recurrencia* $u_n = u_{n-1} + u_{n-2}$ también la verifican las sucesiones definidas en (4.1) sólo que para otros valores diferentes de las constantes A y B ya que ambas tenían la misma fórmula de recurrencia que la sucesión de Fibonacci, es decir, cada término es la suma de los dos anteriores. □

4.2 Recurrencias lineales no homogéneas

Definición 4.5 [Recurrencias lineales no homogéneas]

Reciben el nombre de recurrencias lineales no homogéneas de orden k (RLnH) aquellas recurrencias lineales de orden k cuyo término independiente es no nulo, en general, una función de n.

$$u_n + a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k} = f(n) \quad n \geq k$$

Definición 4.6 *Dada la RLnH*

$$u_n + a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k} = f(n) \quad n \geq k$$

se denomina recurrencia lineal homogénea asociada a la RLH resultante de sustituir por cero el término independiente de la RLnH.

$$u_n + a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k} = 0 \quad n \geq k$$

Teorema 4.3 [Solución general de una RLnH]

Una RLnH tiene como solución general

$$u_n = u_n^{(h)} + u_n^{(p)} \quad \text{con} \quad \begin{cases} u_n^{(h)} = \text{solución general de la RLH asociada} \\ u_n^{(p)} = \text{una solución particular de la RLnH.} \end{cases}$$

Demostración. Sean $u_n^{(p)}$ una solución particular y v_n una solución cualquiera de la RLnH.

Por ser ambas soluciones de la no homogénea, verifican que

$$u_n^{(p)} + a_1 u_{n-1}^{(p)} + a_2 u_{n-2}^{(p)} + \cdots + a_k u_{n-k}^{(p)} = f(n) \quad n \geq k$$

$$v_n + a_1 v_{n-1} + a_2 v_{n-2} + \cdots + a_k v_{n-k} = f(n) \quad n \geq k$$

Restando obtenemos que

$$(u_n^{(p)}-v_n)+a_1(u_{n-1}^{(p)}-v_{n-1})+a_2(u_{n-2}^{(p)}-v_{n-2})+\cdots+a_k(u_{n-k}^{(p)}-v_{n-k})=0 \quad n\geq k$$

es decir, la sucesión $(u_n^{(p)}-v_n)$ es solución de la RLH asociada, o lo que es lo mismo, v_n es la suma de $u_n^{(p)}$ y una solución de la RLH asociada, por lo que recorriendo todas las soluciones posibles (solución general) de la homogénea asociada obtendremos todas las soluciones (solución general) de la RLnH dada. En otras palabras,

$$u_n = u_n^{(h)} + u_n^{(p)}$$ ■

Es evidente que como ya sabemos calcular la solución general de la RLH asociada sólo nos resta saber cómo encontrar una solución particular de la completa o no homogénea.

Método de los coeficientes indeterminados

Aunque no existe un método general para encontrar una solución particular, el *método de los coeficientes indeterminados* nos va a proporcionar esta solución en función de la forma que tiene la función $f(n)$.

- Si $f(n)=P_k(n)$ (un polinomio de grado k)

  $$u_n^{(p)} = Q_k(n)\cdot n^m$$

  donde m representa la multiplicidad de la raíz 1 en la ecuación característica de la RLH asociada.

- Si $f(n)=P_k(n)\cdot a^n$ donde k representa el grado del polinomio $P_k(n)$

  $$u_n^{(p)} = Q_k(n)\cdot n^m\cdot a^n$$

  donde m representa la multiplicidad de la raíz a en la ecuación característica de la RLH asociada.

Obsérvese que el caso $f(n)=P_k(n)$ no es más que un caso particular de $f(n)=P_k(n)\cdot a^n$ cuando $a=1$.

