E.T.S. DE INGENIERÍA INFORMÁTICA

Apuntes de

INTRODUCCIÓN
A LA
MATEMÁTICA DISCRETA

para la titulación de

INGENIERÍA INFORMÁTICA

Curso 2002-2003

por

Fco. Javier Cobos Gavala

DEPARTAMENTO DE

MATEMÁTICA APLICADA I

Contenido

1. Aritmética entera

Dado que se supone que el alumno está familiarizado con las operaciones definidas en el conjunto $\mathbf{Z}$ 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 $\mathbf{Z}$, de números enteros no es más que 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*:

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 neutros 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.

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

Axioma 7 EL producto posee la propiedad *cancelativa*.

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

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

Axioma 8 Propiedad *reflexiva*: $\forall a \in \mathbf{Z} \Longrightarrow a \leq a$.

Axioma 9 Propiedad *antisimétrica*:
$$\left.\begin{array}{c} a \leq b \\ \text{y} \\ b \leq a \end{array}\right\} \Longrightarrow a = b.$$

Axioma 10 Propiedad *transitiva*:
$$\left.\begin{array}{c} a \leq b \\ \text{y} \\ b \leq c \end{array}\right\} \Longrightarrow a \leq c.$$

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 11 [buena ordenación] Todo subconjunto de $\mathbf{Z}$ no vacío y acotado inferiormente (superiormente) posee un primer (último) elemento.

Axioma 12
$$\begin{cases} a \leq b \ \text{ y } \ c > 0 \implies ac \leq bc \\ a \leq b \implies a + c \leq b + c \end{cases}$$

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 $\mathbf{Z}$ 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 Definiciones recursivas

Muchas veces nos habremos encontrado con expresiones del tipo

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

y lo primero que podemos preguntarnos es qué significado tienen los puntos suspensivos.

El significado de estos no es más que hacernos 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.

NOTA: 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.

1.3 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.

En nuestro ejemplo tenemos que

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

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.

1.3.1 Conjuntos inductivos

Un conjunto S se dice que es *inductivo* si se verifican:

$$\begin{aligned} &\text{a) } 1 \in S \\ &\text{b) } x \in S \Longrightarrow x + 1 \in S \end{aligned} \tag{1.2}$$

Teorema 1.1 *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, $S = \mathbf{N}$. ■

1.3.2 El método de inducción

Teorema 1.2 [Método de inducción] *Sea P_n una proposición matemática. Si se verifican:*

a) P_1 es verdadera y

b) P_k verdadera implica que P_{k+1} también lo es,

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:

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

es decir, la propiedad P_n es cierta cualquiera que sea el número natural n que se elija. ■

Ejemplo 1.1 Si nos fijamos en el ejemplo (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 1.3 [Método de inducción completa] *Sea P_n una proposición matemática. Si se verifican:*

a) $P_1, P_2, \ldots, P_r$ *son verdaderas y*

b) $P_1,\ P_2, \ldots, P_k$, *con* $k \leq r$, *verdaderas implica que* P_{k+1} *también lo es,*

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

1.4 Divisores

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

Teorema 1.4 *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 $S = \{a - nb \mid n \in \mathbf{Z}\} = \{a,\ a \pm b,\ a \pm 2b,\ \ldots\}$. 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 $r = 3$. □

Definición 1.2 Con la notación del Teorema 1.4 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

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

por lo que q viene dado por la *parte entera por defecto* o *suelo* de a/b (el mayor entero i con $i \leq \frac{a}{b}$) y que denotaremos por $\left\lfloor \frac{a}{b} \right\rfloor$. Esto facilita el cálculo de q. El de r se realiza posteriormente mediante la igualdad $r = a - qb$.

Si consideramos ahora el caso $b < 0$, dado que $-b > 0$, el Teorema 1.4 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 1.4, podemos establecer el siguiente corolario:

Corolario 1.5 *Si a y b son dos enteros con $b \neq 0$, existe un único par de enteros q y r tales que*

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

(Nótese que si $b < 0$ se tiene que

$$\frac{a}{b} = q + \frac{r}{b} \qquad \text{con} \qquad 0 \geq \frac{r}{b} > -1$$

por lo que en este caso q es la *parte entera por exceso* o *techo* del cociente a/b que denotaremos por $\left\lceil \frac{a}{b} \right\rceil$, es decir, el menor entero i tal que $i \geq \frac{a}{b}$).

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 1.4 (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 $n = 4(4q^2 + 2qr) + 0 \implies$ el resto es 0,

b) si $r = 1$ que $n = 4(4q^2 + 2qr) + 1 \implies$ el resto es 1,

c) si $r = 2$ que $n = 4(4q^2 + 2qr + 1) + 0 \implies$ el resto es 0,

d) y si $r = 3$ que $n = 4(4q^2 + 2qr + 2) + 1 \implies$ el resto es 1.

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

Definición 1.3 Si a y b son enteros y $a = qb$ para algún entero q, diremos que b *divide* a a, o bien que b es un *factor* o un *divisor* de a, o también que a es *múltiplo* de b. Así, por ejemplo, los factores de 6 son ± 1, ± 2, ± 3 y ± 6. Cuando b divide a a lo denotaremos por $b \,|\, a$ y se utiliza la notación $b \nmid a$ cuando b no divide a a. Para evitar errores 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. Debido a ello, dado un entero n, sólo los divisores de n distintos de 1 y del propio n se consideran *divisores propios* de dicho número.

Recordamos a continuación algunas propiedades simples pero útiles de la divisibilidad, probando dos de ellas y dejando la demostración de las otras a modo de ejercicios para el alumno.

Teorema 1.6

a) $a \,|\, b$ *y* $b \,|\, c \implies a \,|\, c$.

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

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

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

Demostración.

a)

$$\left.\begin{array}{lll} a \,|\, b \implies b = aq_1 & \text{con} & q_1 \in \mathbf{Z} \\ b \,|\, c \implies c = bq_2 & \text{con} & q_2 \in \mathbf{Z} \end{array}\right\} \implies$$

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

b)

$$\left.\begin{array}{lll} a \,|\, b \implies b = aq_1 & \text{con} & q_1 \in \mathbf{Z} \\ c \,|\, d \implies d = cq_2 & \text{con} & q_2 \in \mathbf{Z} \end{array}\right\} \implies$$

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

c) c.1)

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

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

c.2)

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

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 $|d| \leq |a|$. ■

Teorema 1.7

a) 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 $u_1, u_2, \ldots, u_k$.

b) $a \,|\, b$ y $b \,|\, a$ si, y sólo si, $a = \pm b$.

Demostración.

a) Si $c \,|\, a_i$ se tiene que $a_i = q_ic$ 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 $c \,|\, (a_1u_1 + a_2u_2 + \cdots + a_ku_k)$.

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

Recíprocamente, si $a \mid b$ y $b \mid a$ es $b = qa$ y $a = q'b$ para algunos enteros q y q'. Si $b = 0$, de la segunda igualdad se obtiene que $a = 0$, por lo que $a = \pm b$. Podemos suponer, por tanto, que $b \neq 0$. Eliminando a de ambas expresiones, obtenemos que $b = qq'b$ y como $b \neq 0$, por la propiedad cancelativa podemos asegurar que $qq' = 1$, por lo que $q, q' = \pm 1$ (utilizar el Teorema 1.6–(d)), por lo que $a = \pm b$. ■

La forma más usual del Teorema 1.7–(a) 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.*

1.5 Máximo común divisor

Definición 1.4 Si $d \mid a$ y $d \mid b$ 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. Si a y b son no nulos, el Teorema 1.6–(d) prueba que ninguno de sus divisores comunes puede ser mayor que máx$(|a|, |b|)$, por lo que de entre todos sus divisores comunes debe existir uno que sea el mayor de ellos. Este es el *máximo común divisor* de a y b; siendo el *único* entero d que satisface

a) $d \mid a$ y $d \mid b$ (por ser d un divisor común),

b) Si $c \mid a$ y $c \mid b \Longrightarrow c \leq d$ (pues d es el mayor divisor común de a y b).

Teorema 1.9 *El máximo común divisor de dos números enteros es único.*

Demostración. Supongamos que existiesen dos d y d'.

$$\left.\begin{array}{l} d = \text{mcd}\,(a,b) \Longrightarrow d \mid a \text{ y } d \mid b. \text{ Al ser } d' = \text{mcd}\,(a,b) \Longrightarrow d \leq d' \\ d' = \text{mcd}\,(a,b) \Longrightarrow d' \mid a \text{ y } d' \mid b. \text{ Al ser } d = \text{mcd}\,(a,b) \Longrightarrow d' \leq d \end{array}\right\}$$

y teniendo en cuenta la antisimetría de la relación de orden en el conjunto $\mathbf{Z}$ de los números enteros, obtenemos que $d = d'$. ■

Sin embargo, el caso $a = b = 0$ debe ser excluido; cualquier entero divide a 0 y es, por tanto, un divisor común de a y b, por lo que, en este caso, no existe el máximo común divisor. Cuando existe, denotamos el máximo común divisor de a y b por mcd (a, b), o simplemente por (a, b). Esta definición puede obviamente extenderse al máximo común divisor de cualquier conjunto de enteros (no todos nulos).

1.5.1 Algoritmo de Euclides

Una forma de encontrar el máximo común divisor de a y b es simplemente construir las listas de todos los divisores de a y todos los de b para buscar el mayor entero que aparece en ambas. Evidentemente basta con buscar la lista de los divisores positivos: si, por ejemplo, $a = 12$ y $b = -18$, los divisores positivos de 12 son 1,2,3,4,6,12 y los de -18 son 1,2,3,6,9,18, con lo que inmediatamente vemos que el máximo común divisor es 6. Este método resulta muy tedioso cuando a o b son grandes, pero afortunadamente existe un método más 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.). Este método se basa en la siguiente observación.

Lema 1.10 *Dados dos enteros a y b se verifica que* mcd $(a, b) =$ 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 dos parejas a y b, y b y r poseen los mismos divisores comunes y, por tanto, tiene el mismo máximo común divisor. ■

El algoritmo de Euclides es usado de forma repetitiva para simplificar el cálculo del máximo común divisor por reducción del tamaño de los enteros sin alterar su máximo común divisor. Supongamos que se tienen dos enteros a y b (no ambos nulos) y que se desea calcular $d =$ mcd (a, b). Si $a = 0$ entonces $d = |b|$, si $b = 0$ entonces $d = |a|$, por lo que sin considerar estos casos triviales, podemos suponer que a y b son ambos no nulos. Como

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

podemos asumir que a y b son ambos positivos. Además, como $\text{mcd}\,(a,b) = \text{mcd}\,(b,a)$ podemos suponer que $a \geq b$ y si despreciamos, por último, el caso trivial $\text{mcd}\,(a,a) = a$ podemos suponer que $a > b$, es decir, que

$$a > b > 0.$$

Utilizamos ahora el algoritmo de la división (Teorema 1.4) para dividir a entre b y escribimos

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

Si $r_1 = 0$ entonces $b \,|\, a$, por lo que $d = b$ y hemos terminado. Si $r_1 \neq 0$ dividimos b entre r_1 y escribimos

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

y repetimos el proceso; como $b > r_1 > r_2 > \cdots \geq 0$ debemos encontrar necesariamente un resto $r_n = 0$ (después de, a lo más, b pasos) y en ese punto finalizamos el proceso. Los dos últimos pasos podemos escribirlos de la forma

$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \qquad \text{con} \qquad 0 < r_{n-1} < r_{n-2},$$

$$r_{n-2} = q_n r_{n-1} + r_n \qquad \text{con} \qquad r_n = 0.$$

Teorema 1.11 *En el proceso de cálculo anterior, $d = r_{n-1}$ (último resto no nulo).*

Demostración. Aplicando el Lema 1.10 a las sucesivas ecuaciones dadas anteriormente para $a, b, r_1, \ldots, r_{n-3}$ observamos que

$$d = \text{mcd}\,(a,b) = \text{mcd}\,(b,r_1) = \text{mcd}\,(r_1,r_2) = \cdots = \text{mcd}\,(r_{n-2},r_{n-1}).$$

La última ecuación $r_{n-2} = q_n r_{n-1}$ prueba que r_{n-1} divide a r_{n-2}, por lo que $\text{mcd}\,(r_{n-2},r_{n-1}) = r_{n-1}$ y, por tanto, $d = r_{n-1}$. ■

Ejemplo 1.4 Para calcular el $\text{mcd}\,(112,70)$, dividimos 112 entre 70 obteniéndose un cociente igual a 1 y un resto $r = 42$.

El Lema 1.10 nos dice que $\text{mcd}\,(112,70) = \text{mcd}\,(70,42)$. Repitiendo ahora este mismo proceso obtenemos:

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

ya que 14 es un divisor de 28 y no existe ningún divisor de 14 mayor que el propio 14. □

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 $r \leftarrow$ el resto de dividir a entre b

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

P4 si no $a \leftarrow b$, $b \leftarrow r$

P5 ir al Paso 2

Ejemplo 1.5 Para calcular $d = \text{mcd}\,(1492, 1066)$ escribimos

$$\begin{aligned} 1492 &= 1 \cdot 1066 + 416 \\ 1066 &= 2 \cdot 426 + 214 \\ 426 &= 1 \cdot 214 + 212 \\ 214 &= 1 \cdot 212 + 2 \\ 212 &= 106 \cdot 2 + 0. \end{aligned}$$

El último resto no nulo es 2, por lo que $d = 2$. □

En muchos casos, el valor de d puede ser identificado antes de obtener un resto nulo: como $d = \text{mcd}\,(a, b) = \text{mcd}\,(b, r_1) = \text{mcd}\,(r_1, r_2) = \ldots$, podemos detener el proceso si conocemos el máximo común divisor de un par de términos consecutivos de la sucesión $a, b, r_1, r_2, \ldots$. Así, en el Ejemplo 1.5 los restos 214 y 212 tiene evidentemente como máximo común divisor al 2, por lo que $d = 2$.

Si nos fijamos en el Ejemplo 1.4 observamos que:

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

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

En general, dados dos enteros a y b, existen otros dos enteros u y v tales que $d = au + bv$.

Una mejora del algoritmo de Euclides y conocida como *Algoritmo extendido de Euclides* permite, no sólo calcular el máximo común divisor d de dos números enteros a y b, sino que nos proporciona los números u y v (que más tarde veremos que no son únicos) de la descomposición $d = au + bv$ que utilizaremos más adelante.

P1 Leer a y b

P2 $m' \leftarrow n \leftarrow 1\ ,\ m \leftarrow n' \leftarrow 0\ ,\ c \leftarrow a\ ,\ d \leftarrow b$

P3 $q \leftarrow \left\lfloor \frac{c}{d} \right\rfloor,\ r \leftarrow c - d \cdot q$

P4 si $r = 0$ entonces FIN $(d = am + bn)$

P5 si no $c \leftarrow d,\ d \leftarrow r,$
$t \leftarrow m',\ m' \leftarrow m,\ m \leftarrow t - qm,$
$t \leftarrow n',\ n' \leftarrow n,\ n \leftarrow t - qn$

P6 ir al Paso 3

Ejemplo 1.6 La Tabla 1.1 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 $b = 551$, obteniéndose que mcd $(1769, 551) = 29$ y además, que podemos expresar este número como:

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

m'	m	n'	n	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

Tabla 1.1: Algoritmo extendido de Euclides aplicado al Ejemplo 1.6. □

En la siguiente sección trataremos de formalizar este resultado.

1.6 La identidad de Bezout

Teorema 1.12 *Si a y b son enteros (no ambos nulos) existen enteros u y v tales que*

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

(Esta ecuación es conocida como *identidad de Bezout*. Veremos más adelante que los valores u y v no quedan unívocamente determinados por a y b.)

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, en la forma

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

expresa d como un múltiplo de r_{n-3} mas otro de 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 un múltiplo de r_{n-4} mas otro de r_{n-3}. Retrocediendo en las ecuaciones del algoritmo podemos ir eliminando sucesivamente $r_{n-3}, r_{n-4}, \ldots$ hasta obtener d como un múltiplo de a mas otro de b, esto es, $d = au + bv$ para algunos enteros u y v. ■

Ejemplo 1.7 En el Ejemplo 1.5 utilizamos el algoritmo de Euclides para calcular d con $a = 1492$ y $b = 1066$. Utilizando las ecuaciones obtenidas en dicho ejemplo obtenemos:

$$\begin{aligned} d &= 2 \\ &= 214 - 1 \cdot 212 \\ &= 214 - 1 \cdot (426 - 1 \cdot 214) \\ &= -1 \cdot 426 + 2 \cdot 214 \\ &= -1 \cdot 426 + 2 \cdot (1066 - 2 \cdot 426) \\ &= 2 \cdot 1066 - 5 \cdot 426 \\ &= 2 \cdot 1066 - 5 \cdot (1492 - 1 \cdot 1066) \\ &= -5 \cdot 1492 + 7 \cdot 1066, \end{aligned}$$

por lo que $u = -5$ y $v = 7$. El siguiente ejercicio prueba que los valores que hemos encontrado para u y v no son únicos. (Más tarde, en el Teorema 1.18 veremos cómo se determinan todos los posibles valores de u y v.) □

Una vez visto cómo se calcula el máximo común divisor de dos enteros, debemos extender el método al cálculo del máximo común divisor de un numero finito de enteros (no todos nulos). El método consiste en repetir el algoritmo de Euclides basándonos en el siguiente resultado, cuya demostración proponemos en forma de ejercicio.

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

Esto reduce el cálculo del máximo común divisor d de k enteros a dos problemas más pequeños: calculamos, en primer lugar, $d_2 = \text{mcd}\,(a_1, a_2)$ y, por consiguiente, $d = \text{mcd}\,(d_2, a_3, \ldots, a_k)$ implicando a dos y $k-1$ enteros respectivamente. Este segundo problema puede reducirse de nuevo calculando $d_3 = \text{mcd}\,(d_2, a_3)$ y, por consiguiente, $d = \text{mcd}\,(d_3, a_4, \ldots, a_k)$ implicando a dos y $k-2$ enteros. Continuando el proceso reducimos el problema a una secuencia de $k-1$ cálculos del máximo común divisor de dos enteros, y resolviendo cada uno de ellos mediante el algoritmo de Euclides: encontramos $d_2 = \text{mcd}\,(a_1, a_2)$, $d_i = \text{mcd}\,(d_{i-1}, a_i)$ para $i = 3, \ldots, k$, y hacemos $d = d_k$.

Ejemplo 1.8 Para hallar $d = \text{mcd}\,(36, 24, 54, 27)$ calculamos en primer lugar $d_2 = \text{mcd}\,(36, 24) = 12$, a continuación $d_3 = \text{mcd}\,(12, 54) = 6$ y, por último, $d = d_4 = \text{mcd}\,(6, 27) = 3$. □

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

El Teorema 1.12 establece que mcd (a, b) puede ser escrito como un múltiplo de a mas otro de b; usando este resultado podemos describir el conjunto de todos los enteros que pueden expresarse de esta forma.

Teorema 1.13 *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, el Corolario 1.7 implica que d divide a c. Recíprocamente, si $c = de$ para algún entero e, escribiendo $d = au + bv$ (ver el Teorema 1.12) 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. ■

Ejemplo 1.9 Vimos en el Ejemplo 1.5 que si $a = 1492$ y $b = 1066$ entonces $d = 2$, por lo que los enteros de la forma $c = 1492x + 1066y$ son los múltiplos de 2.
En el Ejemplo 1.7 se obtuvo que $2 = 1492 \cdot (-5) + 1066 \cdot 7$, por lo que multiplicando ambos miembros por e podemos expresar cualquier entero par $2e$ de la forma $1492x + 1066y$: por ejemplo, $-4 = 1492 \cdot 10 + 1066 \cdot (-14)$. □

Definición 1.5 Dos enteros a y b se dicen *coprimos* (*primos relativos* o *primos entre sí*) si mcd $(a, b) = 1$. Por ejemplo, 10 y 21 son primos entre sí, pero 10 y 12 no lo son. En general, un conjunto de enteros $a_1, a_2, \ldots$ son *coprimos* si mcd $(a_1, a_2, \ldots) = 1$, y son *mutuamente coprimos* si mcd $(a_i, a_j) = 1$ para cualesquiera $i \neq j$. Si son mutuamente coprimos son coprimos (ya que mcd $(a_1, a_2, \ldots) \,|\, \text{mcd}\,(a_i, a_j)$), pero el recíproco es falso: los enteros 6, 10 y 15 son coprimos pero no mutuamente coprimos.

Corolario 1.14 *Dos enteros a y b son coprimos si, y sólo si, existen enteros x e y tales que $ax + by = 1$.*

Demostración. Sea mcd $(a, b) = d$. Si sustituimos $c = 1$ en el Teorema 1.13 vemos que $ax + by = 1$ para algunos $x, y \in \mathbf{Z}$ si, y sólo si, $d \,|\, 1$; es decir, si $d = 1$. ■

Ejemplo 1.10 El hecho de que $10 \cdot (-2) + 21 \cdot 1 = 1$ confirma que 10 y 21 son primos entre sí. □

Corolario 1.15 *Si* mcd $(a, b) = d$

$$\text{mcd}\,(ma, mb) = md$$

para cualquier entero $m > 0$, y

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

Demostración. Por el Teorema 1.13, 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

$$\frac{a}{d} \cdot u + \frac{b}{d} \cdot v = 1,$$

por lo que el Corolario 1.14 implica que a/d y b/d son primos entre sí.

Corolario 1.16 *Sean a y b dos enteros primos entre sí.*

a) Si $a \,|\, c$ y $b \,|\, c \Longrightarrow ab \,|\, c$.

b) Si $a \,|\, bc \Longrightarrow a \,|\, c$.

Demostración.

a) Tenemos que $ax + by = 1, c = ae$ y $c = bf$ para algunos enteros x, y, e y f. Entonces, $c = cax + cby = (bf)ax + (ae)by = ab(fx + ey)$, por lo que $ab \mid c$.

b) Como en (a), $c = cax + cby$. Dado que $a \mid bc$ y $a \mid a$, el Corolario 1.8 implica que $a \mid (cax + cby) = c$ ■

1.7 Mínimo común múltiplo

Definición 1.6 Si a y b son dos enteros, un *múltiplo común* de a y b es un entero c tal que $a \mid c$ y $b \mid c$. Si a y b son ambos no nulos, existen múltiplos comunes positivos (por ejemplo $|ab|$), por lo que el principio de buena ordenación nos asegura la existencia de un *mínimo común múltiplo*, o más concretamente, el menor múltiplo común *positivo*. Este es el único entero positivo m que cumple:

a) $a \mid m$ y $b \mid m$ (ya que m es un múltiplo común), y

b) si $a \mid c$ y $b \mid c$ con $c > 0$, entonces $m \leq c$ (ya que ningún múltiplo común puede ser menor que m).

Usualmente se denota a m como mcm (a, b), o simplemente como $[a, b]$. Por ejemplo, mcm $(15, 10) = 30$, ya que los múltiplos positivos de 15 son $15, 30, 45, \ldots$ y los de 10 son $10, 20, 30, \ldots$. Las propiedades del mínimo común múltiplo pueden deducirse a partir de las del máximo común divisor a través del siguiente resultado.

