CAPÍTULO 7

7

ARITMÉTICA MODULAR - PARTE 2

Miguel Marañón Grandes
Universidad de La Rioja

Palabras clave

- *Módulo*
- *Resto*
- *Congruencia*
- *Teorema de Euler*
- *Pequeño Teorema de Fermat*
- *Criterios de divisibilidad*
- *Ecuación diofántica*
- *Identidad de Bézout*

¿Te imaginas qué ocurriría si el tiempo no se midiese cíclicamente? No podríamos hablar de a qué hora nos acostaríamos, qué día de la semana iríamos al cine, qué día del mes nos pagarían la nómina o el día de nuestro cumpleaños. En su lugar, la humanidad tendría que haber establecido un único momento de referencia a partir del cual se mediría el tiempo transcurrido. En vez de, pongamos por caso, quedar a las ocho y media con nuestros amigos, tendríamos que acordar cuántos segundos después del nacimiento de Cristo tendría lugar nuestra reunión. ¡Todo un caos!

El hecho de que, por suerte, el tiempo se mida cíclicamente se debe en parte gracias a la existencia de la aritmética modular, la cual considera los restos que se obtienen al tomar como divisor un determinado número (al que llamamos *módulo*). De ahí que, como un día tiene 24 horas, estas se establezcan con números comprendidos entre el 0 y el 23, reiniciándose su contador a medianoche. Lo mismo ocurre con las semanas, los meses, los años... No es casualidad que, por ello, a la aritmética modular, que fue introducida por primera vez en 1801 por el matemático Carl Friedrich Gauss, también se la conozca como la aritmética del reloj.

En este tema, aprenderemos a resolver ecuaciones diofánticas (esto es, ecuaciones lineales con coeficientes y soluciones enteras) que nos servirán como herramienta para resolver ecuaciones en congruencias y estudiaremos las propiedades de los conjuntos de restos módulo n (denotados por $\mathbb{Z}_n$), lo cual nos permitirá calcular restos de divisiones cuyos dividendos son números muy grandes que se pueden expresar en forma de potencia (en particular, hallaremos un método para determinar las últimas cifras de ciertas potencias con exponente muy grande) y entender el porqué de los criterios de divisibilidad de los números enteros, entre otras cosas.

7.1 Introducción

Nuestra mente ha ideado numerosos conceptos cuya naturaleza es cíclica: la hora del día, el día de la semana o del mes, las notas musicales... Todos ellos se contabilizan de forma que, en algún momento, su contador se pone a cero; en los ejemplos mencionados, una hora después de las 23 horas de un día son las 0 horas del día siguiente, después del domingo viene el lunes, el día después del 31 de agosto es el 1 de septiembre y la nota posterior al si vuelve a ser el do en la escala musical.

Pensando un poco, esto hace que en muchas ocasiones nos interese conocer el resto que un número deja al ser dividido por otro más que cualquier otro aspecto de la división. Si en este preciso momento es medianoche, dentro de 100 horas serán las 4 de la madrugada, ya que el resto que se obtiene al dividir 100 entre 24 (las horas que tiene el día) es precisamente 4. Del mismo modo, si hoy es martes 10 de agosto, el próximo año este mismo día caerá en miércoles, ya que al dividir los 365 días del año entre los 7 días de la semana, el resto es 1 (si el año que viene fuese bisiesto, con 366 días, el resto sería 2 y caería en jueves).

Figura 7.1: Carl Friedrich Gauss (1777–1855).

Estas ideas no pasaron inadvertidas a Carl Friedrich Gauss (Figura 7.1), también conocido como *el Príncipe de las Matemáticas* y considerado como el padre de la arimética modular, quien en el primer capítulo de su libro *Disquisitiones arithmeticae*, escrito en 1798 y publicado en 1801, introdujo definiciones y notaciones nunca vistas hasta la fecha fundamentadas en el concepto de *congruencia*.

Definición 7.1 (Relación de congruencia)

Dado un número entero n, dos números enteros a y b se encuentran en la misma **clase de congruencia** *módulo n si ambos dejan el mismo resto al dividirlos entre n o, equivalentemente, si $a-b$ es múltiplo de n. Esto se denota $a \equiv b \pmod{n}$.*

Ejemplo 7.1 Observamos que $63 \equiv 83 \pmod{10}$, ya que 63 y 83 dejan el mismo resto (que es 3) al dividirlos entre 10 o, equivalentemente, $63-83=-20$ es un múltiplo de 10.

La noción de módulo como divisor, unida al hecho de que el concepto de congruencia es compatible con las operaciones usuales de la aritmética debido a la gran analogía existente entre ella y la igualdad, permitió la introducción de la **aritmética modular**, la cual a la sazón acabó produciendo un gran impacto en el desarrollo de la teoría de números. Como consecuencia de la naturaleza cíclica de las horas del día, pues habitualmente se cuentan en módulo 12 o 24, a la aritmética modular también se la conoce como la *aritmética del reloj*.

La aritmética modular tiene bastantes aplicaciones. Una de las que más nos van a convenir a nosotros de cara a preparar olimpiadas matemáticas es la de calcular **restos potenciales** (sin necesidad de hacer la división). Un ejercicio tipo podría ser calcular la última cifra del número 7^{93} (o, equivalentemente, calcular el resto

que se obtiene al dividir 7^{93} entre 10). Sin saber nada del tema, aún podríamos intentar llegar a la solución estableciendo una conjetura, como la que se infiere del Cuadro 7.1. Se puede intuir un carácter cíclico que habrá que demostrar formalmente.

k	7^k	Última cifra
1	7	7
2	49	9
3	343	3
4	2.401	1
5	16.807	7
6	117.649	9
7	823.543	3
8	5.764.801	1
9	40.353.607	7
⋮	⋮	⋮

Cuadro 7.1: Última cifra de los números de la forma 7^k, con $k \in \mathbb{N}$.

Según lo observado, parece ser que los números de la forma 7^{4k-3}, con $k \in \mathbb{N}$, terminan en 7. Si esto fuera cierto, se podría deducir que 7^{93} termina en 7, puesto que $93 = 4 \cdot 24 - 3$. Sin embargo, esta conjetura hay que demostrarla, bien sea por inducción o por cualquier otro método válido; nosotros lo haremos en cuanto aprendamos algunas propiedades elementales de las clases de congruencia.

Otra aplicación que será interesante que conozcamos consiste en establecer **criterios de divisibilidad** para determinados números (es decir, saber si un número es múltiplo de otro sin necesidad de realizar la división). Seguramente recuerdes que un número es múltiplo de 3 si y solo si la suma de sus cifras es múltiplo de 3, que es múltiplo de 9 cuando la suma de sus cifras también lo es, que es múltiplo de 11 cuando la suma de las cifras en posición impar menos la de las cifras en posición par resulta ser un múltiplo de 11, y algún criterio de divisibilidad más; pues bien, todos ellos se pueden probar fácilmente usando las propiedades de las clases de congruencia.

Las aplicaciones de la aritmética modular no se terminan ahí. Entre otras cosas, hoy en día se emplea además en la teoría de la codificación, en criptografía (de hecho, forma parte de la base del algoritmo RSA para el cifrado de mensajes) y para definir dígitos de control para la detección de errores en identificadores como los siguientes:

- **NIF (Número de Identificación Fiscal).** ¿Sabías que la letra que acompaña a tu DNI viene determinada por los ocho dígitos precedentes? En efecto, se obtiene hallando el resto de dividir el número del DNI entre 23 (dicho de otro modo, *reduciéndolo* a módulo 23) y aplicando a este resto la siguiente conversión:

$0 \longrightarrow T$	$6 \longrightarrow Y$	$12 \longrightarrow N$	$18 \longrightarrow H$
$1 \longrightarrow R$	$7 \longrightarrow F$	$13 \longrightarrow J$	$19 \longrightarrow L$
$2 \longrightarrow W$	$8 \longrightarrow P$	$14 \longrightarrow Z$	$20 \longrightarrow C$
$3 \longrightarrow A$	$9 \longrightarrow D$	$15 \longrightarrow S$	$21 \longrightarrow K$
$4 \longrightarrow G$	$10 \longrightarrow X$	$16 \longrightarrow Q$	$22 \longrightarrow E$
$5 \longrightarrow M$	$11 \longrightarrow B$	$17 \longrightarrow V$	

- **ISBN (International Standard Book Number).** Los códigos identificativos de los libros editados también echan mano de las clases de congruencia. Estos códigos son de la forma:

$$x_1x_2\text{–}x_3x_4x_5x_6\text{–}x_7x_8x_9\text{–}y.$$

El primer bloque, x_1x_2, es un indicativo geográfico; el segundo, $x_3x_4x_5x_6$, corresponde a la editorial; el tercero, $x_7x_8x_9$, se refiere al libro; y el último dígito, y, es el de control y se calcula de la siguiente forma:

$$y = \sum_{i=1}^{9} i \cdot x_i \pmod{11}.$$

Si $y = 10$, el dígito de control se sustituye por la letra X.

