

# Álgebra Básica

Eugenio Miranda Palacios

## 2. Aritmética entera

### 2.1. El anillo ordenado de los números enteros

Los números enteros son familiares en la aritmética elemental. Aquí queremos expresar esta familiaridad en términos precisos. Enunciaremos una lista de propiedades que poseen los enteros y a partir de ellas sacaremos nuestras deducciones. Todas estas propiedades pueden deducirse de una lista muy corta de axiomas, pero de momento esto es inmaterial.

Denotamos  $\mathbb{N}$  al conjunto de los enteros positivos (también llamados números naturales)  $\{1, 2, 3, \dots\}$ , y denotamos por  $\mathbb{Z}$  al conjunto de todos los enteros positivos, negativos y nulo. La letra  $\mathbb{N}$  es la inicial de la palabra *número* y  $\mathbb{Z}$  es la inicial de *Zahl* (número en alemán). En matemáticas está muy extendido el uso de ambas abreviaturas.

En el conjunto  $\mathbb{Z}$  hay definidas tres operaciones: Suma,  $x+y$ , resta o sustracción,  $x-y$  y multiplicación  $x \cdot y$  o  $xy$ . Con frecuencia es conveniente expresar la resta sumando el opuesto,  $x-y = x+(-y)$ . Estas operaciones verifican las siguientes propiedades:

**Ley asociativa**  $(x+y)+z = x+(y+z)$ ,  $(xy)z = x(yz)$

**Ley commutativa**  $x+y = y+x$   $xy = yx$

**Existencia de neutro**  $x+0 = x$   $x1 = x$

**Existencia de opuesto**  $x+(-x) = 0$ .

El número 0 se llama *neutro para la suma* porque al sumarlo a cualquier número  $x$  el resultado es igual a  $x$ . De la misma forma el número 1 es *neutro para la multiplicación*. Todo entero  $x$  tiene el opuesto  $-x$ , pero salvo 1 y  $-1$  ningún entero tiene un inverso multiplicativo. Mas adelante hallaremos inversos para todo entero no nulo cuando veamos los números racionales.

Además de las propiedades anteriores, existe otra propiedad que relaciona la suma y el producto:

**Ley distributiva**  $x(y + z) = xy + xz$ .

Un conjunto  $R$  con dos operaciones  $x + y$ ,  $xy$  verificando las anteriores propiedades se llama *anillo conmutativo*, así que el conjunto  $\mathbb{Z}$  de todos los enteros es un anillo conmutativo. Sin embargo estas leyes no son suficientes para determinar únicamente a  $\mathbb{Z}$ .

Veamos ahora algunas consecuencias de las leyes anteriores: De la ley distributiva se sigue que para todo  $x \in \mathbb{Z}$  se verifica  $x \cdot 0 = 0 = 0 \cdot x$ . Por la ley asociativa, la suma de cualquier número de términos es independiente de la manera en que introduzcamos paréntesis, y por la ley conmutativa el orden de los términos no altera la suma. Igual ocurre con la multiplicación. De momento aceptamos todo esto sin demostraciones.

La suma de los números  $a_1, \dots, a_n$  se puede escribir  $a_1 + \dots + a_n$ . Normalmente se abrevia esta expresión escribiendo el término general  $a_i$  precedido de una sigma mayúscula  $\Sigma$  con alguna indicación del rango en que se suman los enteros (excepto si esto último está claro del contexto). Así que en lugar de  $a_1 + \dots + a_n$  podemos escribir

$$\sum_{i=1}^n a_i, \quad \Sigma_1^n a_i, \quad \Sigma_i a_i, \quad \Sigma a_i$$

donde en cada caso  $i$  es una *variable muda*. Cuando  $n = 0$  la suma escrita es vacía y, por convención, se toma igual a cero.

Existe una abreviatura similar para productos repetidos usando la pi mayúscula en lugar de  $\Sigma$ . Así que en lugar de  $a_1 a_2 \dots a_n$  podemos escribir

$$\prod_{i=1}^n a_i, \quad \Pi_1^n a_i, \quad \Pi_i a_i, \quad \Pi a_i$$

Por ejemplo, podemos definir la función factorial como  $n! = \prod_1^n i$ . Un producto vacío se toma igual a uno; así que las sumas vacías y los productos vacíos son respectivamente neutros para la suma y el producto.

Una propiedad importante de los enteros es que el producto de dos enteros no nulos no es nunca cero:

**Ley de integridad** Para cualesquiera enteros  $a, b$ , si  $a \neq 0$  y  $b \neq 0$  entonces  $ab \neq 0$ . Además  $1 \neq 0$

Esto tiene una consecuencia muy útil:

**Ley cancelativa** Para cualesquiera  $a, b, c \in \mathbb{Z}$  si  $ca = cb$  y  $c \neq 0$  entonces  $a = b$ .

Esto asegura que “multiplicación por un entero no nulo” es una aplicación inyectiva de  $\mathbb{Z}$  en sí mismo. Para demostrarlo, supongamos que  $a \neq b$ , entonces  $a - b \neq 0$  y por la ley de integridad  $c(a - b) \neq 0$ , por tanto  $ca - cb = c(a - b) \neq 0$ .

En  $\mathbb{Z}$  además de las operaciones existe una relación de orden que escribimos  $x \leq y$  o  $y \geq x$ . Si  $x \leq y$  pero  $x \neq y$  escribimos  $x < y$  y también  $y > x$ . Esta relación es una *relación de orden total* y está relacionada con las operaciones de  $\mathbb{Z}$  por las siguientes reglas:

Si  $x_1 \leq x_2$ ,  $y_1 \leq y_2$  entonces  $x_1 + y_1 \leq x_2 + y_2$ .

Si  $x \leq y$  y  $z > 0$  entonces  $zx \leq zy$ .

Estas reglas indican que  $\mathbb{Z}$  es un *anillo totalmente ordenado*. Usando la ordenación podemos describir el conjunto  $\mathbb{N}$  de los enteros positivos como:

$$\mathbb{N} = \{x \in \mathbb{Z} \mid x > 0\} \quad (2.1)$$

Es costumbre tomar  $\mathbb{N}$  como conjunto de partida dado por algunos axiomas (normalmente los *axiomas de Peano*) y a partir de él se construye  $\mathbb{Z}$ .

Nótese que para todo  $x \in \mathbb{Z}$  se verifica que  $x = 0$  o  $x \in \mathbb{N}$  o  $-x \in \mathbb{N}$  y que estas tres posibilidades son mutuamente excluyentes. De hecho esto es cierto en cualquier anillo ordenado, definiendo  $\mathbb{N}$  por la regla 2.1, debido a que el orden es total.

## 2.2. Inducción. Principios del mínimo y del máximo

Para fijar  $\mathbb{Z}$  completamente utilizamos la siguiente condición sobre el conjunto  $\mathbb{N}$  de los enteros positivos:

**I. Principio de inducción** sea  $S$  un subconjunto de  $\mathbb{N}$  tal que  $1 \in S$  y que  $n \in S \Rightarrow n + 1 \in S$ . Entonces  $S = \mathbb{N}$ .

Este principio forma la base del método familiar de *demostración por inducción*: Sea  $P(n)$  una afirmación acerca de un entero positivo  $n$  (p. e.,  $P(n) =$  “la suma de los  $n$  primeros enteros positivos es  $n(n + 1)/2$ ”) Supongamos que queremos demostrar  $P(n)$  para todo  $n$ . Para ello por el principio de inducción basta demostrar  $P(1)$  y demostrar  $\forall n (P(n) \Rightarrow P(n + 1))$ , porque esto significa que el conjunto  $S = \{n \in \mathbb{N} \mid P(n)\}$  contiene a 1 y que si contiene a  $n$  también contiene a  $n + 1$ . Del principio de inducción se deduce que  $S = \mathbb{N}$ , es decir que todo  $n \in \mathbb{N}$  verifica  $P(n)$ .

Existen formas alternativas del principio de inducción que se usan con frecuencia:

**II. Principio de inducción alternativo** Sea  $S$  un subconjunto de  $\mathbb{N}$  tal que  $1 \in S$  y que  $n \in S$  siempre que para todo  $m < n$   $m \in S$ . Entonces  $S = \mathbb{N}$ .

**III. Principio del mínimo o principio de buena ordenación.** Todo conjunto no vacío de enteros positivos tiene un elemento mínimo.

**IV. Principio del máximo** Todo conjunto no vacío de enteros negativos tiene un elemento máximo.

El principio del mínimo se suele enunciar diciendo que  $\mathbb{N}$  está *bien ordenado*  
Veamos la equivalencia de los principios enunciados:

**I  $\Rightarrow$  II** : Sea  $S$  un conjunto verificando las hipótesis de **II**. Definimos  $T = \{x \in \mathbb{N} \mid \forall y (y \leq x \Rightarrow y \in S)\}$ , es decir que  $x \in T$  precisamente cuando todos los números desde 1 hasta  $x$  pertenecen a  $S$ . Es evidente que  $T \subseteq S$ , así que basta demostrar que  $T = \mathbb{N}$ . Como  $1 \in S$ , tenemos que  $1 \in T$ . Si  $n \in T$  entonces  $y \in S$  para todo  $y \leq n$ , luego  $n + 1 \in S$  y por tanto  $y \in S$  para todo  $y \leq n + 1$ . Pero esto implica que  $n + 1 \in T$ . Por **I** tenemos que  $T = \mathbb{N}$ .

**II  $\Rightarrow$  III** : Sea  $S$  un conjunto de enteros positivos que no tiene elemento mínimo. Vamos a demostrar que  $S$  es el conjunto vacío: Llamamos  $S' = \{x \in \mathbb{N} \mid x \notin S\}$  al complemento de  $S$ . Como  $S$  no tiene primer elemento,  $1 \notin S$  luego  $1 \in S'$ . Si para todo  $m \leq n$  se verifica que  $m \in S'$ , necesariamente  $n \in S'$  (porque en otro caso  $n \in S$  y  $n$  sería un elemento mínimo para  $S$ ). Por **II**,  $S' = \mathbb{N}$  y por tanto  $S = \emptyset$ .

**III  $\Rightarrow$  I** : El elemento mínimo de  $\mathbb{N}$  es 1. Sea  $S$  un subconjunto de  $\mathbb{N}$  que verifique las hipótesis del principio de inducción. Sea  $S' = \{x \in \mathbb{N} \mid x \notin S\}$ . Sabemos que  $1 \notin S'$  y si  $n \in S'$  entonces  $n - 1 \in S'$ . Luego  $S'$  no tiene elemento mínimo, por tanto es el conjunto vacío y  $S = \mathbb{N}$ .

**III  $\Rightarrow$  IV** : Sea  $S$  un conjunto no vacío de enteros negativos. Entonces  $T = \{x \in \mathbb{Z} \mid -x \in S\}$  es un conjunto no vacío de elementos positivos. Por **III**  $T$  tiene elemento mínimo, sea  $n$ . Entonces  $-n \in S$  y para todo  $m \in S$  tenemos que  $-m \in T$ , luego  $n \leq -m$  lo que equivale a  $-n \geq m$  para todo  $m \in T$ , así que  $-n$  es el elemento mínimo de  $S$ .

**IV  $\Rightarrow$  III** : Se demuestra de manera análoga al apartado anterior.

### 2.3. Divisibilidad

**Definición 2.1.** Dados  $a, b \in \mathbb{Z}$  decimos que  $b$  divide  $a$ , que  $a$  es divisible por  $b$  y que  $a$  es un múltiplo de  $b$  si existe un  $c \in \mathbb{Z}$  tal que  $a = bc$ . Lo denotamos por  $b \mid a$ .

Ya que cualquier múltiplo de 0 es 0, se verifica que  $0 \mid a$  sólo cuando  $a = 0$ . Por esta razón en la expresión  $b \mid a$  normalmente se toma  $b \neq 0$ . Para todo  $b \in \mathbb{Z}$  se verifica que  $b \mid 0$ .

La negación de  $b \mid a$  se escribe  $b \nmid a$  que significa que  $a$  no es divisible por  $b$ . La relación de divisibilidad en  $\mathbb{Z}$  satisface las siguientes propiedades:

1.  $c \mid b$  y  $b \mid a$  implican  $c \mid a$ .
2. Para todo  $a \in \mathbb{Z}$  se verifica que  $a \mid a$ .
3. Si  $a \mid b$  y  $b \mid a$  entonces  $a = \pm b$ .

Estas tres propiedades muestran que la divisibilidad es un orden parcial en el conjunto de enteros positivos.