Ejemplo 4.2 Vamos a determinar la sucesión definida por

$$\begin{cases} u_0=0, \quad u_1=2 \\ \\ u_{n+2}+4u_{n+1}+4u_n=n^2 \end{cases}$$

La RLH asociada $u_{n+2}+4u_{n+1}+4u_n=0$ tiene por ecuación característica

$$t^2+4t+4=0 \implies t=-2 \text{ doble}$$

por lo que su solución general es de la forma

$$u_n^{(h)}=(An+B)(-2)^n$$

Dado que 1 no es solución de la ecuación característica de la RLH asociada, tratamos de buscar una solución particular $u_n^{(p)}$ de la completa que sea de la misma forma que su término independiente, es decir, un polinomio de segundo grado $u_n^{(p)}=Cn^2+Dn+E$.

$$u_{n+2}+4u_{n+1}+4u_n=n^2 \implies$$

$$C(n+2)^2+D(n+2)+E+4C(n+1)^2+4D(n+1)+4E+4Cn^2+4Dn+4E=n^2$$

de donde desarrollando e igualando coeficientes obtenemos:

$$\left.\begin{array}{r} 9C=1 \\ 9D+12C=0 \\ 9E+6D+8C=0 \end{array}\right. \Rightarrow \left\{\begin{array}{l} C=1/9 \\ D=-4/27 \\ E=0 \end{array}\right. \Rightarrow u_n^{(p)}=\frac{1}{9}n^2-\frac{4}{27}n=\frac{1}{27}(3n^2-4n)$$

y, por tanto, la solución general de la RLnH es

$$u_n=u_n^{(h)}+u_n^{(p)}=(An+B)(-2)^n+\frac{1}{27}(3n^2-4n)$$

Imponiendo, *por último* las condiciones iniciales $u_0=0$ y $u_1=2$ obtenemos que $A=-55/54$ y $B=0$, por lo que el término general de la sucesión buscada es

$$u_n=-\frac{55}{54}n(-2)^n+\frac{1}{27}(3n^2-4n) \qquad \square$$

Ejemplo 4.3 Determinemos ahora la sucesión definida mediante

$$u_n-3u_{n-1}=5\cdot 7^n \quad \text{con} \quad u_0=2$$

La RLH asociada $u_n-3u_{n-1}=0$ tiene como solución $u_n^{(h)}=A\cdot 3^n$.

Como $f(n)=5\cdot 7^n$, se busca una solución particular $u_n^{(p)}$ de la forma $B\cdot 7^n$ (ya que 7 no es solución de la ecuación característica de la RLH asociada), obteniéndose por sustitución

$$B\cdot 7^n-3B\cdot 7^{n-1}=5\cdot 7^n \iff 7B-3B=5\cdot 7 \iff B=\frac{35}{4}$$

es decir, $u_n^{(p)} = \dfrac{35}{4} \cdot 7^n$ y, por tanto, la solución general de la recurrencia es de la forma

$$u_n = u_n^{(h)} + u_n^{(p)} = A \cdot 3^n + \frac{35}{4} \cdot 7^n$$

teniendo en cuenta que $u_0 = 2$ obtenemos que $A = -\dfrac{27}{4}$, por lo que

$$u_n = \frac{1}{4}(35 \cdot 7^n - 27 \cdot 3^n)$$

□

Ejemplo 4.4 Si tratamos ahora de resolver la recurrencia

$$u_n - 3u_{n-1} = 5 \cdot 3^n \quad \text{con} \quad u_0 = 2$$

observamos que la solución general de la RLH asociada es la misma que en el ejemplo anterior. Sin embargo ahora, dado que 3^n es solución de RLH asociada, no podemos tomar como solución particular $u_n^{(p)} = B \cdot 3^n$ sino que debemos tomar $u_n^{(p)} = B \cdot n \cdot 3^n$, obteniendo por sustitución

$$B \cdot n \cdot 3^n - 3 \cdot B \cdot (n-1) \cdot 3^{n-1} = 5 \cdot 3^n \iff B \cdot n - B \cdot (n-1) = 5 \iff B = 5$$

por lo que

$$u_n = u_n^{(h)} + u_n^{(p)} = A \cdot 3^n + 5 \cdot n \cdot 3^n$$

y dado que $u_0 = 2$ se obtiene que $A = 2$, es decir $u_n = (2 + 5n)3^n$. □

En el caso más general, en que $f(n) = P_k(n) + Q_{k_a}(n) \cdot a^n + \cdots + Q_{k_b}(n) \cdot b^n$, se busca una solución particular que sea suma de las correspondientes a cada uno de sus sumandos.