Teorema 1.17 *Sean a y b dos enteros positivos con $d =$ mcd (a, b) y $m =$ mcm (a, b). Se verifica entonces que*

$$dm = ab.$$

(Como mcd $(a, b) =$ mcd $(|a|, |b|)$ y mcm $(a, b) =$ mcm $(|a|, |b|)$, no supone restricción alguna el suponer $a, b > 0$.)

Demostración. 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 (a) y (b) 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 $a \mid da'b'$ y $b \mid da'b'$, es decir, se satisface la condición (a). En segundo lugar, supongamos que $a \mid c$ y $b \mid c$ con $c > 0$; debemos probar que $da'b' \leq c$. Por el Teorema 1.12 existen enteros u y v tales que $d = au + bv$. Entonces

$$\frac{c}{da'b'} = \frac{cd}{(da')(db')} = \frac{cd}{ab} = \frac{c(au + bv)}{ab} = \frac{c}{b} \cdot u + \frac{c}{a} \cdot v$$

es entero por ser a y b divisores de c; por lo que $da'b' \mid c$ y por tanto (ver el Teorema 1.6–(d)) se tiene que $da'b' \leq c$ como queríamos probar. ■

Ejemplo 1.11 Si $a = 15$ y $b = 10$, entonces $d = 5$ y $m = 30$, por lo que $dm = 150 = ab$ como indica el Teorema 1.17. □

Podemos utilizar el Teorema 1.17 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 1.12 Dado que $\text{mcd}\,(1492, 1066) = 2$ se tiene que

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

1.8 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* $ax + by = c$; utilizaremos algunas de las ideas anteriores para encontrar las soluciones enteras x e y de estas ecuaciones. El siguiente resultado lo dio a conocer el matemático indio Brahmagupta alrededor del año 628:

Teorema 1.18 *Sean a, b y c 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 1.13 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 que

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

en donde dividiendo por d se obtiene que

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0). \tag{1.3}$$

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 (1.3) y, por el Corolario 1.15, es primo con a/d, debe dividir, por el Corolario 1.16–(b) 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 (1.3) 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 $d = \text{mcd}\,(a, b)$, directamente o por el algoritmo 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 $d \,|\, c$ utilizamos el método de la demostración del Teorema 1.12 para encontrar enteros u y v tales que $au + bv = d$; entonces $x_0 = ue$, $y_0 = ve$ es una solución particular de $ax + by = c$.

(4) Utilizamos ahora el Teorema 1.18 para encontrar la solución general x, y de la ecuación.

Ejemplo 1.13 Consideremos la ecuación

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

en la que $a = 1492$, $b = 1066$ y $c = -4$. En el paso (1) usamos el Ejemplo 1.3 para ver que $d = 2$. En el paso (2) comprobamos que d divide a c: en efecto, $c = -2d$, por lo que $e = -2$. En el paso (3), haciendo uso del Ejemplo 1.7 escribimos $d = -5 \cdot 1492 + 7 \cdot 1066$; es decir, $u = -5$ y $v = 7$, por lo que $x_0 = (-5) \cdot (-2) = 10$ e $y_0 = 7 \cdot (-2) = -14$ es una solución particular de la ecuación. Por el Teorema 1.18, la solución general es de la forma

$$x = 10 + \frac{1066n}{2} = 10 + 533n, \quad y = -14 - \frac{1492n}{2} = -14 - 746n \quad (n \in \mathbf{Z}). \quad \square$$

Es frecuente interpretar geométricamente las ecuaciones diofánticas lineales $ax + by = c$. Considerando los valores de x e y como reales, la gráfica de la ecuación es una recta R en el plano xy. Los puntos (x, y) del plano con coordenadas enteras son los *puntos-red enteros*, los vértices de una teselación del plano en cuadrados unitarios. Las parejas de enteros x e y que satisfacen la ecuación corresponden a los puntos-red (x, y) de R; por lo que el Teorema 1.13 asegura que R pasa por algún punto red si, y sólo si, $d \,|\, c$, en cuyo caso pasa por infinitos puntos red, que viene dados por los valores de x e y.

El principal resultado que veremos en lo que resta del capítulo es el Teorema Fundamental de la Aritmética (Teorema 1.22) , 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 (Teorema 1.25) sobre la existencia de infinitos números primos; este resultado es fundamental, ya que a lo largo de este libro, daremos varias demostraciones totalmente diferentes de él para ilustrar diferentes técnicas en la teoría de números. Además de existir infinitos números primos, estos se distribuyen de forma bastante 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.

1.9 Números primos y factorización

Definición 1.7 Un entero $p > 1$ se dice que es *primo* si sus únicos divisores son 1 y el propio p.

Nótese que 1 no es primo. El número primo más pequeño es el 2, y todos los demás primos $(3, 5, 7, 11, \ldots)$ son impares. Un entero $n > 1$ no primo (tal como $4, 6, 8, 9, \ldots$) se dice que es *compuesto*: dichos enteros pueden expresarse de la forma $n = ab$ donde $1 < a < n$ y $1 < b < n$, es decir, donde a y b son *divisores propios* de n.

Lema 1.19 *Sea p primo y sean a y b enteros cualesquiera. Entonces*

$$\text{a)} \begin{cases} p \text{ es un divisor de } a \\ \quad \acute{o} \\ p \text{ y } a \text{ son primos entre sí.} \end{cases} \qquad \text{b) } p \mid ab \Longrightarrow \begin{cases} p \text{ divide a } a \\ \quad \acute{o} \\ p \text{ divide a } b. \end{cases}$$

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) divide a a se tiene que $p \mid a$; si mcd $(a, p) = 1$ los números a y p son primos entre sí.

b) Supongamos que $p \mid ab$. Si p no divide a a, el apartado (a) implica que mcd $(a, p) = 1$. La identidad de Bezout no dice entonces que $1 = au + pv$ para algunos enteros u y v, por lo que $b = aub + pvb$. Como suponemos que $p \mid ab$, divide también a aub y como divide evidentemente a pvb, también divide a b como queríamos probar. ■

Los dos apartados pueden fallar si p no es primo: por ejemplo, si $p = 4$, $a = 6$ y $b = 10$. El Lema 1.19–(b) puede ser generalizado para el producto de cualquier número de factores:

Corolario 1.20 *Si p es primo y p divide a $a_1 \cdots a_k$, entonces p divide a a_i para algún i.*

Demostración. Haremos inducción en k. Si $k = 1$ la hipótesis es que $p \mid a_1$, por lo que la conclusión es automáticamente cierta (para $i = 1$). Supongamos ahora que $k > 1$ 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, $p \mid ab$. Por el Lema 1.19–(b) se tiene que $p \mid a$ o $p \mid b$. En el primero de los casos, la hipótesis de inducción nos dice que $p \mid a_i$ para algún $i = 1, \ldots, k - 1$; en el segundo de los casos $p \mid a_k$. En cualquiera de los casos $p \mid a_i$ para algún i, como se pretendía probar. ■

Como una aplicación del Lema 1.19–(b) consideremos el conjunto de los polinomios con coeficientes enteros. Un polinomio $f(x)$, de dicho tipo, es *reducible* si $f(x) = g(x)h(x)$, donde $h(x)$ y $g(x)$ son polinomios no constantes con coeficientes enteros; en caso contrario, $f(x)$ es *irreducible*.

Teorema 1.21 [Criterio de Eisenstein] *Si $f(x) = a_0 + a_1x + \cdots + a_nx^n$, donde cada $a_i \in \mathbf{Z}$, si p es un primo tal que p divide a $a_0, a_1, \ldots, a_{n-1}$ pero no a a_n y si p^2 no divide a a_0, entonces $f(x)$ es irreducible.*

Demostración. Para probarlo supongamos que $f(x)$ es reducible, es decir, $f(x) = q(x)h(x)$ con $g(x) = b_0 + b_1x + \cdots + b_sx^s$, $h(x) = c_0 + c_1x + \cdots + c_tx^t$ y $s, t \geq 1$. Como $a_0 = b_0c_0$ es divisible por p pero no por p^2, uno y sólo uno entre b_0 y c_0 es divisible por p; trasponiendo $g(x)$ y $h(x)$ 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 $a_n = b_sc_t$; 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 divisor de a_i (ya que $i \leq s = n - t < n$) y de $b_0c_i + \cdots + b_{i-1}c_1$, por lo

que p divide a $b_i c_0$. Entonces, el Lema 1.19–(b) implica que p divide a b_i o a c_0, lo cual es una contradicción, por lo que $f(x)$ debe ser irreducible. ■

Ejemplo 1.14 El polinomio $f(x) = x^3 - 4x + 2$ es irreducible, ya que satisface el criterio de Eisenstein para $p = 2$. □

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, por lo que $n = ab$ 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 $p_1 \mid n$, por lo que el Corolario 1.20 (aplicado a la segunda factorización) implica que

$p_1 \,|\, q_j$ 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 puede requerir *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.

El siguiente resultado parece obvio e intranscendente, pero en posteriores capítulos veremos que puede ser extraordinariamente útil, especialmente para el caso $m = 2$:

Lema 1.23 *Si $a_i, \ldots, a_r$ son enteros positivos primos dos a dos y $a_1 \cdots a_r$ es una potencia m-ésima para algún entero $m \geq 2$, entonces cada a_i es una potencia m-ésima.*

Demostración. De la fórmula dada más arriba para a^m se deduce que un entero positivo es una potencia m-ésima si, y sólo si, el exponente de cada factor primo de su factorización es divisible por m. Si $a = a_1 \cdots a_r$, donde cada los factores a_i son primos dos a dos, cada potencia prima p^e que aparezca en la factorización de cualquiera de los a_i también aparece como la misma potencia de p en la factorización de a; como a es una potencia m-ésima, e es divisible por m, por lo que a_i es también una potencia m-ésima. ■

Por supuesto, es esencial la condición de que $a_1, \ldots, a_r$ sean primos dos a dos ya que, por ejemplo, ni 24 ni 54 son cuadrados perfectos y, sin embargo, su producto $24 \times 54 = 1296 = 36^2$ si lo es.

Podemos utilizar la factorización para generalizar el clásico resultado (conocido por los Pitagóricos en el siglo V a.C.) de que $\sqrt{2}$ es irracional. Un *número racional* es un número real de la forma a/b donde a y b son enteros y $b \neq 0$; todos los demás números reales son *irracionales* . Un *cuadrado perfecto* es un entero de la forma $m = n^2$ donde n es un entero.

Corolario 1.24 *Si un número positivo m no es un cuadrado perfecto, entonces $\sqrt{m}$ es irracional.*

Demostración. Es suficiente con probar el recíproco, es decir, si $\sqrt{m}$ es racional entonces m es un cuadrado perfecto. Supongamos que $\sqrt{m} = a/b$ donde a y b son enteros positivos. Entonces

$$m = a^2/b^2.$$

Si a y b admiten las factorizaciones

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

tenemos que

$$m = p_1^{2e_1-2f_1} \cdots p_k^{2e_k-2f_k}$$

es la factorización de m. Obsérvese que cada primo p_i aparece un número par de veces en dicha factorización y que $e_i - f_i \geq 0$ para cada i, por lo que

$$m = \left(p_1^{e_1-f_1} \cdots p_k^{e_k-f_k}\right)^2$$

es un cuadrado perfecto. ■

1.10 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 1.25 [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. ■

Podemos usar esta demostración para obtener un poco más de información sobre la frecuencia con que aparecen los números primos. Sea p_n el n-ésimo número primo (en orden creciente), es decir, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, y así sucesivamente.

Corolario 1.26 *El n-ésimo primo p_n satisface que $p_n \leq 2^{2^{n-1}}$ para todo $n \geq 1$.*

(Esta estimación es muy débil, ya que en general p_n es significativamente más pequeño que $2^{2^{n-1}}$: por ejemplo $2^{2^3} = 256$, mientras que p_4 sólo es 7. Pronto veremos otras estimaciones mejores.)

Demostración. Utilizaremos la inducción completa en n. El resultado es cierto para $n = 1$, ya que $p_1 = 2 = 2^{2^0}$. Supongamos que el resultado es cierto para cada $n = 1, 2, \ldots, k$. Como en la demostración del Teorema 2.6, $p_1 p_2 \cdots p_k + 1$ debe ser divisible por algún primo p; este primo no puede ser ninguno de los $p_1, p_2, \ldots, p_k$, ya que entonces dividiría a 1 lo cual es imposible. Debe existir entonces un nuevo primo p mayor o igual que el $k+1$-ésimo primo p_{k+1}, es decir

$$\begin{aligned} p_{k+1} \leq p \leq p_1 p_2 \cdots p_k + 1 \leq 2^{2^0} \cdot 2^{2^1} \cdots 2^{2^{k-1}} + 1 &= 2^{1+2+4+\cdots+2^{k-1}} + 1 \\ &= 2^{2^k - 1} + 1 \\ &= \frac{1}{2} \cdot 2^{2^k} + 1 \leq 2^{2^k}. \end{aligned}$$

(Hemos utilizado aquí la hipótesis de inducción, es decir $p_i \leq 2^{2^{i-1}}$ para $i \leq k$, a la vez que la suma de una progresión geométrica $1+2+4+\cdots+2^{k-1} = 2^k - 1$). Esto prueba la desigualdad para $n = k+1$, por lo que por inducción es cierto para cualquier $n \geq 1$. ■

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 $\pi(10) = 4$. Denotemos por $\lg x = \log_2 x$ el logaritmo en base 2 de x definido por $y = \lg x$ si $x = 2^y$ (por ejemplo $\lg 8 = 3$ y $\lg(\frac{1}{2}) = -1$).

Corolario 1.27 $\pi(x) \geq \lfloor \lg(\lg x) \rfloor + 1$.

Demostración. $\lfloor \lg(\lg x) \rfloor + 1$ es el mayor entero n tal que $2^{2^{n-1}} < x$. Por el Corolario 1.26, existen, al menos, n primos $p_1, p_2, \ldots, p_n \leq 2^{2^{n-1}}$. Estos primos son todos menores o iguales a x, por lo que $\pi(x) \geq n = \lfloor \lg(\lg x) \rfloor + 1$. ■

Al igual que el anterior, este resultado es muy débil, y $\pi(x)$ es, en general, mucho mayor que $\lfloor \lg(\lg x) \rfloor + 1$; por ejemplo, si $x = 10^9$ entonces $\lfloor \lg(\lg x) \rfloor + 1 = 5$, mientras que el número de primos $p \leq 10^9$ no es 5 sino, aproximadamente, 5×10^7. Basándose en una extensiva lista de primos, Gauss conjeturó en 1793 que $\pi(x)$ 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

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

(Aquí, $\ln x = \log_e x$ es el logaritmo natural $\int_1^x t^{-1}dt$ de x). Este resultado, conocido como Teorema de los Números Primos, fue probado finalmente por Hadamard y por Vallé Poussin en 1896. Esta demostración escapa de las pretensiones de este curso; ver Hardy y Wright (1979) o Rose (1988), por ejemplo. Uno 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, luego 135 primos entre 1001 y 2000, luego 127 entre 2001 y 3000, y así sucesivamente.

Podemos usar el método de la demostración del Teorema 1.25 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 1.28 *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. ■

También existen infinitos números primos de la forma $4q+1$; sin embargo, la demostración es un poco más sutil, por lo que no la afrontaremos en este curso. (¿Dónde falla el método de la demostración del Teorema 1.28 en este caso?)

Estos resultados son todos casos particulares de un teorema general demostrado por Dirichlet en 1837 sobre números primos en progresión aritmética.

Teorema 1.29 *Si a y b son enteros primos entre sí, existen infinitos números primos de la forma $aq + b$.*

La demostración utiliza técnicas avanzadas, por lo que la omitiremos aquí; puede encontrarse en algunos libros como, por ejemplo, en Apostol (1976). Obsérvese que el teorema falla si a y b tienen máximo común divisor $d > 1$, ya que cualquier entero de la forma $aq + b$ es divisible por d, por lo que, a lo sumo, uno de ellos puede ser primo.

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. Por ejemplo, el intervalo entre primos consecutivos puede ser arbitrariamente grande. 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.

Otra cuestión abierta concerniente a los números primos es la *Conjetura de Goldbach* que dice que cualquier entero par $n \geq 4$ es suma de dos primos: por ejemplo $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$ y así sucesivamente. La evidencia para este resultado es bastante fuerte, sin embargo, el resultado más general en la dirección de dicha conjetura es un teorema de Chen Jing-Run (1973) que dice que cualquier entero par, suficientemente grande, es de la forma $n = p+q$ donde p es primo y q es el producto de, a lo más, dos primos. De manera análoga, Vinogradov prueba en 1973 que cualquier entero impar, suficientemente grande, es la suma de tres primos, por lo que se deduce que cualquier entero par, suficientemente grande, es la suma de, a lo más, cuatro primos.

1.11 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 1.30 *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, entonces es de la forma $2^n q$ para algún $q > 1$ impar. Como el polinomio $f(t) = t^q + 1$ tiene la raíz $t = -1$, es divisible por $t + 1$; además, esta es un factor propio, ya que $q > 1$, por lo que poniendo $t = x^{2^n}$ observamos que el polinomio $g(x) = f(x^{2^n}) = x^m + 1$ tiene el factor propio $x^{2^n} + 1$. Haciendo $x = 2$ vemos que $2^{2^n} + 1$ es un factor propio del entero $g(2) = 2^m + 1$, por lo que no puede ser primo. ■

Los numeros 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 $n \geq 0$. Para $n = 0, \ldots, 4$ los números $F_n = 3, 5, 17, 257, 65537$ con realmente primos pero en 1732 Euler probó que el siguiente número de Fermat

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

es compuesto. 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 1.31 *Distintos números F_n de Fermat son mutuamente primos entre sí.*

Demostración. Sea $d = \text{mcd}\,(F_n, F_{n+k})$ el máximo común divisor de dos números de Fermat F_n y F_{n+k} con $k > 0$. El polinomio $x^{2^k} - 1$ posee la raíz $x = -1$, por lo que es divisible por $x + 1$. Poniendo $x = 2^{2^n}$ vemos que F_n divide a $F_{n+k} - 2$, por lo que d divide a 2 y, por tanto, d es 1 ó 2. Al ser impares todos los numeros de Fermat, se tiene que $d = 1$. ■

Esto nos proporciona otra demostración del Teorema 1.25, ya que se deduce del Lema 1.31 que cualquier conjunto infinito de números de Fermat debe contener infinitos factores primos diferentes.

Teorema 1.32 *Si $m > 1$ y $a^m - 1$ es primo, entonces $a = 2$ y m es primo.*

Los enteros de la forma $2^p - 1$, con p primo, se denominan *números de Mersenne* desde que Mersenne los estudiara en 1644; aquellos que son primos, se denominan *primos de Mersenne*. Para los primos $p = 2, 3, 5, 7$, los números de Mersenne

$$M_p = 3, 7, 31, 127$$

son primos, pero $M_{11} = 2047 = 23 \times 89$, por lo que M_p no es primo para cualquiera que sea el primo p. Hasta ahora han sido encontrados 39 primos de Mersenne. El último conocido fue dado a conocer el 14 de noviembre de 2001 por Michael Cameron y se trata del número $M_{13466917} = 2^{13466917} - 1$ que tiene 4053946 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 1.31, por el que distintos números de Mersenne son coprimos.

1.12 Test de primalidad y factorización

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

(1) ¿Cómo se determina cuando es primo un número entero n?

(2) ¿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 1.33 *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 $1 < p \leq \sqrt{n} < n$ se cumple que n es compuesto. Recíprocamente, si n es compuesto, es $n = ab$ donde $1 < a < n$ y $1 < b < n$; 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 divisible por algún primo $p \leq \sqrt{n}$, el cual también divide a n. ■

Por ejemplo, si queremos ver si 97 es primo, probamos si es divisible por alguno de los primos $p \leq \sqrt{97}$, a saber: 2, 3, 5 y 7. Este método requiere testar si un entero n es divisible por varios primos p. Para ciertos primos

pequeños existen reglas, basadas en propiedades del sistema de numeración decimal. En notación decimal, escribir un número entero positivo n de la forma $a_k a_{k-1} \dots a_1 a_0$, quiere decir que

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$$

donde $a_0, \dots, a_k$ son enteros con $0 \leq a_i \leq 9$ para cualquier i, y $a_k \neq 0$. De aquí podemos deducir que un número es divisible por 2 si, y sólo si, a_0 es divisible por 2, es decir, si $a_0 = 0, 2, 4, 6$ ó 8; de forma análoga, n es divisible por 5 si, y sólo si, $a_0 = 0$ ó 5. Con un poco más de ingenio podemos encontrar test de divisibilidad por 3 y por 11. Si desarrollamos $10^i = (9+1)^i$ por el Teorema del Binomio encontramos un entero de la forma $9q+1$; sustituyendo este resultado para cada i vemos que

$$n = 9m + a_k + a_{k-1} + \cdots + a_1 + a_0$$

para algún entero m, por lo que n es divisible por 3 si, y sólo si, la suma

$$n' = a_k + a_{k-1} + \cdots + a_1 + a_0$$

de sus dígitos es divisible por 3. Por ejemplo, si $n = 21497$, dado que $n' = 2+1+4+9+7 = 23$ no es divisible entre 3, tampoco lo es n. (En general, si no es obvio si n' es divisible entre 3, podemos considerar la suma de sus dígitos $n'' = (n')'$ y repetir el proceso las veces que sea necesario). De manera análoga, poniendo $10^i = (11-1)^i = 11q + (-1)^i$ se puede ver que

$$n = 11m + (-1)^k a_k + (-1)^{k-1} a_{k-1} + \cdots - a_1 + a_0$$

para algún entero m, por lo que n es divisible por 11 si, y sólo si, la suma alternada

$$n^* = (-1)^k a_k + (-1)^{k-1} a_{k-1} + \cdots - a_1 + a_0$$

de sus dígitos, es divisible por 11. Así el número $n = 21497$, dado que $n^* = 2-1+4-9+7 = 3$, no es divisible entre 11. Para primos $p \neq 2, 3, 5$ y 11 debemos dividir n entre p y ver si el resto es 0.

Este método es efectivo para bastantes enteros n 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).

La *criba de Eratóstenes* es 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 $10, 15, 20, \ldots$. 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, aparecen subrayados 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 1.33 implica que todos los elementos no eliminados de la lista en ese momento, han de ser primos).

El segundo problema práctico, 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 si el número es o no primo). 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 algo-

ritmo 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). Un método criptográfico muy efectivo (conocido como sistema de clave pública RSA, debido a sus inventores Rives, Shamir y Adleman, 1978) está basado en el hecho de que es relativamente fácil calcular el producto $n = pq$ de dos primos p y q muy grandes, pero extremadamente difícil el proceso inverso, es decir, obtener p y q a partir de n. Estudiaremos este método con más detalle en el Capítulo 2.

1.13 Ejercicios propuestos

Ejercicio 1.1 Probar que para cualquier entero positivo n, se verifica que

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

Ejercicio 1.2

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.

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

Ejercicio 1.3 Demostrar por inducción que si u_n es la sucesión definida por:

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

entonces, $u_n = 2^n + 1$ para cualquier entero positivo n.