4.  $b \mid a, a > 0$  y  $b > 0$  implican  $b \leq a$
5.  $b \mid a_1$  y  $b \mid a_2$  implican que  $b \mid (xa_1 + ya_2)$  para cualesquiera  $x, y \in \mathbb{Z}$ . En particular  $b \mid (a_1 - a_2)$ .
6.  $b \mid a$  implica que para todo  $c \in \mathbb{Z}$  se verifica  $b \mid ac$ .
7. Si  $c \neq 0, b \mid a$  si y sólo si  $cb \mid ca$

**Definición 2.2.** Dos enteros  $a, b$  tales que  $b \mid a$  y  $a \mid b$  se llaman *asociados*.

De la propiedad 3 anterior vemos que todo entero  $a$  está asociado a un único entero no negativo, que se llama su *valor absoluto* y se representa por  $|a|$ .

## 2.4. Algoritmo de la división euclídea

La primera aplicación del principio de buena ordenación es demostrar el *algoritmo de la división*:

**Teorema 2.3.** Para cualesquiera enteros  $a$  y  $b$ , con  $b > 0$ , existen enteros únicos  $q$  (el cociente) y  $r$  (el resto) tales que  $a = bq + r$  con  $0 \leq r < b$ .

*Demostración.* Consideramos el conjunto  $R = \{s = a - bq \mid q \in \mathbb{Z}, s \geq 0\}$ . Como  $b > 0$ , el elemento  $a - b(-|a|) = a + b \cdot |a|$  es mayor o igual a cero y está en  $R$ . Luego  $R$  no es vacío.

Por el principio de buena ordenación  $R$  tiene un primer elemento, al que llamamos  $r$ . Por definición  $r = a - bq \geq 0$ , y  $a = bq + r$ . Si fuera  $r \geq b$ , entonces  $s = r - b = a - b(q + 1) \geq 0$ , luego  $s \in R$  y  $s < r$ . Esto contradice la minimalidad de  $r$ , luego  $r < b$ .

Para demostrar que  $q$  y  $r$  son únicos, supongamos que  $a = bq + r = bp + s$  con  $0 \leq r, s < b$ . Esto implica que  $|r - s| < b$ . Pero  $r - s = b(q - p)$  lo que muestra que  $b \mid (r - s)$ . El único múltiplo de  $b$  con menor valor absoluto que  $b$  es el cero, luego  $r - s = 0$  y por tanto  $r = s$ . Además  $bp = bq$ , lo que implica  $p = q$ .  $\square$

**Corolario 2.4.** *Dados dos enteros  $a$  y  $b$  con  $b > 0$ ,  $b \mid a$  si y sólo si el resto de la división de  $a$  por  $b$  es 0.*

**Definición 2.5.** Para  $a \in \mathbb{Z}$  definimos el conjunto de todos los múltiplos de  $a$  como  $a\mathbb{Z} = \{aq \mid q \in \mathbb{Z}\}$ .

**Proposición 2.6.** *El conjunto  $a\mathbb{Z}$  es cerrado para la suma y la resta.*

**Teorema 2.7.** *Sea  $I$  un conjunto no vacío de enteros que es cerrado para la suma y la resta. Entonces o  $I$  sólo contiene al cero o contiene un mínimo elemento positivo  $a$ , en cuyo caso  $I = a\mathbb{Z}$ .*

*Demostración.* Ya que  $I$  no es vacío, o sólo contiene al cero o contiene algún entero no nulo  $b$ . En el primer caso hemos terminado. En el segundo caso,  $I$  contiene a  $b - b = 0$  y a  $0 - b = -b$ . Así que  $I$  contiene al entero positivo  $|b|$ . Luego el conjunto  $I^+$  de enteros positivos de  $I$  no es vacío. Por el principio de buena ordenación tiene un elemento mínimo, al que llamamos  $a$ .

Cualquier múltiplo de  $a$  se obtiene sumando  $a$  o  $-a$  consigo mismo un número finito de veces, luego  $a\mathbb{Z} \subseteq I$ .

Por otra parte, sea  $c \in I$  arbitrario. Dividimos entre  $a$ , así que  $c = aq + r$  con  $0 \leq r < a$ . Pero  $r = c - aq \in I$ . Por el carácter minimal de  $a$ , debe ser  $r = 0$ . O sea, que  $c = aq \in a\mathbb{Z}$ . Como  $c$  era un elemento arbitrario de  $I$ , obtenemos que  $I \subseteq a\mathbb{Z}$ . Combinando con el párrafo anterior nos queda que  $I = a\mathbb{Z}$ .  $\square$

## 2.5. Máximo común divisor y mínimo común múltiplo

**Definición 2.8.** Un entero positivo  $d$  se llama *máximo común divisor* de dos enteros dados  $a$  y  $b$  si

1.  $d$  es un divisor de  $a$  y  $b$
2. Todo divisor común de  $a$  y  $b$  es un divisor de  $d$ .

El máximo común divisor de  $a$  y  $b$  se representa como  $d = \text{m. c. d.}(a, b)$  y también como  $d = (a, b)$ .

El hecho de enunciar una definición del máximo común divisor (o de cualquier otro concepto) no garantiza su existencia. Además debemos justificar el uso del artículo determinado “el”, ya que implica su unicidad. Este último punto es fácil

de tratar: Si  $d_1$  y  $d_2$  son máximos comunes divisores de  $a$  y  $b$ , entonces la definición requiere que  $d_1 \mid d_2$  y  $d_2 \mid d_1$ , luego  $d_2 = \pm d_1$ . Ya que ambos son positivos,  $d_2 = d_1$ .

**Definición 2.9.** Sean  $a, b \in \mathbb{Z}$ . Cualquier entero de la forma  $ma + nb$  con  $m, n \in \mathbb{Z}$  se llama *combinación lineal de  $a$  y  $b$* .

El siguiente teorema muestra la existencia del máximo común divisor de dos enteros cualesquiera y su expresión como combinación lineal de ambos:

**Teorema 2.10.** *Dos enteros no nulos arbitrarios  $a$  y  $b$  tienen un máximo común divisor, que se puede expresar como la menor combinación lineal positiva de  $a$  y  $b$ .*

*Además un entero es una combinación lineal de  $a$  y  $b$  si y sólo si es un múltiplo de su máximo común divisor.*

*Demostración.* Sea  $I$  el conjunto de todas las combinaciones lineales de  $a$  y  $b$ , es decir

$$I = \{x \in \mathbb{Z} \mid x = ma + nb, m, n \in \mathbb{Z}\}$$

El conjunto  $I$  no es vacío, porque contiene a los elementos  $a = 1 \cdot a + 0 \cdot b$  y  $b = 0 \cdot a + 1 \cdot b$ . Es fácil comprobar que  $I$  es cerrado para la suma y la resta. Por el teorema 2.7,  $I = d\mathbb{Z}$ , siendo  $d$  el menor entero positivo de  $I$ .

Como  $d \in I$ , existen  $m, n \in \mathbb{Z}$  tales que  $d = ma + nb$ . Como  $a, b \in I$ , necesariamente  $d \mid a$  y  $d \mid b$ .

Sea ahora  $c \in \mathbb{Z}$  tal que  $c \mid a$  y  $c \mid b$ , así que  $a = cq_1$  y  $b = cq_2$ . Entonces

$$d = ma + nb = mcq_1 + ncq_2 = c(mq_1 + nq_2)$$

lo que muestra que  $c \mid d$ .

La última afirmación se sigue del hecho de que  $I$  (el conjunto de todas las combinaciones lineales de  $a$  y  $b$ ) es igual a  $d\mathbb{Z}$  (el conjunto de todos los múltiplos de  $d$ ).  $\square$

La igualdad  $d = ma + nb$  donde  $d = (a, b)$  se conoce como *igualdad de Bezout*.

**Corolario 2.11.** *Para cualquier entero positivo  $c$ ,  $(ca, cb) = c \cdot (a, b)$ .*

*Demostración.* Por el teorema 2.10 tenemos que  $(ca, cb)$  es el menor valor positivo de  $cax + cby$ , que es igual al producto de  $c$  por el menor valor positivo de  $ax + by$ , es decir el producto de  $c$  por  $(a, b)$ .  $\square$

**Corolario 2.12.** *Si  $c \mid a$ ,  $c \mid b$  y  $c > 0$ , entonces*

$$\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c}(a, b)$$

*Si  $(a, b) = d$  entonces  $(a/d, b/d) = 1$ .*

*Demostración.* La primera afirmación es consecuencia directa del corolario anterior reemplazando  $c, a, b$  en dicho corolario por  $c, a/c, b/c$  respectivamente. La segunda afirmación es un caso particular de la primera.  $\square$

**Definición 2.13.** Dos enteros  $a, b$  se llaman *primos relativos* si  $(a, b) = 1$ , es decir si no tienen divisores comunes salvo  $\pm 1$ .

**Teorema 2.14.** Para cualquier  $c \in \mathbb{Z}$ ,  $(a, b) = (b, a) = (a, -b) = (a, b + ac)$ .

**Teorema 2.15.** 1. Si  $b \mid ac$ , entonces  $b \mid (a, b)c$ .

2. Si  $b \mid ac$  y  $(a, b) = 1$  entonces  $b \mid c$ .
3. Si  $b \mid a$ ,  $c \mid a$  y  $(b, c) = 1$  entonces  $bc \mid a$ .
4.  $(a, bc) = 1$  si y sólo si  $(a, b) = 1$  y  $(a, c) = 1$ .

*Demostración.* 1. Supongamos que  $b \mid ac$ . Sea  $ac = bq$ . Escribimos  $(a, b) = ma + nb$  para algunos  $m, n \in \mathbb{Z}$ . Multiplicando por  $c$  obtenemos  $(a, b)c = mac + nbc = (mq + nc)b$ .

2. Simplemente tomamos  $(a, b) = 1$  en el apartado anterior.
3. Sea  $a = bq$ . Si  $c \mid a = bq$  y por el apartado anterior  $c \mid q$ , sea  $q = cq_1$ . Sustituyendo obtenemos  $a = bcq_1$ , luego  $bc \mid a$ .
4. Sea  $(a, bc) = 1$ . Entonces  $ma + n(bc) = 1$  para algunos  $m, n \in \mathbb{Z}$ . Podemos escribir esta igualdad de otras dos formas:  $ma + (nc)b = 1$ ,  $ma + (nb)c$  que muestran que  $(a, b) = 1$  y  $(a, c) = 1$ .

A la inversa, existen enteros  $m_1, m_2, n_1, n_2$  tales que  $1 = m_1a + n_1b = m_2a + n_2c$ . Multiplicando y agrupando términos queda:  $1 = (m_1m_2)(a + n_1m_2b + m_1n_2c) + n_1n_2bc$ , luego  $(a, bc) = 1$ .

$\square$

Probablemente estamos acostumbrados a calcular el máximo común divisor de  $a$  y  $b$  mediante el cálculo de sus factorizaciones en primos. Esta técnica es efectiva para números pequeños, y la estudiaremos mas adelante. Pero en la práctica, puede ser muy largo hallar los factores primos de números grandes, mientras que el máximo común divisor se encuentra en muchos menos pasos usando el método que vamos a describir a continuación.

El máximo común divisor de dos números puede calcularse utilizando un procedimiento conocido como *algoritmo de Euclides* (nuestra demostración del teorema 2.7 no incluye un método explícito para calcularlo). Para describir el algoritmo de Euclides necesitamos las siguientes propiedades:

**Lema 2.16.** 1. Si  $a \neq 0$  y  $b \mid a$ , entonces  $(a, b) = |b|$

2. Si  $a = bq + r$ , entonces  $(a, b) = (b, r)$ .

*Demostración.* 1. Todo divisor de  $b$  es un divisor de  $a$ . Y todo divisor de  $b$  divide a  $|b|$ . Aplicando directamente la definición de máximo común divisor obtenemos el resultado buscado.

2. El elemento  $a$  es una combinación lineal de  $b$  y  $r$ , luego  $(b, r) \mid a$ . Ya que también  $(b, r) \mid b$  obtenemos que  $(b, r) \mid (a, b)$ . Como  $r = a - bq$  es una combinación lineal de  $a$  y  $b$ , un argumento similar muestra que  $(a, b) \mid (b, r)$  y por tanto  $(a, b) = (b, r)$ .