Ejemplo 4.5 Supongamos que la ecuación característica de la RLH asociada tenga de raíces 1 doble, 2 simple y 3 triple y que el término independiente sea

$$f(n) = n^2 - 3n + 2 + (2n - 3) \cdot 2^n + (n - 1) \cdot 3^n + (n^2 - 3) \cdot 5^n$$

La solución particular ha de ser de la forma

$$u_n^{(p)} = (An^2 + Bn + C) \cdot n^2 + (Dn + E) \cdot n \cdot 2^n + (Fn + G) \cdot n^3 \cdot 3^n + (Hn^2 + In + J) \cdot 5^n$$

ya que

$n^2 - 3n + 2$ y 1 es raíz doble $\implies (An^2 + Bn + C) \cdot n^2$

$(2n - 3) \cdot 2^n$ y 2 es raíz simple $\implies (Dn + E) \cdot n \cdot 2^n$

$(n - 1) \cdot 3^n$ y 3 es raíz triple $\implies (Fn + G) \cdot n^3 \cdot 3^n$

$(n^2 - 3) \cdot 5^n$ y 5 no es raíz de la ec. caract. $\implies (Hn^2 + In + J) \cdot 5^n$ □

4.3 Funciones generadoras

Definición 4.7 *Sea $a_0, a_1, a_2, \dots,$ una sucesión de números reales. La función*

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{i=0}^{\infty} a_i x^i$$

se denomina función generadora de la sucesión dada.

Trataremos, en esta sección, de encontrar funciones generadoras para aquellas sucesiones que pueden ser definidas mediante una recurrencia lineal y homogénea.

Búsqueda de la función generadora a partir de la recurrencia

Consideremos la sucesión definida por

$$\begin{cases} a_0,\ a_1, \dots, a_{k-1} \\ a_n + \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \cdots + \alpha_k a_{n-k} = 0 \quad \forall\, n \geq k \end{cases}$$

y supongamos que su función generadora es $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$.

Construyendo la tabla

$$\begin{array}{rl} f(x) = & a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_k x^k + \cdots + a_n x^n + \cdots \\ \alpha_1 x f(x) = & \alpha_1 a_0 x + \alpha_1 a_1 x^2 + \alpha_1 a_2 x^3 + \cdots + \alpha_1 a_{k-1} x^k + \cdots + \alpha_1 a_{n-1} x^n + \cdots \\ \alpha_2 x^2 f(x) = & \alpha_2 a_0 x^2 + \alpha_2 a_1 x^3 + \cdots + \alpha_2 a_{k-2} x^k + \cdots + \alpha_2 a_{n-2} x^n + \cdots \\ \multicolumn{2}{c}{\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots} \\ \alpha_k x^k f(x) = & + \alpha_k a_0 x^k + \cdots + \alpha_k a_{n-k} x^n + \cdots \end{array}$$

y sumando, podemos observar que, a partir de los términos de grado k, la suma de los coeficientes verifican la relación de recurrencia y por tanto se anulan, quedándonos, en el segundo miembro, un polinomio de grado $k-1$.

Si denotamos por $P_{k-1}(x)$ a dicho polinomio, nos queda que

$$(1 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_k x^k) f(x) = P_{k-1}(x)$$

por lo que la función generadora buscada será

$$f(x) = \frac{P_{k-1}(x)}{1 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_k x^k}$$

Ejemplo 4.6 Se considera la sucesión de Fibonacci definida por

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

Denotemos por $f(x) = f_0 + f_1 x + f_2 x^2 + f_3 x^3 + \cdots$ a su función generadora. Se verifica entonces que

$$\begin{aligned} f(x) &= f_0 + f_1 x + f_2 x^2 + f_3 x^3 + \cdots \\ -xf(x) &= \quad -f_0 x - f_1 x^2 - f_2 x^3 - \cdots \\ -x^2 f(x) &= \qquad\quad -f_0 x^2 - f_1 x^3 - \cdots \end{aligned}$$

de donde

$$(1 - x - x^2) f(x) = f_0 + (f_1 - f_0)x + (f_2 - f_1 - f_0)x^2 + (f_3 - f_2 - f_1)x^3 - \cdots$$

y teniendo en cuenta que por definición es

$$f_2 - f_1 - f_0 = f_3 - f_2 - f_1 = \cdots = f_n - f_{n-1} - f_{n-2} = 0$$

se tiene que

$$(1 - x - x^2) f(x) = f_0 + (f_1 - f_0)x = 0 + (1 - 0)x = x$$

por lo que la función generadora de la sucesión de Fibonacci es

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

□

Ejemplo 4.7 Para buscar la función generadora de la sucesión $a_n = n^2 + 4$ debemos comenzar por definir la sucesión de manera recursiva.