Ejercicio 1.4 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 $\begin{cases} a_1 = 1,\ a_2 = 3 \\ a_n = a_{n-1} + a_{n-2} \quad \forall\, n \geq 3 \end{cases}$

Ejercicio 1.5 Se considera la sucesión definida por

$$\begin{cases} u_0 = 5, \quad u_1 = 12 \\ u_n = 5u_{n-1} - 6u_{n-2} \quad \forall\, n \geq 2 \end{cases}$$

Probar que $u_n > 2(2^n + 3^n) \ \ \forall\, n \geq 0$.

Ejercicio 1.6 ¿Qué restos se pueden obtener al dividir un cuadrado perfecto entre 3?, ¿y entre 5?, ¿y entre 6?

Ejercicio 1.7 ¿Si a divide a b, y c divide a d, debe $a + c$ dividir a $b + d$?

Ejercicio 1.8 Probar o encontrar un contraejemplo a las siguientes implicaciones

a) $a^3 \,|\, b^2 \implies a \,|\, b$

b) $a^2 \,|\, b^3 \implies a \,|\, b$

Ejercicio 1.9 Expresar mcd $(1485, 1745)$ de la forma $1485u + 1745v$.

Ejercicio 1.10 Probar que $c \,|\, a$ y $c \,|\, b$ si, y sólo si, $c \,|$ mcd (a, b).

Ejercicio 1.11 Sea $A = \{(\alpha, \beta) \in \mathbf{Z} \times \mathbf{Z} \ : \ \alpha a + \beta b = d\}$ donde a y b son dos enteros positivos y $d =$ mcd (a, b).

a) Probar que si $(\alpha, \beta) \in A$ entonces, α es primo con β.

b) Probar que si a y b son primos entre sí y los pares (α_1, β_1) y (α_2, β_2) pertenecen a A, existe $k \in \mathbf{Z}$ tal que

$$\alpha_2 = \alpha_1 + kb \qquad \beta_2 = \beta_1 - ka$$

c) Probar que, en general, si $(\alpha_1, \beta_1),\ (\alpha_2, \beta_2) \in A$ existe $k \in \mathbf{Z}$ tal que

$$\alpha_2 = \alpha_1 + k\frac{b}{d} \qquad \beta_2 = \beta_1 - k\frac{a}{d}$$

Ejercicio 1.12 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 $\text{mcd}\,(a_1,\ldots,a_k) = a_1u_1 + \cdots + a_ku_k$. Encontrar dicha expresión cuando $k = 3$ con $a_1 = 1092$, $a_2 = 1155$ y $a_3 = 2002$.

Ejercicio 1.13 Hallar $\text{mcd}\,(910, 780, 286, 195)$.

Ejercicio 1.14 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 1.15 Sean a y b dos números enteros positivos. Demostrar que si $m = \text{mcm}\,(a, b)$, entonces $\text{mcd}\,(m/a, m/b) = 1$

Ejercicio 1.16 ¿Tiene soluciones enteras la ecuación $12x + 21y = 46$? Justifíquese la respuesta.

Ejercicio 1.17 Hallar la solución general de la ecuación $1485x + 1745y = 15$.

Ejercicio 1.18 Encontrar todas las soluciones positivas de la ecuación diofántica lineal $5x + 12y = 71$.

Ejercicio 1.19 Se desean cambiar 5.000 pesetas en dólares y marcos alemanes. Suponiendo que el cambio se estima en 150 pesetas el dólar y 80 pesetas el marco alemán, encontrar todos los posibles cambios que pueden realizarse.

Ejercicio 1.20 Si $a_1, \ldots, a_k$ y c son números enteros, ¿cuándo tiene soluciones enteras $x_1, \ldots, x_k$ la ecuación diofántica $a_1x_1 + \cdots + a_kx_k = c$?

Ejercicio 1.21 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?

Ejercicio 1.22 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 100000 ptas. cada vez que lo emite y CTV2 sólo cobra 10000?

Ejercicio 1.23 Probar que si a y b son enteros con $b \neq 0$, existe un único par de enteros q y r tales que $a = qb + r$ y $-|b|/2 < r \leq |b|/2$. Utilizar dicho resultado para dar un algoritmo alternativo al de Euclides para el cálculo del máximo común divisor (*algoritmo del mínimo resto*).

Ejercicio 1.24 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.

Ejercicio 1.25 Probar que si a y b son enteros positivos primos entre sí, cualquier entero $c \geq ab$ tiene la forma $ax + by$ donde x e y son enteros no negativos. Probar que el entero $ab - a - b$ no tiene esta forma.

Ejercicio 1.26 Probar que si p es primo y $p \,|\, a^k$, entonces $p \,|\, a$ y, por tanto, $p^k \,|\, a^k$; ¿es también válido si p es compuesto?

Ejercicio 1.27 Aplicar el criterio de Eisenstein para probar que el polinomio $P(x) = x^3 - 4x + 2$ es irreducible.

Ejercicio 1.28 Probar que el polinomio $P(x) = x^2 + x + 1$ es irreducible. ¿Se pude aplicar, en este caso, el criterio de Eisenstein?

Ejercicio 1.29 ¿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 $(a^2, p^2) = p^2$.

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

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

d) Si mcd $(a, p^2) = p$ entonces mcd $(a + p, p^2) = p$.

Ejercicio 1.30 Probar que cualquier número primo $p \neq 3$ es de la forma $3q + 1$ ó $3q + 2$ para algún entero q. Probar que existen infinitos primos de la forma $3q + 2$.

Ejercicio 1.31 Encontrar cinco enteros compuestos consecutivos. Probar que para cada entero $k \geq 1$ existe una secuencia de k enteros compuestos consecutivos.

Ejercicio 1.32 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 1.33 Probar que si $m > 1$ y $a^m - 1$ es primo, entonces $a = 2$ y m es primo.

Ejercicio 1.34 Usar la criba de Eratóstenes para hallar todos los primos menores que 100.

Ejercicio 1.35 Evaluar el número de Mersenne $M_{13} = 2^{13} - 1$. ¿Es primo?

Ejercicio 1.36 Utilizar un ordenador, o una calculadora programable, para factorizar 3992003. (¡A mano podrían tardarse varios años!).

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

Ejercicio 1.38 ¿Cuál es la relación entre el número de ceros en que termina la expresión decimal de un entero n y su descomposición en factores primos? Encontrar el correspondiente resultado para la expresión de n en base b (donde escribimos $n = \sum_{i=0}^{k} a_i b^i$ con $0 \leq a_i < b$).

Ejercicio 1.39 Probar que si $p > 1$ y p divide a $(p - 1)! + 1$, entonces p es primo.

Ejercicio 1.40 Se consideran los números de Fermat $F_n = 2^{2^n} + 1$. Probar que para cualquier $n \geq 1$ se verifica que

$$F_0 F_1 \cdots F_{n-1} = F_n - 2.$$

Ejercicio 1.41 Usar la identidad $2^{rs}-1 = (2^r-1)(2^{(s-1)r}+2^{(s-2)r}+\cdots+2^r+1)$ para demostrar que si $2^n - 1$ es primo entonces n es primo. Encontrar un contraejemplo a la afirmación recíproca.

Ejercicio 1.42 Demostrar que todo número primo mayor que 3 es de la forma $6n + 1$ o $6n + 5$.

Ejercicio 1.43 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

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

Ejercicio 1.44 ¿En cuántos ceros termina la expresión decimal de 1000!?

Ejercicio 1.45 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 del Resto y sus generalizaciones juegan un importante papel.

El interés de este tema para un estudiante de Informática, independientemente de los problemas planteados, responde a que cuando se utiliza una máquina binaria, supongamos de 8 bits, ésta trabaja con registros de memoria compuestos de 8 casillas para almacenar ceros y unos. Cuando tiene las ocho ocupadas por unos y se suma 1 convierte todas sus casillas en ceros y el uno que debería obtenerse a la izquierda se pierde por no tener capacidad para almacenarlo, por lo que para dicha máquina $11111111 + 1 = 0$ es decir, $255 + 1 = 0$ o lo que es lo mismo, para la máquina es $256 = 0$. Esto se debe a que una máquina binaria trabaja con aritmética modular y no con aritmética entera.

2.1 Aritmética modular

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 Sea n un entero positivo y sean a y b dos enteros cualesquiera. Se dice que a es *congruente con* b *módulo* n, o que a es un *resto de* 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. (Escribiremos sólo $a \equiv b$ cuando el valor de n se sobrentienda). Para ser más preciso, utilizando la notación del algoritmo de la división (Teorema 1.4) para expresar $a = qn+r$ con $0 \leq r < n$ y $b = q'n+r'$ con $0 \leq r' < n$ podemos decir que $a \equiv b \pmod{n}$ si, y sólo si, $r = r'$. Así, por ejemplo, $100 \equiv 2 \pmod{7}$ en el Ejemplo 2.1 y $22051946 \equiv 46 \equiv 2 \pmod{4}$ en el Ejemplo 2.2. De igual forma, utilizaremos la notación $a \not\equiv b \pmod{n}$ para denotar que a y b no son congruentes módulo n, es decir, que dan diferentes restos al dividirlos entre n. Nuestro primer resultado viene a dar una definición alternativa de congruencia módulo n.

Lema 2.1 *Para cualquier entero dado $n \geq 1$ se tiene que $a \equiv b \pmod{n}$ si, y sólo si, $n|(a-b)$.*

Demostración. Expresando $a = qn + r$ y $b = q'n + r'$ como hemos hecho más arriba, tenemos que $a - b = (q - q')n + (r - r')$ con $-n < r - r' < n$. Si $a \equiv b \pmod{n}$ entonces $r = r'$, por lo que $r - r' = 0$ y $a - b = (q - q')n$, por lo que es divisible por n. Recíprocamente, si n divide a $a - b$ entonces divide a $(a - b) - (q - q')n = r - r'$; como el único entero, estrictamente contenido entre $-n$ y n, que es divisible por n es 0, se tiene que $r - r' = 0$, de donde $r = r'$ y, por tanto, $a \equiv b \pmod{n}$. ■

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

Lema 2.2 *Para cualquier entero fijo $n \geq 1$ se verifican las propiedades:*

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

b) Simétrica: $a \equiv b \pmod{n} \Longrightarrow a \equiv b \pmod{n}$*;*

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

Demostración.

a) Se verifica que $n \,|\, (a - a)$ cualquiera que sea a.

b) Si $n \,|\, (a - b)$ entonces $n \,|\, (b - a)$.

c) Si $n \,|\, (a - b)$ y $n \,|\, (b - c)$ entonces $n \,|\, (a - b) + (b - c) = a - c$. ■

Estas tres propiedades definen una *relación de equivalencia* , por lo que el Lema 2.2 prueba que, para cada entero n, la congruencia módulo n es una relación de equivalencia en $\mathbf{Z}$. Queda así particionado $\mathbf{Z}$ en clases de equivalencia disjuntas; las *clases de congruencia* o *clases de equivalencia*

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

para $a \in \mathbf{Z}$. (Si se quiere hacer espacial énfasis en el valor de n que se está utilizando, pondremos $[a]_n$). Cada clase corresponde a uno de los n posibles

restos $r = 0, 1, \ldots, n-1$ de la división entre n, por lo que existen n clases de congruencia. Estas son

$$\begin{aligned}
[0] &= \{\ldots, -2n, -n, 0, n, 2n, \ldots,\} \\
[1] &= \{\ldots, 1-2n, 1-n, 1, 1+n, 1+2n, \ldots,\} \\
&\vdots \\
[n-1] &= \{\ldots, -n-1, -1, n-1, 2n-1, 3n-1, \ldots,\}
\end{aligned}$$

No existen más clases diferentes de ellas, así, por ejemplo

$$[n] = \{\ldots, -n, 0, n, 2n, 3n, \ldots\} = [0]$$

De forma más general, se tiene que

$$[a] = [b] \quad \text{si, y sólo si,} \quad a \equiv b \pmod{n}$$

Cuando $n = 1$ todos los enteros son congruentes unos con otros, es decir, sólo existe una clase de congruencia que coincide con $\mathbf{Z}$. Cuando $n = 2$ se tienen dos clases, la clase $[0] = [0]_2$ y la $[1] = [1]_2$ consistentes en los enteros pares y los impares respectivamente. Podemos interpretar el Teorema 1.28 como una aseveración de que existen infinitos números primos $p \equiv 3 \pmod{4}$, es decir, la clase $[3]_4$ contiene infinitos números primos.

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. Nuestra próxima meta es estudiar cómo operar con las clases de congruencia, de tal forma que $\mathbf{Z}_n$ sea un sistema numérico con propiedades similares a las de $\mathbf{Z}$. Hacemos uso de la suma, la resta y el producto en $\mathbf{Z}$ para definir las correspondientes operaciones con las clases de congruencias en $\mathbf{Z}_n$. Si $[a]$ y $[b]$ son elementos de $\mathbf{Z}_n$ (es decir, clases de congruencia módulo n), definimos su suma, diferencia y producto como las clases

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

que contienen a los enteros $a + b$, $a - b$ y ab respectivamente. (Dejaremos la cuestión de la división para el final; la dificultad se debe a que si a y b son

enteros, a/b puede no serlo, en cuyo caso no existe la clase de congruencia $[a/b]$.

Antes de continuar debemos probar que las tres operaciones están bien definidas, en el sentido de que el lado derecho de les tres ecuaciones que las definen dependen 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. Con más precisión, debemos probar que si $[a] = [a']$ y $[b] = [b']$ entonces $[a + b] = [a' + b']$, $[a - b] = [a' - b']$ y $[ab] = [a'b']$. Ello se sigue inmediatamente del siguiente resultado:

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. Si $a' \equiv a$ entonces $a' = a + kn$ para algún entero k y análogamente se tiene que $b' = b + ln$ para algún entero l; entonces $a' \pm b' = (a \pm b) + (k \pm l)n \equiv a \pm b$, y $a'b' = ab + (al + bk + kln)n \equiv ab$. ■

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. En particular, si repetimos las definiciones de suma y producto podemos definir sumas finitas, productos y potencias de clases en $\mathbf{Z}_n$ por

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

para cualquier entero $k \geq 2$.

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 elementos b y b' de la misma clase $[b]$, a saber, $b = 1$ y $b' = 4$. Esto es debido a que $a' \equiv a$ y $b' \equiv b$ *no* implica que $a^b \equiv a'^{b'}$, por lo que la exponencial de clases de congruencias no está bien definida. 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.

Un conjunto de n enteros que contiene a un representante de cada una de las n clases de congruencia en $\mathbf{Z}_n$ se denomina *conjunto completo de restos módulo* n. Una adecuada selección de dicho conjunto puede simplificar los cálculos considerablemente. Una selección adecuada la proporciona el algoritmo de la división (Teorema 1.4): podemos dividir cualquier entero a entre n y expresar $a = qn + r$ para algún único r que satisface $0 \leq r < n$; por lo que cada clase $[a] \in \mathbf{Z}_n$ contiene a un único $r = 0, 1, \ldots, n-1$, por lo que estos n enteros forman un conjunto completo de restos módulo n. La mayoría de las veces, estos son los restos más convenientes de usar, pero algunas veces es mejor sustituir el Teorema 1.4 con el Ejercicio 1.23 del Capítulo 1 tomando un resto r que satisfaga $-n/2 < r \leq n/2$. Estos restos son los que tienen menor valor absoluto y se denominan *menores restos absolutos módulo* n; cuando n es impar estos son $0, \pm 1, \pm 2, \ldots, \pm(n-1)/2$, y cuando n es par son $0, \pm 1, \pm 2, \ldots, \pm(n-2)/2, \pm n/2$. El siguiente cálculo ilustra los conjuntos completos de restos.

Ejemplo 2.3 Calculemos el menor resto no negativo de $28 \times 33 \bmod 35$. Usando los menores restos absolutos $\bmod 35$ se tiene que $28 \equiv -7$ y $33 \equiv -2$, por lo que el Lema 2.3 implica que $28 \times 33 \equiv (-7) \times (-2) \equiv 14$. Como $0 \leq 14 < 35$ se deduce que 14 es el menor resto, no negativo, requerido. □

Ejemplo 2.4 Calcular el menor resto absoluto de $15 \times 59 \bmod 75$. Tenemos que $15 \times 59 \equiv 15 \times (-16)$, y una forma sencilla de evaluarlo es realizar la multiplicación en varios pasos y reduciendo el producto $\pmod{75}$ en cada uno de ellos. De este modo

$$15 \times (-16) = 15 \times (-4) \times 4 = (-60) \times 4 \equiv 15 \times 4 = 60 \equiv -15,$$

y dado que $-75/2 < -15 \leq 75/2$, el resto requerido es -15. □

Ejemplo 2.5 Calculemos el menor resto no negativo de $3^8 \bmod 13$. De nuevo lo realizaremos en varios pasos, reduciendo $\bmod 13$ siempre que sea posible:

$$3^2 = 9 \equiv -4,$$

por lo que

$$3^4 = (3^2)^2 \equiv (-4)^2 = 16 \equiv 3,$$

y, por tanto,

$$3^8 = (3^4)^2 \equiv 3^2 = 9,$$

por lo que el resto requerido es 9. □

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 2.6 Probar que $a(a+1)(2a+1)$ es divisible por 6 cualquiera que sea el entero a. Tomando el menor resto absoluto (mod 6) vemos que $a \equiv 0, \pm 1, \pm 2$ ó 3. Si $a \equiv 0$ entonces $a(a+1)(2a+1) \equiv 0 \cdot 1 \cdot 1 = 0$, si $a \equiv 1$ entonces $a(a+1)(2a+1) \equiv 1 \cdot 2 \cdot 3 = 6 \equiv 0$, y cálculos similares (que debe realizar el lector) prueban que $a(a+1)(2a+1) \equiv 0$ en los otros cuatro casos, por lo que $6 \mid a(a+1)(2a+1)$ cualquiera que sea a. □

Una única congruencia mod n puede ser reemplazada, en algunos casos, por un sistema de congruencias mod p^e para las distintas potencias de primos p^e que dividen a n (y estas son, a menudo, más fáciles de obtener que la congruencia original):

Teorema 2.4 *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 se tiene que $a \equiv b \pmod{n}$ si, y sólo si, $a \equiv b \pmod{p_i^{e_i}}$ para cada $i = 1, \ldots, k$.

Es bastante fácil probarlo directamente (hágase uso del Corolario 1.16), pero lo deduciremos más tarde en éste capítulo como un corolario del Teorema Chino del Resto, que trata de sistemas de congruencias en términos más generales.

Una vez visto cómo sumar, restar y multiplicar clases de congruencias, podemos ver cómo combinar estas operaciones para formar polinomios.

Lema 2.5 *Sea $f(x)$ un polinomio con coeficientes enteros, y sea $n \geq 1$. Si $a \equiv b \pmod{n}$ entonces $f(a) \equiv f(b) \pmod{n}$.*

Demostración. Escribimos $f(x) = c_0 + c_1x + \cdots + c_kx^k$ donde cada $c_i \in \mathbf{Z}$. Si $a \equiv b \pmod{n}$ entonces la utilización reiterada del Lema 2.3 implica que $a^i \equiv b^i$ para cualquier $i \geq 0$, por lo que $c_ia^i \equiv c_ib^i$ para cualquier i y, por tanto, $f(a) = \sum c_ia^i \equiv \sum c_ib^i = f(b)$. ■

Para ilustrarlo, observemos el Ejemplo 2.6 poniendo $f(x) = x(x+1)(2x+2) = 2x^3 + 3x^2 + x$ y $n = 6$; donde podemos usar el hecho de que si $a \equiv 0, \pm1, \pm2$ ó 3 entonces $f(a) \equiv f(0), f(\pm1), f(\pm2)$ o $f(3)$ respectivamente, y todos los casos pueden verse fácilmente que son congruentes con 0 módulo 6.

Supongamos que un polinomio $f(x)$, con coeficientes enteros, tiene una raíz entera $x = a \in \mathbf{Z}$, es decir, que $f(a) = 0$. Entonces $f(a) \equiv 0 \pmod{n}$ para cualquier entero $n \geq 1$. Podemos, a menudo, utilizar el recíproco para probar que ciertos polinomios carecen de raíces enteras: si existe un entero $n \geq 1$ para el que la congruencia $f(x) \equiv 0 \pmod{n}$ no tiene soluciones x. Si n es pequeño podemos probar si $f(x) \equiv 0 \pmod{n}$ admite alguna solución simplemente evaluando $f(x_1), \ldots, f(x_n)$ donde $x_1, \ldots, x_n$ forman un conjunto completo de restos mod n; cada $x \in \mathbf{Z}$ es congruente a algún x_i, por lo que el Lema 2.5 implica que $f(x) \equiv f(x_i)$, y podemos determinar si algún $f(x_1), \ldots, f(x_n)$ es divisible por n.

Ejemplo 2.7 Probemos que el polinomio $f(x) = x^5 - x^2 + x - 3$ no tiene raíces enteras. Para ello hagamos $n = 4$ (una opción que explicaremos más tarde) y consideremos la congruencia

$$f(x) = x^5 - x^2 + x - 3 \equiv 0 \pmod{4}.$$

Utilizando los menores restos absolutos $0, \pm1$ y 2, como un conjunto completo de restos mod 4, encontramos que

$$f(0) = -3, \quad f(1) = -2, \quad f(-1) = -6 \quad \text{y} \quad f(2) = 27.$$

Ninguno de esos valores es divisible por 4, por lo que $f(x) \equiv 0 \pmod{4}$ no tiene soluciones y, por tanto, el polinomio $f(x)$ carece de raíces enteras. □

La razón por la que tomamos $n = 4$ en este ejemplo es la siguiente: se puede probar fácilmente que para cada $n < 4$ la congruencia $f(x) \equiv 0 \pmod{n}$ *tiene* una solución $x \in \mathbf{Z}$, aunque la ecuación $f(x) = 0$ no la tiene; entonces 4 es el menor valor de n para el que el método es efectivo. En general, la correcta selección de n es un problema de insistencia, experiencia o simplemente de tanteo: si un valor de n falla en la prueba de que un polinomio no tiene raíces enteras, como ocurrió anteriormente (en ningún caso debemos asumir que existe una raíz entera); debemos probar más valores y, si estos también fallan, entonces surge la posibilidad real de que pueda existir una raíz entera.

Ejemplo 2.8 Desafortunadamente, el método utilizado en el Ejemplo 2.7 no es siempre lo suficientemente fuerte como para probar la no existencia de raíces enteras. Por ejemplo, el polinomio

$$f(x) = (x^2 - 13)(x^2 - 17)(x^2 - 221)$$

claramente no tiene raíces enteras: de hecho, como 13, 17 y 221$= (13 \times 17)$ no son cuadrados perfectos, las raíces $\pm\sqrt{13}$, $\pm\sqrt{17}$ y $\pm\sqrt{221}$ son todas irracionales por el Corolario 1.24. Sin embargo, se puede probar (nosotros no lo haremos) que para cualquier entero $n \geq 1$ existe una solución de $f(x) \equiv 0 \pmod{n}$, por tanto, en este caso, no existe ninguna elección satisfactoria de n para el método de las congruencias. □

Como una segunda aplicación del Lema 2.5, consideraremos valores primos de polinomios. El polinomio

$$f(x) = x^2 + x + 41$$

tiene la propiedad de que $f(x)$ 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 si existen polinomios $f(x)$ tales que $f(x)$ sea primo para cualquier valor de x. Aparte de los ejemplos triviales de polinomios constantes $f(x) = p$ (p primo) no existe ninguno.