□

Dados enteros  $a > b > 0$  el algoritmo de Euclides utiliza repetidamente el algoritmo de la división para obtener

$$\begin{array}{ll} a = bq_1 + r_1 & \text{con } 0 \leq r_1 < b \\ b = r_1q_2 + r_2 & \text{con } 0 \leq r_2 < r_1 \\ r_1 = r_2q_3 + r_3 & \text{con } 0 \leq r_3 < r_2 \\ & \text{etc.} \end{array}$$

Ya que  $r_1 > r_2 > \dots \geq 0$ , los restos van menguando y tras un número finito de pasos obtenemos un resto  $r_{n+1} = 0$ . El algoritmo acaba con la ecuación

$$r_{n-1} = r_nq_{n+1} + 0$$

Esto nos da el máximo común divisor:

$$(a, b) = (b, r_1) = (r_1, r_2) = \dots = (r_{n-1}, r_n) = r_n$$

*Ejemplo 2.17.* Para mostrar que  $(24, 18) = 6$  tenemos:

$$\begin{array}{ll} 24 = 18 \cdot 1 + 6 & (24, 18) = (18, 6) \\ 18 = 6 \cdot 3 + 0 & (18, 6) = 6 \end{array}$$

*Ejemplo 2.18.* Veamos que  $(126, 35) = 7$ :

$$\begin{array}{ll} 126 = 35 \cdot 3 + 21 & (126, 35) = (35, 21) \\ 35 = 21 \cdot 1 + 14 & (35, 21) = (21, 14) \\ 21 = 14 \cdot 1 + 7 & (21, 14) = (14, 7) \\ 14 = 7 \cdot 2 + 0 & (14, 7) = 7 \end{array}$$

*Ejemplo 2.19.* Calculamos  $(83, 38) = 1$ :

$$\begin{array}{ll}
 83 = 38 \cdot 2 + 7 & (83, 38) = (38, 7) \\
 38 = 7 \cdot 5 + 3 & (38, 7) = (7, 3) \\
 7 = 3 \cdot 2 + 1 & (7, 3) = (3, 1) \\
 3 = 1 \cdot 3 + 0 & (3, 1) = 1
 \end{array}$$

Si sólo se necesita calcular el máximo común divisor, paramos en cuanto podamos calcularlo en la cabeza. Para mostrar que  $(83, 38) = 1$ , nótese que ya que 7 no tiene divisores positivos salvo 1 y 7 y no es un divisor de 38, es claro de inmediato que  $(38, 7) = 1$ .

*Ejemplo 2.20.* A veces queremos conocer la combinación lineal de  $a$  y  $b$  que nos da  $(a, b)$ . Al calcular  $(126, 35)$  en el ejemplo 2.18 tenemos las siguientes ecuaciones:

$$\begin{array}{ll}
 a = bq_1 + r_1 & 126 = 35 \cdot 3 + 21 \\
 b = r_1q_2 + r_2 & 35 = 21 \cdot 1 + 14 \\
 r_1 = r_2q_3 + r_3 & 21 = 14 \cdot 1 + 7 \\
 r_2 = dq_4 + 0 & 14 = 7 \cdot 2 + 0
 \end{array}$$

El siguiente paso es despejar el resto no nulo en cada una de las ecuaciones, omitiendo la última y sustituyendo los anteriores para expresarlos como combinación lineal de  $a$  y  $b$ :

$$\begin{aligned}
 r_1 &= a + (-q_1)b \\
 r_2 &= b + (-q_2)r_1 & = (-q_2)a + (1 + q_1q_2)b \\
 d &= r_1 + (-q_3)r_2 & = (1 + q_2q_3)a + (-q_1 - q_3 - q_1q_2q_3)b
 \end{aligned}$$

es decir:

$$\begin{aligned}
 21 &= 126 + (-3)35 \\
 14 &= 35 + (-1)21 & = (-1)126 + 4 \cdot 35 \\
 7 &= 21 + (-1)14 & = 2 \cdot 126 - 7 \cdot 35
 \end{aligned}$$

La técnica usada en el ejemplo precedente puede extenderse fácilmente a la situación general en que se quiere expresar  $(a, b)$  como una combinación lineal de  $a$  y  $b$ . Después de despejar para el resto en cada ecuación relevante nos queda

$$\begin{array}{ll}
\cdots & \\
r_{j-1} = r_{j-3} + (-q_{j-1})r_{j-2} & = m_{j-1}a + n_{j-1}b \\
r_j = r_{j-2} + (-q_j)r_{j-1} & = m_ja + n_jb \\
r_{j+1} = r_{j-1} + (-q_j)r_j & = m_{j+1}a + n_{j+1}b \\
\cdots &
\end{array}$$

donde  $m_{j+1} = m_{j-1} - q_j m_j$  y  $n_{j+1} = n_{j-1} - q_j n_j$ .

El algoritmo de Euclides puede expresarse en una forma matricial conveniente que arrastra al mismo tiempo los restos y las combinaciones lineales: Empezamos con la matriz

$$\begin{array}{ccc}
a & 1 & 0 \\
b & 0 & 1
\end{array}$$

y dividimos  $a = bq_1 + r_1$ . La tercera fila de la matriz se obtiene restando a la primera el producto de la segunda por  $q_1$ :

$$\begin{array}{ccc}
a & 1 & 0 \\
b & 0 & 1 \\
r_1 & 1 & -q_1
\end{array}$$

Ahora tomamos  $b = r_1 q_2 + r_2$  y restamos el producto de  $q_2$  por la tercera fila de la segunda:

$$\begin{array}{ccc}
a & 1 & 0 \\
b & 0 & 1 \\
r_1 & 1 & -q_1 \\
r_2 & -q_2 & 1 + q_1 q_2
\end{array}$$

Es fácil comprobar que este algoritmo produce filas sucesivas  $(r_j m_j n_j)$  compuestas de los restos  $r_j$  y los coeficientes tales que  $r_j = m_j a + n_j b$ . Se continúa el proceso hasta que el primer coeficiente de la fila es 0. En ese momento la penúltima fila nos da el máximo común divisor y los coeficientes de la combinación lineal buscada.

*Ejemplo 2.21.* Usamos la forma matricial del algoritmo de Euclides para calcular una vez mas el máximo común divisor de  $a = 126$  y  $b = 35$ :

$$\begin{array}{ccc}
126 & 1 & 0 \\
35 & 0 & 1 \\
21 & 1 & -3 \\
14 & -1 & 4 \\
7 & 2 & -7 \\
0 & -5 & 18
\end{array}$$

y obtenemos que  $(126, 35) = 7 = 2 \cdot 126 - 7 \cdot 35$ .

La última línea  $0 = -5 \cdot 126 + 18 \cdot 35$  también nos da información interesante: Podemos sumar cualquier múltiplo de esta combinación lineal a la representación anterior del máximo común divisor. Por ejemplo,  $7 = (-3) \cdot 126 + 11 \cdot 35$  y también  $7 = (-8) \cdot 126 + 29 \cdot 35$ .

*Ejemplo 2.22.* En forma matricial, el cálculo de  $(83, 38)$  es el siguiente:

$$\begin{array}{rrr} 83 & 1 & 0 \\ 38 & 0 & 1 \\ 7 & 1 & -2 \\ 3 & -5 & 11 \\ 1 & 11 & -24 \\ 0 & -38 & 83 \end{array}$$

Así que  $(83, 38) = 1 = 11 \cdot 83 + (-24) \cdot 38$ .

El número  $(a, b)$  puede escribirse de infinitas maneras como combinación lineal de  $a$  y  $b$ : El método matricial nos da una combinación lineal  $0 = m_1a + n_1b$ , que sumado a la igualdad de la penúltima fila nos da  $d = (m + km_1)a + (n + kn_1)b$  para cualquier  $k \in \mathbb{Z}$ .

Dual al concepto de máximo común divisor es el de mínimo común múltiplo:

**Definición 2.23.** Un entero positivo  $m$  se llama *mínimo común múltiplo* de los enteros no nulos  $a$  y  $b$  si

1.  $m$  es un múltiplo de ambos  $a$  y  $b$ .
2. Cualquier múltiplo de  $a$  y  $b$  es un múltiplo de  $m$ .

Usamos la notación  $\text{m. c. m.}(a, b)$  o bien  $[a, b]$  para el mínimo común múltiplo de  $a$  y  $b$ .

**Teorema 2.24.** *El conjunto  $I$  de todos los múltiplos de dos enteros no nulos  $a$  y  $b$  contiene un entero no nulo y es cerrado para la suma y la resta.*

*Dicho conjunto  $I$  es de la forma  $I = m\mathbb{Z}$ , donde  $m = \text{m. c. m.}(a, b)$ . En particular, dos enteros no nulos cualesquiera tienen un mínimo común múltiplo.*

*Demostración.* El entero  $ab$  es distinto de cero y pertenece a  $I$ . Si  $c_1 = q_1a = p_1b$  y  $c_2 = q_2a = p_2b$ , entonces  $c_1 \pm c_2 = (q_1 \pm q_2)a = (p_1 \pm p_2)b$ . Por 2.7 tenemos el segundo resultado.  $\square$

**Teorema 2.25.** *Si  $c > 0$ ,  $[ca, cb] = c[a, b]$ . También  $[a, b](a, b) = |ab|$ .*

*Demostración.* Sean  $[ca, cb] = cq$  y  $[a, b] = m$ . Como  $a \mid m$  y  $b \mid m$ , tenemos que  $ac \mid mc$  y  $bc \mid mc$ , luego  $cq \mid mc$  y por tanto  $q \mid m$ . Por otra parte,  $ca \mid cq$ ,  $cb \mid cq$  de donde  $a \mid q$ ,  $b \mid q$  y por tanto  $m \mid q$ . Como ambos son positivos,  $m = q$ .

Para demostrar la segunda parte podemos suponer que  $a, b > 0$  porque  $[a, b] = [a, -b]$ . Empezamos con el caso especial  $(a, b) = 1$ . Ahora  $[a, b] = ac$ . Entonces  $b \mid ac$  y como  $(a, b) = 1$  necesariamente  $b \mid c$ , luego  $ab \mid ac = [a, b]$ . Siempre se cumple que  $[a, b] \mid ab$  y como ambos son positivos, son iguales.

En el caso general sea  $d = (a, b)$ . Tenemos  $(a/d, b/d) = 1$ . Aplicando el resultado del caso particular se obtiene

$$\left[ \frac{a}{d}, \frac{b}{d} \right] \left( \frac{a}{d}, \frac{b}{d} \right) = \frac{a}{d} \frac{b}{d}$$

Multiplicando por  $d^2$  obtenemos  $[a, b](a, b) = ab$ . □

## 2.6. Ecuaciones diofánticas

El estudio de la aritmética elemental de los enteros se divide en varias partes: Divisibilidad y factorización, congruencias, funciones aritméticas y ecuaciones diofánticas. Vamos a introducir estas últimas.

Una *ecuación diofántica* es una ecuación polinómica con coeficientes y raíces enteros. De la misma forma un sistema de ecuaciones diofánticas es un conjunto finito de ecuaciones diofánticas simultáneas. Resolver una ecuación diofántica (o un sistema de ellas) es hallar explícitamente sus raíces enteras.

*Ejemplo 2.26.* Consideremos la ecuación  $x^2 + y^2 = z^2$ . Las soluciones enteras de esta ecuación se llaman *ternas pitagóricas* por motivos obvios. Algunas soluciones conocidas desde antiguo son  $(4, 3, 5)$ ,  $(12, 5, 13)$  y  $(20, 21, 29)$ . Si exigimos que  $\text{m. c. d.}(x, y, z) = 1$ , la solución general viene dada por  $(2uv, u^2 - v^2, u^2 + v^2)$  con  $u, v$  de distinta paridad,  $u > v$  y  $\text{m. c. d.}(u, v) = 1$

*Ejemplo 2.27.* Una generalización de la anterior es la *ecuación de Fermat*:  $x^n + y^n = z^n$  con  $n \geq 3$ . El llamado *último teorema de Fermat* establece que esta ecuación no tiene solución entera con  $xyz \neq 0$ . Para dar una idea de la dificultad de la aritmética, este teorema fué enunciado a mediados del siglo XVII por Fermat y su demostración se remató sólo a finales del siglo XX por Wiles, mas de 300 años después.

Si una ecuación (o sistema) es *determinada*, es decir tiene un número finito de soluciones en  $\mathbb{Q}$  o en  $\mathbb{R}$ , podemos resolverla en uno de estos cuerpos y comprobar sus raíces una a una para ver cuales son enteras. Por ello, las ecuaciones diofánticas interesantes son las *indeterminadas*, que admiten infinitas soluciones en  $\mathbb{Q}$  y debemos caracterizar cuales de ellas son enteras.