- **Número de cuenta corriente.** Por último, veamos cómo se establecen los dígitos de control en los códigos de cuenta corriente asociados a las cuentas bancarias. Dichos códigos siempre constan de 20 cifras y son de la forma:

$$a_1a_2a_3a_4\text{–}b_1b_2b_3b_4\text{–}xy\text{–}c_1c_2c_3c_4c_5c_6c_7c_8c_9c_{10},$$

donde $a_1a_2a_3a_4$ representa la entidad bancaria; $b_1b_2b_3b_4$, la oficina bancaria; $c_1c_2c_3c_4c_5c_6c_7c_8c_9c_{10}$, el número de cuenta; y x e y son los dígitos de control que se calculan de la siguiente manera:

$$x = 7a_1 + 3a_2 + 6a_3 + a_4 + 2b_1 + 4b_2 + 8b_3 + 5b_4 \pmod{11},$$
$$y = 10c_1 + 9c_2 + 7c_3 + 3c_4 + 6c_5 + c_6 + 2c_7 + 4c_8 + 8c_9 + 5c_{10} \pmod{11}.$$

Si el resultado de alguna de las anteriores operaciones para x o y fuera igual a 10, pondríamos un 1 como dígito de control en su lugar.

7.2 Ecuaciones diofánticas

En ocasiones, se nos plantean ecuaciones con coeficientes enteros para las cuales solo tiene sentido que sus soluciones sean también enteras. A este tipo de ecuaciones se las denomina **ecuaciones diofánticas**, pues Diofanto de Alejandría (Figura 7.2), a quien deben su nombre en su honor, fue de los primeros en dedicarse al estudio de sus propiedades en su obra *Arithmetica*, la cual ejerció una gran influencia en el desarrollo del álgebra entre los árabes y en la teoría de números moderna.

Figura 7.2: Diofanto de Alejandría fue un matemático de la antigua Grecia del siglo III d.C. que es considerado como el padre del álgebra, ya que generalmente se le atribuye la introducción del simbolismo en las matemáticas.

Nota: *Poco se conoce de la vida de Diofanto, pero hay un dato de la misma del que estamos muy seguros: la edad a la que falleció. Esto es así porque en su epitafio aparecía escrito el siguiente problema:*

"Transeúnte, esta es la tumba de Diofanto: es él quien con esta sorprendente distribución te dice el número de años que vivió. Su niñez ocupó la sexta parte de su vida; después, durante la doceava parte su mejilla se cubrió con el primer bozo. Pasó aún una séptima parte de su vida antes de tomar esposa y, cinco años después, tuvo

un precioso niño que, una vez alcanzada la mitad de la edad de su padre, pereció de una muerte desgraciada. Su padre tuvo que sobrevivirle, llorándole, durante cuatro años. De todo esto se deduce su edad".

Llamando x a la edad a la que murió Diofanto, la siguiente ecuación resuelve el problema:

$$\frac{x}{6}+\frac{x}{12}+\frac{x}{7}+5+\frac{x}{2}+4=x.$$

*Resolviéndola, te resultará fácil comprobar que Diofanto vivió **84 años**.*

Definición 7.2 (Ecuación diofántica)

Una **ecuación diofántica** *es una ecuación algebraica con coeficientes enteros en la que aparecen varias variables cuyas soluciones son números enteros. Es decir, resolver una ecuación diofántica consiste en determinar qué números enteros la cumplen. En particular, las* ecuaciones diofánticas lineales *de n incógnitas son las de la forma:*

$$\sum_{i=1}^{n} a_i x_i = m,$$

con $a_1, a_2 \ldots, a_n, m \in \mathbb{Z}$.

A lo largo de todo el capítulo, solamente consideraremos las ecuaciones diofánticas lineales de 2 incógnitas; es decir, las de la forma

$$ax+by=m, \text{ con } a,b,m\in\mathbb{Z}$$

Las usaremos no solo para resolver problemas, sino además como herramienta para resolver ecuaciones en congruencias del tipo $px \equiv q \pmod{m}$, con $p, q, m \in \mathbb{Z}$.

Estas ecuaciones pueden tener infinitas soluciones (enteras)... o pueden no tener ninguna. Para discernir si tienen solución o no, los siguientes resultados serán de mucha utilidad.

Lema 7.1 (de Bézout)

Si a y b son números enteros diferentes de cero con máximo común divisor d, entonces existen enteros x e y tales que:

$$ax+by=d.$$

*A esta identidad se le denomina **identidad de Bézout**.*

Lema 7.2 (de Euclides)

Si $n \mid ab$ y $\text{m. c. d.}(n,a)=1$, entonces necesariamente $n \mid b$.

Demostración Como n y a son coprimos, por el Lema 7.1 (de Bézout) sabemos que existen $x, y \in \mathbb{Z}$ tales que $ax+ny=1$. Multiplicando por b ambos miembros, se tiene que $abx+nyb=b$. Por otro lado, como $n \mid ab$, existe $k \in \mathbb{Z}$ tal que $nk=ab$, por lo que $nkx+nyb=b$. Equivalentemente, $n(kx+yb)=b$, por lo que necesariamente $n \mid b$.

Teorema 7.1

Una ecuación diofántica lineal de la forma $ax + by = m$ tiene solución si y solo si el máximo común divisor de a y b es un divisor de m. Además, si esta ecuación diofántica tiene solución, necesariamente tiene infinitas soluciones y todas son de la forma:

$$\begin{cases} x = x_0 + \lambda \frac{b}{d} \\ y = y_0 - \lambda \frac{a}{d} \end{cases}, \qquad \lambda \in \mathbb{Z}, \tag{7.1}$$

donde $d = \text{m. c. d.}(a, b)$ y (x_0, y_0) es una solución particular de la ecuación.

Demostración Supongamos que la ecuación

$$ax + by = m \tag{7.2}$$

tiene solución entera. Entonces, existen x_0 e y_0 tales que $ax_0 + by_0 = m$. Como $d = \text{m. c. d.}(a, b)$ es divisor común de a y b, entonces $a = a_1 d$ y $b = b_1 d$, con $a_1, b_1 \in \mathbb{Z}$. Por tanto,

$$m = ax_0 + by_0 = a_1 dx_0 + b_1 dy_0 = (a_1 x_0 + b_1 y_0)d,$$

por lo que $d \mid m$.

Recíprocamente, supongamos que $d \mid m$. Entonces, existe $k \in \mathbb{Z}$ tal que $m = kd$. Por otra parte, por el Lema 7.1 (de Bézout) existen $\alpha, \beta \in \mathbb{Z}$ tales que $d = \alpha a + \beta b$. Al multiplicar los dos miembros de esta identidad por k, resulta que $kd = k(\alpha a + \beta b) = (k\alpha)a + (k\beta)b = m$, por lo que $(k\alpha, k\beta)$ es una solución de la ecuación diofántica. De hecho,

$$\begin{cases} x_0 = k\alpha = \dfrac{m}{d} \cdot \alpha \\ y_0 = k\beta = \dfrac{m}{d} \cdot \beta \end{cases}, \qquad \alpha, \beta \in \mathbb{Z},$$

es solución particular de la ecuación (7.2).