Teorema 2.6 *No existen polinomios no constantes $f(x)$, con coeficientes enteros, tales que $f(x)$ sea primo para todos los enteros x.*

Demostración. Supongamos que $f(x)$ es primo para cualquier entero x y que no es constante. Si elegimos un entero a, entonces $f(a)$ es un primo p. Para cada $b \equiv a \pmod{p}$, el Lema 2.5 implica que $f(b) \equiv f(a) \pmod{p}$, por lo que $f(b) \equiv 0 \pmod{p}$ y, por tanto, p divide a $f(b)$. Por nuestra hipótesis, $f(b)$ es primo, por lo que $f(b) = p$. Como existen infinitos enteros $b \equiv a \pmod{p}$, el polinomio $g(x) = f(x) - p$ tiene infinitas raíces. Sin embargo, esto no es posible: teniendo grado $d \geq 1$, $g(x)$ puede tener, a lo sumo, d raíces, por lo que tales polinomios $f(x)$ no existen. ■

El Teorema 1.29 prueba que si a y b son primos entre sí, entonces el polinomio lineal $f(x) = ax + b$ toma infinitos valores primos, pero no se conoce ningún polinomio $f(x)$ de grado $d \geq 2$, tal como $x^2 + 1$, que tenga esta propiedad. Existen polinomios en *varias* variables $f(x_1, \ldots, x_m)$ cuyos valores positivos coincide con el conjunto de primos cuando el rango $x_1, \ldots, x_m$ actúa sobre los enteros positivos, pero desgraciadamente los ejemplos conocidos son demasiado complicados.

2.1.1 Criterios de divisibilidad

Una aplicación directa de relación de congruencia es la obtención de criterios de divisibilidad. Así, por ejemplo, podemos obtener un criterio para conocer si un entero n es divisible por 9 sin necesidad de realizar la división.

Ejemplo 2.9 En efecto: sea $x = x_n x_{n-1} \dots x_1 x_0$ un número entero positivo en el que el dígito x_i representa el cifra que ocupa el lugar $i+1$-ésimo de su representación, es decir,

$$x = x_n 10^n + x_{n-1} 10^{n-1} \cdots x_2 10^2 + x_1 10 + x_0 = \sum_{i=0}^{n} x_i 10^i$$

Como $10^n \equiv 1 \pmod 9$ $\forall n \in \mathbf{N} \Rightarrow x_i 10^i \equiv x_i \pmod 9$ y por tanto,

$$x = \sum_{i=0}^{n} x_i 10^i \equiv \sum_{i=0}^{n} x_i \pmod 9.$$

Esto nos dice que un número es divisible por 9 si, y sólo si, lo es la suma de sus cifras. □

2.2 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 1.18 al lenguaje de las congruencias, se tiene:

Teorema 2.7 *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 1.18 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 2.10 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 2.11 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 2.8 *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 2.7. ■

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 2.12 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 2.10, 2.11 y 2.12 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 algoritmo para ello, basado en el Teorema 2.7, pero primero necesitamos algunos resultados previos que ayudan a simplificar el problema.

Lema 2.9

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

$$ax \equiv b \pmod{n} \quad \textit{si, y sólo si,} \quad a'x \equiv b' \pmod{n'}.$$

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

$$ax \equiv b \pmod{n} \quad \textit{si, y sólo si,} \quad a'x \equiv b' \pmod{n}.$$

Demostración.

a) Tenemos que $ax \equiv b \pmod{n}$ si, y sólo si, $ax - b = qn$ para algún entero q; dividiendo por m vemos que esto es equivalente a $a'x - b' = qn'$, es decir, a $a'x \equiv b' \pmod{n'}$.

b) Si $ax \equiv b \pmod{n}$ entonces, como en el apartado anterior, tenemos que $ax - b = qn$ y de ahí que $a'x - b' = qn/m$; en particular, m divide a qn. Como m es un divisor de a, el cual es primo con n, m también es primo con n y, por tanto, m debe dividir a q según el Corolario 1.16(b). 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 que $ax - b = mq'n$ y, por tanto, $ax \equiv b \pmod{n}$. ■

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 algoritmo para resolver la congruencia lineal $ax \equiv b \pmod{n}$. Para comprender mejor cada paso es útil ir aplicando dicho algoritmo a la congruencia $10x \equiv 6 \pmod{14}$; una vez finalizado puede comprobar su resultado con el que damos en el Ejemplo 2.13.

Algoritmo de resolución

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

El Teorema 2.7 nos da la solución general una vez conocida una solución particular x_0, por lo que nos centraremos en dar un método para hallar x_0. La estrategia general es reducir $|a|$ hasta $a = \pm 1$ ya que, en este caso, la solución $x_0 = \pm b$ es trivial.

Paso 2 Como d es un divisor de a, b y n, el Lema 2.9(a) implica que podemos reemplazar la congruencia original por

$$a'x \equiv b' \pmod{n'},$$

donde $a' = a/d$, $b' = b/d$ y $n' = n/d$. Por el Corolario 1.15, a' y n' son primos entre sí.

Paso 3 Podemos ahora hacer uso del Lema 2.9(b) para dividir esta nueva congruencia entre $m = \text{mcd}\,(a', b')$ para obtener

$$a''x \equiv b'' \pmod{n'}$$

donde $a'' = a'/m$ es primo con $b'' = b'/m$ y con n'. Si $a'' = \pm 1$, $x_0 = \pm b''$ es la solución buscada. En caso contrario vamos al paso 4.

Paso 4 Observando que

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

somos capaces de reemplazar b'' por alguno de sus congruentes $b''' = b'' + kn'$ de tal forma que $\text{mcd}\,(a'', b''') > 1$; aplicando ahora el paso 3 a la congruencia $a''x \equiv b'''$ (mod n') podemos reducir $|a''|$. Una alternativa a este paso es multiplicar, por una constante adecuada c, para obtener $ca'' \equiv cb''$ (mod n'); si c es adecuada para que el resto de menor valor absoluto a''' de ca'' satisfaga que $|a'''| < |a''|$, hemos reducido así $|a''|$ para obtener la congruencia lineal $a'''x \equiv b'''$ (mod n') con $b''' = cb''$.

Una combinación de los métodos del paso 4 puede, eventualmente, reducir a hasta ± 1, en cuyo caso puede obtenerse la solución x_0; el Teorema 2.7 nos dará la solución general.

Ejemplo 2.13 Consideremos la congruencia

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

El paso 1 nos dice que $\text{mcd}\,(10, 14) = 2$ el cual divide a 6 y, por tanto, existe solución. Si x_0 es una solución, la solución general es $x = x_0 + (14/2)t = x_0 + 7t$, donde $t \in \mathbf{Z}$; estas constituyen las clases $[x_0]$ y $[x_0+7]$ en $\mathbf{Z}_{14}$. Para encontrar x_0 utilizamos el paso 2: dividimos la congruencia original entre $\text{mcd}\,(10, 14) = 2$ para obtener

$$5x \equiv 3 \pmod{7}.$$

Como $\text{mcd}\,(5, 3) = 1$, el paso 3 no tiene efecto, por lo que pasamos al paso 4. Obsérvese que $3 \equiv 10 \pmod{7}$, siendo 10 divisible por 5, por lo que reemplazamos la congruencia por

$$5x \equiv 10 \pmod{7}$$

y dividimos por 5 (que es primo con 7), con lo que

$$x \equiv 2 \pmod{7}.$$

Por tanto, $x_0 = 2$ es una solución y la solución general es de la forma

$$x = 2 + 7t \quad (t \in \mathbf{Z})$$ □

Ejemplo 2.14 Consideremos la congruencia

$$4x \equiv 13 \pmod{47}.$$

El paso 1 nos dice que $\text{mcd}\,(4, 47) = 1$ el cual divide a 13 y, por tanto, la congruencia tiene solución. Si x_0 es una solución, la solución general es $x = x_0 + 47t$ donde $t \in \mathbf{Z}$, constituyendo una única clase $[x_0]$ en $\mathbf{Z}_{47}$. Como $\text{mcd}\,(4, 47) = 1$, el paso 2 no produce ningún efecto, por lo que nos vamos al paso 3. Dado que $\text{mcd}\,(4, 13) = 1$ el paso 3 tampoco produce efecto alguno, por lo que nos vamos al paso 4. Podemos utilizar el método aplicado en el ejemplo anterior, pero vamos a ilustrar la otra técnica descrita en el paso 4; obsérvese que $4 \times 12 = 48 \equiv 1 \pmod{47}$, por lo que multiplicando por 12 obtenemos

$$48x \equiv 12 \times 13 \pmod{47},$$

es decir

$$x \equiv 3 \times 4 \times 13 \equiv 3 \times 52 \equiv 3 \times 5 \equiv 15 \pmod{47}.$$

En este caso $x_0 = 15$ y la solución general viene dada por $x = 15 + 47t$. □

2.3 El Teorema Chino del Resto

Estudiaremos ahora soluciones de sistemas de congruencias lineales. En el siglo I el matemático chino Sun-Tsu 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 del resto*, da una muy satisfactoria solución a este tipo de problemas.

Teorema 2.10 [Teorema Chino del Resto] *Sean $n_1, n_2, \ldots, n_k$ enteros positivos tales que* 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. Sean $c_i = n/n_i = n_1 \cdots n_{i-1} n_{i+1} \cdots n_k$ para cada $i = 1, \ldots, k$. Como cada uno de los factores n_j $(j \neq i)$ es primo con n_i, también lo es con c_i. El Corolario 2.8 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. Para verlo, obsérvese que cada c_j (diferente a c_i) es divisible por n_i, por lo que $a_j c_j d_j \equiv 0$ y, por tanto, $x_0 \equiv a_i c_i d_i \pmod{n_i}$; ahora $c_i d_i \equiv 1$, por elección de d_i, por lo que $x_o \equiv a_i$ como se requería. Así pues, x_0 es una solución del sistema de congruencias 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, por lo que cada n_i divide a $x - x_0$. Como $n_1, \ldots, n_k$ son mutuamente primos entre sí, utilizando reiteradamente el Corolario 1.16(a) probamos que su producto n también divide a $x - x_0$, por lo que $x \equiv x_0 \pmod{n}$. ■

Comentarios

1 La demostración del Teorema 2.4, que pospusimos para más tarde, se sigue ahora inmediatamente: dado $n = p_1^{e_1} \cdots p_k^{e_k}$, hacemos $n_i = p_i^{e_i}$ para cada $i = 1, \ldots, k$, por lo que $n_1, \ldots, n_k$ son mutuamente primos entre sí y de producto n; el Teorema Chino del Resto implica además que las soluciones del sistema de congruencias $x \equiv b \pmod{n_i}$ constituyen una única clase de congruencia módulo n; claramente b es una solución, por lo que dichas congruencias son equivalentes a $x \equiv b \pmod{n}$.

2 Obsérvese que la demostración del Teorema Chino del Resto no sólo prueba que existe una solución para el sistema de congruencias; también nos da una fórmula para la solución particular x_0 y, por tanto, la solución general $x = x_0 + nt$ $(t \in \mathbf{Z})$.

Ejemplo 2.15 En nuestro problema original

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

tenemos que $n_1 = 3$, $n_2 = 5$ y $n_3 = 7$, por lo que $n = 105$, $c_1 = 35$, $c_2 = 21$ y $c_3 = 15$. Necesitamos encontrar, en primer lugar, una solución $x = d_1$ de $c_1 x \equiv 1 \pmod{n_1}$ o, lo que es lo mismo, de $35x \equiv 1 \pmod{3}$; que es equivalente a $-x \equiv 1 \pmod{3}$, por lo que, por ejemplo, $x = d_1 = -1$. De forma análoga $c_2 x \equiv 1 \pmod{n_2}$ viene dada por $21x \equiv 1 \pmod{5}$, esto es, $x \equiv 1 \pmod{5}$, por lo que $x = d_2 = 1$, por último, $c_3 x \equiv 1 \pmod{n_3}$ es $15x \equiv 1 \pmod{7}$ equivalente a $x \equiv 1 \pmod{7}$ y, por tanto, $x = d_3 = 1$. Por supuesto, pueden hacerse diferentes elecciones de los d_i y obtener diferentes valores de x_0, pero todos ellos pertenecen a la misma clase de las soluciones módulo 105. Tenemos ahora que

$$x_0 = a_1 c_1 d_1 + a_2 c_2 d_2 + a_3 c_3 d_3 = 2 \cdot 35 \cdot (-1) + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 23,$$

por lo que las soluciones forman la clase de congruencia [23] módulo 105, es decir, la solución general es $x = 23 + 105t$ $(t \in \mathbf{Z})$. □

Podemos utilizar también el Teorema Chino del Resto como base para un segundo método de resolución de sistemas de congruencias lineales, el cual es menos directo pero más eficiente.

Algoritmo de resolución de sistemas de congruencias lineales

Comenzamos buscando una solución $x = x_1$ de una de las congruencias. Usualmente se comienza por la congruencia que tiene mayor módulo, en el Ejemplo 2.15 comenzamos por $x \equiv 2 \pmod 7$; la cual tiene, obviamente, la solución $x = 2$. Las restantes soluciones de la congruencia se encuentran añadiendo o restando múltiplos de 7 y, entre ellas, podemos encontrar un entero x_2 de la forma $x_2 = x_1 + 7t$ que también verifique la segunda congruencia, es decir, que $x_2 \equiv 3 \pmod 5$: probando x_1, $x_1 \pm 7$, $x_1 \pm 14, \ldots$ sucesivamente, encontramos que $x_2 = 2 - 14 = -12$. Esta verifica el sistema $x \equiv 2 \pmod 7$ y $x \equiv 3 \pmod 5$ y, por el Teorema Chino del Resto, la solución general de este par de congruencias viene dada por $x_2 + 35t = -12 + 35t$ ($t \in \mathbf{Z}$). Probando $x_2, x_2 \pm 35, x_2 \pm 70, \ldots$ buscamos una solución del tipo $x_3 = -12 + 35t$ que satisfaga además la tercera congruencia $x_3 \equiv 2 \pmod 3$, obteniéndose como solución $x_3 = -12 + 35 = 23$, la cual satisface las tres congruencias, por lo que, por el Teorema Chino del Resto, la solución general constituye la clase de congruencia [23] módulo 105.

Las congruencias lineales en el Teorema Chino del Resto son todas de la forma $x \equiv a_i \pmod{n_i}$. Si damos un sistema de congruencias lineales en el que una (o más) de ellas es de la forma, más general, $ax \equiv b \pmod{n_i}$, necesitamos entonces hacer uso del algoritmo dado anteriormente para resolver dicha congruencia, expresando la solución general como una clase de congruencia módulo algún divisor de n_i; se podrán aplicar entonces las técnicas basadas en el Teorema Chino del Resto para resolver las congruencias resultantes.

Ejemplo 2.16 Consideremos el sistema de congruencias

$$7x \equiv 3 \pmod{12}, \quad 10x \equiv 6 \pmod{14}.$$

Vimos en los Ejemplos 2.12 y 2.13 que la primera de las congruencias tiene por solución general $x = 9 + 12t$, y la segunda $x = 2 + 7t$. Podemos, por tanto, sustituir el sistema de congruencias original por el sistema

$$x \equiv 9 \pmod{12}, \quad x \equiv 2 \pmod 7.$$

Claramente, $x = 9$ es una solución particular; como los módulos 7 y 12 son primos entre sí con producto 84, el Teorema Chino del Resto nos dice que la solución general es de la forma $9 + 84t$. □

El Teorema Chino del Resto puede utilizarse para convertir una única congruencia con un módulo grande en un sistema de congruencias con módulos pequeños, que es más fácil de resolver.

Ejemplo 2.17 Consideremos la congruencia lineal

$$13x \equiv 71 \pmod{380}.$$

En vez de usar el algoritmo descrito anteriormente para resolver una única congruencia lineal, podemos hacer uso de la factorización $380 = 2^2 \times 5 \times 19$ junto con el Teorema 2.4 para reemplazar esta congruencia por el sistema de congruencias

$$13x \equiv 71 \pmod{4}, \quad 13x \equiv 71 \pmod{5}, \quad 13x \equiv 71 \pmod{19}.$$

Este se reducen inmediatamente a

$$x \equiv 3 \pmod{4}, \quad 3x \equiv 1 \pmod{5}, \quad 13x \equiv 14 \pmod{19}.$$

La primera de ellas no necesita simplificación, pero podemos aplicar el algoritmo de la congruencia para simplificar cada una de las otras dos. Escribimos la segunda congruencia como $3x \equiv 6 \pmod{5}$, por lo que dividiendo por 3 (que es primo con 5) nos queda $x \equiv 2 \pmod{5}$. De forma análoga podemos escribir la tercera congruencia de la forma $-6x \equiv 14 \pmod{19}$, por lo que dividiendo por -2 obtenemos $3x \equiv -7 \equiv 12 \pmod{19}$ y dividiendo ahora por 3 tenemos $x \equiv 4 \pmod{19}$. Nuestra congruencia original es, por tanto, equivalente al sistema de congruencias

$$x \equiv 3 \pmod{4}, \quad x \equiv 2 \pmod{5}, \quad x \equiv 4 \pmod{19}.$$

Como tienen módulos mutuamente primos entre sí, podemos aplicar el Teorema Chino del Resto y podemos hacer uso de cualquiera de los dos métodos para encontrar la solución general. Usando el segundo método encontramos una solución $x_1 = 4$ de la tercera congruencia; sumando y restando múltiplos de 19 encontramos que $x_2 = 42$ también satisface la segunda congruencia y añadiendo y restando múltiplos de $19 \times 5 = 95$ encontramos que 327 (o equivalentemente -53) también satisface la primera congruencia. Por tanto, la solución general es de la forma $x = 327 + 380t$ ($t \in \mathbf{Z}$). □

Nuestro resultado final, obtenido por Yih-Hing en el siglo VII, generaliza el Teorema Chino del Resto al caso en el que los módulos no son necesariamente primos entre sí. Consideremos, en primer lugar, un ejemplo sencillo:

Ejemplo 2.18 Vimos, en los comentarios previos al Teorema 2.10, que el sistema de congruencias

$$x \equiv 3 \pmod{9} \quad \text{y} \quad x \equiv 2 \pmod{6}$$

no tienen solución, por lo que debemos considerar bajo qué circunstancias tiene solución un sistema de dos congruencias

$$x \equiv a_1 \pmod 9 \quad \text{y} \quad x \equiv a_2 \pmod 6.$$

El máximo común divisor de los módulos 9 y 6 es 3 y las dos congruencias implican que

$$x \equiv a_1 \pmod 3 \quad \text{y} \quad x \equiv a_2 \pmod 3,$$

por lo que existe solución si $a_1 \equiv a_2 \pmod 3$, es decir, si 3 divide a $a_1 - a_2$. Recíprocamente, supongamos que 3 divide a $a_1 - a_2$, por lo que $a_1 = a_2 + 3c$ para algún entero c. La solución general de la primera congruencia $x \equiv a_1 \pmod 9$ tiene la forma

$$x = a_1 + 9s = a_2 + 3c + 9s = a_2 + 3(c + 3s) \quad \text{donde} \quad s \in \mathbf{Z},$$

mientras que la solución general de la segunda congruencia $x \equiv a_2 \pmod 6$ es

$$x = a_2 + 6t \quad \text{donde} \quad t \in \mathbf{Z}.$$

Esto significa que un entero $x = a_1 + 9s$ puede verificar ambas congruencias si $c+3s = 2t$ para algún t, es decir, si $s \equiv c \pmod 2$. De este modo el sistema de congruencias admite solución si, y sólo si, $3|(a_1 - a_2)$, en cuyo caso la solución general es

$$x = a_1 + 9(c + 2u) = a_1 + 9c + 18u \quad \text{donde} \quad u \in \mathbf{Z},$$

constituyendo una única clase $[a_1 + 9c]$ módulo 18. □

El módulo final 18, es el mínimo común múltiplo de los módulos 9 y 6. Un razonamiento similar (que deberá probar usted) prueba que, en general, un sistema de dos congruencias

$$x \equiv a_1 \pmod{n_1} \quad \text{y} \quad x \equiv a_2 \pmod{n_2}$$

admite solución si, y sólo si, mcd (n_1, n_2) divide a $a_1 - a_2$, en cuyo caso la solución general es una única clase de congruencia módulo mcm (n_1, n_2). El resultado de Yih-Hing generaliza esto a un conjunto finito de congruencias lineales, probando que existe solución si, y sólo si, cada pareja de congruencias admite solución.

Teorema 2.11 [Teorema Chino del Resto: generalización] *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*

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

admiten una solución x 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 $n_1, \ldots, n_k$.*

(Obsérvese que si los módulos n_i son mutuamente primos entre sí entonces $\text{mcd}\,(n_i, n_j) = 1$ para cualesquiera que sean $i \neq j$, por lo que la condición $\text{mcd}\,(n_i, n_j)|(a_i - a_j)$ siempre se verifica; además, el mínimo común múltiplo n de $n_1, \ldots, n_k$ es el producto $n_1 \cdots n_k$, por lo que se obtiene el Teorema Chino del Resto como un caso particular del Teorema 2.11).

Demostración. Si existe una solución x entonces $x \equiv a_i \pmod{n_i}$ y, por tanto, $n_i|(x - a_i)$ para cada i. Para cada par $i \neq j$ sea $n_{ij} = \text{mcd}\,(n_i, n_j)$, como n_{ij} divide a n_i y a n_j, también divide a $x - a_i$ y a $x - a_j$, por lo que divide a $(x - a_i) - (x - a_j) = a_i - a_j$ como se requería.

Sea x_0 una solución; un entero x es solución si, y sólo si $x \equiv x_0 \pmod{n_i}$ para cada i, es decir, $x - x_0$ es divisible por cada n_i, o lo que es equivalente, por el mínimo común múltiplo $n = \text{mcm}\,(n_1, \ldots, n_k)$. Por tanto, la solución general constituye una única clase $[x_0] \pmod{n}$.