Vamos a discutir un método para resolver los sistemas diofánticos lineales. El caso mas sencillo es el de una ecuación con dos incógnitas:

$$ax + by = c \quad (2.2)$$

- Teorema 2.28.**
1. La ecuación 2.2 tiene solución si y sólo si  $\text{m. c. d.}(a, b) \mid c$ .
  2. Una solución particular de 2.2 se obtiene por el algoritmo extendido de Euclides.
  3. Sea  $d = \text{m. c. d.}(a, b)$  y sea  $(x_0, y_0)$  una solución particular de 2.2. La solución general  $(x, y)$  viene dada por

$$x = x_0 + k \frac{b}{d}, \quad y = y_0 - k \frac{a}{d}$$

con  $k \in \mathbb{Z}$  arbitrario.

*Demostración.* 1. Supongamos que 2.2 tiene una solución  $(x_0, y_0)$  y sea  $d = \text{m. c. d.}(a, b)$ . Entonces

$$c = ax_0 + by_0 = d\left(\frac{a}{d}x_0 + \frac{b}{d}y_0\right)$$

y por tanto  $d \mid c$ .

A la inversa, sea  $c = dc_1$ . Por el teorema de Bezout existen  $m, n \in \mathbb{Z}$  tales que  $am + bn = d$ . Entonces  $(x_0, y_0) = (mc_1, nc_1)$  es una solución de 2.2.

2. Por el algoritmo extendido de Euclides encontramos  $m, n \in \mathbb{Z}$  tales que  $am + bn = d$ . El último párrafo del punto anterior termina la demostración.
3. Sea  $(x_0, y_0)$  una solución particular, es decir  $ax_0 + by_0 = c$ . Llamamos  $x = x_0 + k \frac{b}{d}$ ,  $y = y_0 - k \frac{a}{d}$  y calculamos  $ax + by = a(x_0 + k \frac{b}{d}) + b(y_0 - k \frac{a}{d}) = c$ . A la inversa, sea  $ax + by = c$ . Restando la solución particular tenemos que  $(x - x_0)a + (y - y_0)b = 0$ . Dividimos por  $d = \text{m. c. d.}(a, b)$  y despejamos:  $(x - x_0)(a/d) = -(y - y_0)(b/d)$ . Como  $\text{m. c. d.}(a/d, b/d) = 1$ , necesariamente  $x - x_0 = k \cdot b/d$  y  $-(y - y_0) = h \cdot a/d$ . Sustituyendo y simplificando vemos que  $k = h$ . Finalmente despejando vemos que  $x = x_0 + k \frac{b}{d}$  y  $y = y_0 - k \frac{a}{d}$

□

Las ideas subyacentes al algoritmo de Euclides pueden aplicarse también para hallar una *solución general en enteros* de cualquier conjunto de ecuaciones lineales con coeficientes enteros. El procedimiento es el siguiente:

1. Buscamos un coeficiente no nulo  $c$  de mínimo valor absoluto en el sistema de ecuaciones. Supongamos que este coeficiente aparece en una ecuación que tiene la forma

$$cx_0 + c_1x_1 + \cdots + c_kx_k = d;$$

y por sencillez supongamos  $c > 0$ .

2. Si  $c = 1$ , usamos esta ecuación para eliminar la variable  $x_0$  de las otras ecuaciones del sistema. Si no quedan mas ecuaciones, el cálculo acaba y hemos obtenido una solución general en términos de las variables no eliminadas.
3. Si  $c > 1$ , entonces

- Si  $c \mid c_1, \dots, c \mid c_k$ , comprobamos si  $c \nmid d$  en cuyo caso no hay solución en enteros.
- Si  $c \mid d$  dividimos ambos miembros por  $c$  y eliminamos  $x_0$  como en el caso  $c = 1$ .

4. Si  $c > 1$  y existe un  $c_i$  no divisible por  $c$ , dividimos los  $c_i$  entre  $c$ :  $c_i = q_i c + r_i$ . Introducimos una nueva variable

$$x_0 + q_1x_1 + \cdots + q_kx_k = t;$$

eliminamos la variable  $x_0$  de las otras ecuaciones en favor de  $t$  y reemplazamos la ecuación original por

$$ct + r_1x_1 + \cdots + r_kx_k = d$$

Este proceso debe terminar ya que cada paso reduce el número de ecuaciones o el valor absoluto del mínimo coeficiente no nulo del sistema.

Cuando se aplica este proceso a la ecuación  $ax + by = 1$  para  $a, b$  dados, el proceso anterior es esencialmente el algoritmo de Eulides extendido.

*Ejemplo 2.29.* Queremos resolver el sistema

$$\begin{aligned} 10w + 3x + 3y + 8z &= 1 \\ 6w - 7x - 5z &= 2 \end{aligned}$$

El coeficiente de menor valor absoluto es 3 que multiplica a  $y$  en la primera ecuación y es positivo. Como  $3 \nmid 10$ , introducimos una nueva variable

$$\lfloor 10/3 \rfloor w + \lfloor 3/3 \rfloor x + \lfloor 3/3 \rfloor y + \lfloor 8/3 \rfloor z = 3w + x + y + 2z = t_1$$

y la usamos para eliminar  $y$ . La primera ecuación se convierte en

$$(10 \pmod 3)w + (3 \pmod 3)x + 3t_1 + (8 \pmod 3)z = w + 3t_1 + 2z = 1$$

y la segunda ecuación queda igual.

Ahora el coeficiente de  $w$  en la primera ecuación es 1. Usamos dicha ecuación para eliminar  $w$  y la segunda ecuación se convierte en

$$6(1 - 3t_1 - 2z) - 7x - 5z = 2$$

esto es

$$7x + 18t_1 + 17z = 4$$

Introducimos una nueva variable

$$x + 2t_1 + 2z = t_2$$

y eliminamos  $x$ :

$$7t_2 + 4t_1 + 3z = 4.$$

Introducimos otra variable para eliminar  $z$ , que tiene el menor coeficiente:

$$2t_2 + t_1 + z = t_3$$

Eliminando  $z$  nos queda

$$t_2 + t_1 + 3t_3 = 4$$

y finalmente utilizamos esta ecuación para eliminar  $t_2$ . Nos quedan dos variables independientes  $t_1$  y  $t_3$ . Sustituyendo hacia atrás en las variables originales obtenemos la solución general:

$$\begin{aligned} w &= 17 - 5t_1 - 14t_3 \\ x &= 20 - 5t_1 - 17t_3 \\ y &= -55 + 19t_1 + 45t_3 \\ z &= -8 + t_1 + 7t_3 \end{aligned}$$

En otras palabras, todas las soluciones enteras  $(w, x, y, z)$  del sistema original se obtienen de las últimas igualdades cuando  $t_1$  y  $t_3$  recorren independientemente todos los enteros.

El proceso de eliminación de variables descrito (que es reminiscente del método de eliminación de Gauss para sistemas lineales en un cuerpo) es sencillo y directo pero no es el mejor método disponible para este problema. El método que quizás sea el más elegante y sistemático se basa en la teoría de módulos sobre dominios de ideales principales, teoría general que no se estudia en este curso.

## 2.7. Primos

**Definición 2.30.** Un entero  $p > 1$  se llama *número primo* si sus únicos divisores son  $\pm 1$  y  $\pm p$ . Un entero  $a > 1$  se llama *compuesto* si no es primo.

**Lema 2.31** (Euclides). *Un entero  $p > 1$  es primo si y sólo si satisface la siguiente propiedad: Si  $p \mid ab$  para  $a, b \in \mathbb{Z}$ , entonces o  $p \mid a$  o  $p \mid b$ .*

*Demostración.* Supongamos que  $p$  es un primo y  $p \mid ab$ . Si  $a = 0$  el resultado es claro. Si  $a \neq 0$  sabemos que  $\text{o}(p, a) = p$  o  $\text{o}(p, a) = 1$  porque  $(p, a)$  siempre es un divisor de  $p$  y  $p$  es primo. En el primer caso  $p \mid a$  y ya está. En el segundo caso aplicamos el segundo punto del teorema 2.15 para mostrar que  $p \mid ab$  implica  $p \mid b$ .

A la inversa, supongamos que  $p$  verifica la condición dada. Si  $p = ab$  la condición implica que  $\text{o}(p, a) = a$  (ya que  $p \mid a$  y  $p > a$ ) o  $p = b$  y por tanto  $p$  es primo.  $\square$

**Teorema 2.32** (Teorema fundamental de la aritmética). *Todo entero  $a > 1$  se factoriza de manera única como producto de primos en la forma*

$$a = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$$

donde  $p_1 < p_2 < \cdots < p_n$  y los exponentes  $e_1, e_2, \dots, e_n$  son todos positivos.

*Demostración.* Supongamos que existe algún entero mayor que 1 que no es un producto de números primos. Entonces el conjunto  $I$  de todos los enteros positivos que no tienen factorización en primos es no vacío. Por el principio de buena ordenación ese conjunto tiene un primer elemento, sea  $b$ . Este  $b$  no puede ser primo, porque en este caso tendría una factorización en primos. Así que  $b = cd$  donde  $c, d$  son positivos y menores que  $b$ . Luego  $c, d \notin I$  y por tanto ambos se pueden escribir como producto de primos. Pero entonces  $b = cd$  también es un producto de números primos. Luego  $I$  es vacío y todo entero mayor que 1 se puede escribir como producto de primos. Además, como la multiplicación de enteros es conmutativa, los factores primos de  $b$  pueden ordenarse de la forma deseada.

Si existe un entero mayor que 1 para el que la factorización no es única, por el principio de buena ordenación existe un mínimo entre tales enteros, sea  $a$ . Sea  $a = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} = q_1^{f_1} q_2^{f_2} \cdots q_m^{f_m}$  con  $p_1 < p_2 < \cdots < p_n$  y  $q_1 < q_2 < \cdots < q_m$ . Por el lema de Euclides  $q_1 \mid p_k$  para algún  $k$  y  $p_1 \mid q_j$  para algún  $j$ . Como todos los  $p_i$  y todos los  $q_j$  son primos, necesariamente  $q_1 = p_k$  y  $p_1 = q_j$ . Como  $q_1 \leq q_j$  y  $p_1 \leq p_k$ , necesariamente  $p_1 = q_1$ . Podemos tomar

$$s = \frac{a}{p_1} = \frac{a}{q_1} = p_1^{e_1-1} p_2^{e_2} \cdots p_n^{e_n} = q_1^{f_1-1} q_2^{f_2} \cdots q_m^{f_m}$$

Si  $s=1$  entonces  $a = p_1$  tiene una factorización única, en contra de la elección de  $a$ . Si  $s > 1$ , como  $s < a$  y  $s$  tiene dos factorizaciones obtenemos otra vez una contradicción con la elección de  $a$ .  $\square$

Podemos considerar a los primos como los elementos a partir de los cuales se obtienen por multiplicación todos los demás números enteros positivos, de la misma forma en que todo número entero positivo se obtiene a partir del 1 mediante suma reiterada.

**Proposición 2.33.** *Sean  $a = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$  y  $b = p_1^{f_1} p_2^{f_2} \dots p_n^{f_n}$  dos enteros positivos descompuestos en factores primos. Entonces  $b \mid a$  si y sólo si  $f_i \leq e_i$  para todo  $i = 1, \dots, n$ .*

La factorización en primos permite escribir directamente el máximo común divisor y el mínimo común múltiplo de dos enteros dados:

**Proposición 2.34.** *Sean  $a, b$  enteros positivos con factorizaciones primas*

$$a = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n} \quad y \quad b = p_1^{f_1} p_2^{f_2} \dots p_n^{f_n}$$

con  $e_i, f_i \geq 0$  para todo  $i$ .

Para cada  $i$  sean  $g_i = \min(e_i, f_i)$  y  $h_i = \max(e_i, f_i)$ . Entonces

$$\begin{aligned} \text{m. c. d.}(a, b) &= p_1^{g_1} p_2^{g_2} \dots p_n^{g_n} \\ \text{m. c. m.}(a, b) &= p_1^{h_1} p_2^{h_2} \dots p_n^{h_n} \end{aligned}$$

*Demostración.* La demostración se sigue inmediatamente del teorema fundamental de la aritmética y las definiciones de máximo común divisor y mínimo común múltiplo.  $\square$

Para números pequeños probablemente es mas fácil usar sus factorizaciones primas para hallar el máximo común divisor y el mínimo común múltiplo. Pero para números grandes hallar su factorización en primos es muy lento, aún usando algoritmos sofisticados sobre ordenadores potentes. En contraste, el algoritmo de Euclides es mucho mas rápido y eficiente para calcular el máximo común divisor de grandes números.