Finalmente, supongamos que (x_0, y_0) es solución particular de la ecuación (7.2). Por tanto, se cumple que $ax_0 + by_0 = m$. Notemos que, entonces, las expresiones de la ecuación (7.1) también son solución de la ecuación (7.2):

$$a\left(x_0 + \frac{b}{d} \cdot \lambda\right) + b\left(y_0 - \frac{a}{d} \cdot \lambda\right) = ax_0 + by_0 + a \cdot \frac{b}{d} \cdot \lambda - b \cdot \frac{a}{d} \cdot \lambda = m.$$

Por consiguiente, falta por probar que todas las soluciones de la ecuación (7.2) son de la forma descrita en la ecuación (7.1). En efecto, si (x, y) es la solución general de la ecuación (7.2), tenemos que se cumplen las dos ecuaciones siguientes:

$$ax + by = m,$$

$$ax_0 + by_0 = m.$$

Al restar ambas ecuaciones, se obtiene que $a(x - x_0) + b(y - y_0) = 0$, o equivalentemente

$$a(x - x_0) = b(y_0 - y). \tag{7.3}$$

Dividiendo ambos miembros de la ecuación (7.3) entre d, se tiene que $\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$. Por tanto, $\frac{a}{d}$ divide a $\frac{b}{d}(y_0 - y)$. Pero $\frac{a}{d}$ y $\frac{b}{d}$ son coprimos (ya que $d = \text{m. c. d.}(a, b)$), por lo que, por el Lema 7.2 (de Euclides), se deduce que $\frac{a}{d}$ ha de dividir a $(y_0 - y)$. Esto nos lleva a que debe existir $\lambda \in \mathbb{Z}$ tal que:

$$y_0 - y = \lambda \frac{a}{d} \Longrightarrow y = y_0 - \lambda \frac{a}{d}.$$

Sustituyendo este valor de y en la ecuación (7.3), se llega fácilmente a que

$$x = x_0 + \lambda\frac{b}{d}, \quad \lambda \in \mathbb{Z}.$$

■

Por tanto, según nos indica el Teorema 7.1, encontrar las soluciones de una ecuación diofántica lineal de 2 incógnitas se puede reducir a hallar una solución particular (x_0, y_0) de la ecuación (hallando previamente los coeficientes enteros α y β que aparecen en la demostración del teorema). Con este fin, el algoritmo de Euclides resulta ser tremendamente útil, pues no solo permite encontrar el máximo común divisor de a y b para determinar si la ecuación tiene solución, sino que además nos proporciona un método para llegar a la identidad de Bézout y, a partir de ella, llegar a una solución particular. Puesto que dicho método puede llegar a ser demasiado intrincado y complicado de explicar para el caso general, lo aprenderemos a través de la estrategia seguida en la resolución del Problema 7.1.

Nota: *Seguramente ya conozcas un procedimiento para calcular el máximo común divisor de un par de números enteros: el de descomponerlos en factores primos y tomar de esos factores solo los comunes con el menor exponente para después multiplicarlos. Pues bien, otro método igual de válido es el algoritmo de Euclides. Consiste en seguir las siguientes reglas:*

1. *Si* $b = 0$*, entonces* $\mathrm{m.\,c.\,d.}(a, b) = a$ *y el algoritmo termina.*
2. *En otro caso,* $\mathrm{m.\,c.\,d.}(a, b) = \mathrm{m.\,c.\,d.}(b, r)$*, donde* r *es el resto de dividir* a *entre* b*. Para calcular* $\mathrm{m.\,c.\,d.}(b, r)$*, se utilizan estas mismas reglas.*

Este procedimiento suele quedar recogido en un esquema como el siguiente, en el que $q_1, q_2, q_3, \ldots, q_k$ *son los cocientes que se van obteniendo y* $r_1, r_2, r_3, \ldots, r_{k-1}$*, los restos:*

	q_1	q_2	q_3	$\cdots$	q_{k-1}	q_k
a	b	r_1	r_2	$\cdots$	r_{k-2}	$\mathbf{r_{k-1}}$
r_1	r_2	r_3	$\cdots$	r_{k-1}	0	

Recordemos que $a = bq_1 + r_1$*,* $b = r_1q_2 + r_2$*,* $r_k = 0$ *y* $r_{i-1} = r_iq_{i+1} + r_{i+1}$*, con* $i = 2, \ldots, k-1$*. Se tendría que* $\mathrm{m.\,c.\,d.}(a, b) = r_{k-1}$*. A modo de ejemplo,*

$$\mathrm{m.\,c.\,d.}(2366, 273) = \mathrm{m.\,c.\,d.}(273, 182) = \mathrm{m.\,c.\,d.}(182, 91) = \mathrm{m.\,c.\,d.}(91, 0) = 91,$$

siendo el esquema asociado:

	8	1	2
2366	273	182	**91**
182	91	0	

Problema 7.1 Encuentra los valores enteros $10 \leq x \leq 20$ para los que tiene solución la ecuación diofántica $84x + 990y = c$. Resuélvela en uno de los casos encontrados.

Solución *En primer lugar, aplicamos el algoritmo de Euclides con los números* 990 *y* 84*:*

	11	1	3	1	2
990	84	66	18	12	**6**
66	18	12	6	0	

Para que la ecuación diofántica tenga solución, c tiene que ser múltiplo de $\mathrm{m.\,c.\,d.}(84, 990) = 6$. *Por tanto, c sólo puede valer* 12 *o* 18. *Tomaremos* $c = 12$*; es decir, resolveremos la ecuación diofántica* $84x + 990y = 12$. *Para ello, primero hemos de hallar una solución particular* (x_0, y_0) *usando la información obtenida en el algoritmo anterior, mediante la cual podemos asegurar que:*

$$990 = 11 \cdot 84 + 66 \Longrightarrow 66 = 990 - 11 \cdot 84; \tag{7.4}$$

$$84 = 66 + 18 \Longrightarrow 18 = 84 - 66; \tag{7.5}$$

$$66 = 3 \cdot 18 + 12 \Longrightarrow 12 = 66 - 3 \cdot 18; \tag{7.6}$$

$$18 = 12 + 6 \Longrightarrow 6 = 18 - 12. \tag{7.7}$$

Sustituyendo la identidad (7.4) en (7.5), se tiene que:

$$18 = 84 - (990 - 11 \cdot 84) \Longrightarrow 18 = 12 \cdot 84 - 990. \tag{7.8}$$

Sustituyendo las identidades (7.4) y (7.8) en (7.6), se tiene que:

$$12 = 990 - 11 \cdot 84 - 3 \cdot (12 \cdot 84 - 990) \Longrightarrow 12 = 4 \cdot 990 - 47 \cdot 84. \tag{7.9}$$

Y al fin, sustituyendo las identidades (7.8) y (7.9) en (7.7), se tiene que:

$$6 = 12 \cdot 84 - 990 - (4 \cdot 990 - 47 \cdot 84) \Longrightarrow 59 \cdot 84 - 5 \cdot 990 = 6. \tag{7.10}$$

Notemos que la identidad (7.10) es la identidad de Bézout correspondiente a los coeficientes de la ecuación diofántica. A partir de ella, es fácil deducir que $x_0 = \dfrac{12}{6} \cdot 59 = 118$ *e* $y_0 = \dfrac{12}{6} \cdot (-5) = -10$ *determinan una solución particular de la misma. Así, las soluciones son de la forma:*

$$\begin{cases} x = 118 + \lambda \frac{990}{6} \\ y = -10 - \lambda \frac{84}{6} \end{cases}, \quad \lambda \in \mathbb{Z} \Longrightarrow \begin{cases} x = 165\lambda + 118 \\ y = -14\lambda - 10 \end{cases}, \quad \lambda \in \mathbb{Z}.$$

7.3 Congruencias

Recordemos que dos enteros a y b se dicen ***congruentes*** (o que se encuentran en la misma ***clase de congruencia***) módulo $n \in \mathbb{Z}$ si n es un divisor de la diferencia de ambos:

$$a \equiv b \pmod{n} \iff n \mid a - b \iff \exists k \in \mathbb{Z} \colon a - b = k \cdot n.$$

Equivalentemente, dos enteros a y b son congruentes módulo $n \in \mathbb{Z}$ si dan el mismo resto al dividirlos entre n.