Al ser de la forma $a_n = P_2(n) \cdot 1^n$, la ecuación característica de la RLH que define a la sucesión debe tener como única raíz al 1 y dado que va acompañado de un polinomio de segundo grado, debe ser una raíz triple, es decir

$$(t-1)^3 = t^3 - 3t^3 + 3t - 1$$

por lo que dicha sucesión puede definirse, de forma recursiva, de la siguiente manera:

$$\begin{cases} a_0 = 4,\ a_1 = 5,\ a_2 = 8 \\ \\ a_n = 3a_{n-1} - 3a_{n-2} + a_{n-3} \quad \forall\, n \geq 3 \end{cases}$$

Si la función generadora es $f(x) = a_0 + a_1x + a_2x^2 + \cdots$ se tiene:

$$\begin{aligned} f(x) &= a_0 + \ a_1x + \ a_2x^2 + \ a_3x^3 + \ a_4x^4 + \cdots \\ -3xf(x) &= \quad -3a_0x - 3a_1x^2 - 3a_2x^3 - 3a_3x^4 - \cdots \\ 3x^2f(x) &= \quad\quad 3a_0x^2 + 3a_1x^3 + 3a_2x^4 + \cdots \\ -x^3f(x) &= \quad\quad\quad -a_0x^3 - \ a_1x^4 - \cdots \end{aligned}$$

de donde, sumando, se obtiene

$$\begin{aligned} (1 - 3x + 3x^2 - x^3)\, f(x) &= a_0 + (a_1 - 3a_0)x + (a_2 - 3a_1 + 3a_0)x^2 + \\ &+ (a_3 - 3a_2 + 3a_1 - a_0)x^3 + \cdots = \\ &= a_0 + (a_1 - 3a_0)x + (a_2 - 3a_1 + 3a_0)x^2 \end{aligned}$$

ya que el resto de los términos del desarrollo son nulos por verificar la recurrencia.

Dado que $a_0 = 4$, $a_1 = 5$ y $a_2 = 8$, obtenemos

$$(1 - x)^3 f(x) = 4 + (5 - 12)x + (8 - 15 + 12)x^2 = 4 - 7x + 5x^2 \implies$$

$$f(x) = \frac{4 - 7x + 5x^2}{(1 - x)^3}$$

□

Búsqueda de a_n a partir de la función generadora

Trataremos, a continuación, el problema inverso, es decir: dada la sucesión (a_n) definida mediante su función generadora $f(x)$, encontrar una fórmula explícita para los términos de (a_n).

Para ello recordemos algunos desarrollos conocidos:

- $\dfrac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots = \displaystyle\sum_{n=0}^{\infty} x^n$
- $\dfrac{1}{1-ax} = 1 + ax + a^2x^2 + a^3x^3 + \cdots = \displaystyle\sum_{n=0}^{\infty} a^n x^n$
- $\dfrac{1}{(1-x)^2} = 1 + 2x + 3x^2 + 4x^3 + \cdots = \displaystyle\sum_{n=0}^{\infty} (n+1)x^n$
- $\dfrac{1}{(1-ax)^2} = 1 + 2ax + 3a^2x^2 + 4a^3x^3 + \cdots = \displaystyle\sum_{n=0}^{\infty} (n+1)a^n x^n$

y cambiando x por $-x$

- $\dfrac{1}{1+x} = 1 - x + x^2 - x^3 + \cdots = \displaystyle\sum_{n=0}^{\infty} (-1)^n x^n$
- $\dfrac{1}{1+ax} = 1 - ax + a^2x^2 - a^3x^3 + \cdots = \displaystyle\sum_{n=0}^{\infty} (-1)^n a^n x^n$
- $\dfrac{1}{(1+x)^2} = 1 - 2x + 3x^2 - 4x^3 + \cdots = \displaystyle\sum_{n=0}^{\infty} (-1)^n (n+1)x^n$
- $\dfrac{1}{(1+ax)^2} = 1 - 2ax + 3a^2x^2 - 4a^3x^3 + \cdots = \displaystyle\sum_{n=0}^{\infty} (-1)^n (n+1)a^n x^n$

Para resolver nuestro problema, bastará con descomponer la función generadora en suma de fracciones de numeradores constantes, escribir sus desarrollos y estudiar el comportamiento de sus coeficientes.

Veámoslo con los siguientes ejemplos.