*Ejemplo 2.35.* Calculamos una vez mas  $(126, 35)$ . Descomponemos en factores primos:  $126 = 2^1 \cdot 3^2 \cdot 5^0 \cdot 7^1$  y  $35 = 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^1$ . Así que  $(126, 35) = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^1 = 7$  y  $[126, 35] = 2^1 \cdot 3^2 \cdot 5^1 \cdot 7^1 = 630$

Si conocemos la factorización de un entero es fácil listar todos sus divisores: Si  $a = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$  entonces  $b$  es un divisor de  $a$  si y sólo si  $b = p_1^{f_1} p_2^{f_2} \dots p_n^{f_n}$  con  $f_i \leq e_i$  para todo  $i$ . Así que podemos listar todos los divisores de  $a$  disminuyendo sistemáticamente los exponentes de cada uno de sus factores primos.

**Teorema 2.36** (Euclides). *Existen infinitos primos*

*Demostración.* Supongamos que sólo hubiese un número finito de primos, sean  $p_1, p_2, \dots, p_n$ . Formamos el número  $a = p_1 p_2 \dots p_n + 1$ . Por el teorema 2.32 existe un divisor primo de  $a$ , sea  $p$ . Este debe estar en la lista así que  $p \mid (p_1 p_2 \dots p_n)$ , luego  $p \mid (a - p_1 \dots p_n) = 1$ . Pero un primo no puede dividir a 1.  $\square$

## 2.8. Congruencias

Para muchos problemas aritméticos, la información importante está en los restos obtenidos al dividir por un entero fijo  $n$ . Como sólo son posibles los  $n$  restos diferentes  $0, 1, \dots, n-1$ , pueden producirse considerables simplificaciones. Para valores pequeños de  $n$  es posible incluso utilizar el método de prueba y error.

*Ejemplo 2.37.* Un teorema de Lagrange establece que todo entero positivo puede escribirse como suma de cuatro cuadrados. Vamos a ver que si  $n$  es un entero positivo que al dividirlo por 8 da de resto 7, no puede expresarse como suma de tres cuadrados, por lo que el teorema de Lagrange es el mejor posible:

Sea  $n = a^2 + b^2 + c^2$ . Al dividir ambos miembros por 8 los restos deben ser iguales. Por la proposición 2.42 podemos calcular el resto de  $a^2 + b^2 + c^2$  calculando los restos de  $a, b$  y  $c$ , elevándolos al cuadrado y sumándolos (y dividiendo por 8 si es necesario). Los posibles valores para  $a^2, b^2, c^2$  son 0, 1, 4. Para comprobar los posibles valores del resto de  $a^2 + b^2 + c^2$  sólo tenemos que sumar tres de tales valores. Un estudio de todos los casos muestra que no podemos obtener 7 como resto de  $a^2 + b^2 + c^2$ . Luego si  $n$  da de resto 7 al dividirlo por 8, no puede ser suma de tres cuadrados.

La técnica de prueba y error puede usarse para ver que una ecuación polinómica no tiene raíces enteras:

*Ejemplo 2.38.* Sea  $f(x) = x^3 + 3412x^2 - 1235x + 678443$ . Supongamos que existiese un  $n \in \mathbb{Z}$  tal que  $f(n) = 0$ . Al tomar los restos módulo 2 nos queda  $n^3 + n + 1 = 0$ . Pero  $n^3 + n + 1$  es impar para cualquier valor de  $n$ , luego  $f(n) \neq 0$  para todo valor de  $n$ .

Una situación familiar en la que efectuamos los cálculos tras dividir por un valor fijo es en la suma de horas, donde el entero fijo es 12. Las reglas de los signos es hacer el cálculo con los restos al dividir por 2. Gauss introdujo la notación de congruencia que simplifica los cálculos de este tipo:

**Definición 2.39.** Sea  $n$  un entero positivo. Los enteros  $a$  y  $b$  se llaman *congruentes módulo n* si tienen el mismo resto al dividirlos por  $n$ . Esto se denota por  $a \equiv b$  (mód  $n$ ) o  $a \equiv b \pmod{n}$

Si utilizamos el algoritmo de la división para escribir  $a = nq + r$  donde  $0 \leq r < n$  entonces  $r = n \cdot 0 + r$ . Es inmediato de la definición precedente que  $a \equiv r \pmod{n}$ . En particular cualquier entero es congruente módulo  $n$  a uno de los enteros  $0, 1, 2, \dots, n - 1$ .

La definición 2.39 proporciona la mejor visión intuitiva del concepto de congruencia, pero en casi todas las demostraciones es más fácil utilizar la siguiente caracterización, que permite usar los hechos sobre divisibilidad que ya hemos estudiado:

**Proposición 2.40.** *Sean  $a, b, n \in \mathbb{Z}$  con  $n > 0$ . Entonces  $a \equiv b \pmod{n}$  si y sólo si  $n \mid (a - b)$ .*

*Demostración.* Si  $a \equiv b \pmod{n}$ , entonces  $a = nq_1 + r$  y  $b = nq_2 + r$ . Despejando el resto tenemos  $r = a - nq_1 = b - nq_2$ . Trasponiendo términos  $a - b = n(q_1 - q_2)$ , luego  $n \mid (a - b)$ .

A la inversa sea  $n \mid (a - b)$ , así que  $a - b = nq$ . Por el algoritmo de la división  $b = nq_1 + r$  con  $0 \leq r < n$ . Sumando ambas igualdades tenemos que  $a = n(q_1 + q) + r$ , luego los restos de dividir  $a$  por  $n$  y  $b$  por  $n$  son iguales y por tanto  $a \equiv b \pmod{n}$ .  $\square$

Esta proposición nos dice que  $a \equiv b \pmod{n}$  si y sólo si  $a - b = nq$  para algún entero  $q$ , lo que podemos escribir como  $a = b + nq$ . Esta observación proporciona un método muy útil de reemplazar una congruencia por una ecuación diofántica.

**Proposición 2.41.** *La relación  $a \equiv b \pmod{n}$  es una relación de equivalencia.*

**Proposición 2.42.** *Sea  $n > 0$  un entero. Cualesquiera  $a, b, c, d \in \mathbb{Z}$  verifican las siguientes propiedades:*

1. *Si  $a \equiv c \pmod{n}$  y  $b \equiv d \pmod{n}$ , entonces  $a + b \equiv c + d \pmod{n}$ ,  $a - b \equiv c - d \pmod{n}$  y  $ab \equiv cd \pmod{n}$ .*
2. *Si  $a + c \equiv a + d \pmod{n}$  entonces  $c \equiv d \pmod{n}$ . Si  $ac \equiv ad \pmod{n}$  y  $(a, n) = 1$  entonces  $c \equiv d \pmod{n}$ .*

*Demostración.* Sean  $a \equiv c \pmod{n}$  y  $b \equiv d \pmod{n}$ . Entonces  $n \mid (a - c)$  y  $n \mid (b - d)$ . Sumando tenemos que  $n \mid ((a + b) - (c + d))$  y restando  $n \mid ((a - b) - (c - d))$ . También tenemos que  $n \mid (a - c)b = ab - cb$  y  $n \mid c(b - d) = cb - cd$ . Sumando tenemos  $n \mid (ab - cd)$ .

Sea ahora  $a + c \equiv a + d \pmod{n}$ . Entonces  $n \mid ((a + c) - (a + d)) = c - d$ . Si  $ac \equiv ad \pmod{n}$  tenemos que  $n \mid (ac - ad) = a(c - d)$  y como  $(a, n) = 1$ , se sigue que  $n \mid (c - d)$ .  $\square$

Las principales consecuencias de esta proposición son:

1. Podemos sustituir cualquier entero de la congruencia por un entero congruente. Por ejemplo para mostrar que  $99^2 \equiv 1 \pmod{100}$  lo mas fácil es sustituir 99 por  $-1$  y calcular  $(-1)^2 = 1$ .
2. Podemos sumar o restar el mismo entero a ambos miembros de una congruencia.
3. Podemos multiplicar ambos miembros de una congruencia por el mismo entero.
4. Hay que tener mucho cuidado al simplificar o dividir ambos miembros de la congruencia por el mismo entero  $a$ : Sólo puede hacerse cuando  $(a, n) = 1$ . Por ejemplo  $30 \equiv 6 \pmod{8}$  pero al dividir ambos miembros por 6 tenemos  $5 \equiv 1 \pmod{8}$ , lo cual es falso. Pero al dividir por 3 tenemos  $10 \equiv 2 \pmod{8}$  lo que es correcto porque  $(3, 8) = 1$ .
5. Cualquier ecuación diofántica puede convertirse a una congruencia módulo  $n$  simplemente cambiando el signo  $=$  por  $\equiv$  y cualquier término congruente a 0 puede sencillamente omitirse. Este proceso se conoce como *reducción módulo n*. Por ejemplo la ecuación  $x^3 + 5x^2 + 6x - 11 = 0$  se convierte en  $x^3 + x^2 + 1 \equiv 0 \pmod{2}$ .

*Ejemplo 2.43.* La proposición 2.42 muestra que para calcular el resto de dividir  $a + b$  o  $ab$  por  $n$  podemos calcular los restos de dividir  $a$  y  $b$  entre  $n$  y sumarlos o multiplicarlos, dividiendo otra vez por  $n$  si es necesario. Por ejemplo,  $101 \equiv 5 \pmod{8}$  y  $142 \equiv 6 \pmod{8}$ , así que  $101 \cdot 142 \equiv 5 \cdot 6 \equiv 6 \pmod{8}$ .

*Ejemplo 2.44.* Vamos a calcular las potencias de 2 módulo 7. En vez de calcular cada potencia y entonces dividir por 7, reducimos módulo 7 en cada paso del cálculo:

$$\begin{aligned} 2^2 &\equiv 4 \pmod{7}, \\ 2^3 &\equiv 2^2 \cdot 2 \equiv 4 \cdot 2 \equiv 1 \pmod{7}, \\ 2^4 &\equiv 2^3 \cdot 2 \equiv 1 \cdot 2 \equiv 2 \pmod{7}, \\ 2^5 &\equiv 2^4 \cdot 2 \equiv 2 \cdot 2 \equiv 4 \pmod{7} \end{aligned}$$

Tal como hemos hecho los cálculos, está claro que las potencias se repiten. De hecho como sólo hay un número finito de posibles restos módulo  $n$ , las potencias módulo  $n$  de cualquier entero siempre acaban repitiéndose.

**Proposición 2.45.** *Sean  $a, n \in \mathbb{Z}$  con  $n > 1$ . Existe un entero  $b$  tal que  $ab \equiv 1 \pmod{n}$  si y sólo si  $(a, n) = 1$ .*

*Demostración.* Supongamos que existe  $b \in \mathbb{Z}$  tal que  $ab \equiv 1 \pmod{n}$ . Luego  $ab = 1 + nq$  con  $q \in \mathbb{Z}$ . Esto puede reescribirse como una combinación lineal  $ab - nq = 1$ . Luego  $(a, n) = 1$ .

A la inversa sea  $(a, n) = 1$ . Entonces existen  $b, t \in \mathbb{Z}$  tales que  $ab + tn = 1$ . Reduciendo módulo  $n$  obtenemos  $ab \equiv 1 \pmod{n}$ .  $\square$

## 2.9. Sistemas de ecuaciones en congruencias

Vamos a presentar un estudio sistemático de ecuaciones lineales en congruencias. En muchos aspectos resolver congruencias es como resolver ecuaciones sobre los enteros. Pero existen algunas diferencias: Una ecuación lineal en una incógnita sobre los enteros tiene como máximo una solución, mientras que  $2x \equiv 2 \pmod{4}$  tiene dos soluciones:  $x \equiv 1 \pmod{4}$  y  $x \equiv 3 \pmod{4}$ . También puede ocurrir que no existan soluciones, por ejemplo  $3x \equiv 2 \pmod{6}$  no las tiene. Así que el primer paso es obtener un teorema para determinar si existe o no alguna solución. Naturalmente para  $a, b, n$  pequeños, las soluciones de  $ax \equiv b \pmod{n}$  se pueden encontrar probando todas las posibilidades.

La proposición 2.45 muestra que la congruencia

$$ax \equiv 1 \pmod{n}$$

tiene solución si y sólo si  $(a, n) = 1$ . De hecho la demostración de dicha proposición muestra que se obtiene una solución utilizando el algoritmo extendido de Euclides para expresar  $1 = ab + nq$  con  $b, q \in \mathbb{Z}$ .

**Definición 2.46.** Dos soluciones  $r$  y  $s$  a la congruencia  $ax \equiv b \pmod{n}$  son distintas módulo  $n$  si  $r$  y  $s$  no son congruentes módulo  $n$ .