Algunas propiedades básicas de las clases de congruencia son las siguientes. Dados $a, b, c, d \in \mathbb{Z}$:

1. $a \equiv a \pmod{n}$ *(propiedad reflexiva).*
2. Si $a \equiv b \pmod{n}$, $b \equiv a \pmod{n}$ *(propiedad simétrica).*
3. Si $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$, $a \equiv c \pmod{n}$ *(propiedad transitiva).*
4. Si $a \equiv b \pmod{n}$ y $k \in \mathbb{Z}$, $a + k \equiv b + k \pmod{n}$.
5. Si $a \equiv b \pmod{n}$ y $k \in \mathbb{Z}$, $ka \equiv kb \pmod{n}$.
6. Si $a \equiv b \pmod{n}$ y $k \in \mathbb{N}$, $a^k \equiv b^k \pmod{n}$.
7. Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, $a + c \equiv b + d \pmod{n}$.
8. Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, $a \cdot c \equiv b \cdot d \pmod{n}$.

Demostración Las propiedades 1, 2, 3, 4, 5 y 7 son fáciles de probar a partir de la definición y quedan propuestas al lector. La propiedad 6 también es sencilla de demostrar si se tiene en cuenta que $a^k - b^k = (a-b)\sum_{i=0}^{k-1} a^i b^{k-1-i}$. Por último, para la propiedad 8, supongamos que existen $k, k' \in \mathbb{Z}$ tales que $a-b = kn$ y $c-d = k'n$. Entonces, $a = b + kn$ y $c = d + k'n$. Por tanto, se tiene que:

$$ac - bd = (b+kn)(d+k'n) - bd = bd + k'bn + kdn + kk'n^2 - bd = n(k'b + kd + kk'n),$$

por lo que existe $K = k'b + kd + kk'n \in \mathbb{Z}$ tal que $ac - bd = Kn$. ■

Notemos que las tres primeras propiedades hacen que la relación de congruencia sea de equivalencia.

La definición que se muestra a continuación nos permitirá trabajar con las relaciones de congruencia de una forma mucho más cómoda.

Definición 7.3 (Conjunto de restos)

Definimos el **conjunto de restos** *módulo $n \in \mathbb{Z}$ como el conjunto $\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}$, donde $[k]_n$ representa el subconjunto de todos los enteros que son congruentes con k módulo n. Notemos que $[a]_n = [b]_n$ si y solo si a y b dejan el mismo resto al dividirlos entre n.*

Ejemplo 7.2 En $\mathbb{Z}_7$ se cumple que $[9]_7 = [16]_7 = [23]_7 = [2]_7$ y $[-6]_7 = [8]_7 = [1]_7$.

Las propiedades de la aritmética de $\mathbb{Z}_n$ que describiremos ahora son fundamentales para operar en ella. Dados $[a]_n, [b]_n \in \mathbb{Z}_n$:

1. $[a]_n + [b]_n = [a+b]_n$.
2. $[a]_n \cdot [b]_n = [a \cdot b]_n$.
3. $[a^k]_n = ([a]_n)^k$, con $k \in \mathbb{N}$. Por abreviar la notación, escribiremos $([a]_n)^k = [a]_n^k$.

Las dos primeras propiedades están bien definidas debido a las dos últimas de las relativas a las clases de congruencia. La tercera propiedad es consecuencia inmediata de la segunda y en ocasiones es tremendamente útil para simplificar los cálculos, como se puede ver en el siguiente ejemplo.

Ejemplo 7.3 En $\mathbb{Z}_6$, $[7^{100}]_6 = [7]_6^{100} = [1]_6^{100} = [1^{100}]_6 = [1]_6$. No perdamos de vista que esto quiere decir que el resto que se obtiene al dividir 7^{100} entre 6 es 1. Para saber esto, no ha sido necesario realizar la división.

Hasta ahora, ninguno de los aspectos de $\mathbb{Z}_n$ que hemos estudiado nos resulta extraño o, al menos, inesperado. Sin embargo, las propiedades en cuanto a la multiplicación que pueden surgir en $\mathbb{Z}_n$ podrían ser muy distintas a las del conjunto de los números enteros $\mathbb{Z}$. Por lo pronto, los únicos elementos invertibles en $\mathbb{Z}$ (es decir, elementos para los cuales existe otro tal que al multiplicarlos el resultado es la unidad) son el 1 y el -1, pero en $\mathbb{Z}_n$ puede haber muchos más según el valor que tome el módulo $n \in \mathbb{Z}$.

Definición 7.4 (Elemento invertible, o unidad, en $\mathbb{Z}_n$)

Se dice que $[a]_n$ es un **elemento invertible** *(o* **unidad***) en $\mathbb{Z}_n$ si existe $[b]_n$ en $\mathbb{Z}_n$ tal que $[a]_n \cdot [b]_n = [1]_n$. Ese elemento $[b]_n$ será el* **inverso** *de $[a]_n$ en $\mathbb{Z}_n$ y se denota como $[a^{-1}]_n$.*

Ejemplo 7.4

a) En $\mathbb{Z}_7$, $[3^{-1}]_7 = [5]_7$, ya que $[3]_7 \cdot [5]_7 = [15]_7 = [1]_7$.

b) En $\mathbb{Z}_9$, $[4^{-1}]_9 = [7]_9$, ya que $[4]_9 \cdot [7]_9 = [28]_9 = [1]_9$.

Proposición 7.1

$[a]_n$ es invertible en $\mathbb{Z}_n$ si y solo si $\mathrm{m.\,c.\,d.}(a,n)=1$. *Además, en caso de que exista, su elemento inverso es único.*

Demostración Supongamos que $[a]_n$ es invertible en $\mathbb{Z}_n$. Entonces, debe existir $[b]_n \in \mathbb{Z}_n$ tal que:

$$[a]_n \cdot [b]_n = [1]_n \Longrightarrow [a]_n \cdot [b]_n - [1]_n = [0]_n \Longrightarrow [a\cdot b - 1]_n = [0]_n.$$

Por tanto, ha de existir $k \in \mathbb{Z}$ tal que $ab-1=kn$. Por otro lado, sea $d=\mathrm{m.\,c.\,d.}(a,n)$. Por ser d divisor común de a y n, existen $a', n' \in \mathbb{Z}$ tales que $a=da'$ y $n=dn'$. Por consiguiente,

$$da'b-1=kdn' \Longrightarrow da'b-dn'k=1 \Longrightarrow d(a'b-n'k)=1 \Longrightarrow d=1.$$

Para demostrar el recíproco, supongamos que $\mathrm{m.\,c.\,d.}(a,n)=1$. Por el Lema 7.1 (de Bézout), existen $x, y \in \mathbb{Z}$ tales que $ax+ny=1$. Tomando clases de congruencia módulo n, se tiene que:

$$[a\cdot x + n\cdot y]_n = [1]_n \Longrightarrow [a\cdot x]_n + [n\cdot y]_n = [1]_n \Longrightarrow [a\cdot x]_n = [1]_n \Longrightarrow [a]_n\cdot[x]_n = [1]_n,$$

por lo que $[a^{-1}]_n = [x]_n$ y $[a]_n$ es invertible en $\mathbb{Z}_n$.

Finalmente, para probar la unicidad del elemento inverso, supongamos que existen $[b]_n, [b']_n \in \mathbb{Z}_n$ tales que $[a]_n\cdot[b]_n=[1]_n$ y $[a]_n\cdot[b']_n=[1]_n$. Esto implica que:

$$[a]_n\cdot[b]_n = [a]_n\cdot[b']_n \Longrightarrow [a\cdot b]_n = [a\cdot b']_n \Longrightarrow [a\cdot(b-b')]_n = [0]_n.$$

Por tanto, debe existir $k \in \mathbb{Z}$ tal que $a(b-b')=kn$. De aquí se deduce que $n \mid a(b-b')$. Puesto que $\mathrm{m.\,c.\,d.}(a,n)=1$, por el Lema 7.2 (de Euclides) se tiene que $n \mid b-b'$, por lo que $b \equiv b' \pmod{n}$ y el elemento inverso es único.