Para completar la demostración, debemos probar que si n_{ij} divide a $a_i - a_j$ para cada par $i \neq j$, existe solución. La estrategia consiste en sustituir el sistema de congruencias dado por otro equivalente, pero con módulos mutuamente primos entre sí, y aplicar entonces el Teorema Chino del Resto para probar que este nuevo sistema tiene solución. Hacemos uso, en primer lugar, del Teorema 2.4 para reemplazar cada congruencia $x \equiv a_i \pmod{n_i}$ por un conjunto finito de congruencias $x \equiv a_i \pmod{p^e}$ donde p^e recorre todas las potencias primas de la factorización de n_i. En este nuevo sistema de congruencias, equivalente al primero, todos los módulos son potencias primas. Estos módulos no son necesariamente primos entre sí, ya que algunos primos p pueden ser divisores de n_i para distintos i. Para un primo dado p, escojamos i de forma que n_i sea divisible por la mayor potencia de p y sea esta potencia p^e. Si $p^f|n_j$, por tanto $f \leq e$, se tiene que p^f divide a n_{ij} por lo que, (por nuestra hipótesis) divide a $a_i - a_j$; se deduce entonces que $a_i \equiv a_j \pmod{p^f}$, por lo

que si la congruencia $x \equiv a_i \pmod{p^e}$ es cierta, implica que $x \equiv a_i \pmod{p^f}$ y, por tanto, $x \equiv a_j \pmod{p^f}$. Esto significa que podemos eliminar, de nuestro sistema, 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 otras. Si hacemos esto con cada primo p, nos quedamos con un conjunto finito de congruencias de la forma $x \equiv a_i \pmod{p^e}$ involucrando a los distintos primos p; dado que los módulos p^e son mutuamente primos entre sí, el Teorema Chino del Resto implica que las congruencias tienen una solución común, la cual es, automáticamente, una solución del sistema original. ■

Ejemplo 2.19 Consideremos las congruencias

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

Aquí, $n_1 = 36$, $n_2 = 40$, y $n_3 = 75$, por lo que

$$n_{12} = \text{mcd}\,(36, 40) = 4,\ n_{13} = \text{mcd}\,(36, 75) = 3 \ \text{ y } \ n_{23} = \text{mcd}\,(40, 75) = 5.$$

Como

$$a_1 - a_2 = 11 - 7 = 4,\ a_1 - a_3 = 11 - 32 = -21 \ \text{ y } \ a_2 - a_3 = 7 - 32 = -25,$$

se satisfacen todas las condiciones $n_{ij} | (a_i - a_j)$, por lo que existen soluciones, las cuales constituyen una única clase módulo n donde $n = \text{mcm}\,(36, 40, 75) = 1800$. Para encontrar la solución general seguimos el procedimiento descrito en el último párrafo de la demostración del Teorema 2.11. Factorizamos cada n_i y reemplazamos la primera congruencia por

$$x \equiv 11 \pmod{2^2} \quad \text{y} \quad x \equiv 11 \pmod{3^2},$$

la segunda por

$$x \equiv 7 \pmod{2^3} \quad \text{y} \quad x \equiv 7 \pmod{5},$$

y la tercera por

$$x \equiv 32 \pmod{3} \quad \text{y} \quad x \equiv 32 \pmod{5^2}.$$

Esto da un conjunto de seis congruencias en las que los módulos son potencias de los primos $p = 2, 3$ y 5. De entre ellas, seleccionamos la congruencia que involucra a la mayor potencia de cada primo: para $p = 2$ debemos escoger $x \equiv 7 \pmod{2^3}$ (la cual implica $x \equiv 11 \pmod{2^2}$), para $p = 3$ debemos elegir $x \equiv 11 \pmod{3^2}$ (la cual implica $x \equiv 32 \pmod{3}$), y para $p = 5$ debemos

quedarnos con $x \equiv 32 \pmod{5^2}$ (la cual implica $x \equiv 7 \pmod 5$). Estas tres congruencias, que pueden reducirse a

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

tienen módulos mutuamente primos entre sí, y podemos aplicarles los métodos anteriores, basados en el Teorema Chino del Resto, para encontrar la solución general $x \equiv 407 \pmod{1800}$. □

Hemos visto que una única congruencia módulo n es equivalente a un sistema de congruencias cuyos módulos son las potencias primas p^e que aparecen en la factorización de n. Por ello, en este capítulo estudiaremos las congruencias módulo p^e cuando p es primo. Trataremos en, primer lugar, el caso más simple $e = 1$ y más tarde, después de un paréntesis sobre test de primalidad, consideraremos el caso $e > 1$. Una buena razón para comenzar con el caso primo es que mientras que la suma, la resta y el producto se comportan de igual forma tanto si el módulo es primo como compuesto, la división es mucho más fácil cuando es primo.

2.4 La aritmética en Z_p

Recordemos que los elementos de $\mathbf{Z}_m$ (donde $m \in \mathbf{Z}^+$) son clases de equivalencia módulo m, es decir, $x \in \mathbf{Z}_m$ representa que $x = [x]_m$.

Podemos definir en $\mathbf{Z}_m$ la suma y el producto de la forma

$$x + y = [x]_m + [y]_m = [x + y]_m$$

$$x \cdot y = [x]_m \cdot [y]_m = [x \cdot y]_m$$

Estas dos operaciones verifican las siguientes propiedades:

a) Internas: $\forall x, y \in \mathbf{Z}_m \Rightarrow x + y,\ xy \in \mathbf{Z}_m$.

b) Asociativas: $\forall x, y, z \in \mathbf{Z}_m \Rightarrow x + (y + z) = (x + y) + z \quad x(yz) = (xy)z$.

c) Conmutativas: $\forall x, y \in \mathbf{Z}_m \Rightarrow x + y = y + x, \quad xy = yx$.

d) Distributiva: $\forall x, y, z \in \mathbf{Z}_m \Rightarrow x(y + z) = xy + xz$.

e) Existencia de neutro y unidad: existen $0, 1 \in \mathbf{Z}_m$ tales que $\forall x \in \mathbf{Z}_m \Rightarrow$

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

f) Existencia de opuestos: $\forall x \in \mathbf{Z}_m$ existe un único elemento, que denotaremos por $-x \in \mathbf{Z}_m$ tal que $x + (-x) = (-x) + x = 0$.

Aunque en general un elemento de $\mathbf{Z}$ no tenía elemento inverso, se verificaba la propiedad cancelativa del producto, es decir: si $x \neq 0$ y $xy = xz$ entonces $y = z$. Sin embargo, cuando trabajamos en $\mathbf{Z}_m$ ya no se verifica esta propiedad.

$+$	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

Tabla 2.1: La suma y el producto en Z_4.

Si confeccionamos, por ejemplo, las tablas de la suma y el producto en $\mathbf{Z}_4$ (Tabla 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.

Observamos además que en $\mathbf{Z}$ se verificaba $xy = 0 \iff x = 0$ o $y = 0$ y sin embargo en $\mathbf{Z}_4$ se tiene que $2 \neq 0$ y $2 \times 2 = 0$. En otras palabras, en $\mathbf{Z}_m$ pueden existir lo que llamaremos *divisores de cero* es decir, elementos no nulos cuyo producto es cero.

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 su propio inverso). Cabe entonces hacerse la pregunta de ¿cuándo va a tener inverso un elemento de $\mathbf{Z}_m$?

Sea $r \in \mathbf{Z}_m$. Decimos que r es un *elemento unitario* o simplemente que es una *unidad* en $\mathbf{Z}_m$, si existe otro elemento $s \in \mathbf{Z}_m$ tal que $sr = rs = 1$.

Teorema 2.12 *El inverso de un elemento unitario es único.*

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

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

Esto nos permite denotar al elemento inverso como r^{-1} y hablar de *el* elemento inverso y no de *un* elemento inverso de r.

Teorema 2.13 *Un elemento $r \in \mathbf{Z}_m$ es inversible si, y sólo si, r y m son primos entre si, es decir, si* mcd $(m, r) = 1$.

Demostración.

Si r es inversible

existe $r^{-1} \in \mathbf{Z}_m$ tal que $rr^{-1} = 1 \Rightarrow rr^{-1} \equiv 1 \pmod{m} \Rightarrow rr^{-1} - 1 = km$ con $k \in \mathbf{Z}$, por lo que $rr^{-1} - km = 1$ es decir, r y m son primos entre sí ya que de lo contrario, cualquier divisor común debería dividir a 1 y 1 no tiene divisores. Por tanto, mcd $(m, r) = 1$

Si mcd $(m, r) = 1$

existen enteros a y b tales que $ar + bm = 1$ por lo que $ar - 1 = -bm = \dot{m}$ es decir $ar \equiv 1 \pmod{m}$ o lo que es lo mismo, $ar = 1$. Vemos entonces que r posee elemento inverso $r^{-1} = a$. ■

El algoritmo extendido de Euclides nos proporciona el inverso de los elementos unitarios de Z_m.

Ejemplo 2.20 Las unidades de $\mathbf{Z}_8$ son $[1], [3], [5]$ y $[7]$, en efecto: $[1][1] = [3][3] = [5][5] = [7][7] = [1]$, por lo que cada una de estas unidades es su propio inverso multiplicativo. En $\mathbf{Z}_9$ las unidades son $[1], [2], [4], [5], [7]$ y $[8]$, por ejemplo, $[2][5] = [1]$, por lo que $[2]$ y $[5]$ son uno el inverso del otro. □

Obsérvese que si p es primo, dado que cualquier elemento de $\mathbf{Z}_p$ es menor que p es primo con este y, por tanto, todos los elementos no nulos de $\mathbf{Z}_p$ son inversibles. Este resultado nos dice que si p es primo entonces $[\mathbf{Z}_p, +, \cdot]$ tiene estructura de *cuerpo* .

Si m no es primo existen elementos no inversibles (todos los elementos no primos con de m), por lo que $[\mathbf{Z}_m, +, \cdot]$ no tiene estructura de cuerpo. Además, si p y q son dos divisores de m tales que $pq = m$ tenemos que $p, q \in \mathbf{Z}_m$ y $pq = 0$ con $p \neq 0$ y $q \neq 0$, es decir, $\mathbf{Z}_m$ posee divisores de cero. En este caso $[\mathbf{Z}_m, +, \cdot]$ es un *anillo con divisores de cero.*

2.4.1 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 2.14 *Si p es primo y $a \not\equiv 0 \pmod{p}$, $a^{p-1} \equiv 1 \pmod{p}$.*

Demostración. Los enteros $1, 2, \ldots, p-1$ constituyen un conjunto completo de restos, no nulos, módulo p. Si $a \not\equiv 0 \pmod{p}$, por el Lema 2.9 (b), $xa \equiv ya$ implica que $x \equiv y$, por lo que los enteros $a, 2a, \ldots, (p-1)a$ pertenecen a distintas clases módulo p. Ninguno de ellos es divisible por p, por lo que constituyen un sistema completo de restos, no nulos, módulo p. Se deduce entonces que $a, 2a, \ldots, (p-1)a$ son congruentes con $1, 2, \ldots, p-1$ en algún orden. (Por ejemplo, si $p = 5$ y $a = 3$ multiplicando los restos $1, 2, 3$ y 4 por 3 obtenemos $3, 6, 9$ y 12 que son congruentes con $3, 1, 4$ y 2 respectivamente). Los productos de estos dos conjuntos de enteros pertenecen, por tanto, a la misma clase, esto es

$$1 \times 2 \times \cdots \times (p-1) \equiv a \times 2a \times \cdots \times (p-1)a \pmod{p},$$

o lo que es lo mismo,

$$(p-1)! \equiv (p-1)!a^{p-1} \pmod{p}.$$

Como $(p-1)!$ es primo con p, el Lema 2.9 (b) nos dice que podemos dividir por $(p-1)!$ y se deduce entonces que $a^{p-1} \equiv 1 \pmod{p}$. ■

El Teorema 2.14 establece que todas las clases de $\mathbf{Z}_p$, excepto $[0]$, son raíces del polinomio $x^{p-1} - 1$. De este polinomio al que anulan *todas* las clases de $\mathbf{Z}_p$, multiplicando simplemente por x, se obtiene $x^p - x$:

Corolario 2.15 *Si p es primo, para cualquier entero a se verifica que*

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

Demostración. Si $a \not\equiv 0$, el Teorema 2.14 nos dice que $a^{p-1} \equiv 1$, y multiplicando por a se obtiene el resultado. Si $a \equiv 0$ entonces $a^p \equiv 0$, por lo que también se verifica el resultado. ■

Este último resultado es el que se conoce generalmente como *Pequeño Teorema de Fermat* ya que el del Teorema 2.14 puede ser considerado como un caso particular del Teorema de Euler que estudiaremos más adelante. Cualquiera de ellos resulta muy útil cuando se trabaja con grandes potencias de enteros.

Ejemplo 2.21 Encontrar el menor resto, no negativo, de dividir 2^{68} entre 19. Como 19 es primo y 2 no es divisible entre 19, podemos aplicar el Teorema 2.14 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

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

por lo que $2^{68} \equiv 6 \pmod{19}$ □

Ejemplo 2.22 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 2.15, 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 2.15 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

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

como queríamos. 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

$$\begin{aligned} a^{25} = (a^2)^{12} a \equiv a^{12} a = (a^2)^6 a \equiv a^6 a = (a^2)^3 a \\ \equiv a^3 a = a^4 = (a^2)^2 \equiv a^2 \equiv a \pmod{2}. \end{aligned}$$ □

El Corolario 2.15 prueba que si $f(x)$ es un polinomio de grado $d \geq p$, reemplazando reiteradamente x^p por x podemos encontrar un polinomio $g(x)$ de grado más pequeño que p con la propiedad de que $f(x) \equiv g(x)$ para cualquier entero x. En otras palabras, cuando consideramos polinomios módulo P, es suficiente restringir nuestra atención a los de grado $d < p$. De forma análoga, los coeficientes pueden reducirse módulo p.

2.4.2 El Teorema de Wilson

Como otra aplicación del Pequeño Teorema de Fermat, proponemos un resultado conocido como *Teorema de Wilson*, que fue probado por primera vez por Lagrange en 1770:

Teorema 2.16 [Teorema de Wilson] *Un entero positivo n es primo si, y sólo si, $(n-1)! \equiv -1 \pmod{n}$.*

2.5 Los tests de base a: pseudoprimos y números de Carmichael

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 el contrarrecíproco del Corolario 2.15, el cual asegura que si existe un entero a que verifica $a^n \not\equiv a \pmod{n}$, entonces n es compuesto. Este test es 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.

Test de base a

El método es el siguiente. Si tenemos un entero n y queremos saber si es primo, elegimos un entero a y computamos $a^n \pmod{n}$, reduciendo los números módulo n, siempre que sea posible, para simplificar los cálculos. Diremos que n supera el test de base a si $a^n \equiv a \pmod{n}$, y que no lo supera si $a^n \not\equiv a \pmod{n}$; por lo que si, para n, falla el test de base a para algún a, el Corolario 2.15 implica que n debe ser compuesto, mientras que si n supera el test puede ser primo o compuesto. Por simplicidad computacional, es sensato comenzar con $a = 2$ (evidentemente $a = 1$ es inútil). Si encontramos que $2^n \not\equiv 2 \pmod{n}$, entonces n no supera el test de base 2, por lo que resulta ser compuesto y acabamos. Por ejemplo, $2^6 = 64 \not\equiv 2 \pmod{6}$, por lo que 6 no supera el test de base 2 y, por tanto, es compuesto. Los chinos conocían este test y conjeturaron hace 25 siglos que el recíproco también era cierto, se decir, que si n supera el test de base 2, entonces n es primo. Esto resultó ser falso, pero hasta 1819 no se encontró un contraejemplo: existen números compuestos n que verifican $2^n \equiv 2 \pmod{n}$, es decir, que superan el test de base 2 y que, sin embargo, no son primos. A dichos enteros los denominamos *pseudoprimos*: parecen que son primos, pero de hecho son compuestos.

Ejemplo 2.23 Apliquemos el test de base 2 al entero $n = 341$. El cálculo de $2^{341} \pmod{341}$ se simplifica enormemente observando que $2^{10} = 1024 \equiv 1 \pmod{341}$, por lo que

$$2^{341} = (2^{10})^{34} \cdot 2 \equiv 2 \pmod{341}$$

y 341 supera el test de primalidad. Sin embargo, $341 = 11 \cdot 31$, por lo que no es primo sino pseudoprimo. (De hecho, previamente conocida esta factorización, uno puede "hacer trampas" en el test de base 2 para evitar grandes cálculos: como 11 y 31 son primos, el Teorema 2.14 nos dice que $2^{10} \equiv 1 \pmod{11}$ y que $2^{30} \equiv 1 \pmod{31}$, de donde se deduce, fácilmente, que $2^{341} - 2$ es divisible por 11 y por 31 y, por tanto, por 341). Ningún número compuesto $n < 341$ supera el test de base 2, por lo que 341 es el pseudoprimo más pequeño. □

Afortunadamente, los pseudoprimos son bastante raros pero, sin embargo, existen infinitos.

Teorema 2.17 *Existen infinitos pseudoprimos.*

Demostración. Vamos a probar que si n es pseudoprimo, $2^n - 1$ también lo es. Como $2^n - 1 > n$ podemos reiterar el proceso, partiendo de $n = 341$, para generar una secuencia infinita de pseudoprimos.

Si n es pseudoprimo, es compuesto, por lo que el Teorema 1.32 implica que $2^n - 1$ es compuesto. La demostración del Teorema 1.32 estaba puesta como un ejercicio, por lo que si no lo ha hecho, aquí la tiene. Tenemos que $n = ab$, donde $1 < a < n$ y $1 < b < n$. En la identidad de polinomios

$$x^m - 1 = (x - 1)(x^{m-1} + x^{m-2} + \cdots + 1), \tag{2.1}$$

la cual es válida para cualquier $m \geq 1$, ponemos $x = 2^a$ y $m = b$, obteniendo

$$2^n - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots 1).$$

Como $1 < 2^a - 1 < 2^n - 1$, esto prueba que $2^n - 1$ es compuesto.

Debemos probar ahora que $2^{2^n-1} \equiv 2 \pmod{2^n - 1}$. Como n es pseudoprimo, tenemos que $2^n \equiv 2 \pmod{n}$, por lo que $2^n = nk + 2$ para algún entero $k \geq 1$. Si hacemos $x = 2^n$ y $m = k$ en (2.1), vemos que $2^n - 1$ divide a $(2^n)^k - 1$; por tanto, $2^{nk} \equiv 1 \pmod{2^n - 1}$, por lo que $2^{2^n-1} = 2^{nk+1} = 2^{nk} \cdot 2 \equiv 2 \pmod{2^n - 1}$ como se quería probar. ■

Volvamos a nuestro método de testeo de primalidad. Si n no supera el test de base 2 entonces podemos parar, sabemos que n es compuesto; sin embargo, si n lo supera puede ser primo o pseudoprimo, pero no sabemos más. Podemos repetir el test con un valor diferente de a. Al igual que con $a = 2$, si no supera el test, probamos que n es compuesto, mientras que si lo pasa no nos dice nada. En general, testamos n repetidamente utilizando cada vez un valor diferente

de a. Obsérvese que si n supera el test para bases a y b (posiblemente iguales), por lo que $a^n \equiv a$ y $b^n \equiv b \pmod{n}$, entonces $(ab)^n \equiv ab \pmod{n}$, por lo que n también supera el test de base ab, no aportando nada nuevo la aplicación de este test, por lo que parece sensato restringir los valores de a a los sucesivos números primos. Diremos que n es un *pseudoprimo para la base* a si n es compuesto y verifica que $a^n \equiv a \pmod{n}$, de tal forma que un pseudoprimo para la base 2 es sólo un pseudoprimo, como se definió anteriormente.

Ejemplo 2.24 Tomemos de nuevo $n = 341$. Supera el test de base 2, por lo que probaremos ahora con la base 3. Podemos calcular $3^{341} \pmod{341}$ haciéndolo primero módulo 11 y módulo 31. Como $3^5 = 243 \equiv 1 \pmod{11}$ y $341 \equiv 1 \pmod{5}$, se tiene que $3^{341} \equiv 3 \pmod{11}$. El Teorema 2.14 nos dice que $3^{30} \equiv 1 \pmod{31}$, y como $341 \equiv 11 \pmod{30}$ tenemos que $3^{341} \equiv 3^{11} \pmod{31}$; dado que $3^5 \equiv -5 \pmod{31}$, se tiene que $3^{341} \equiv 3(-5)^2 = 75 \not\equiv 3 \pmod{31}$. Por tanto, $3^{341} \not\equiv 3 \pmod{341}$, es decir: 341 no supera el test de base 3. □

En nuestras implementaciones de los tests de base a, hemos evitado, hasta ahora, el cálculo directo de $a^n \pmod{n}$, haciendo uso de nuestro conocimiento de algunas potencias más pequeñas de a (tal como $2^10 \equiv 1 \pmod{341}$ en el Ejemplo 2.23) o utilizando una factorización de n para reemplazar el módulo n por otros módulos más pequeños (tales como 11 y 31 en el Ejemplo 2.24). En general, no disponemos de ninguna de estas reducciones, por lo que ¿cómo calcular $a^n \pmod{n}$ de una manera eficiente cuando n es grande? Calculando directamente $a, a^2, a^3, \ldots, a^n \pmod{n}$ se requiere mucho tiempo, un método mucho mejor es elevar al cuadrado y multiplicar las potencias obtenidas, una técnica que también es efectiva para calcular potencias n-ésimas de otros objetos tales como enteros o matrices. La idea básica es que si $n = 2m$ es par, $x^n = (x^m)^2$ y si $n = 2m + 1$ es impar, $x^n = (x^m)^2 x$, por lo que reiterando el uso de esta regla se reduce el cálculo de potencias n-ésimas a un número bastante pequeño de aplicaciones de las funciones

$$f : \mathbf{Z}_n \to \mathbf{Z}_n, \quad x \mapsto x^2 \qquad \text{y} \qquad g : \mathbf{Z}_n \to \mathbf{Z}_n, \quad x \mapsto x^2 a,$$

las cuales son fácilmente evaluables.

Visto de otra manera: supongamos que debemos calcular $n^\alpha \bmod m$.

Si expresamos α en binario, $\alpha = (1\alpha_{r-1}\alpha_{r-2}\ldots\alpha_1\alpha_0)_2$ con $\alpha_i = 0 \; o \; 1 \Rightarrow$

$$\alpha = 2^r + \alpha_{r-1}2^{r-1} + \cdots + \alpha_1 2 + \alpha_0$$

Para convertir α en decimal calculamos el valor numérico del polinomio

$$x^r + \alpha_{r-1}x^{r-1} + \cdots + \alpha_1 x + \alpha_0$$

para $x = 2$ y este, por el *Teorema del resto*, se puede calcular dividiendo dicho polinomio entre $x - 2$ por la regla de Ruffini, es decir, empezando por 1 multiplicamos por 2, sumamos α_{r-1} y volvemos a multiplicar por 2, así sucesivamente hasta sumar α_0. Al llegar a este punto tenemos el valor de α.

Para calcular n^α, al ser α el exponente, las operaciones se corresponden con elevar al cuadrado cuando antes multiplicábamos por 2 y a multiplicar por n^{α_i} cuando antes sumábamos α_i. Como $\alpha_i = 1$ *o* 0, si es 1 equivale a multiplicar por n y si es 0 equivale a multiplicar por $n^0 = 1$, es decir, a no realizar operación alguna.

Por ello, si por ejemplo es $\alpha = 19 = (10011)_2$ realizaremos el siguiente proceso:

a) Intercalamos C entre cada dos cifras consecutivas:

$$1\ \mathrm{C}\ 0\ \mathrm{C}\ 0\ \mathrm{C}\ 1\ \mathrm{C}\ 1$$

b) Sustituimos los unos por M y eliminamos los ceros

$$\mathrm{M}\ \mathrm{C}\ \mathrm{C}\ \mathrm{C}\ \mathrm{M}\ \mathrm{C}\ \mathrm{M}$$

c) Empezando por 1, M equivale a multiplicar por n mientras que C equivale a elevar al cuadrado.

Así pues:

$$1 \xrightarrow{\mathrm{M}} n \xrightarrow{\mathrm{C}} n^2 \xrightarrow{\mathrm{C}} n^4 \xrightarrow{\mathrm{C}} n^8 \xrightarrow{\mathrm{M}} n^9 \xrightarrow{\mathrm{C}} n^{18} \xrightarrow{\mathrm{M}} n^{19}$$

Este método nos asegura que, para cualquier 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 $2(1 + \lfloor \log n \rfloor)$.