**Teorema 2.47.** *La congruencia  $ax \equiv b \pmod{n}$  tiene solución si y sólo si  $b$  es divisible por  $d = \text{m. c. d.}(a, n)$ . Si  $d \mid b$ , existen  $d$  soluciones distintas módulo  $n$  y estas soluciones son congruentes módulo  $n/d$ .*

*Demostración.* La congruencia  $ax \equiv b \pmod{n}$  tiene solución si y sólo si existen enteros  $s, q \in \mathbb{Z}$  tales que  $as = b + nq$  o lo que es lo mismo,  $as + (-q)n = b$ . Así que existe una solución si y sólo si se puede expresar  $b$  como combinación lineal de  $a$  y  $n$ . Pero tales combinaciones son precisamente los múltiplos de  $d$ .

Sea ahora  $d \mid b$  y sea  $m = n/d$ . Sean  $x_1, x_2$  soluciones de la congruencia  $ax \equiv b \pmod{n}$ , así que  $ax_1 \equiv ax_2 \pmod{n}$ . Luego  $n \mid (ax_1 - ax_2)$  y por tanto  $n \mid d(x_1 - x_2)$  y  $m = (n/d) \mid (x_1 - x_2)$  con lo que  $x_1 \equiv x_2 \pmod{m}$ .

A la inversa, si  $x_1 \equiv x_2 \pmod{m}$  entonces  $m \mid (x_1 - x_2)$ ,  $n = dm \mid d(x_1 - x_2)$ . Como  $d \mid a$  podemos concluir que  $n \mid a(x_1 - x_2)$  o lo que es lo mismo, que  $ax_1 \equiv ax_2 \pmod{n}$ .

Las distintas soluciones están entre los restos  $0, 1, \dots, n - 1$ . Dada una de las soluciones, todas las otras se hallan sumando múltiplos de  $n/d$ , lo que nos da un total de  $d$  soluciones distintas.  $\square$

Vamos a describir un algoritmo para resolver congruencias lineales de la forma

$$ax \equiv b \pmod{n} \quad (2.3)$$

1. Calculamos  $d = (a, n)$ . Si  $d \nmid b$ , la ecuación no tiene solución.
2. Si  $d \mid b$  escribimos la congruencia 2.3 como una ecuación diofántica  $ax = b + qn$ .
3. Ya que  $d$  es un divisor común de  $a, b$  y  $n$  podemos tomar  $a = da_1, b = db_1$  y  $n = dn_1$ . Dividiendo la anterior ecuación por  $d$  nos queda  $a_1x = b_1 + qn_1$ .
4. La congruencia 2.3 es por tanto equivalente a

$$a_1x \equiv b_1 \pmod{n_1}$$

donde ahora  $(a_1, n_1) = 1$ .

5. Por la proposición 2.45 hallamos un entero  $c$  tal que  $ca_1 \equiv 1 \pmod{n_1}$ . Multiplicando ambos miembros por  $c$  obtenemos

$$x \equiv cb_1 \pmod{n_1}$$

6. Finalmente, ya que la congruencia original era módulo  $n$ , debemos dar nuestra respuesta módulo  $n$ . La solución módulo  $n_1$  determina  $d$  soluciones distintas módulo  $n$ :  $x \equiv b_1c + kn_1$  con  $k = 0, \dots, d - 1$ .

*Ejemplo 2.48* (Congruencias lineales homogéneas). Vamos a considerar el caso especial de una ecuación homogénea lineal

$$ax \equiv 0 \pmod{n}$$

En este caso siempre existe una solución,  $x \equiv 0 \pmod{n}$ , pero puede que no sea la única.

En el segundo paso de la solución obtenemos  $a_1x \equiv 0 \pmod{n}$ . Ya que  $(a_1, n_1) = 1$ , por la proposición 2.42 podemos cancelar  $a_1$  y nos queda  $x \equiv 0 \pmod{n_1}$ , luego las  $d$  soluciones son  $x \equiv 0, n_1, 2n_1, \dots, (d - 1)n_1 \pmod{n}$ .

Por ejemplo la congruencia  $28x \equiv 0 \pmod{48}$  tiene cuatro soluciones distintas módulo 48:  $x \equiv 0, 12, 24, 36 \pmod{48}$

*Ejemplo 2.49.* Para resolver la congruencia  $60x \equiv 90 \pmod{105}$  primero calculamos  $D = (60, 105) = 15$ . Como  $15 \mid 90$ , la ecuación tiene solución. Dividiendo por  $d$  obtenemos la ecuación

$$4x \equiv 6 \pmod{7} \quad (2.4)$$

Buscamos un entero  $c$  tal que  $4c \equiv 1 \pmod{7}$ , a saber  $c = 2$ . Multiplicamos ambos miembros de 2.4 por  $c$  y obtenemos  $8x \equiv 12 \pmod{7}$ , que se reduce a  $x \equiv 5 \pmod{7}$ .

La ecuación original tiene pues quince soluciones:

$$x \equiv 5 + 7k \pmod{105} \text{ con } k = 0, 1, \dots, 14$$

## 2.10. Teorema chino de los restos

Vamos a estudiar ahora la resolución de sistemas de ecuaciones en congruencias. Empezamos por el caso de dos congruencias:

**Teorema 2.50.** *Dos congruencias simultáneas*

$$x \equiv a \pmod{m} \quad x \equiv b \pmod{n} \quad (2.5)$$

tienen solución si y sólo si  $a \equiv b \pmod{(m, n)}$ . En este caso la solución es única módulo  $[m, n]$ .

*Demostración.* De la primera congruencia de 2.5 se sigue que  $x = a + mt$ . Sustituyendo en la segunda obtenemos que  $t$  debe verificar la ecuación  $a + mt \equiv b \pmod{n}$  lo que es lo mismo que  $mt \equiv b - a \pmod{n}$ . Hemos visto anteriormente que esta ecuación tiene solución si y sólo si  $d = (m, n)$  divide a  $(b - a)$ , y en ese caso es equivalente a la congruencia

$$\frac{m}{d}t \equiv \frac{b-a}{d} \pmod{\frac{n}{d}}$$

Sea  $t_0$  una solución particular de esta congruencia. La solución general es

$$t \equiv t_0 \pmod{\frac{n}{d}}$$

así que  $t = t_0 + u(n/d)$  con  $u \in \mathbb{Z}$ . La solución general de la congruencia original es

$$x \equiv a + m\left(t_0 + \frac{n}{d}u\right) = x_0 + u\frac{mn}{d}$$

o sea  $x \equiv x_0 \pmod{[m, n]}$ . □

*Ejemplo 2.51.* Vamos a resolver el sistema

$$x \equiv 5 \pmod{11}, \quad x \equiv 3 \pmod{23}$$

La primera congruencia dice que  $x = 5 + 11t$ . Sustituyendo en la segunda obtenemos la ecuación  $5 + 11t \equiv 3 \pmod{23}$ , es decir  $11t \equiv -2 \pmod{23}$ . La única solución de esta última es  $t \equiv 4 \pmod{23}$ . La forma general de  $t$  es pues  $t = 4 + 23u$ . Sustituido en la expresión para  $x$  tenemos que  $x = 5 + 11(4 + 23u) = 49 + (11 \cdot 23)u$ . Luego la solución general del sistema propuesto es  $x \equiv 49 \pmod{11 \cdot 23}$ .

*Ejemplo 2.52.* El sistema

$$x \equiv 7 \pmod{42}, \quad x \equiv 15 \pmod{51}$$

no tiene solución porque  $d = (42, 51) = 3$  y  $7 \not\equiv 15 \pmod{3}$ .

*Ejemplo 2.53.* Sea el sistema

$$x \equiv 3 \pmod{14}, \quad x \equiv 7 \pmod{16}$$

Aquí  $d = (14, 16) = 2$  y  $3 \equiv 7 \pmod{2}$ , luego existe una solución única módulo  $[14, 16] = 112$ . Realizando los cálculos vemos que la solución es  $x \equiv 87 \pmod{112}$ .

Cuando los módulos  $m$  y  $n$  de 2.5 son primos relativos existe otro método para obtener la solución del sistema: Por el algoritmo extendido de Euclides determinamos  $u, v \in \mathbb{Z}$  tales que  $um + vn = 1$ . Entonces  $x = avn + bum$  es una solución. En efecto  $vn \equiv 1 \pmod{m}$  y  $um \equiv 1 \pmod{n}$ . Por tanto  $x = avn + bum \equiv a(vn) \equiv a \pmod{m}$  y  $x \equiv b(um) \equiv b \pmod{n}$ .

*Ejemplo 2.54.* Vamos a resolver el sistema

$$x \equiv 7 \pmod{8}, \quad x \equiv 3 \pmod{5}$$

El algoritmo extendido de Euclides nos dice que  $2 \cdot 8 + (-3) \cdot 5 = 1$ . Luego la solución general del sistema propuesto es

$$x = 7 \cdot (-3) \cdot 5 + 3 \cdot 2 \cdot 8 = -105 + 48 = -57 \equiv 23 \pmod{40}$$

Consideramos ahora el caso general, donde hay  $r \geq 2$  congruencias simultáneas. Necesitamos un resultado que conecta máximos comunes divisores y mínimos comunes múltiplos:

**Lema 2.55.** Para  $a, b, c \in \mathbb{Z}$  arbitrarios se verifican las propiedades distributivas:

$$\begin{aligned} (a, [b, c]) &= [(a, b), (a, c)] \\ [a, (b, c)] &= ([a, b], [a, c]) \end{aligned}$$

*Demostración.* Sea  $p$  un primo arbitrario y sean  $p^i, p^j, p^k$  las máximas potencias de  $p$  que dividen respectivamente a  $a, b, c$ . Como el enunciado es simétrico para  $b$  y  $c$ , podemos tomar  $j \geq k$ . Entonces la máxima potencia de  $p$  que divide a  $[b, c]$  es  $p^j$  y el exponente de la máxima potencia de  $p$  que divide a  $(a, [b, c])$  es  $\min(i, j)$ . Por otra parte los exponentes de las máximas potencias de  $p$  que dividen a  $(a, b)$  y  $(a, c)$  son respectivamente  $\min(i, j)$  y  $\min(i, k)$ . Como  $j \geq k$ , tenemos que  $\min(i, j) \geq \min(i, k)$ . Luego el exponente de la máxima potencia de  $p$  que divide a  $[(a, b), (a, c)]$  es  $\min(i, j)$ . Así que  $(a, [b, c])$  y  $[(a, b), (a, c)]$  tienen la misma descomposición en primos y por tanto son iguales.

La demostración de la segunda propiedad es análoga.  $\square$

**Teorema 2.56.** *Un sistema de  $r$  congruencias simultáneas*

$$x \equiv a_i \pmod{m_i} \quad i = 1, 2, \dots, r \quad (2.6)$$

tiene solución si y sólo si para todo par de índices  $i, j$  se verifica

$$a_i \equiv a_j \pmod{(m_i, m_j)} \quad (2.7)$$

y en este caso la solución es única módulo  $M_r = [m_1, \dots, m_r]$ .

*Demostración.* En primer lugar hay que observar que si las congruencias 2.6 tienen solución, dos cualesquiera de ellas también la tienen, así que por el teorema 2.5, deben verificarse las condiciones 2.7.

Demostramos por inducción que estas condiciones son suficientes: El teorema 2.5 es el caso  $r = 2$ . Supongamos que el resultado es cierto para  $r-1$  congruencias. Con esta hipótesis existe una solución

$$x_0 \equiv a_i \pmod{m_i} \quad i = 1, 2, \dots, r-1 \quad (2.8)$$

y cualquier otra solución  $x$  debe ser de la forma  $x \equiv x_0 \pmod{M_{r-1}}$ ,  $M_{r-1} = [m_1, \dots, m_{r-1}]$ . Para que  $x$  sea solución de todas las ecuaciones 2.6 debe satisfacer además  $x \equiv a_r \pmod{m_r}$ . Por el teorema 2.5 concluimos que este conjunto de congruencias tiene solución sólo cuando

$$x_0 \equiv a_r \pmod{(M_{r-1}, m_r)} \quad (2.9)$$

y que en este caso existe una solución única módulo  $[M_{r-1}, m_r] = M_r$ .