■

Corolario 7.1

Si $[a]_n$ o $[b]_n$ son elementos invertibles en $\mathbb{Z}_n$ y $[a]_n\cdot[b]_n=[0]_n$, entonces o bien $[a]_n=[0]_n$ o $[b]_n=[0]_n$. Además, si $\mathrm{m.\,c.\,d.}(c,n)=1$ *y $[x]_n\cdot[c]_n=[y]_n\cdot[c]_n$ en $\mathbb{Z}_n$, entonces $[x]_n=[y]_n$ en $\mathbb{Z}_n$* (propiedad cancelativa del producto).

Demostración Supongamos, sin pérdida de generalidad, que $[a]_n$ es invertible en $\mathbb{Z}_n$. Entonces, por la Proposición 7.1, $\mathrm{m.\,c.\,d.}(a,n)=1$. Ahora, si $[a]_n\cdot[b]_n=[0]_n$, entonces $[a\cdot b]_n=[0]_n$ y, por tanto, existe $k\in\mathbb{Z}$ tal que $ab=kn$. Esto significa que $n \mid ab$. Pero por el Lema 7.1 (de Bézout), $n \mid b$, ya que a y n son coprimos. De aquí se sigue inmediatamente que $[b]_n=[0]_n$.

Para probar la propiedad cancelativa del producto, notemos que si $\mathrm{m.\,c.\,d.}(c,n)=1$, nuevamente por la Proposición 7.1 existe el inverso de $[c]_n$ en $\mathbb{Z}_n$, al que denotaremos por $[c^{-1}]_n$. Multiplicando por este elemento ambos miembros de la ecuación $[x]_n\cdot[c]_n=[y]_n\cdot[c]_n$, se llega a que:

$$[x]_n\cdot([c]_n\cdot[c^{-1}]_n) = [y]_n\cdot([c]_n\cdot[c^{-1}]_n) \Longrightarrow [x]_n\cdot[1]_n = [y]_n\cdot[1]_n \Longrightarrow [x]_n=[y]_n.$$

■

Nota: *Cuando tenemos dos elementos* ***no nulos*** *$[a]_n$ y $[b]_n$ que* ***no son invertibles*** *en $\mathbb{Z}_n$, puede darse el caso de que su producto sea nulo; es decir, que $[a]_n\cdot[b]_n=[0]_n$ aunque $[a]_n\neq[0]_n$ y $[b]_n\neq[0]_n$. Por ejemplo, en $\mathbb{Z}_6$ se cumple que $[2]_6\cdot[3]_6=[6]_6=[0]_6$. Notemos que esto nunca ocurre en el conjunto de los números enteros $\mathbb{Z}$.*

Definición 7.5 (Conjunto de unidades en $\mathbb{Z}_n$)

El **conjunto de unidades** *de $\mathbb{Z}_n$ se denota por U_n y se define como el conjunto de elementos de $\mathbb{Z}_n$ que tienen inverso:* $U_n = \{[a]_n \in \mathbb{Z}_n : \text{ m. c. d.}(a, n) = 1\}$.

Ejemplo 7.5

a) En $\mathbb{Z}_7$, $U_7 = \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}$.
b) En $\mathbb{Z}_9$, $U_9 = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\}$.
c) En $\mathbb{Z}_{12}$, $U_{12} = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}$.

Como consecuencia de la Proposición 7.1 y el Corolario 7.1, si p es un número primo, se cumplen las siguientes propiedades en $\mathbb{Z}_p$:

1. Si $[a]_p \in \mathbb{Z}_p$ es tal que $[a]_p \neq [0]_p$, entonces $[a]_p$ es invertible.
2. $U_p = \mathbb{Z}_p \setminus \{[0]_p\}$.
3. $\mathbb{Z}_p$ es un *dominio de integridad*: si $[a]_p, [b]_p \in \mathbb{Z}_p$ y $[a]_p \cdot [b]_p = [0]_p$, entonces o bien $[a]_p = [0]_p$ o $[b]_p = [0]_p$.
4. Todo elemento no nulo en $\mathbb{Z}_p$ posee la *propiedad cancelativa del producto*. Sean $[a]_p, [b]_p, [c]_p \in \mathbb{Z}_p$ tales que $[a]_p \neq [0]_p$, $[b]_p \neq [0]_p$ y $[c]_p \neq [0]_p$. Si $[a]_p \cdot [c]_p = [b]_p \cdot [c]_p$, entonces $[a]_p = [b]_p$.

Terminaremos la actual sección resolviendo un problema que ponga en práctica la teoría vista en ella.

Problema 7.2 Encuentra todos los enteros x tales que $x^2 - 3x + 3 \equiv 0 \pmod 7$.

Solución *La ecuación en congruencias planteada puede expresarse como:*

$$x^2 - 3x - 4 \equiv 0 \pmod 7 \Longrightarrow (x+1)(x-4) \equiv 0 \pmod 7.$$

Equivalentemente, tomando clases de congruencia en $\mathbb{Z}_7$,

$$[x+1]_7 \cdot [x-4]_7 = [0]_7.$$

Como 7 es primo, $\mathbb{Z}_7$ es un dominio de integridad y entonces, o bien $[x+1]_7 = [0]_7 \Rightarrow [x]_7 = [-1]_7$ o $[x-4]_7 = [0]_7 \Rightarrow [x]_7 = [4]_7$. Por tanto, los enteros que cumplen la ecuación son los de la forma $7k-1$ y $7k+4$, con $k \in \mathbb{Z}$.

7.4 Teoremas de Euler y Fermat

Si bien no serán los únicos resultados relacionados con la aritmética modular que vamos a estudiar, el Teorema de Euler y el Pequeño Teorema Fermat son la base para resolver ejercicios y problemas de restos modulares. Para entender el enunciado del Teorema de Euler, hemos de conocer primero el concepto de *cardinal* de un conjunto y la función Φ de Euler.

Definición 7.6 (Cardinal)

Se define el **cardinal** *de un conjunto C como la cantidad de elementos que contiene. Se denota $|C|$.*

Definición 7.7 (Función Φ de Euler)

La **función Φ de Euler**, $\Phi : \mathbb{N} \to \mathbb{N}$, *se define como* $\Phi(1) = 1$ *y* $\Phi(n) = |U_n|$, $\forall n \geq 2$.

La función Φ de Euler posee tres propiedades clave para poder operar con ella:

1. $\Phi(p) = p - 1$, con p primo.
2. $\Phi(p^k) = (p-1)p^{k-1}$, con p primo y $k \in \mathbb{N}$.
3. $\Phi(a \cdot b) = \Phi(a)\Phi(b)$, con a y b primos entre sí.

Ejemplo 7.6

a) $\Phi(10) = \Phi(2 \cdot 5) = \Phi(2)\Phi(5) = (2-1) \cdot (5-1) = 1 \cdot 4 = 4$.
b) $\Phi(72) = \Phi(2^3 \cdot 3^2) = \Phi(2^3)\Phi(3^2) = (2-1)2^{3-1} \cdot (3-1)3^{2-1} = 1 \cdot 2^2 \cdot 2 \cdot 3^1 = 1 \cdot 4 \cdot 2 \cdot 3 = 24$.

Teorema 7.2 (de Euler)

Dados $a, n \in \mathbb{N}$ tales que $n \geq 2$ y $\text{m. c. d.}(a, n) = 1$, se tiene que:

$$a^{\Phi(n)} \equiv 1 \pmod{n}.$$

Ejemplo 7.7 Tal y como conjeturamos en la sección 7.1, la última cifra de 7^{93} es 7. En efecto, como $\text{m. c. d.}(7, 10) = 1$ y $\Phi(10) = 4$, por el Teorema 7.2 (de Euler) tenemos que $7^4 \equiv 1 \pmod{10}$. Por tanto, $(7^4)^k \equiv 1^k \pmod{10}$ para todo número natural k; en particular, $(7^4)^{23} \equiv 1 \pmod{10}$. Así,

$$7^{93} = 7^{4 \cdot 23 + 1} = (7^4)^{23} \cdot 7 \equiv 1 \cdot 7 \equiv 7 \pmod{10}.$$

El Pequeño Teorema de Fermat es en realidad un corolario del Teorema de Euler.