Ejemplo 2.25 Como la expresión binaria de 91 es 1011011, el proceso anterior nos dice que construyamos, en primer lugar la secuencia

$$1\ \mathrm{C}\ 0\ \mathrm{C}\ 1\ \mathrm{C}\ 1\ \mathrm{C}\ 0\ \mathrm{C}\ 1\ \mathrm{C}\ 1$$

y que, a continuación eliminemos los ceros y sustituyamos los unos por emes, para obtener

M C C M C M C C M C M

por lo que podemos calcular n^{91} partiendo de 1 y aplicando la regla definida anteriormente, lo que requiere de un total de 12 multiplicaciones, lo cual es significativamente más eficiente que las 90 que se requieren para calcular sucesivamente $a, a^2, a^3, \ldots, a^{91}$. □

Volviendo al test de primalidad, si encontramos, eventualmente, un entero a para el que n no supera el test de base a, habremos probado que n es compuesto. Si, en cambio, n continúa superando sucesivos tests, entonces no tenemos probado nada definitivo acerca de n; de cualquier modo, se puede probar que la probabilidad de que n sea primo se aproxima rápidamente a 1 cuando supera más y más tests independientes, así después de un número suficiente de tests podemos afirmar que n tiene una probabilidad muy alta de ser primo. Aunque esto no supone ninguna prueba rigurosa de primalidad, para muchas aplicaciones prácticas (como puede ser la criptografía) un alto nivel de probabilidad es totalmente adecuado: la posibilidad de que n sea compuesto después de haber pasado un número suficiente de tests es, significativamente, más pequeña que la posibilidad de un error humano o de la máquina al trabajar con n. Es este un típico ejemplo de un algoritmo probabilístico, donde admitimos un cierto grado de incertidumbre acerca del resultado para obtener una respuesta en un tiempo razonable. Por contraste, el test de primalidad basado en el Teorema de Wilson es absolutamente cierto (si podemos garantizar el cálculo exacto), a costa de un tiempo de cálculo irrazonable.

Es tentador conjeturar que si n es compuesto, no superará el test de base a para algún a, por lo que el algoritmo anterior lo detectará (posiblemente después de haber superado un gran número de tests). Desgraciadamente, este no es el caso: existen números compuestos n que superan el test de base a cualquiera que sea a, por lo que no es posible detectarlo mediante este algoritmo. Estos son los *números de Carmichael*, enteros compuestos n con la propiedad de que $a^n \equiv a \pmod{n}$ para cualquier entero a, por lo que satisfacen la conclusión del Corolario 2.15 sin ser primos.

El ejemplo más pequeño de un número de Carmichael es $n = 561 = 3 \cdot 11 \cdot 17$. Evidentemente es compuesto, por lo que para probar que es un número de Carmichael debemos probar que $a^{561} \equiv a \pmod{561}$ para cualquier entero a y, para ello, es suficiente con probar que la congruencia $a^{561} \equiv a$ se satisface

módulo 3, 11 y 17 para cualquier a. Consideremos, en primer lugar, $a^{561} \equiv a \pmod{17}$. Si $a \equiv 0 \pmod{17}$ es evidente, por lo que podemos asumir que $a \not\equiv 0 \pmod{17}$. Como 17 es primo, el Teorema 2.14 nos dice que $a^{16} \equiv 1 \pmod{17}$; como $561 \equiv 1 \pmod{16}$, se tiene que $a^{561} \equiv a^1 = a \pmod{17}$. Unos cálculos similares prueban que $a^{561} \equiv a \pmod{3}$ y que $a^{561} \equiv a \pmod{11}$, por lo que $a^{561} \equiv a \pmod{561}$ como queríamos probar. Como en el caso de los pseudoprimos, probar que este es el menor número de Carmichael depende de la tediosa tarea de rutina de comprobar que cualquier número compuesto más pequeño, no supera el test de base a para algún a.

Los números de Carmichael se dan con mucha menor frecuencia que los primos, y son bastante difíciles de construir. En 1912, Carmichael conjeturó que existen infinitos, y fue probado en 1992 por Alford, Granville y Pomerance. La demostración es difícil, pero un paso crucial es el siguiente resultado elemental:

Lema 2.18 *Si n es libre de cuadrados (un producto de primos distintos) y $p-1$ divide a $n-1$ para cada primo p que divide a n, o n es primo o es un número de Carmichael.*

De hecho, el recíproco del Lema 2.18 también es cierto, pero no lo probaremos, pues necesitaremos conceptos que se salen de nuestro propósito.

Ejemplo 2.26 El número $n = 561 = 3 \cdot 11 \cdot 17$ es libre de cuadrados y compuesto; como $n - 1 = 560$ es divisible por $p - 1 = 2, 10$ y 16, el Lema 2.18 implica que 561 es un número de Carmichael. □

2.6 Test de Lucas-Lehmer

Para la obtención de números primos muy grandes se utilizan los números de Mersenne ($2^p - 1$ con p primo). El siguiente algoritmo nos proporciona un test determinista de primalidad eficiente para los números de Mersenne.

Teorema 2.19 *Sea p un primo impar y consideremos la secuencia*

$$S_1 = 4 \quad S_2 \equiv S_1^2 - 2 \bmod M_p \quad \cdots \quad S_{p-1} \equiv S_{p-2}^2 - 2 \bmod M_p.$$

Se verifica entonces que el número de Mersenne M_p es primo si, y sólo si, $S_{p-1} \equiv 0 \pmod{M_p}$.

Así, por ejemplo, el número de Mersenne $M_7 = 2^7 - 1 = 127$ es primo ya que

$$S_1 = 4$$
$$S_2 = 4^2 - 2 = 14 \equiv 14 \bmod 127$$
$$S_3 = 14^2 - 2 = 194 \equiv 67 \bmod 127$$
$$S_4 = 67^2 - 2 = 4487 \equiv 42 \bmod 127$$
$$S_5 = 42^2 - 2 = 1762 \equiv 111 \equiv -16 \bmod 127$$
$$S_6 = (-16)^2 - 2 = 254 \equiv 0 \bmod 127$$

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 el número de Mersenne $M_{6972593}$ es primo.

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 da el número de clases de congruencia $[a] \in \mathbf{Z}_n$ que tienen inverso para la multiplicación. 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 codificado de mensajes secretos.

Por ejemplo, un importante resultado de este capítulo es el Pequeño Teorema de Fermat: si p es primo, $a^{p-1} \equiv 1 \pmod{p}$ cualquiera que sea el entero $a \not\equiv 0 \pmod{p}$. Nos gustaría encontrar un resultado similar para módulos compuestos, pero si reemplazamos p por un entero compuesto n, la congruencia resultante $a^{n-1} \equiv 1 \pmod{n}$ no es cierta en general: si $\mathrm{mcd}\,(a, n) > 1$ 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 pero, 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.

Denotemos por U_n al conjunto de las unidades de $\mathbf{Z}_n$. Por el Teorema 2.13 el número $|U_n|$ de elementos de U_n equivale al número de enteros $a = 1, 2, \ldots, n$ tales que mcd $(a, n) = 1$.

Definición 2.2 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

Tabla 2.2: Los primeros valores de la función de Euler.

Decimos que un subconjunto R de $\mathbf{Z}$ es un *conjunto reducido de restos módulo* n si contiene a un elemento de cada una de las $\phi(n)$ clases de congruencia de U_n. Por ejemplo, $\{1, 3, 5, 7\}$ y $\{\pm 1, \pm 3\}$ son conjuntos reducidos de restos módulo 8.

Lema 2.20 *Si R es un conjunto reducido de restos módulo n y un entero a es una unidad módulo n, el conjunto $aR = \{ar \mid r \in R\}$ es también un conjunto reducido de restos módulo n.*

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

Teorema 2.21 [Teorema de Euler] *Si* mcd $(a, n) = 1$, $a^{\phi(n)} \equiv 1 \pmod n$.

Demostración. Sustituyamos los enteros $1, 2, \ldots, p-1$ con un conjunto reducido $R = \{r_1, \ldots, r_{\phi(n)}\}$ de restos módulo n en la demostración del Teorema 2.14. Si mcd $(a, n) = 1$, aR es también un conjunto reducido de restos

módulo n (ver el Lema 2.20), por lo que el producto de todos los elementos de aR debe ser congruente con el de todos los elementos de R. Esto nos dice que $a^{\phi(n)} r_1 r_2 \cdots r_{\phi(n)} \equiv r_1 r_2 \cdots r_{\phi(n)}$ y como todos los factores r_i son unidades, podemos cancelarlos y quedarnos con $a^{\phi(n)} \equiv 1$. ■

Ejemplo 2.27 El Pequeño Teorema de Fermat es un caso especial de este resultado: si n es un primo p, por el Teorema 2.13, las unidades de $\mathbf{Z}_p$ son $1, 2, \ldots, p-1$, por lo que $\phi(p) = p - 1$ y, por tanto, $a^{p-1} \equiv 1 \pmod{p}$. □

Ejemplo 2.28 Si tomamos $n = 12$, $U_{12} = \{\pm 1, \pm 5\}$ y $\phi(12) = 4$; tenemos que $(\pm 1)^4 = 1$ y $(\pm 5)^4 = 625 \equiv 1 \pmod{12}$, por lo que $a^4 \equiv 1 \pmod{12}$ cualquiera que sea a primo con 12. □

Busquemos ahora una fórmula general para $\phi(n)$. Hemos visto únicamente el caso $\phi(p) = p - 1$ para cualquier primo p, y una simple extensión de éste trata el caso en que n es una potencia prima.

Lema 2.22 *Si $n = p^e$ donde p es primo,*

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

Demostración. $\phi(p^e)$ es el número de enteros en $(1, \ldots, p^e)$ que son primos con p^e, es decir, no divisibles por p; este conjunto tiene p^e elementos, de los cuales $p^e/p = p^{e-1}$ son múltiplos de p, por lo que $\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$. ■

Se puede interpretar este resultado en términos de probabilidad. Un entero a es una unidad módulo p^e si, y sólo si, no es divisible por p. Si elegimos a al azar, será divisible por p con probabilidad $1/p$, y de será primo con p^e con probabilidad $1 - 1/p$. Por tanto, la proporción $\phi(p)/p$ de clases de $\mathbf{Z}_n$ que son unidades debe ser $1 - 1/p$, por lo que $\phi(n) = n(1 - 1/p)$ para $n = p^e$.

Para dar una fórmula de $\phi(n)$ válida para cualquier número natural, necesitamos un resultado que combine la información dada en el Lema 2.22 para distintas potencias de primos. El Teorema 2.24 nos la da, pero para probarlo es necesario ver el siguiente resultado sobre conjuntos completos de restos.

Lema 2.23 *Si A es un conjunto completo de restos módulo n, m es un entero primo con n y c un entero cualquiera, el conjunto $Am + c = \{am + c \mid a \in A\}$ es también un conjunto completo de restos módulo n.*

Demostración. Si $am + c \equiv a'm + c \pmod{n}$, donde $a, a' \in A$, restando c y cancelando la unidad m, vemos que $a \equiv a' \pmod{n}$ y, por tanto, a=a'. Entonces, los n elementos $am + c$ ($a \in A$) se encuentran cada uno en una clase de congruencia diferente, por lo que constituyen un conjunto completo de restos módulo n. ■

Teorema 2.24 *Si m y n son primos entre sí, $\phi(mn) = \phi(m)\phi(n)$.*

Demostración. 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 el Lema 2.23 es 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. ■

Ejemplo 2.29 Los enteros $m = 3$ y $n = 4$ son primos entre sí con $\phi(3) = \phi(4) = 2$; aquí $mn = 12$ y $\phi(12) = 2 \cdot 2 = 4$. □

El resultado del Teorema 2.24 falla si mcd $(m, n) > 1$: por ejemplo, $2^2 = 4$ pero $\phi(2)^2 \neq \phi(4)$.

Corolario 2.25 *Si la descomposición en factores primos de un número n es $n = p_1^{e_1} \cdots p_k^{e_k}$*

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

Demostración. Vamos a probar la primera de las expresiones por inducción en k (las otras expresiones se deducen fácilmente). El Lema 2.22 prueba el caso $k = 1$, por lo que asumimos que $k > 1$ y que el resultado es cierto para todos los enteros divisibles por un número de primos menor que k. Tomemos $n = p_1^{e_1} \cdots p_{k-1}^{e_{k-1}} p_k^{e_k}$, donde $p_1^{e_1} \cdots p_{k-1}^{e_{k-1}}$ y $p_k^{e_k}$ son primos entre sí. El Teorema 2.24 nos dice que

$$\phi(n) = \phi(p_1^{e_1} \cdots p_{k-1}^{e_{k-1}})\phi(p_k^{e_k}).$$

La hipótesis de inducción nos dice que

$$\phi(p_1^{e_1} \cdots p_{k-1}^{e_{k-1}}) = \prod_{i=1}^{k-1}(p_i^{e_i} - p_i^{e_i-1}),$$

y el Lema 2.22 que

$$\phi(p_k^{e_k}) = (p_k^{e_k} - p_k^{e_k-1}),$$

combinando ambos resultados obtenemos que

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

■

Una forma más concisa de escribir este resultado es $\phi(n) = n\prod_{p|n}(1 - \frac{1}{p})$, donde $\prod_{p|n}$ representa el producto sobre todos los primos p que dividen a n.

Ejemplo 2.30 Los primos que dividen a 60 son 2, 3 y 5, por lo que

$$\phi(60) = 60\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 16.$$

Podemos comprobarlo escribiendo los enteros $i = 1, 2, \ldots, 60$ y borrando aquellos para los que mcd $(i, 60) > 1$. Inicialmente tenemos 60 números; borrando los múltiplos de 2 nos quedamos con la mitad de ellos, borrando ahora los múltiplos de 3 eliminamos la tercera parte de los que nos quedan y borrando finalmente los múltiplos de 5 eliminamos la quinta parte del resto. Nos queda los 16 números 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53 y 59 que constituyen un conjunto reducido de restos módulo 60. □

2.8 Aplicaciones

Una vez estudiado cómo calcular la función de Euler $\phi(n)$, veremos algunas aplicaciones suyas. Hemos visto cómo utilizar el Pequeño Teorema de Fermat $a^{p-1} \equiv 1$ para simplificar congruencias módulo p donde p es primo, y podemos hacer ahora un uso similar del Teorema de Euler $a^{\phi(n)} \equiv 1$ para simplificar congruencias módulo n cuando n es compuesto.

Ejemplo 2.31 Vamos a calcular los dos últimos dígitos de 3^{1492}. Esto es equivalente a encontrar el menor resto, no negativo, de $3^{1492} \pmod{100}$. Dado que 3 es primo con 100, por el Teorema 2.21 (con $a = 3$ y $n = 100$) tenemos que $3^{\phi(100)} \equiv 1 \pmod{100}$. Los primos que dividen a 100 son 2 y 5, por lo que el Corolario 2.25 nos dice que $\phi(100) = 100 \cdot (1/2) \cdot (4/5) = 40$, por lo que tenemos que $3^{40} \equiv 1 \pmod{100}$. Como $1492 \equiv 12 \pmod{40}$ se deduce que $3^{100} \equiv 3^{12} \pmod{100}$. Al ser $3^4 = 81 \equiv -19 \pmod{100}$, se tiene que $3^8 \equiv (-19)^2 = 361 \equiv -39$ y, por tanto, $3^12 \equiv -19 \cdot (-39) = 741 \equiv 41$. Las dos últimas cifras son, por tanto, 41. □

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.

Muchos códigos están basados en teoría de números. Uno muy simple es sustituir cada letra del alfabeto por la siguiente. Matemáticamente, podemos representar las letras como enteros $\sqcup = 0$ $A = 1$, $B = 2, \ldots, Z = 27$ y añadir 1 a cada una. Para codificar la Z como $\sqcup$ debemos sumar en módulo 28, por lo que $27 + 1 = 0$. Códigos similares se obtienen sumando un entero fijo k (conocido como *clave*), en lugar de 1: Julio Cesar utilizaba la clave $k = 3$. Para decodificar debemos realizar, simplemente, la transformación inversa, restar k (mod 28).

Estos códigos son fáciles de romper. Podemos probar todos los posibles valores de k hasta obtener un mensaje comprensible, o podemos comparar las letras más frecuentes en el mensaje con las que se saben que son más frecuentes en la lengua original (E y T en Inglés), para encontrar k.

Un tipo de código, ligeramente más seguro utiliza transformaciones afines de la forma $x \mapsto ax + b \pmod{28}$, para distintos enteros a y b. Para poder decodificar con éxito debemos poder recuperar un único valor de x a partir de

$ax + b$, y esto es posible si, y sólo si, a es una unidad en $\mathbf{Z}_{28}$, por lo que si contamos las posibles parejas a, b observamos que existen $\phi(28) \cdot 28 = 14 \cdot 28 = 392$ posibles códigos. Romper tal codificación probando todas las posibles parejas a y b resultaría tedioso a mano (aunque es fácil con un ordenador) pero, de nuevo, investigar la frecuencia puede hacer la tarea mucho más fácil.

Se puede mejorar bastante con códigos basados en el Pequeño Teorema de Fermat. La idea es la siguiente: Elegimos un primo grande p y un entero e primo con $p - 1$. Para codificar, utilizamos la transformación $\mathbf{Z}_p \to \mathbf{Z}_p$ dada por $x^e \pmod p$ (hemos visto cómo calcular de forma eficiente grandes potencias en $\mathbf{Z}_p$). Si $0 < x < p$, x es primo con p, por lo que $x^{p-1} \equiv 1 \pmod p$. Para decodificar debemos hallar primero el inverso f de e módulo $p - 1$, es decir, debemos resolver la congruencia $ef \equiv 1 \pmod{p-1}$ utilizando el método descrito en la página 71; esto es posible por ser e una unidad módulo $p-1$. Por tanto, $ef = (p-1)k + 1$ para algún entero k, por lo que $(x^e)^f = x^{(p-1)k+1} = (x^{p-1})^k \cdot x \equiv x \pmod p$. De este modo, podemos determinar x a partir de x^e, simplemente elevando a la potencia f-ésima , por lo que el mensaje puede ser decodificado de forma eficiente.

Ejemplo 2.32 Supongamos que $p = 29$ (que, aunque en la realidad no es útil, lo elegimos para ilustrar el ejemplo). Debemos elegir e primo con $p-1 = 28$ y hallar f tal que $ef \equiv 1 \pmod{28}$. Si tomamos, por ejemplo, $e = 5$ codificamos aplicando $x \mapsto x^5 \pmod{29}$ y al ser $f = 17$ decodificamos mediante $x \mapsto x^{17} \pmod{29}$. Obsérvese que $(x^5)^{17} = x^{85} = (x^{28})^3 \cdot x \equiv x \pmod{29}$, ya que $x^{28} \equiv 1 \pmod{29}$ para cualquier x primo con 29, por lo que la decodificación es la inversa de la codificación. □

Representar, individualmente, las letras como números, no es seguro, ya que quien espía puede hacer uso del conocimiento de la frecuencia de las letras. Un método mejor consiste en agrupar las letras en bloques de longitud k y representar cada bloque como un entero x (si la longitud del texto no es un múltiplo de k, se pueden añadir al final una serie de letras sin sentido). Elegimos p suficientemente grande para que los distintos bloque de longitud k puedan representarse mediante diferentes clases de congruencia $x \not\equiv 0 \pmod p$ y codificamos y decodificamos mediante $x \mapsto x^e$ y $x \mapsto x^f \pmod p$ respectivamente.

Romper estos códigos resulta muy difícil. Supongamos, por ejemplo, que un espía ha descubierto el valor de p utilizado y que también conoce una pareja x e $y \equiv x^e \pmod p$. Para romper el código necesita conocer el valor de f (o equivalentemente, de e), pero como p es suficientemente grande (digamos de,

al menos, un centenar de dígitos), no se conoce ningún algoritmo eficiente para calcular e a partir de la congruencia $y \equiv x^e \pmod{p}$ donde x e y son conocidos. A veces se le llama *problema del logaritmo discreto*, ya que podemos ver esta congruencia como una versión modular de la ecuación $e = \log_x y$. La seguridad del método consiste en que mientras que las potencias son fáciles de calcular en aritmética modular, los logaritmos parece ser que son difíciles.

Un inconveniente de este tipo de código es que el remitente y receptor deben estar de acuerdo, con anterioridad, en los valores de p y e (llamados la *clave* del código). Teniendo en cuenta que, por seguridad, deberán cambiar la *clave* de vez en cuando, ¿de qué modo pueden hacerlo de forma segura? Podrían, por supuesto, intercambiar esta información en forma codificada, pero entonces tendrían que estar de acuerdo acerca de los detalles de la codificación utilizada para discutir la clave, de forma que nadie resuelva el problema.

2.8.1 Criptografía RSA

Esta dificultad puede evitarse utilizando un *sistema criptográfico de clave pública*. Nosotros nos limitaremos a estudiar el método desarrollado en 1978 por R.L. Rivest, A. Shamir y L. Adleman y que es conocido como *sistema criptográfico RSA* (iniciales de sus autores).

Para codificar un mensaje con un código R.S.A. 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)(␣A␣T)(ODOS). Asignando a cada letra un elemento de $\mathbf{Z}_{28}$ (ver la biyección establecida anteriormente) convertimos cada grupo en un número, pero teniendo en cuenta que cada letra va a ser representada por dos dígitos, es decir, A no 1 sino 01, B será 02, etc. ya que de lo contrario no sabríamos más tarde si 11 es AA o K. De esta manera nuestros grupos se transforman en 08161201, 00010021 y 16041620 respectivamente. A cada uno de estos números lo denominaremos *palabra* y vamos a codificar palabra a palabra.

Elijamos ahora dos números q y s de tal forma que q sea primo con todas las palabras del texto (esto se puede garantizar tomando q de tal manera que todos sus divisores primos sean mayores que la mayor palabra posible, en nuestro caso 27272727) y s sea primo con $\phi(q)$ (función de Euler). El texto se codifica sustituyendo cada palabra n por $n^s \bmod q$.

Así, la palabra 9171302 tomando $q = 3524084471 = 59359 \times 59369$ y $s = 5$ (ya que $\phi(q) = 59358 \times 59368 = 3523965744$ y 5 es primo con $\phi(q)$), se convertirá

en la palabra codificada $9171302^5 \bmod q = 2839270855$.

Al ser s primo con $\phi(q)$ sabemos que existe $t = s^{-1} \bmod \phi(q)$ verificando que $ts + \alpha\phi(q) = 1$.

Entonces:

$$n = n^{ts+\alpha\phi(q)} = n^{ts} n^{\alpha\phi(q)}$$

Como q es primo con n (q se eligió primo con todas las palabras del texto), por el *Teorema de Fermat* sabemos que $n^{\phi(q)} = 1 \bmod q$, por lo que $n^{ts} \bmod q = n$.

Así pues, si la palabra codificada es $c = n^s \bmod q$ donde n es la palabra original, entonces $c^t \bmod q = n^{st} \bmod q = n$. Es decir, decodificar el mensaje consiste en volver a codificarlo utilizando ahora q y t con $t = s^{-1} \bmod \phi(q)$.