Queda por comprobar que el  $x_0$  hallado verifica las condiciones 2.9. Por el lema 2.55 tenemos que

$$(M_{r-1}, m_r) = ([m_1, \dots, m_{r-1}], m_r) = [(m_1, m_r), \dots, (m_{r-1}, m_r)]$$

por lo que el sistema de congruencias 2.9 es equivalente al sistema

$$x_0 \equiv a_r \pmod{(m_i, m_r)}, \quad i = 1, 2, \dots, r-1$$

Pero estas últimas se derivan fácilmente de las hipótesis.  $\square$

*Ejemplo 2.57.* En *Disquisitiones Arithmeticae* de Gauss aparece el siguiente sistema:

$$x \equiv 17 \pmod{504}, \quad x \equiv -4 \pmod{35}, \quad x \equiv 33 \pmod{16}$$

Al resolver las dos primeras congruencias obtenemos  $x \equiv 521 \pmod{2520}$  y combinando esta con la tercera de las congruencias dadas el resultado final es  $x \equiv 3041 \pmod{5040}$

*Ejemplo 2.58.* Muchos entretenimientos matemáticos pertenecen al tipo de problemas que se resuelven por congruencias simultáneas. Existen diversos manuscritos medievales que contienen colecciones de problemas populares y muchos de estos problemas, con pequeñas variantes, se pueden reconocer casi todas las semanas en las revistas actuales. Un ejemplo:

*Una anciana va al mercado con un canasto de huevos y un caballo pisa el canasto y rompe los huevos. El jinete acepta pagar los daños y pregunta cuántos huevos ha roto. Ella no recuerda el número exacto, pero cuando los tomaba de dos en dos sobraba un huevo. Lo mismo sucedía cuando los cogía en grupos de tres, cuatro, cinco o seis respectivamente; pero cuando los agrupaba de siete en siete no sobraba ninguno. ¿Cuál es el menor número de huevos que había en el canasto?* En términos matemáticos esto significa que

$$\begin{aligned} x &\equiv 1 \pmod{2, 3, 4, 5, 6} \\ x &\equiv 0 \pmod{7} \end{aligned}$$

donde  $x$  es el número de huevos. Las cinco primeras condiciones pueden combinarse para dar  $x \equiv 1 \pmod{60}$ . Resolviendo con la última de las congruencias dadas obtenemos la solución  $x \equiv 301 \pmod{420}$ , así que el mínimo número de huevos que contenía el cesto es 301.

El caso especial en que los módulos de las congruencias 2.6 son primos relativos dos a dos ocurre en muchas aplicaciones. De acuerdo con el teorema 2.56 existe una solución única a estas congruencias módulo el producto de todos los  $m_i$ . Gauss introdujo un procedimiento especial, usado previamente por Euler, para determinar la solución. Pero el método es aún más antiguo y aparece en las obras de varios matemáticos. La primera fuente conocida es la *Aritmética* del autor chino Sun-Tse, alrededor del siglo I de nuestra era, y la fórmula resultante se conoce como *teorema chino de los restos*.

Empezamos formando el producto  $M = m_1 m_2 \dots m_r$ . Al dividir  $M$  entre  $m_i$  el cociente

$$\frac{M}{m_i} = m_1 \dots m_{i-1} m_{i+1} \dots m_r \tag{2.10}$$

es divisible por todos los módulos excepto por  $m_i$ , con el que es primo relativo. Por tanto podemos resolver para todo  $i$  la congruencia lineal

$$b_i \frac{M}{m_i} \equiv 1 \pmod{m_i}$$

y podemos enunciar:

**Teorema 2.59** (Teorema chino de los restos). *Sea dado un sistema de congruencias 2.6 donde los módulos  $m_i$  son primos relativos dos a dos. Para cada  $i$  se determina un  $b_i$  que satisfaga la congruencia lineal 2.10. La solución del sistema de congruencias es*

$$x \equiv a_1 b_1 \frac{M}{m_1} + a_2 b_2 \frac{M}{m_2} + \cdots + a_r b_r \frac{M}{m_r} \pmod{M} \quad (2.11)$$

*Demostración.* La verificación es sencilla:  $m_i$  divide a todos los  $M/m_j$  salvo a  $M/m_i$  así que

$$x \equiv a_i b_i \frac{M}{m_i} \equiv a_i \pmod{m_i}$$

□

*Ejemplo 2.60.* El ejemplo dado por Sun-Tse corresponde a las tres congruencias

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

Aquí  $M = 3 \cdot 5 \cdot 7 = 105$  y

$$\frac{M}{m_1} = 35, \quad \frac{M}{m_2} = 21, \quad \frac{M}{m_3} = 15$$

El conjunto de congruencias lineales

$$35b_1 \equiv 1 \pmod{3} \quad 21b_2 \equiv 1 \pmod{5} \quad 15b_3 \equiv 1 \pmod{7}$$

tiene las soluciones  $b_1 = 2$ ,  $b_2 = 1$ ,  $b_3 = 1$  así que de acuerdo con la fórmula 2.11 la solución es

$$x \equiv 2 \cdot 2 \cdot 35 + 3 \cdot 1 \cdot 21 + 2 \cdot 1 \cdot 15 \equiv 233 \pmod{105}$$

Las congruencias son una herramienta muy útil en cuestiones de calendario, tales como la determinación de la Pascua, el día de la semana de una fecha concreta y problemas parecidos. Gauss ilustra el teorema chino de los restos con el problema de encontrar los años que tienen un cierto período respecto a los ciclos solar y lunar y al índice romano. Anteriormente el matemático indio Brahmagupta (siglo VII) trató problemas similares respecto a los ciclos planetarios.

En la fórmula 2.11 para calcular los multiplicadores  $b_i M/m_i$  sólo hacen falta los números  $m_i$ . Por tanto, si hay que resolver varios sistemas de congruencias con los mismos módulos, la expresión 2.11 es particularmente adecuada porque hay que calcular los multiplicadores sólo una vez.

*Ejemplo 2.61.* Leonardo discute en el *Liber Abaci* la siguiente cuestión: *Se le pide a alguien que piense un número. Entonces se le piden los restos del número al dividirlo por 5, 7 y 9 y con esta información se adivina el número pensado.*

Vamos a denotar como  $x$  al número desconocido y por  $a_1, a_2, a_3$  a los tres restos de forma que

$$x \equiv a_1 \pmod{5} \quad x \equiv a_2 \pmod{7} \quad x \equiv a_3 \pmod{9}$$

Los módulos son primos relativos y  $M = 5 \cdot 7 \cdot 9 = 315$ ,

$$\frac{M}{m_1} = 63, \quad \frac{M}{m_2} = 45, \quad \frac{M}{m_3} = 35$$

Las congruencias lineales

$$63b_1 \equiv 1 \pmod{5}, \quad 45b_2 \equiv 1 \pmod{7}, \quad 35b_3 \equiv 1 \pmod{9}$$

tienen las soluciones  $b_1 = 2, b_2 = 5, b_3 = 8$  así que la fórmula 2.11 nos da

$$x \equiv 126a_1 + 225a_2 + 280a_3 \pmod{315}$$

De esta expresión obtenemos  $x$  según los restos conocidos  $a_1, a_2, a_3$ . La solución es única sólo si se exige que el número requerido sea menor que 315.

*Ejemplo 2.62. ((Regiomontanus).* Hallar un número  $x$  tal que

$$x \equiv 3 \pmod{10}, \quad x \equiv 11 \pmod{13}, \quad x \equiv 15 \pmod{17}$$

*Ejemplo 2.63. ((Euler).* Hallar un número  $x$  tal que

$$x \equiv 3 \pmod{11}, \quad x \equiv 5 \pmod{19}, \quad x \equiv 10 \pmod{29}$$

Concluimos con una observación que se aplicará después: Supongamos que al resolver un problema hay que determinar un número  $x$  que para un módulo  $m_1$  tiene  $s_1$  valores admisibles

$$x \equiv a_1, \dots, a_{s_1} \pmod{m_1}$$

y para otro módulo  $m_2$  hay  $s_2$  valores admisibles

$$x \equiv b_1, \dots, b_{s_2} \pmod{m_2}$$

Cuando  $(m_1, m_2) = 1$  cada valor  $m_i$  puede combinarse con cada valor  $b_j$ , así que en total hay  $s_1 s_2$  soluciones módulo  $m_1 m_2$ . Esta observación puede generalizarse a  $r$  módulos primos relativos dos a dos.

*Ejemplo 2.64.* Vamos a resolver la ecuación

$$x^2 \equiv 1 \pmod{40}$$

Es inmediato comprobar que esa ecuación equivale al sistema

$$x^2 \equiv 1 \pmod{5} \quad x^2 \equiv 1 \pmod{8}$$

Como los módulos son pequeños, por prueba y error vemos que las soluciones de estas ecuaciones son

$$x \equiv 1, 4 \pmod{5} \quad x \equiv 1, 3, 5, 7 \pmod{8}$$

El algoritmo de Euclides nos dice que  $(-3) \cdot 5 + 2 \cdot 8 = 1$ . El teorema chino de los restos nos dice que  $x \equiv 16a_i - 15b_j \pmod{40}$  donde  $a_i = 1, 4$  y  $b_j = 1, 3, 5, 7$ . Despues de reducir módulo 40 obtenemos todas las soluciones:

$$x \equiv 1, 11, 21, 31, 9, 19, 29, 39 \pmod{40}$$

Resulta bastante mas difícil resolver congruencias del tipo  $a_kx^k + \dots + a_1x + a_0 \equiv 0 \pmod{n}$ . Utilizando el teorema chino de los restos el problema se reduce a resolver congruencias módulo  $p^e$  para factores primos de  $n$ . Y las soluciones módulo  $p^e$  se determinan a partir de las soluciones módulo primo  $p$ . Si el primo  $p$  es pequeño, estas últimas pueden obtenerse por prueba y error, sencillamente sustituyendo sucesivamente  $0, 1, \dots, p-1$  en la congruencia. Además podemos utilizar el teorema de Fermat que hay mas adelante para reducir el problema a uno donde el grado del polinomio sea menor que  $p$

## 2.11. Los anillos $\mathbb{Z}_n$

Al trabajar con congruencias hemos visto que en cualquier cálculo los números congruentes son intercambiables. Vamos a formalizar este punto de vista. Consideramos como un ente individual a toda una clase de enteros congruentes y trabajamos con estas clases igual que con los enteros ordinarios. El motivo de introducir la notación que viene a continuación es permitirnos usar nuestra experiencia con los enteros ordinarios como una guía para trabajar con congruencias. Muchas de las propiedades de la aritmética entera se verifican también en la aritmética de congruencias. La excepción mas notable es que el producto de dos clases de congruencia no nulas puede ser cero.

**Definición 2.65.** San  $a, n \in \mathbb{Z}$  con  $n > 0$ . Llamamos *clase de congruencia de a módulo n* al conjunto de todos los enteros que son congruentes con  $a$  módulo  $n$ . La denotamos por  $a + n\mathbb{Z}$  o por  $[a]_n$ :

$$a + n\mathbb{Z} = [a]_n = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$$

El conjunto de todas las clases de congruencia módulo  $n$  se llama *conjunto de los enteros módulo  $n$*  y se representa por  $\mathbb{Z}_n$ .

Nótese que  $[a]_n = [b]_n$  si y sólo si  $a \equiv b$  (mód  $n$ ). Cuando el módulo  $n$  está claro del contexto suprimimos el índice y escribimos sólo  $[a]$ .

Una clase de congruencia puede designarse de infinitas maneras. Por ejemplo,  $[5]_3 = [8]_3 = [-1]_3 = \dots$ . A un elemento  $a$  de la clase  $[a]_n$  le llamamos *representante* de la clase. Toda clase de congruencia  $[a]_n$  tiene un único representante  $r$  tal que  $0 \leq r < n$  (a saber,  $r$  es el resto de dividir  $a$  entre  $n$ ). Esto demuestra que hay exactamente  $n$  clases de congruencias módulo  $n$  distintas. Por ejemplo, los elementos de  $\mathbb{Z}_3$  son

$$\begin{aligned}[0]_3 &= \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\} \\ [1]_3 &= \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\} \\ [2]_3 &= \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\}\end{aligned}$$

Cada entero pertenece exactamente a una clase de congruencia módulo 3, porque el resto de dividir por 3 es único. En general, cada entero pertenece a una única clase de congruencia módulo  $n$ , luego

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$$

El conjunto  $\mathbb{Z}_2$  tiene exactamente dos elementos:  $[0]_2$  es el conjunto de los enteros pares y  $[1]_2$  es el de los impares. Con esta notación las conocidas reglas “par + par = par”, “impar + par = impar”, “impar + impar = par” se expresan como  $[0]_2 + [0]_2 = [0]_2$ ,  $[1]_2 + [0]_2 = [1]_2$ ,  $[1]_2 + [1]_2 = [0]_2$ . De la misma forma, las reglas “par  $\times$  par = par”, “impar  $\times$  par = par”, “impar  $\times$  impar = impar” se expresan como  $[0]_2 \cdot [0]_2 = [0]_2$ ,  $[1]_2 \cdot [0]_2 = [0]_2$ ,  $[1]_2 \cdot [1]_2 = [1]_2$ . Estas reglas pueden resumirse dando una tabla de adición y una tabla de multiplicación para  $\mathbb{Z}_n$ :

+	0	1	·	0	1
0	0	1	0	0	0
1	1	0	1	0	1

En estas tablas hemos utilizado una simplificación habitual al tratar con congruencias: Omitimos el subíndice e incluso los corchetes y escribimos  $a$  en lugar de  $[a]_n$ .