Corolario 7.2 (Pequeño Teorema de Fermat)

Si p es primo, para cada $a \in \mathbb{N}$ no divisible por p se tiene que:

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

Demostración Es inmediato a partir del Teorema 7.2 (de Euler) y la propiedad 1 de la función Φ de Euler. ■

Ejemplo 7.8 El resto de dividir 21^{5432} entre 11 es 1. En efecto, como 11 es primo y no es divisor de 21, por el Corolario 7.2 (Pequeño Teorema de Fermat) tenemos que $21^{10} \equiv 1 \pmod{11}$. Ahora, $5432 = 543 \cdot 10 + 2$ y $21 \equiv -1 \pmod{11}$, luego:

$$21^{5432} \equiv (21^{10})^{543} \cdot 21^2 \equiv 1^{543} \cdot 21^2 \equiv 21^2 \equiv (-1)^2 \equiv 1 \pmod{11}.$$

Para poner en práctica ambos resultados, plantearemos y resolveremos los siguientes dos problemas.

Problema 7.3 Halla el resto de dividir 3^{15} entre 17.

Solución *Según el Corolario 7.2 (Pequeño Teorema de Fermat),* $3^{16} \equiv 1 \pmod{17}$. *Esto es equivalente a escribir* $[3^{16}]_{17} = [1]_{17}$ *en* $\mathbb{Z}_{17}$. *Así,*

$$[3^{15}]_{17} = [3^{16-1}]_{17} = [3^{16}]_{17} \cdot [3^{-1}]_{17} = [1]_{17} \cdot [3^{-1}]_{17} = [3^{-1}]_{17}.$$

Como $[3]_{17} \cdot [6]_{17} = [18]_{17} = [1]_{17}$, *se tiene que* $[3^{-1}]_{17} = [6]_{17}$. *Por tanto,* $3^{15} \equiv 6 \pmod{17}$ *y el resto de dividir* 3^{15} *entre* 17 *es* 6.

Problema 7.4 Halla la última cifra del número 2^{56}.

Solución *Hallar la última cifra de un número equivale a determinar el resto que se obtiene al dividir dicho número entre* 10. *Notemos que, en principio, no podemos usar el Teorema 7.2 (de Euler) para calcular el resto que se obtiene al dividir* 2^{56} *entre* 10, *ya que* $\text{m. c. d.}(2, 10) = 2 \neq 1$. *En su lugar, calcularemos el resto de la división* 2^{55} *entre* 5 *aplicando el Corolario 7.2 (Pequeño Teorema de Fermat).*

Como $2^4 \equiv 1 \pmod 5$ *y* $55 = 4 \cdot 13 + 3$*, se tiene que:*

$$2^{55} \equiv 2^3 \equiv 8 \equiv 3 \pmod 5.$$

Por tanto, existe un número entero m *tal que* $2^{55} = 5m + 3$*. Multiplicando ambos lados de esta igualdad por* 2*, se llega a que:*

$$2^{56} = 10m + 6,$$

con $m \in \mathbb{Z}$*. Por tanto,* $2^{56} \equiv 6 \pmod{10}$ *y la última cifra de* 2^{56} *es* 6*.*

7.5 Ejercicios resueltos mediante aritmética modular

En esta sección, observaremos de manera práctica algunas aplicaciones de la aritmética modular en la realización de ejercicios y problemas variados. Se divide en tres partes: en la primera, veremos uno de los numerosos ejemplos de cómo los teoremas de Euler y Fermat permiten deducir ciertas propiedades de los números primos; en la segunda, usaremos las ecuaciones diofánticas como herramienta para resolver ecuaciones en congruencias; y en la tercera, probaremos por qué funcionan los criterios de divisibilidad de algunos números.

En primer lugar, plantearemos y resolveremos un problema en el que se pide probar una propiedad de los números primos apoyándonos en el Teorema de Euler y después se dejará propuesto otro para que el lector lo resuelva por su cuenta.

Problema 7.5 Si p es un número primo distinto de 2 y 5, entonces o bien $p^2 - 1$ o $p^2 + 1$ es divisible por 10.

Solución *Si* p *es un número primo distinto de* 2 *y* 5*, entonces* $\mathrm{m.c.d.}(p, 10) = 1$*. Por tanto, aplicando el Teorema 7.2 (de Euler),* $p^{\Phi(10)} \equiv 1 \pmod{10}$*. Como* $\Phi(10) = \Phi(2) \cdot \Phi(5) = 1 \cdot 4 = 4$*, se tiene que* $p^4 \equiv 1 \pmod{10}$ *y así* $p^4 - 1$ *es múltiplo de* 10*. Por otro lado,* p *es impar, pues es un número primo distinto de* 2*. Entonces, tanto* $p^2 - 1$ *como* $p^2 + 1$ *son múltiplos de* 2*. Pero* $p^4 - 1 = (p^2 + 1) \cdot (p^2 - 1)$*, por lo que uno de los dos factores, o bien* $p^2 - 1$ *o* $p^2 + 1$*, ha de ser múltiplo de* 5*. Finalmente, puesto que ese factor también es múltiplo de* 2*, es divisible por* 10*.*

Los métodos de resolución de ecuaciones diofánticas que vimos en la sección 7.2 no solo sirven para resolver problemas que requieren del planteamiento de este tipo especial de ecuaciones para llegar a su solución, sino que también se pueden emplear como herramienta para resolver ecuaciones en congruencias como la que se muestra a continuación.

Problema 7.6 Resuelve, si es posible, la siguiente ecuación en congruencias:

$$91x \equiv 84 \pmod{147}.$$

Solución *Notemos que* $91x \equiv 84 \pmod{147} \Rightarrow \exists k \in \mathbb{Z}\colon 91x - 84 = 147k$*. Luego resolver la ecuación en congruencias dada equivale a encontrar los valores de* x *que cumplen la ecuación diofántica* $91x - 147k = 84$*, para algún* $k \in \mathbb{Z}$*. La ecuación tiene solución, pues* $\mathrm{m.c.d.}(91, 147) = 7$*, que es divisor de* 84*. Por medio del algoritmo de Euclides (Lema 7.2) y de la identidad de Bézout (Lema 7.1), se deduce que una solución particular de la ecuación es* $(x_0, k_0) = (-96, -60)$*. Así, las soluciones para* x *son de la forma:*

$$x = -96 + \lambda \frac{-147}{7} = -21\lambda - 96, \quad \lambda \in \mathbb{Z}.$$

Estas soluciones son también las de la ecuación en congruencias inicial.

En particular, las ecuaciones diofánticas también permiten hallar el inverso multiplicativo de un elemento $[a]_n \in \mathbb{Z}_n$, con $\mathrm{m.c.d.}(a, n) = 1$, pues al fin y al cabo para ello es necesario resolver la ecuación en congruencias

$[a]_n \cdot [x]_n = [1]_n$, la cual equivale a que $ax - kn = 1$, donde $k \in \mathbb{Z}$ y $0 < x < n$. Veámoslo con un ejemplo de cálculo.

Problema 7.7 Halla el inverso multiplicativo de $[65]_{98}$ en $\mathbb{Z}_{98}$.

Solución *Hay que resolver la ecuación en congruencias*

$$[65]_{98} \cdot [x]_{98} = [1]_{98},$$

que se traduce en la ecuación diofántica

$$65x + (-98) \cdot k = 1, \quad k \in \mathbb{Z}.$$

Notemos que la ecuación tiene solución, ya que $\mathrm{m.c.d.}(65, 98) = 1$. *Aplicando el algoritmo de Euclides, se obtiene el siguiente esquema:*

	1	1	1	32
98	65	33	32	**1**
33	32	1	0	

A su vez, del esquema se derivan las siguientes identidades:

$$98 = 65 + 33 \Longrightarrow 33 = 98 - 65; \tag{7.11}$$

$$65 = 33 + 32 \Longrightarrow 32 = 65 - 33; \tag{7.12}$$

$$33 = 32 + 1 \Longrightarrow 1 = 33 - 32. \tag{7.13}$$

Sustituyendo la identidad 7.11 en 7.12, se tiene que:

$$32 = 65 - (98 - 65) \Longrightarrow 32 = 2 \cdot 65 - 98. \tag{7.14}$$

Sustituyendo las identidades 7.11 y 7.14 en 7.13, se tiene que:

$$1 = 98 - 65 - (2 \cdot 65 - 98) \Longrightarrow 65 \cdot (-3) + (-98) \cdot (-2) = 1. \tag{7.15}$$

La identidad 7.15 es la identidad de Bézout asociada a la ecuación diofántica inicial, de la cual es fácil deducir que $(x_0, k_0) = (-3, -2)$ *es una solución particular. Así, las soluciones para* x *son de la forma:*

$$x = -3 - 98\lambda, \quad \lambda \in \mathbb{Z}.$$

Recordemos que $0 < x < 98$. *Tomando* $\lambda = -1$, $x = 95$. *Por consiguiente,* $[65^{-1}]_{98} = [95]_{98}$.