Nos encontramos en este proceso con dos dificultades, a saber:

a) Para codificar hemos elevado cada palabra a la potencia s y para decodificar debemos elevarlas a $t = s^{-1} \bmod \phi(q)$. Si como en nuestro ejemplo $q = 3524084471$ y $s = 5$ entonces, $t = 740793149$.

b) Para hallar t es necesario conocer primero $\phi(q)$ y para ello es necesario factorizar previamente q.

El primer problema hemos visto que tiene fácil solución sin más que aplicar el método descrito en la página 71, sin embargo, el segundo no tiene solución, ya que un número de más de 10 o 12 cifras es muy difícil saber si es o no primo. Es más, existen algoritmos para encontrar números con la garantía de que ningún otro algoritmo pueda decidir si este es o no primo.

Precisamente la imposibilidad de poder factorizar un número de este tipo es lo que garantiza la seguridad del método.

Ejemplo 2.33 Supongamos que se han elegido $q_1 = 89$ y $q_2 = 97$, por lo que se hace público $q = 89 \cdot 97 = 8633$, mientras que $\phi(q) = 88 \cdot 96 = 8448 = 2^8 \cdot 3 \cdot 11$ se mantiene en secreto. El receptor elige y publica un entero s primo con $\phi(q)$, digamos que $s = 71$. Se halla (y se mantiene en secreto) el inverso $t = s^{-1} = 71^{-1} = 119 \pmod{8448}$.para enviar un mensaje, cualquiera puede buscar el par $q = 8633$ y $s = 71$ y codificar mediante $n \mapsto n^{71} \pmod{8633}$. Para decodificar, el receptor utiliza la transformación $n \mapsto n^{119} \pmod{8633}$, que no está disponible por nadie que no conozca que $t = 119$. Un espía necesitaría factorizar $q = 8633$ para hallar $\phi(q)$ y, a partir de él, encontrar t. Por supuesto que la factorización de 8633 no presenta ninguna dificultad, pero esto sólo es una simple ilustración del método. La elección de dos primos p_1 y p_2 significativamente mayores, hace el problema mucho más duro. □

Este sistema proporciona también una *firma* del mensaje para demostrar a un receptor que viene de mi y no de ningún otro. Primero decodifica su nombre utilizando su n y f (que se mantiene en secreto). Se codifica después el resultado utilizando la clave q y s del receptor (que es de conocimiento público) y se envía. Descifrará este mensaje con su propio q y t y codificará el resultado con nuestro q y s (que también son públicos). Al final de este proceso, el receptor debe tener su nombre, ya que ha invertido las dos aplicaciones utilizadas. Sólo usted puede haber aplicado correctamente la primera transformación, por lo que él sabe que el mensaje ha sido enviado por usted.

El sistema de comunicación es el siguiente. Establecido el número r (longitud de los grupos a codificar) entre los interlocutores A, B y C, cada uno de ellos construye un número q_A, q_B y q_C respectivamente y hacen *públicas* sus respectivas claves (q_A, s_A), (q_B, s_B) y (q_C, s_C).(La norma para elegir q es tomar el producto de dos primos de más de $2r + 1$ dígitos cada uno). Los números $t_A = s_A^{-1} \bmod \phi(q_A)$, t_B y t_C sólo son conocidos y sólo pueden ser calculados por A, B y C respectivamente.

Si A desea enviar el mensaje M a B, realiza el siguiente proceso: codifica (M,q_A,s_A) dos veces, la primera con la clave (q_A, t_A) y la segunda con la clave (q_B, s_B).

$$(\mathrm{M}, \mathrm{q_A}, \mathrm{s_A}) \xrightarrow{\mathrm{q_A,t_A}} (\mathrm{M'}, \mathrm{q'}, \mathrm{s'}) \xrightarrow{\mathrm{q_B,s_B}} (\mathrm{E}, \mathrm{q}, \mathrm{s})$$

B recibe de A el mensaje $(\mathrm{E}, \mathrm{q}, \mathrm{s})$ y lo codifica otras dos veces, la primera con la clave (q_B, t_B) y la segunda con (q_A, s_A).

$$(\mathrm{E}, \mathrm{q}, \mathrm{s}) \xrightarrow{\mathrm{q_B,t_B}} (\mathrm{M'}, \mathrm{q'}, \mathrm{s'}) \xrightarrow{\mathrm{q_A,s_A}} (\mathrm{M}, \mathrm{q_A}, \mathrm{s_A})$$

Si C enviase un mensaje a B para que este crea que procede de A, como C no conoce t_A realizaría el siguiente proceso:

$$(\mathrm{M}, \mathrm{q_A}, \mathrm{s_A}) \xrightarrow{\mathrm{q_A,t'_A}} (\mathrm{M'}, \mathrm{q'}, \mathrm{s'}) \xrightarrow{\mathrm{q_B,s_B}} (\mathrm{E}, \mathrm{q}, \mathrm{s})$$

B recibe, supuestamente de A $(\mathrm{E}, \mathrm{q}, \mathrm{s})$ y decodifica como antes:

$$(\mathrm{E}, \mathrm{q}, \mathrm{s}) \xrightarrow{\mathrm{q_B,t_B}} (\mathrm{M'}, \mathrm{q'}, \mathrm{s'}) \xrightarrow{\mathrm{q_A,s_A}} (\mathrm{M''}, \mathrm{q'_A}, \mathrm{s'_A})$$

pero observa que (q'_A, s'_A) no es la clave de A, por lo que deduce inmediatamente que el mensaje no puede provenir de A.

2.9 Ejercicios propuestos

Ejercicio 2.1 Sin realizar los productos, calcular los restos de dividir:

a) 28×33 entre 35, b) 15×59 entre 75, c) 3^8 entre 13,
d) 5^{28574} entre 17, e) 35^{346} entre 41.

Ejercicio 2.2 Sin hacer uso de una calculadora, encontrar el resto de dividir:

a) 34×17 entre 29, mb) 19×14 entre 23,
c) 5^{10} entre 19, md) $1! + 2! + 3! + \cdots + 10!$ entre 10.

Ejercicio 2.3 Probar, mediante congruencias, que $3^{2n+5} + 2^{4n+1}$ es divisible por 7 cualquiera que sea el entero $n \geq 1$.

Ejercicio 2.4

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 $a^{2k} - 1 = (a^k - 1)(a^k + 1)$.

Ejercicio 2.5 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 2.6 Encontrar la solución general de la congruencia

$$12x \equiv 9 \pmod{15}.$$

Ejercicio 2.7 Para cada una de las siguientes congruencias, decidir cuáles tienen solución y cuáles no, encontrando la solución general.

a) $3x \equiv 5 \pmod{7}$, b) $12x \equiv 15 \pmod{22}$,
c) $19x \equiv 42 \pmod{50}$, d) $18x \equiv 42 \pmod{50}$.

Ejercicio 2.8 Si $x \equiv 2 \pmod 3$ y $x \equiv 3 \pmod 5$, ¿cuánto es x mod 15?

Ejercicio 2.9 Resolver el sistema de congruencias

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

Ejercicio 2.10 Resolver el sistema de congruencias

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

Ejercicio 2.11 Resolver el sistema de congruencias

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

Ejercicio 2.12 Resolver la congruencia $91x \equiv 419 \pmod{440}$.

Ejercicio 2.13 Hallar la solución general de la congruencia

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

Ejercicio 2.14 ¿Puede conocerse un entero positivo sabiendo que es menor que 100 y conociendo los restos de sus divisiones entre 3, 5 y 7?

Ejercicio 2.15 Determinar cuáles de los siguientes sistemas de congruencias tienen solución y, en caso de tenerla, encontrar la solución general:

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

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

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

Ejercicio 2.16 Resolver el sistema de congruencias:

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

Ejercicio 2.17 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.

Ejercicio 2.18 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?

Ejercicio 2.19 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.

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.

Ejercicio 2.20 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?

Ejercicio 2.21 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.

Ejercicio 2.22 Considérese el sistema de congruencias lineales

$$\begin{cases} 2x & \equiv & 4 & \pmod{10} \\ 7x & \equiv & 19 & \pmod{24} \\ 2x & \equiv & -1 & \pmod{45} \end{cases}$$

a) Encontrar los enteros positivos a, b, c, n_1, n_2 y n_3 tales que el sistema dado sea equivalente a este otro

$$\begin{cases} x & \equiv & a & (\text{mod } n_1) \\ x & \equiv & b & (\text{mod } n_2) \\ x & \equiv & c & (\text{mod } n_3) \end{cases}$$

b) Probar que se verifican las hipótesis del Teorema Chino del Resto generalizado y que, por tanto, el sistema admite solución. Reducirlo a otro sistema equivalente en el que los módulos sean mutuamente primos entre sí.

c) Encontrar **todas** las soluciones del sistema comprendidas entre 1000 y 2000.

d) 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.

Ejercicio 2.23

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

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?

Ejercicio 2.24 Aplicar a $n = 341$ los test de base a para estudiar si es primo.

Ejercicio 2.25 Probar que 1729 y 2821 son números de Carmichael.

Ejercicio 2.26 Encontrar un número de Carmichael de la forma $7 \cdot 23 \cdot p$, donde p es primo.

Ejercicio 2.27 Encontrar dos números de Carmichael de la forma $13 \cdot 61 \cdot p$ donde p es primo.

Ejercicio 2.28 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 2.29

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

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

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, $(p_i - 1) \mid (n - 1)$ cualquiera que sea $i = 1, 2, \ldots k$.

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 2.30 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.

Ejercicio 2.31

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.

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

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

Ejercicio 2.32 ¿Para qué valores de n es $\phi(n) \equiv 2 \pmod 4$?

Ejercicio 2.33 Encontrar todos los valores de n para los que $\phi(n) = 16$.

Ejercicio 2.34

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

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

Ejercicio 2.35 Utilizar un código de Caesar con clave (3,0) en $\mathbf{Z}_{28}$ para codificar la cadena de caracteres "HOLA A TODOS"

Ejercicio 2.36 El siguiente texto está codificado usando un código de Caesar en $\mathbf{Z}_{28}$ de clave $(a, 0)$:

"DZ VJÑLÑD HÑÑA ÑDGÑ ÑNJNIZCLS ÑD YJÑ UC WCD AÑDJÑHGS ÑH VASFHÑKC"

Hallar con qué elemento está codificado y decodificarlo.

Ejercicio 2.37 Realizar la codificación RSA de "HELLO" utilizando $r = 1,\ q = 101,\ s = 3$. Comprobar decodificando el resultado.

Ejercicio 2.38 Decodificar el mensaje 1914, sabiendo que la clave pública es $(2803, 113)$.

Ejercicio 2.39 Tomando $r = 1,\ q = 29,\ s = 5$, codificar y decodificar el mensaje "CODIFICAME".

Ejercicio 2.40 Realizar la codificación RSA tomando $r = 4$, $s = 5$ y q el producto de los dos primos $q = 59359 \times 59369 = 3524084471$ de la palabra "HOLA". Comprobar el resultado decodificando.

Ejercicio 2.41 Utilizando el alfabeto {␣, E, M, N, O, P, R, S} (donde ␣ designa el espacio en blanco), y numerando sus elementos del 0 al 7 respectivamente, decodificar el mensaje $\mathbf{061-026-091-014-035-094-021}$ sabiendo que fue codificado mediante un código RSA con $r = 2$ y que la clave es $(q, s) = (101, 67)$.

Ejercicio 2.42 Considérese el alfabeto {␣, A, B, C, D, E} (donde ␣ designa el espacio en blanco), y enumérense sus elementos del 0 al 5 respectivamente. Si tomamos, para un código RSA, la clave $(q, s) = (12, 5)$ con $r = 2$ se pide:

a) Codificar el mensaje **BECA**.

b) Decodificar el mensaje codificado en el apartado anterior.

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

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, por lo que una función $f : X \to Y$ debe verificar:

$$\left.\begin{array}{l} x = y \Longrightarrow f(x) = f(y) \\ \\ \forall x \in X \Rightarrow \exists\, y \in Y \ : \ y = f(x) \end{array}\right\} \tag{3.1}$$

que son los dos requisitos lógicos que debía cumplir cualquier función.

Ejemplo 3.1 $f : \mathbf{N} \to \mathbf{N}$ dada por $f(n) = n^2$ es una función, ya que

a) $n = m \Longrightarrow n^2 = m^2$

b) $\forall n \in \mathbf{N} \Longrightarrow \exists\, n^2 \in \mathbf{N}$

que son las dos condiciones exigidas en (3.1). □

Ejemplo 3.2 $f : \mathbf{Z} \to \mathbf{R}$ dada por $f(x) = +\sqrt{x}$ no es una función ya que, por ejemplo, $-4 \in \mathbf{Z}$ y $f(-4) = +\sqrt{-4} \notin \mathbf{R}$, es decir, no existe $f(-4)$. □

Una función también puede venir definida de forma recursiva como la definida en el siguiente ejemplo:

Ejemplo 3.3

$$u(1) = 1 \qquad \text{y} \quad \forall n \in \mathbf{N} \ \ u(n+1) = \begin{cases} \frac{1}{2}u(n) & \text{si } u(n) \text{ es par} \\ \\ 5u(n) + 1 & \text{si } u(n) \text{ es impar} \end{cases}$$

obteniéndose:

$$u(2) = 6,\ u(3) = 3,\ u(4) = 16,\ u(5) = 8,\ u(6) = 4,\ u(7) = 2,\ u(8) = 1,\ \cdots$$

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 entonces preguntarse ¿que funciones van a producir transformados distintos para originales distintos?

Definición 3.1 Una función $f : X \to Y$ se dice que es *inyectiva* si a elementos distintos de X le asocia imágenes distintas en Y. Es decir:

$$f \text{ inyectiva} \iff f(x) = f(y) \Longrightarrow x = y \tag{3.2}$$

Ejemplo 3.4 $f : \mathbf{N} \to \mathbf{N}$ definida por $f(n) = 2n$ es inyectiva, ya que

$$f(n_1) = f(n_2) \Rightarrow 2n_1 = 2n_2 \Longrightarrow n_1 = n_2. \qquad \square$$

Ejemplo 3.5 $f : \mathbf{Z} \to \mathbf{Z}$ 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 del Ejemplo 3.4 es inyectiva, si denotamos por Imp al subconjunto de $\mathbf{N}$ constituido por los naturales impares, es evidente que ningún elemento de $\mathbf{N}$ se transforma mediante f en ninguno de Imp. Es decir, f transforma $\mathbf{N}$ en un subconjunto de $\mathbf{N}$ pero no en *todo* $\mathbf{N}$. En otras palabras, existen elementos del conjunto final que no son transformados de ninguno del conjunto inicial.

Cabe entonces el preguntarse ¿qué funciones transforman el conjunto original en *todo* el conjunto final?

Definición 3.2 Una función $f : X \to Y$ se dice que es *sobreyectiva* si cualquier elemento del conjunto final es transformado de alguno del conjunto original.

$$f \text{ sobreyectiva} \iff \forall y \in Y \ \ \exists\, x \in X \ : \ f(x) = y \tag{3.3}$$

Ejemplo 3.6 La función $f : \mathbf{R} \cup \{0\} \to \mathbf{R}^+$ definida por $f(x) = x^2$ es sobreyectiva, ya que cualquier número real positivo es el cuadrado de otro número real (su raíz cuadrada). 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 3.3 Una función $f : X \to Y$ se dice que es *biyectiva*, o que se trata de una *biyección* si es simultáneamente inyectiva y sobreyectiva.

$$f \text{ biyectiva} \iff \begin{cases} \text{1.- Es inyectiva} & f(x) = f(y) \Rightarrow x = y \\ \text{2.- Es sobreyectiva} & \forall y \in Y \ \exists\, x \in X \ : \ f(x) = y \end{cases} \tag{3.4}$$

Ejemplo 3.7 La función $f : \mathbf{N} \to \mathbf{N} \cup \{0\}$ definida por $f(n) = n - 1$ es una biyección. $\square$

3.1.1 Enumeración

Una aplicación inmediata de las funciones inyectivas 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.

Si construimos para cada $n \in \mathbf{N}$ el subconjunto $\mathbf{N}_n$ de $\mathbf{N}$ definido por $\mathbf{N}_n = \{1,\ 2, \ldots,\ n\}$, el decir que X tiene n elementos equivale a decir que se puede establecer una biyección entre $\mathbf{N}_n$ y X.

Al número de elementos de un conjunto X 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.

Dados dos conjuntos A y B, se define el conjunto *unión* y se denota por $A \cup B$ como el conjunto de todos los elementos que pertenecen a A o a B.

$$x \in A \cup B \iff \begin{cases} x \in A \\ \text{ó} \\ x \in B \end{cases}$$

Se define el conjunto *intersección* y se denota por $A \cap B$ como el conjunto de los elementos que pertenecen simultáneamente a ambos conjuntos.

$$x \in A \cap B \iff \begin{cases} x \in A \\ \text{y} \\ x \in B \end{cases}$$

Ejemplo 3.8 Si $A = \{1,\ 2,\ 3\}$ y $B = \{2,\ 4,\ 6\}$, tenemos que

$$A \cup B = \{1,\ 2,\ 3,\ 4,\ 6\} \qquad \text{y} \qquad A \cap B = \{2\}$$ □

Si la intersección de dos conjuntos es vacía, diremos que dichos conjuntos son *disjuntos*.

$$A \text{ y } B \text{ disjuntos} \iff A \cap B = \emptyset$$

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

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|.$$

Otro resultado que se obtiene del Lema 3.1 es el denominado *principio de las cajas* que describimos a continuación.

Teorema 3.3 [Principio de las cajas] *Si queremos repartir n objetos en m cajas con $rm < n$, 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:

$$|A_1| + |A_2| + \cdots + |A_m| \leq m \cdot \max_i |A_i| \Rightarrow n \leq m \cdot \max_i |A_i|$$

Si fuese $\max\limits_i |A_i| \leq r$ tendríamos que $n \leq mr$ contra la hipótesis de que $n > rm$. Por tanto , ha de ser $\max\limits_i |A_i| > r$, es decir, alguna de las cajas ha de recibir más de r objetos. ■

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 $A \cap B = \emptyset \Longrightarrow |A \cap B| = 0$, en cuyo caso no tenemos otra cosa que el principio de adición.

Para el caso de tres conjuntos se verifica

$$\begin{aligned}
|A \cup B \cup C| &= |A \cup (B \cup C)| = |A| + |B \cup C| - |A \cap (B \cup C)| = \\
&= |A| + |B| + |C| - |B \cap C| - |(A \cap B) \cup (A \cap C)|^{(1)} \; = \\
&= |A| + |B| + |C| - |B \cap C| - \{|A \cap B| + |A \cap C| - |A \cap B \cap C|\} = \\
&= |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|
\end{aligned}$$

Llamando $\begin{aligned} \alpha_1 &= |A| + |B| + |C| \\ \alpha_2 &= |A \cap B| + |A \cap C| + |B \cap C| \\ \alpha_3 &= |A \cap B \cap C| \end{aligned}$

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*

$$\begin{aligned}
\alpha_1 &= |A_1| + |A_2| + \cdots + |A_n| \\
\alpha_2 &= |A_1 \cap A_2| + |A_1 \cap A_3| + \cdots + |A_{n-1} \cap A_n| \\
&\vdots \\
\alpha_n &= |A_1 \cap A_2 \cap \cdots \cap A_n|
\end{aligned}$$

se verifica

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \alpha_1 - \alpha_2 + \cdots + (-1)^{n+1}\alpha_n.$$

(1) Debido a la distributividad de la intersección respecto a la unión de conjuntos. Consúltese cualquier texto elemental de teoría de conjuntos.

3.4 Contar en tablas

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 $X \times Y$

$$X \times Y = \{(x, y) \ : \ x \in X, \ y \in Y\}$$

verificándose que $|X \times Y| = |X| \times |Y|$.

Un subconjunto T del conjunto producto cartesiano $X \times Y$ recibe el nombre de *tabla*

	y_1	y_2	y_3	y_4	y_5	y_6
x_1	•	•		•		
x_2	•			•		•
x_3					•	
x_4		•	•			
x_1	•					•

Tabla 3.1: Una 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. Una vez representados todos los elementos de T contamos los elementos de cada fila y sumamos los parciales obtenidos. Este resultado ha de ser el mismo que si contamos los elementos de cada columna y sumamos los resultados obtenidos.

Ejemplo 3.9 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. El hecho de que x conozca a y lo señalaremos escribiendo en una lista el par (x, y).

Sea $x \in X$, llamamos F_x al número de alumnas que conoce el alumno x:

$$F_x = |\{y \in Y \ : \ (x, y) \in T\}|$$

Dado $y \in Y$, llamamos C_y al número de alumnos que conoce la alumna y:

$$C_y = |\{x \in X \ : \ (x, y) \in T\}|$$

Contar en filas no es más que calcular $\sum_{x \in X} F_x$ mientras que contar en columnas es calcular $\sum_{y \in Y} C_y$. Evidentemente ha de verificarse que

$$\sum_{x \in X} F_x = \sum_{y \in Y} C_y = |T|$$

En nuestro ejemplo, 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.

$$\left.\begin{array}{l} \sum_{x \in X} F_x = 5 + 5 + \overset{(32}{\cdots} + 5 = 5 \cdot 32 = 160 \\ \sum_{y \in Y} C_y = 8 + 8 + \overset{(n}{\cdots} + 8 = 8n \end{array}\right\} \Rightarrow 160 = 8n \Rightarrow n = 20$$

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

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

$$f(1) = \text{c},\ f(2) = \text{a},\ f(3) = \text{s y } f(4) = \text{a}.$$

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* de n elementos con longitud m.

Teorema 3.5 *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 3.10 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 $2^{|X|} = 2^n$. □

3.5.1 Variaciones sin repetición

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 3.6 *Si $|X| = n$ el número de variaciones sin repetición de longitud m es*

$$n(n-1)(n-2)\cdots(n-m+1) \tag{3.5}$$

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. ■

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 biyecciones las llamaremos *permutaciones*, ya que al ser sobreyectiva la función, lo único que hacemos es permutar el orden de los elementos de X.

Frecuentemente se toma como conjunto X al propio $\mathbf{N}_n$, por lo que una permutación de, por ejemplo, $\mathbf{N}_5$ sería la dada por

$$\alpha(1) = 2 \qquad \alpha(2) = 4 \qquad \alpha(3) = 5 \qquad \alpha(4) = 1 \qquad \alpha(5) = 3$$

Evidentemente, al tratarse de una biyección es inyectiva por lo que su número vendrá dado por la fórmula (3.5) y por ser además sobreyectiva se verifica que $m = n$, por lo que el número de permutaciones de n elementos, que se denota por $n!$ y se lee n *factorial* viene dado por

$$n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$$

Al conjunto de todas las permutaciones de $\mathbf{N}_n$ se le denota por S_n.