Ejemplo 4.8 Vamos a buscar el término general de la sucesión (a_n) definida a través de su función generadora

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

Dado que

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

$$\left.\begin{array}{l} \dfrac{1}{1-x} = \displaystyle\sum_{n=0}^{\infty} x^n \\ \dfrac{1}{1-2x} = \displaystyle\sum_{n=0}^{\infty} 2^n x^n \end{array}\right\} \implies f(x) = -\sum_{n=0}^{\infty} x^n + \sum_{n=0}^{\infty} 2^n x^n = \sum_{n=0}^{\infty} (2^n - 1)x^n$$

y por ser la función generadora de (a_n) sabemos que $f(x) = \displaystyle\sum_{i=0}^{\infty} a_n x^n$, por lo que

$$a_n = 2^n - 1 \quad \forall\, n \geq 0$$ □

Ejemplo 4.9 Dada la sucesión $a_n = 2n + 1 \;\; \forall\, n \geq 0$ de los números impares, vamos a buscar su función generadora y, basándonos en ella, vamos a calcular el término general y comprobar que efectivamente obtenemos que $a_n = 2n+1$.

La definición, en forma recurrente, de dicha sucesión es

$$\begin{cases} a_0 = 1 \\ a_n - a_{n-1} = 2 \end{cases}$$

por lo que haciendo

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$

$$-xf(x) = \quad -a_0 x - a_1 x^2 - \cdots$$

se obtiene que

$$(1-x)f(x) = a_0 + (a_1 - a_0)x + (a_2 - a_1)x^2 + \cdots =$$

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

$$= 2 \cdot \frac{1}{1-x} - 1 = \frac{1+x}{1-x}$$

es decir, la función generadora de los números impares es

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

Teniendo en cuenta ahora que

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$$

$$\frac{1}{(1-x)^2} = \sum_{n=0}^{\infty} (n+1)x^n$$

obtenemos

$$f(x) = -\sum_{n=0}^{\infty} x^n + 2\sum_{n=0}^{\infty}(n+1)x^n = \sum_{n=0}^{\infty}(2n+1)x^n$$

por lo que el coeficiente del término de grado n del desarrollo de la función es $2n+1$ y, por tanto, $a_n = 2n+1 \ \ \forall\, n \geq 0$. □

4.4 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

$$a_{n+2} = 4a_{n+1} - 3a_n \tag{4.3}$$

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

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

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 4.3), $a_{n+1} = 4a_n - 3a_{n-1}$ 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

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

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

■

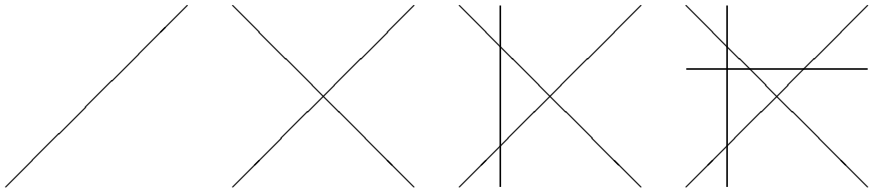
Ejercicio 4.3

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:

$$B[(n+1)^2 - n^2] + C[(n+1) - n] = n+1 \Rightarrow B(2n+1) + C = n+1 \Rightarrow \begin{cases} B = 1/2 \\ C = 1/2 \end{cases}$$

Por tanto, $u_n = \dfrac{1}{2}(n^2 + n) + A$ 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

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

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

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

o lo que es lo mismo

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

■

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ejercicio 4.13

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

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

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

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

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

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

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

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

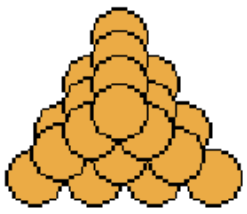
Ejercicio 4.17 Nos regalan tres sellos y decidimos iniciar una colección. El año siguiente, la incrementamos con 8 sellos más (tendríamos entonces 11 sellos). Si cada año compramos un número de sellos igual al doble de los que compramos el año anterior, ¿al cabo de cuántos años habremos superado el millón 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: $\dfrac{1}{6}n^3 + \dfrac{1}{2}n^2 + \dfrac{1}{3}n = \dfrac{1}{6}n(n+1)(n+2).$

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

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

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

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*: $a_n = (9n - \dfrac{16}{3})(-1)^n + \dfrac{19}{3} \cdot 2^n \quad \forall\, n \geq 0$.

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

Bibliografía

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

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

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

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