La aritmética modular explica el porqué de las reglas que aprendimos para determinar si unos números son múltiplos de otros sin necesidad de realizar divisiones para comprobarlo. Demostraremos que el criterio de divisibilidad del 3 funciona y dejaremos propuesto probar que también lo hacen otros, como el del 9 o el del 11.

Problema 7.8 Prueba que un número entero es divisible por 3 si la suma de sus cifras es múltiplo de 3.

Solución *Supongamos que el número* $n \in \mathbb{Z}$ *se escribe* $a_k a_{k-1} \ldots a_1 a_0$. *Entonces:*

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

Como $[10^k]_3 = [10]_3^k = [1]_3^k = [1^k]_3 = [1]_3$, $\forall k \in \mathbb{N}$, *se tiene que:*

$$\begin{aligned}[n]_3 &= [a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0]_3 \\ &= [a_k]_3 \cdot [10^k]_3 + [a_{k-1}]_3 \cdot [10^{k-1}]_3 + \cdots + [a_1]_3 \cdot [10]_3 + [a_0]_3 \\ &= [a_k]_3 + [a_{k-1}]_3 + \cdots + [a_1]_3 + [a_0]_3 = \\ &= [a_k + a_{k-1} + \cdots + a_1 + a_0]_3.\end{aligned}$$

Ahora, si la suma de las cifras de n *es múltiplo de* 3*, tenemos que* $[n]_3 = [a_k + a_{k-1} + \cdots + a_1 + a_0]_3 = [0]_3$ *y por tanto* n *es también múltiplo de* 3*.*

7.6 Problemas de olimpiadas matemáticas

Para finalizar este capítulo, vamos a echar un vistazo a unos cuantos problemas propuestos en olimpiadas anteriores de diverso tipo. Además, aprovecharemos para explicar algunas técnicas que no está de más conocer para enfrentarse a ellos.

Para empezar, a veces está muy bien conocer el resto que dejan los cuadrados de los números al dividirlos por determinados módulos. Estos *restos cuadráticos* proporcionan la clave para resolver problemas como los que se muestran a continuación, en los que se utiliza que los cuadrados módulo 4 son solamente 0 y 1 (y que, en consecuencia, la suma de dos cuadrados módulo 4 nunca es 3).

Problema 7.9 Halla todas las posibles formas de escribir 2003 como suma de dos cuadrados de números enteros positivos.

Solución *Se trata de buscar las soluciones enteras positivas de la ecuación* $x^2 + y^2 = 2003$*. Para ello, utilizaremos congruencias módulo* 4*. Notemos que si* n *es un número natural, entonces o bien* $n^2 \equiv 0 \pmod 4$ *o* $n^2 \equiv 1 \pmod 4$*. En efecto,* n *puede ser de la forma* $4k + r$*, con* $k \in \mathbb{N}$ *y* $r \in \{0, 1, 2, 3\}$*, y de este modo:*

- *Si* $r = 0$, $n^2 = (4k)^2 = 16k^2 \equiv 0 \pmod 4$.
- *Si* $r = 1$, $n^2 = (4k + 1)^2 = 16k^2 + 8k + 1 \equiv 1 \pmod 4$.
- *Si* $r = 2$, $n^2 = (4k + 2)^2 = 16k^2 + 16k + 4 \equiv 0 \pmod 4$.
- *Si* $r = 3$, $n^2 = (4k + 3)^2 = 16k^2 + 24k + 9 \equiv 1 \pmod 4$.

Así, $x^2 + y^2$ *sólo puede ser congruente con* 0*,* 1 *o* 2 *módulo* 4*. Pero* $2003 \equiv 3 \mod 4$*. Por lo tanto, no es posible escribir* 2003 *como suma de dos cuadrados de números enteros positivos.*

Problema 7.10 Encuentra todos los enteros x, y, z que cumplen $x^2 + y^2 + z^2 - 2xyz = 0$.

Solución *La ecuación se puede transformar en:*

$$x^2 + y^2 + z^2 = 2xyz.$$

Si x*,* y *y* z *fuesen impares, entonces el lado izquierdo sería impar, pero el derecho sería par. Así que al menos uno de los enteros* x, y, z *es par. Por tanto,* $2xyz$ *ha de ser múltiplo de* 4*. Puesto que los cuadrados módulo* 4 *pueden ser* 0 *o* 1*, la ecuación obliga a que* x*,* y *y* z *sean pares.*

Escribamos $x = 2x_1$*,* $y = 2y_1$*,* $z = 2z_1$*, para ciertos* $x_1, y_1, z_1 \in \mathbb{Z}$*. Sustituyendo estas variables en la ecuación inicial y simplificando, queda:*

$$4x_1y_1z_1 = x_1^2 + y_1^2 + z_1^2.$$

En este punto, nos percatamos de que se puede repetir el razonamiento anterior, y que así $x_1 = 2x_2$*,* $y_1 = 2y_2$*,* $z_1 = 2z_2$*, para ciertos* $x_2, y_2, z_2 \in \mathbb{Z}$*. Reiterando el mismo argumento con estos* x_2, y_2, z_2 *y con los sucesivos* $x_i = 2x_{i+1}$*,* $y_i = 2y_{i+1}$*,* $z_i = 2z_{i+1}$ *que obtengamos, al final llegamos a que* x, y, z *son divisibles por infinitas*

potencias de 2. *Esto sólo lo cumplen*

$$x = 0, \quad y = 0, \quad z = 0.$$

Otra idea interesante que aparece en la resolución de algunos problemas olímpicos, como en el Problema 7.9 o el Problema 7.11 que se muestra a continuación, es la de clasificar los números enteros en clases de congruencia módulo un determinado número.

Problema 7.11 Sea n un número natural. Prueba que si la última cifra de 7^n es 3, entonces la penúltima es 4.

Solución *Si* n *es un número natural,* 7^n *acaba en* 3 *sólo cuando* $n = 4k + 3$, *con* $k \in \mathbb{N}$. *En efecto,* n *puede ser de la forma* $4k + r$, *con* $k \in \mathbb{N}$ *y* $r \in \{0, 1, 2, 3\}$. *Por el teorema 7.2 (de Euler), como* $\text{m. c. d.}(7, 10) = 1$, *se tiene que* $7^{\Phi(10)} \equiv 7^4 \equiv 1 \pmod{10}$, *por lo que:*

- *Si* $r = 0$, $7^n \equiv 7^{4k} \equiv (7^4)^k \equiv 1^k \equiv 1 \pmod{10}$.
- *Si* $r = 1$, $7^n \equiv 7^{4k+1} \equiv 7^{4k} \cdot 7 \equiv 7 \pmod{10}$.
- *Si* $r = 2$, $7^n \equiv 7^{4k+2} \equiv 7^{4k} \cdot 7^2 \equiv 49 \equiv 9 \pmod{10}$.
- *Si* $r = 3$, $7^n \equiv 7^{4k+3} \equiv 7^{4k} \cdot 7^3 \equiv 343 \equiv 3 \pmod{10}$.

Por otro lado, tenemos que $7^4 = 2401 \equiv 1 \pmod{100}$. *Por tanto, si* $k \in \mathbb{N}$,

$$7^{4k+3} \equiv (7^4)^k \cdot 7^3 \equiv 1 \cdot 343 \equiv 343 \equiv 43 \pmod{100}.$$

Esto significa que, si $k \in \mathbb{N}$, 7^{4k+3} *termina en* 43, *como queríamos demostrar.*

En el Problema 7.11, aparte de la estrategia que acabamos de comentar, también se echa mano del Teorema de Euler. Evidentemente, no es el único en el que ha aparecido este resultado u otros derivados de él, como el Pequeño Teorema de Fermat, que se usa en el Problema 7.12.