Consideremos el permutación β definida por

$$\beta(1) = 3 \qquad \beta(2) = 5 \qquad \beta(3) = 1 \qquad \beta(4) = 4 \qquad \beta(5) = 2$$

Como dos permutaciones α y β son funciones biyectivas de $\mathbf{N}_n$ en $\mathbf{N}_n$, pueden componerse obteniéndose una nueva función biyectiva sobre el mismo conjunto $\mathbf{N}_n$, es decir, podemos definir la permutación producto $\beta\alpha$ como la aplicación compuesta $\beta \circ \alpha$.

$$\begin{array}{rccl} \beta\alpha: & \mathbf{N}_n & \longrightarrow & \mathbf{N}_n \\ & i & \longmapsto & \beta\alpha(i) = \beta[\alpha(i)] \end{array}$$

De esta forma en nuestro ejemplo obtenemos

$$\beta\alpha(1) = 5 \qquad \beta\alpha(2) = 4 \qquad \beta\alpha(3) = 2 \qquad \beta\alpha(4) = 3 \qquad \beta\alpha(5) = 1$$

Por tratarse de aplicaciones sobreyectivas verifican las propiedades enunciadas a continuación.

Propiedades

a) Si $\pi\ ,\ \sigma \in S_n$ se tiene que $\pi\sigma \in S_n$.

b) Cualesquiera que sean $\pi\,\sigma,\ \tau \in S_n$ se verifica que $\pi(\sigma\tau) = (\pi\sigma)\tau$.

c) Denotando por i a la permutación identidad, es decir, a aquella para la cual es $i(n) = n$ cualquiera que sea el elemento $n \in \mathbf{N}_n$, se cumple $i\sigma = \sigma i = \sigma$ para cualquier permutación σ de S_n.

d) Cualquier permutación $\sigma \in S_n$ posee una permutación inversa $\sigma^{-1} \in S_n$, es decir, existe una permutación σ^{-1} tal que $\sigma\sigma^{-1} = \sigma^{-1}\sigma = i$.

Descomposición en producto de ciclos

Consideremos la permutación α de $\mathbf{N}_5$ de nuestro ejemplo. Se puede observar que

$$1 \xrightarrow{f} 2 \xrightarrow{f} 4 \xrightarrow{f} 1$$

$$3 \xrightarrow{f} 5 \xrightarrow{f} 3$$

Podemos expresar esta situación poniendo $\alpha = (124)(35)$ lo que nos dice que considerando (124) como un *ciclo*, el 1 se transforma en el 2, este en el 4 y este en el 1. El ciclo (35) nos dice que 3 se transforma en 5 y 5 en 3.

Esta manera de expresar una permutación se dice que es descomponerla en producto de ciclos. Obsérvese que (35) indica que 3 se transforma en 5 y 5 en tres, pero se trataría de una permutación que deja invariantes a los otros tres elementos de $\mathbf{N}_5$, de aquí que se trate de un *producto* de ciclos. Téngase en cuenta también que por ser un producto se trata de una composición de funciones y que esta operación *no* es conmutativa. En nuestro ejemplo, dado que los elementos que se alteran en el primer ciclo son independientes de los que se alteran en el segundo, el producto sí sería conmutativo pero si los ciclos no fuesen disjuntos hay que realizar las operaciones de derecha a izquierda.

Ejemplo 3.11 Sean $\alpha,\ \beta$ las permutaciones de $\mathbf{N}_9$ definidas por

$$\alpha = (1237)(49)(58) \qquad \beta = (135)(246)(789)$$

entonces:

a) $\alpha\beta = (17529)(3846)$ b) $\beta\alpha = (14738)(2596)$

c) $\alpha^2 = (13)(27)$ d) $\beta^2 = (153)(264)(798)$

e) $\alpha^{-1} = (1732)(49)(58)$ f) $\beta^{-1} = (153)(264)(798)$ □

3.6 Números binómicos

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 3.7 *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

***U*:** Subconjuntos de r elementos que contienen a x.

***V*:** Subconjuntos de r elementos que no contienen a x.

por lo que

$$\binom{n}{r} = |U| + |V| \tag{3.6}$$

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

$$|U| = \binom{n-1}{r-1} \tag{3.7}$$

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. Por tanto

$$|V| = \binom{n-1}{r} \tag{3.8}$$

Llevando (3.7) y (3.8) a (3.6) queda probado el teorema. ■

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.

Este teorema permite calcular los números binómicos de forma recursiva construyendo el denominado *triángulo de Pascal*.

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

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.

$$\begin{array}{ccccccccccc}
 & & & 1 & & & & 1 & & & \\
 & & 1 & & & 2 & & & 1 & & \\
 & 1 & & & 3 & & & 3 & & & 1 \\
\ldots & & \ldots & & & \ldots & & & \ldots & & \ldots
\end{array}$$

Teorema 3.8 *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 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 3.9 *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

$$[i \cdot (i-1) \cdot (i-2) \cdots 2 \cdot 1] \,|\, [p \cdot (p-1) \cdot (p-2) \cdots (p-i+1)]$$

y como $[i \cdot (i-1) \cdot (i-2) \cdots 2 \cdot 1] \perp p$ por ser p primo, necesariamente

$$[i \cdot (i-1) \cdot (i-2) \cdots 2 \cdot 1] \,|\, [(p-1) \cdot (p-2) \cdots (p-i+1)]$$

por lo que

$$\binom{p}{i} = p \cdot \frac{(p-1) \cdot (p-2) \cdots (p-i+1)}{i \cdot (i-1) \cdot (i-2) \cdots 2 \cdot 1} = pq \quad \text{con} \quad q \in \mathbf{Z}$$

y, por tanto, $p \,|\, \binom{p}{i}$. ■

Una propiedad que se deduce de manera inmediata es expuesta en el siguiente teorema.

Teorema 3.10 *Si n y r son dos enteros no negativos, se verifica que*

$$\binom{n}{r} = \binom{n}{n-r}$$

Demostración. Basta observar que

$$\binom{n}{n-r} = \frac{n!}{(n-r)!\,[n-(n-r)]!} = \frac{n!}{(n-r)!\,r!} = \binom{n}{r}.$$ ■

Obsérvese que la definición de $\binom{n}{0}$ hace que la propiedad se cumpla siempre ya que se debe verificar que $\binom{n}{0} = \binom{n}{n}$ y dado que un conjunto de n elementos sólo posee un subconjunto de n elementos (el propio conjunto), si hubiésemos definido $\binom{n}{0} \neq 1$ la propiedad no sería cierta.

3.6.1 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 sean colocadas). Podemos formar los grupos:

$$\begin{array}{cccccccc} aaaa & aaab & aaac & aabb & aabc & aacc & abbb & abbc \\ abcc & accc & bbbb & bbbc & bbcc & bccc & cccc & \end{array}$$

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 3.11 *El numero 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,

$$\begin{array}{ccc} aabc & \longrightarrow & 110101 \\ abbc & \longrightarrow & 101101 \end{array}$$

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 3.12 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 (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 3.13 En el Ejemplo 3.12 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 $N(c_i) = \binom{7}{3} = 35$. 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

$$S_1 = N(c_1) + N(c_2) + N(c_3) + N(c_4) = \binom{4}{1} N(c_i) = 4 \cdot 680 = 2720$$

$$S_2 = \binom{4}{2} N(c_1 c_j) = 6 \cdot 35 = 210$$

$$S_3 = \binom{4}{3} N(c_i c_j c_k) = 0$$

$$S_4 = \binom{4}{4} N(c_i c_j c_k c_l) = 0$$

por lo que

$$N(\bar{c_1}\bar{c_2}\bar{c_3}\bar{c_4}) = 3276 - 2720 + 210 - 0 + 0 = 766.$$

es decir, sólo existen ahora 766 soluciones a nuestro problema. □

Ejemplo 3.14 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

$$\binom{36}{33} = \binom{36}{3} = 7140.$$

□

3.6.2 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 3.12 [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

$$(a+b)\cdot(a+b)\overset{(n}{\cdots}\cdot(a+b)$$

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 3.15 Basándose en el Teorema 3.9 podemos demostrar, por inducción, el Pequeño Teorema de Fermat, es decir, que si p es primo se verifica que $p \mid a^p - a$ cualquiera que sea el entero a. En efecto:

Para $a = 1$ se reduce a probar que $p \mid 1^p - 1 = 0$ 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 3.9), 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 propuestos

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.

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.

Ejercicio 3.3 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?

Ejercicio 3.4 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?

Ejercicio 3.5 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?

Ejercicio 3.6 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.

Ejercicio 3.7 Usar la fórmula del cardinal de una unión para encontrar el valor de $\phi(60)$.

Ejercicio 3.8

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

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

Ejercicio 3.9 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.

Ejercicio 3.10 ¿Cuántos números de teléfono de 5 dígitos tienen un dígito que aparece más de una vez?

Ejercicio 3.11 Si V_{nk} designa en número de posibles elecciones de k objetos de entre n, importando el orden, probar que $V_{n(n-1)} = V_{nn}$, interpretando el por qué.

Ejercicio 3.12 ¿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 $\phi(n) = 10082272$?

Ejercicio 3.13 ¿De cuántas maneras se pueden ordenar las letras de la palabra XSIAON de modo que las palabras ASI y NO nunca aparezcan?

Ejercicio 3.14 ¿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)?

Ejercicio 3.15 Definimos la *distancia* entre dos secuencias binarias de longitud n como el número de lugares en que difieren. ¿Cuántas secuencias están a una distancia d de una secuencia dada? Obtener una expresión para el número de secuencias que están a una distancia, no superior a d, de una dada.

Ejercicio 3.16 Describir un método para generar todas las permutaciones de n elementos a partir de las de $n-1$ elementos.

Ejercicio 3.17

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 3.18 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.

Ejercicio 3.19 Probar las igualdades:

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

Ejercicio 3.20 Probar la identidad:

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

Ejercicio 3.21 Probar la identidad:

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n}$$

Ejercicio 3.22 Usar la igualdad $k^2 = 2\binom{k}{2} + \binom{k}{1}$ para demostrar la fórmula:

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

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 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?

Ejercicio 3.25 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.

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.

Una forma particular de la recurrencia general es aquella en que u_n viene dada en función de $u_{n-1},\ u_{n-2}, \ldots, u_{n-k}$.

$$u_0 = c_0,\ u_1 = c_1, \ldots, u_{k-1} = c_{k-1}$$
$$u_n + a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k} = 0 \quad n \geq k$$

donde $c_0,\ c_1, \ldots, c_{k-1}$ y $a_1,\ a_2, \ldots,\ a_k$ son constantes conocidas. Esta forma particular de recurrencia recibe el nombre de *recurrencia lineal homogénea* de orden k y veremos que, en este caso, siempre existe una fórmula explícita que la define, aunque no siempre será factible utilizarla. Aquí nos limitaremos a probar el caso $k = 2$, aunque a continuación daremos el teorema para el caso general de $k \in \mathbf{N}$.

Teorema 4.1

Sea u_n una sucesión que satisface la recurrencia lineal

$$u_0 = c_0,\ u_1 = c_1$$
$$u_n + a_1 u_{n-1} + a_2 u_{n-2} = 0 \quad (n \geq 2)$$

y sean α y β las raíces de la ecuación auxiliar

$$t^2 + a_1 t + a_2 = 0$$

Si $\alpha \neq \beta$, entonces existen constantes A y B tales que

$$u_n = A\alpha^n + B\beta^n \quad (n \geq 0)$$

mientras que si $\alpha = \beta$, existen constantes C y D tales que

$$u_n = (Cn + D)\alpha^n \quad (n \geq 0)$$

Las constantes A y B (o bien C y D según el caso), están determinadas por c_1 y c_2.

Demostración.

a) $\boldsymbol{\alpha \neq \beta}$

Las ecuaciones

$$A + B = c_0, \qquad A\alpha + B\beta = c_1$$

determinan A y B:

$$A = \frac{c_1 - c_0\beta}{\beta - \alpha}, \qquad B = \frac{c_1 - c_0\alpha}{\alpha - \beta}$$

Por lo tanto, si asignamos a A y B estos valores, se verificará para u_1 y u_2. 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 cuadrática.

Por el principio de inducción tenemos entonces que el resultado es cierto para cualquier $n \in \mathbf{N}$.

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 *Sea (u_n) una sucesión definida por recurrencia lineal homogénea y sean $\alpha_1,\ \alpha_2, \ldots,\ \alpha_s$ las raíces de la ecuación auxiliar 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

$$A_0 + A_1n + \cdots + A_{m_i-1}n^{m_i-1}$$

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:

$$F_1 = 1\ ,\ F_2 = 1$$
$$F_n = F_{n-1} + F_{n-2}$$

En este caso, la ecuación auxiliar es

$$t^2 - t - 1 = 0$$

cuyas raíces son $\dfrac{1+\sqrt{5}}{2}$ y $\dfrac{1-\sqrt{5}}{2}$, por lo que

$$F_n = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Sustituyendo los valores conocidos para $n = 1$ y $n = 2$ obtenemos los valores de A y B quedándonos por último que

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right] \quad (n \geq 2)$$

□

4.2 Recurrencias lineales no homogéneas

Trataremos ahora de resolver relaciones de recurrencia en las que el término independiente no es nulo, es decir, recurrencias del tipo

$$u_{n+1} + a_1 u_n = f(n) \quad n \geq 0 \quad \text{con } u_0 = c_0$$

$$u_{n+2} + a_1 u_{n+1} + a_2 u_n = f(n) \quad n \geq 0 \quad \text{con } u_0 = c_0 \text{ y } u_1 = c_1$$

Este tipo de recurrencias tiene como solución $u_n = u_n^{(h)} + u_n^{(p)}$ donde $u_n^{(h)}$ es la solución general de la *recurrencia lineal homogénea* (RLH) *asociada* (la resultante de sustituir $f(n)$ por 0) y $u_n^{(p)}$ es una solución particular de la recurrencia no homogénea.

Aunque no existe un método general para encontrar una solución particular $u_n^{(p)}$, el *método de los coeficientes indeterminados* nos va a proporcionar esta solución en función de la forma que tiene la función $f(n)$.

Ejemplo 4.2 Para resolver la relación de recurrencia

$$u_n - 3u_{n-1} = 5 \cdot 7^n \quad \text{con} \quad u_0 = 2,$$

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^n no es una solución 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 4.3 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 $u_n = (2 + 5n)3^n$. □

Los ejemplos anteriores nos permiten observar que si $f(n) = k \cdot r^n$ donde k es una constante, $n \geq 0$ y la recurrencia es de primer orden, que $u_n^{(p)} = C \cdot r^n$ (donde C representa una constante) si r^n no satisface la RLH asociada, mientras que $u_n^{(p)} = C \cdot n \cdot r^n$ en caso contrario.

Para recurrencias de segundo orden se tiene que

a) $u_n^{(p)} = C \cdot r^n$ si r^n no es solución de la RLH asociada.

b) $u_n^{(p)} = C \cdot n \cdot r^n \quad$ si $\quad u_n^{(h)} = A \cdot r^n + B \cdot r_1^n \quad$ con $\quad r_1 \neq r$.

c) $u_n^{(p)} = C \cdot n^2 \cdot r^n \quad$ si $\quad u_n^{(h)} = (A + Bn) \cdot r^n$.

En los casos en los que $f(n) = P(n)$ se trata de buscar, en función del orden de la recurrencia y del grado de $P(n)$, una solución particular de la RLH asociada $u_n^{(p)}$ que también sea un polinomio.

Ejemplo 4.4 Consideremos la recurrencia $u_{n+2}+4u_{n+1}+4u_n = n^2$ con $u_0 = 0$ y $u_1 = 2$. La RLH asociada $u_{n+2} + 4u_{n+1} + 4u_n = 0$ tiene por solución $u_n^{(h)} = (An + B)(-2)^n$.

Tratemos de buscar un polinomio de segundo grado que sea solución particular de la recurrencia. Sea $u_n^{(p)} = Cn^2 + Dn + E$, entonces

$$C(n+2)^2+D(n+2)+E+4C(n+1)^2+4D(n+1)+4E+4Cn^2+4Dn+4E = n^2$$

de donde desarrollando e igualando coeficientes obtenemos:

$$\begin{array}{rl} 9C = 1 & \\ 9D + 12C = 0 & \Longrightarrow \left\{ \begin{array}{l} C = \frac{1}{9} \\ D = -\frac{4}{27} \\ E = 0 \end{array} \right. \\ 9E + 6D + \ 8C = 0 & \end{array}$$

por lo que $u_n^{(p)} = \dfrac{1}{9}n^2 - \dfrac{4}{27}n = \dfrac{1}{27}(3n^2 - 4n)$ y, por tanto

$$u_n = (An + B)(-2)^n + \frac{1}{27}(3n^2 - 4n)$$

de $u_0 = 0$ y $u_1 = 2$ obtenemos que $A = -\frac{55}{54}$ y $B = 0$, por lo que la solución general de la recurrencia es

$$u_n = -\frac{55}{54}n(-2)^n + \frac{1}{27}(3n^2 - 4n)$$

□

4.3 Ejercicios propuestos

Ejercicio 4.1 Encontrar una fórmula explícita para los términos de la sucesión definida por:

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

Ejercicio 4.2 Hallar una fórmula explícita para los términos de la sucesión definida por:

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

Ejercicio 4.3 Hallar una fórmula explícita para los términos de la sucesión definida por:

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

Ejercicio 4.4 Hallar una fórmula explícita para el término general de la sucesión definida mediante

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

Ejercicio 4.5 Resolver el Ejercicio 1.5 calculando, previamente, una fórmula explícita para el término general.

Ejercicio 4.6 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).

Ejercicio 4.7 Resolver las relaciones de recurrencia

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

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

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

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

Ejercicio 4.8 Resolver las siguientes relaciones de recurrencia

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

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

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 $u_1 = 4$.

Ejercicio 4.9

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

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

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

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

Ejercicio 4.10

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.

b) Hallar una fórmula explícita para el término general de la sucesión definida mediante la recurrencia lineal y homogénea

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

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.

Ejercicio 4.11 Del libro *"El Diablo de los Números"* de Hans Magnus Enzensberger. Ed. Siruela. 1997

– ¿Por qué no tecleas unos cuantos números de Bonatschi[(1)] ?
– ¡Tú y tu Bonatschi! –dijo Robert–. ¿Es tu favorito o qué?
Tecleó, y en la pantalla del cine apareció la serie de Bonatschi:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$$

– Ahora prueba a dividirlos –dijo el viejo maestro–. siempre por parejas sucesivas. El mayor dividido entre el menor.
– Bien –respondió Robert. Tecleó y tecleó, curioso por saber lo que leería en la gran pantalla:

$$\begin{aligned}
1 &: \ \ 1 = 1 \\
2 &: \ \ 1 = 2 \\
3 &: \ \ 2 = 1,5 \\
5 &: \ \ 3 = 1,666666666\ldots \\
8 &: \ \ 5 = 1,6 \\
13 &: \ \ 8 = 1,625 \\
21 &: 13 = 1,615384615\ldots \\
34 &: 21 = 1,619047619\ldots \\
89 &: 55 = 1,618181818\ldots
\end{aligned}$$

(1) Números de Fibonacci

≫ ¡Es una locura –dijo Robert–. Otra vez esos números no cesan. El 18 que se muerde la cola[(2)] . Y alguno de los otros tienen un aspecto completamente irrazonable[(3)] .
– Sí, pero aún hay otra cosa –le hizo notar el anciano. Robert reflexionó y dijo:
– Todos esos números van arriba y abajo. El segundo es mayor que el primero, el tercero menor que el segundo, el cuarto otra vez un poquito mayor, y así sucesivamente. Siempre arriba y abajo. Pero cuanto más dura esto, menos se alteran.
– Exactamente. Cuando coges Bonatschis cada vez más grandes, el péndulo oscila cada vez más hacia una cifra media, que es

$$1,618\,033\,988\ldots$$

≫ Pero no creas que este es el final de la historia, porque lo que sale es un número irrazonable[(3)] que nunca se termina. Te aproximas a él cada vez más, pero por más que calcules nunca lo alcanzarás del todo.
– Está bien –dijo Robert–. Los Bonatschi son así. Pero ¿*por qué* oscilan así en torno a esa cifra particular?
– Eso –afirmó el anciano– no tiene nada de particular. Es lo que hacen todos.
– ¿Qué quieres decir con todos?
– No tienen por qué ser los Bonatschi. Tomemos dos números apestosamente normales. Dime los dos primeros que se te ocurran.
– Diecisiete y once –dijo Robert.
– Bien. Ahora por favor súmalos.
– Puedo hacerlo de cabeza: 28.
– Magnífico. Te enseñaré en la pantalla cómo sigue:

$$\begin{array}{rcrcrcrcrcrcr}
11 & + & 17 & = & 28 & & & & & & & & \\
 & & 17 & + & 28 & = & 45 & & & & & & \\
 & & & & 28 & + & 45 & = & 73 & & & & \\
 & & & & & & 45 & + & 73 & = & 118 & & \\
 & & & & & & & & 73 & + & 118 & = & 191 \\
 & & & & & & & & & & 118 & + & 191 \quad = \quad 309
\end{array}$$

– Comprendido –dijo Robert–. ¿Y ahora qué?
– Haremos lo mismo que hemos hecho con los Bonatschi. Dividir. ¡Repartir! Prueba tranquilamente a hacerlo.

(2) Hace referencia a los números periódicos
(3) Hace referencia a los números irracionales

En la pantalla aparecieron las cifras que Robert tecleaba, y lo que resultó fue esto:

$$\begin{aligned}
17 : \ \ 11 &= 1,545\,454\ldots \\
28 : \ \ 17 &= 1,647\,058\ldots \\
45 : \ \ 28 &= 1,607\,142\ldots \\
73 : \ \ 45 &= 1,622\,222\ldots \\
118 : \ \ 73 &= 1,616\,438\ldots \\
191 : 118 &= 1,618\,644\ldots \\
309 : 191 &= 1,617\,801\ldots
\end{aligned}$$

– Exactamente la misma cifra absurda –exclamó Robert–. No lo entiendo. ¿Es que está dentro de todos los números? ¿Funciona esto de verdad *siempre?* ¿Empezando por dos números cualesquiera? ¿Sin importar cuáles elija?
– Sin duda –dijo el viejo maestro–. Por otra parte, si te interesa, te enseñaré qué otra cosa es $1,618\ldots$

En la pantalla apareció entonces algo espantoso:

$$1,618\ldots = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\ldots}}}}}}$$

a) Demostrar que la sucesión definida por los cocientes $\dfrac{F_{n+1}}{F_n}$, de números de Fibonacci consecutivos, converge a $1,618\,033\,988\ldots$ y dar el valor exacto de dicho número.

b) Demostrar que dicho límite no depende de los dos términos iniciales a_1 y a_2 sino sólo del tipo de recurrencia: $a_{n+2} = a_{n+1} + a_n$.

c) Expresar el cociente $c_{n+1} = \dfrac{F_{n+1}}{F_n}$ en función de c_n y utilizar el resultado para probar que el número $1,618\,033\,988\ldots$ puede expresarse de la forma indicada al final del texto.

Ejercicio 4.12 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?

Ejercicio 4.13

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.

Ejercicio 4.14 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?

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?

Ejercicio 4.15

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

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 $s = a_9 + 2$.

c) Decodificar el mensaje 709–932–214 sabiendo que ha sido codificado (letra a letra) mediante el sistema RSA utilizando la clave (q, s) donde $q = 29 \times 37$ y $s = 605$.

El alfabeto utilizado ha sido el español:

$\sqcup$	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	$\tilde{N}$	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

Índice