Problema 7.12 Encuentra todas las parejas de números primos p, q tales que $p^3 - q^5 = (p + q)^2$.

Solución *Resulta claro que, para que se cumpla la igualdad,* $p > q$. *De primeras, supongamos que* $p \neq 3$ *y* $q \neq 3$. *Por el Corolario 7.2 (Pequeño Teorema de Fermat), se tiene que* $p - q \equiv (p + q)^2 \pmod{3}$. *Así, si* $p \equiv q \pmod{3}$, *entonces* $0 \equiv q^2 \not\equiv 0$, *lo cual no es posible. Por tanto,* $p \not\equiv q \pmod{3}$. *Pero, en este caso,* $(p + q)^2 \equiv 0 \pmod{3}$, *mientras que* $p - q \not\equiv 0 \pmod{3}$, *lo que nuevamente no es posible. Por consiguiente, no queda más remedio que o bien* $p = 3$ *o* $q = 3$. *Como* $3^3 - 2^5 < 0$, *la única posibilidad es* $q = 3$. *En ese caso,* $p^3 - 243 = p^2 + 6p + 9$ *implica que* p *divide a* 252, *por lo que solamente puede ser* $p = 7$ *y la única pareja de números primos que cumple la ecuación es* $(p, q) = (7, 3)$.

El Pequeño Teorema de Fermat no es el único corolario que se puede extraer del Teorema de Euler relacionado con congruencias módulo un cierto número primo. Por ejemplo, también se tiene que:

- Para cualquier entero a, $a^p \equiv a \pmod{p}$.
- Para cualesquiera enteros a y b, $(a + b)^p \equiv a^p + b^p \pmod{p}$.

Obviamente, estos trucos pueden emplearse siempre que sea pertinente en la resolución de problemas. Sin embargo, el Teorema de Euler tampoco es la única fuente de creación de propiedades de números primos en clases de congruencia. De hecho, por ejemplo, el siguiente teorema se halla dentro del ámbito de la aritmética modular y permite caracterizar a los números primos, pues da una condición necesaria y suficiente para que un número lo sea. [1]

[1] Aunque el Teorema de Wilson permite identificar tanto si un número es primo como si no lo es, habitualmente no se utiliza como test de primalidad en la práctica, puesto que calcular $(n-1)! \pmod{n}$ para un número n grande es muy costoso y se conocen tests mucho más sencillos y rápidos.

Teorema 7.3 (de Wilson)

p es un número primo si y solo si

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

El nombre del teorema 7.3 se eligió en honor a John Wilson, matemático inglés del siglo XVIII. Veamos ahora un ejemplo de aplicación de dicho teorema a un problema olímpico.

Problema 7.13 Sea a el entero que cumple la igualdad $\sum_{i=1}^{23} \frac{1}{i} = \frac{a}{23!}$. Calcula el resto de dividir a entre 13.

Solución *Multiplicando ambos miembros de la ecuación por* 23!*, tenemos que* $a = \sum_{i=1}^{23} \frac{23!}{i}$*. Todos estos sumandos son nulos módulo* 13*, excepto* $\frac{23!}{13}$*, que es congruente con* $12! \cdot 10!$ *módulo* 13*. Usando el Teorema 7.3 (de Wilson), se tiene que:*

$$[a]_{13} = [12!]_{13} \cdot [10!]_{13} = [12!]_{13} \cdot [12!]_{13} \cdot [12^{-1}]_{13} \cdot [11^{-1}]_{13} = [-1]_{13} \cdot [-1]_{13} \cdot [-1]_{13} \cdot [6]_{13} = [-6]_{13} = [7]_{13}.$$

Por tanto, el resto es 7*.*

Terminaremos resolviendo problemas relacionados con criterios de divisibilidad.

Problema 7.14 Dado un número entero n escrito en el sistema de numeración decimal, formamos el número entero k restando del número formado por las tres últimas cifras de n el número formado por las cifras anteriores restantes. Demuestra que n es divisible por 7, 11 o 13 si y solo si k también lo es.

Solución *Sea A el número formado por las tres últimas cifras de n y B el número formado por todas las cifras anteriores. Esto significa que $n = 1000B + A$ y $k = A - B$. De este modo, se tiene que:*

$$n - k = 1001B = 7 \cdot 11 \cdot 13 \cdot B.$$

Por tanto, n y k son congruentes módulo 7*,* 11 *y* 13*.*

Con esta misma técnica, se puede resolver el siguiente problema, que queda propuesto para el lector.

Ejercicios Propuestos

1. Determina cuáles de los siguientes números son congruentes con 4 módulo 7: 81, 445, -74, 332, -52.

2. Conjetura, aunque no lo demuestres, en qué cifra debería acabar el número 3^{2021}.

3. ¿Qué letra hay que añadir al DNI 16620864 para obtener el correspondiente NIF?

4. Ayer fui a la biblioteca para que me prestaran un libro. Al ser un poco viejo, se le ha borrado el último dígito de su ISBN. Aun así, sí que pude leer los anteriores: $038796254\square$. ¿Qué dígito se ha borrado?

5. Al ir a hacer una transferencia a través de la aplicación web de su banco, Félix tecleó el siguiente código de cuenta corriente: 20387444716000004303. ¿Debería permitirle la aplicación web efectuar la transferencia? En caso negativo, y suponiendo que los dígitos que no son de control son correctos, ¿qué código tendría que haber tecleado?

6. ¿Para cuántos valores enteros c comprendidos entre 100 y 200 tiene solución la ecuación diofántica $56x + 378y = c$?

7. En la ecuación diofántica del ejercicio anterior, halla una solución particular (x_0, y_0) por medio del algoritmo de Euclides y la identidad de Bézout cuando $c = 112$.

8. Un viejo turista tenía 5000 pesetas y en su día quiso cambiarlas por francos franceses y marcos alemanes. El cambio que le ofrecía un banco era el siguiente: un franco equivalía a 24 pesetas y por un marco le daban 84 pesetas. Sabiendo que el banco no proporcionaba fracciones de ninguna moneda:
   a) ¿Pudo hacer el cambio?
   b) ¿Podría haberlo hecho si hubiera cambiado 6000 pesetas?
   c) Para ambos apartados, en caso afirmativo, ¿de cuántas formas diferentes pudo hacerlo?

9. Un hombre acude a un banco a cobrar un cheque por valor de D dólares y C céntavos. El cajero, por error, le entrega un sobre con C dólares y D centavos. El cliente no se da cuenta del error hasta que gasta 23 centavos y, además, observa que en ese momento tiene $2D$ dólares y $2C$ centavos. ¿Cuál es el valor del cheque?

10. ¿Qué resto se obtiene al dividir 6^{2021} entre 7?

11. Halla todas las soluciones de la ecuación $[4]_{18} \cdot a = [0]_{18}$ en $\mathbb{Z}_{18}$.

12. Encuentra todas las posibles soluciones para la ecuación $[7]_{12}^{-1} = [x]_{12}$ en $\mathbb{Z}_{12}$.

13. ¿Cuántos elementos invertibles hay en $\mathbb{Z}_{37}$?

14. Escribe todos los elementos de los conjuntos U_8 en $\mathbb{Z}_8$, U_{15} en $\mathbb{Z}_{15}$ y U_{18} en $\mathbb{Z}_{18}$.

15. Calcula $\Phi(6615)$.

16. Calcula las dos últimas cifras del número 63^{282}.

17. Calcula el resto de dividir 67^{9539} entre 17.

18. Halla el resto de dividir 215^{7371} entre 29.

19. Halla la última cifra del número 2018^{2019}.

20. Halla el resto de dividir 125^{4577} entre 13.

21. Halla el resto de dividir 2^{4k} entre 5 para todo $k \in \mathbb{N}$.

Bibliografía Adicional

1. Engel, A. (1998). Number Theory. *Problem-Solving Strategies*. Editorial Springer, 117-160.
2. García Merayo, F. (2015). *Matemática discreta*. Editorial Ediciones Paraninfo, SA.