Para  $\mathbb{Z}_n$  se introducen una suma y un producto análogos: Dados  $[a]_n, [b]_n \in \mathbb{Z}_n$  definimos

$$\begin{aligned}[a]_n + [b]_n &= [a + b]_n \\ [a]_n \cdot [b]_n &= [a \cdot b]_n\end{aligned}$$

**Proposición 2.66.** *Sea  $n$  un entero positivo y sean  $a, b, a_1, b_1 \in \mathbb{Z}$  tales que  $[a]_n = [a_1]_n$  y  $[b]_n = [b_1]_n$ . Entonces  $[a + b]_n = [a_1 + b_1]_n$  y  $[a \cdot b]_n = [a_1 \cdot b_1]_n$ .*

Esta proposición dice que la suma y multiplicación de clases de congruencia están bien definidas, es decir que son independientes de los representantes que escojamos en cada clase.

Las leyes asociativas y conmutativas de la suma y el producto, la ley distributiva y la existencia de neutros son válidas en  $\mathbb{Z}_n$ . Si  $[a]_n + [b]_n = [0]_n$ , la clase  $[b]_n$  se llama *opuesta* a la clase  $[a]_n$ . El opuesto de una clase es único. Es fácil ver que de hecho el opuesto de  $[a]_n$  es  $[-a]_n$ . Se denota por  $-[a]_n = [-a]_n$ . En general no se verifican las leyes de integridad y cancelativa.

**Definición 2.67.** Sean  $[a]_n, [b]_n \in \mathbb{Z}_n$  con  $[b]_n \neq [0]_n$  y  $[a]_n[b]_n = [0]_n$ . Entonces  $[a]_n$  se llama *divisor de cero*.

**Proposición 2.68.** *Sea  $[a]_n$  un no divisor de cero y sea  $[a]_n[b]_n = [a]_n[c]_n$ . Entonces  $[b]_n = [c]_n$ .*

**Definición 2.69.** Sean  $[a]_n, [b]_n \in \mathbb{Z}_n$  tales que  $[a]_n[b]_n = [1]_n$ . Entonces decimos que  $[a]_n, [b]_n$  son elementos *invertibles* o *unidades* de  $\mathbb{Z}_n$  y que  $[b]_n$  es un *inverso* de  $[a]_n$ . Denotamos  $[b]_n = [a]_n^{-1}$ .

Obsérvese que si  $[a]$  es invertible, no puede ser divisor de cero.

**Proposición 2.70.** *Sea  $n$  un entero positivo.*

1. *La clase  $[a]_n$  tiene un inverso multiplicativo en  $\mathbb{Z}_n$  si y sólo si  $(a, n) = 1$ .*
2. *Un elemento no nulo de  $\mathbb{Z}_n$  o es invertible o es divisor de cero.*

*Demostración.* 1. Supongamos que  $[a]$  tiene un inverso  $[a]^{-1} = [b]$ . Entonces  $[ab] = [a][b] = [1]$ , luego  $ab \equiv 1 \pmod{n}$ , lo que implica que  $ab = qn + 1$  para algún entero  $q$ . O sea que  $ab + (-q)n = 1$  y por tanto  $(a, n) = 1$ .

A la inversa sea  $(a, n) = 1$ . Entonces existen  $b, c \in \mathbb{Z}$  tales que  $ab + cn = 1$ . Reduciendo módulo  $n$  vemos que  $ab \equiv 1 \pmod{n}$  y por tanto  $[a][b] = [ab] = [1]$ .

2. Sea  $[a] \neq [0]$  lo que equivale a  $n \nmid a$ . Si  $(a, n) = 1$  entonces  $[a]$  tiene un inverso. En otro caso  $(a, n) = d > 1$ . Como  $d \mid a$  y  $d \mid n$  existen enteros  $k, b$  tales que  $n = kd$  y  $a = bd$ . Entonces  $[k] \neq [0]$  pero  $[a][k] = [ak] = [bdk] = [bn] = [0]$ , lo que muestra que  $[a]$  es un divisor de cero.

□

**Corolario 2.71.** *Para un módulo  $n > 0$  las siguientes condiciones son equivalentes:*

1. *El número  $n$  es primo.*
2.  $\mathbb{Z}_n$  no tiene divisores de cero no nulos.
3. *Todo elemento no nulo de  $\mathbb{Z}_n$  tiene un inverso multiplicativo.*

La demostración de la proposición 2.70 muestra que si  $(a, n) = 1$  entonces podemos calcular el inverso multiplicativo de  $a$  utilizando el algoritmo extendido de Euclides:

*Ejemplo 2.72.* Para hallar  $[11]^{-1} \in \mathbb{Z}_{16}$  realizamos el siguiente cálculo:

$$\begin{array}{rrr} 16 & 0 & 1 \\ 11 & 1 & 0 \\ 5 & -1 & 1 \\ 1 & 3 & -2 \\ 0 & -16 & 11 \end{array}$$

luego  $11 \cdot 3 + 16 \cdot (-2) = 1$ , lo que muestra que  $[11]^{-1} = [3]$ .

Hay otros dos métodos para hallar el inverso multiplicativo de  $[a]_n$  en  $\mathbb{Z}_n$ : Si el módulo  $n$  es pequeño, a veces es mas corto hacerlo por prueba y error. La otra forma es calculando las potencias sucesivas de  $[a]$ . Si  $(a, n) = 1$ , entonces  $[a]$  no es divisor de cero en  $\mathbb{Z}_n$  y por tanto ninguna potencia  $[a]^k$  puede ser cero. El conjunto  $\{[a], [a]^2, [a]^3, \dots\}$  tiene menos de  $n$  elementos distintos, luego en algún punto debe repetirse. Sean  $k < m$  tales que  $[a]^m = [a]^k$ . Entonces  $[a]^{m-k} = [a]^0 = [1]$ . Esto muestra que en la primera repetición debe ser  $k = 0$  y por tanto  $[a]^m = [1]$ . De aquí vemos que  $[a]^{m-1} = [1]$ .

*Ejemplo 2.73.* Volvamos a calcular  $[11]_{16}^{-1}$ . Para ello listamos las potencias sucesivas de  $[11]_{16}$ :

$$\begin{aligned} [11]^2 &= [-5]^2 = [25] = [9] \\ [11]^3 &= [11]^2[11] = [9][11] = [99] = [3] \\ [11]^4 &= [11]^3[11] = [3][11] = [33] = [1] \end{aligned}$$

luego  $[11]^{-1} = [11]^3 = [3]$ .

Podemos ahora estudiar ecuaciones en  $\mathbb{Z}_n$ . La congruencia lineal  $ax \equiv b$  (mód  $n$ ) puede verse ahora como una ecuación lineal  $[a]_n[x]_n = [b]_n$  en  $\mathbb{Z}_n$ . Si  $[a]_n$  tiene inverso, esta ecuación tiene solución única  $[x] = [a]_n^{-1}[b]_n$ . Nótese que sin la noción de clase de congruencia tenemos que modificar la afirmación de unicidad para decir que si  $x_0$  es una solución de  $ax \equiv b$  (mód  $n$ ), también lo es  $x_0 + qn$  para cualquier entero  $q$ .

Vamos a ver finalmente dos teoremas que permiten rebajar el grado de las ecuaciones polinómicas en  $\mathbb{Z}_n$ .

**Definición 2.74.** Sea  $n$  un entero positivo. El número de enteros positivos menores o iguales que  $n$  y que son primos relativos con  $n$  se denota  $\varphi(n)$ . Esta función se llama *función  $\varphi$  de Euler* o *función tociente*.

Nótese que  $\varphi(1) = 1$ . Para  $n > 1$  el valor de  $\varphi(n)$  puede obtenerse de la factorización en primos:

**Lema 2.75.** *Sea  $n = p^e$ . Entonces  $\varphi(n) = p^e - p^{e-1} = n(1 - 1/p)$*

*Demostración.* Un entero  $m$  es primo relativo con  $p^e$  si y sólo si es primo con  $p$ . Como  $p$  es primo, esto quiere decir que  $m$  no es primo relativo con  $p^e$  si y sólo si es un múltiplo de  $p$ . El número de todos los enteros entre 1 y  $p^e$  es  $p^e$ . El número de múltiplos de  $p$  entre 1 y  $p^e$  es  $p^{e-1}$ . Restando obtenemos el resultado del lema.  $\square$

**Lema 2.76.** *Sean  $m, n$  enteros positivos primos relativos. Entonces  $\varphi(mn) = \varphi(m)\varphi(n)$ .*

*Demostración.* Definimos una aplicación  $f : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$  (el producto cartesiano mediante  $f([a]_{mn}) = ([a]_m, [a]_n)$ ). Por el teorema chino de los restos,  $f$  es una biyección. Es fácil comprobar que  $f[a]_{mn}[b]_{mn} = f([a]_{mn})f([b]_{mn})$ . En particular  $[a]_{mn}$  será invertible si y sólo si lo son ambas  $[a]_m$  y  $[a]_n$ . Pero para cualquier  $k$  la clase  $[a]_k$  es invertible si y sólo si  $(a, k) = 1$ . Así que por restricción,  $f$  establece una biyección entre los enteros positivos menores o iguales que  $mn$  primos relativos con  $mn$  con el conjunto de pares de enteros positivos donde la primera componente sea menor o igual que  $m$  y primo relativo con  $m$  y la segunda sea menor o igual que  $n$  y primo relativo con  $n$ . Contando estos pares obtenemos el resultado buscado.  $\square$

**Proposición 2.77.** *Sea  $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$  la factorización en primos de  $n$ . Entonces*

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

*Demostración.* Consecuencia inmediata de los dos lemas anteriores:

$$\varphi(n) = \varphi(p_1^{e_1}) \dots \varphi(p_k^{e_k})$$

por el lema 2.76 y aplicando a cada factor el lema 2.75 obtenemos el resultado final.  $\square$

*Ejemplo 2.78.* Las fórmulas de la proposición anterior nos dicen que

$$\varphi(10) = 10 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 4$$

y que

$$\varphi(36) = 36 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 12$$

**Definición 2.79.** El conjunto de unidades de  $\mathbb{Z}_n$ , es decir el conjunto de clases  $[a]_n$  con  $(a, n) = 1$  se denota por  $\mathbb{Z}_n^\times$ .

**Proposición 2.80.** *El conjunto  $\mathbb{Z}_n^\times$  es cerrado para la multiplicación.*

*Demostración.* Es inmediato comprobar que  $([a][b])^{-1} = [b]^{-1}[a]^{-1}$ .  $\square$

El conjunto  $\mathbb{Z}_n^\times$  tiene  $\varphi(n)$  elementos. El siguiente teorema debe verse como un resultado sobre potencias de elementos de  $\mathbb{Z}_n^\times$ :

**Teorema 2.81** (Euler). *Sea  $(a, n) = 1$ . Entonces  $a^{\varphi(n)} \equiv 1$  (mód  $n$ ).*

*Demostración.* En el conjunto  $\mathbb{Z}_n$  existen  $\varphi(n)$  elementos que tienen un representante primo relativo a  $n$ . Sean estos  $\{a_1, \dots, a_{\varphi(n)}\}$ . Las clases representadas por  $\{aa_1, \dots, aa_{\varphi(n)}\}$  son todas distintas porque  $(a, n) = 1$ . Como cada producto  $aa_i$  es primo relativo con  $n$ , tenemos un representante de cada una de las clases de partida. Por tanto

$$a_1a_2 \dots a_{\varphi(n)} \equiv (aa_1)(aa_2) \dots (aa_{\varphi(n)}) \equiv a^{\varphi(n)}a_1a_2 \dots a_{\varphi(n)} \pmod{n}$$

Ya que el producto  $a_1a_2 \dots a_{\varphi(n)}$  es primo relativo con  $n$  podemos simplificarlo y nos queda la congruencia

$$1 \equiv a^{\varphi(n)}$$

$\square$

**Corolario 2.82** (Teorema de Fermat). *Sea  $p$  un primo. Entonces  $a^p \equiv a$  para todo entero  $a$ .*

*Demostración.* Si  $p \mid a$ , entonces  $a^p \equiv 0 \equiv a$  (mód  $p$ ). Si  $p \nmid a$  entonces  $(a, p) = 1$  y el teorema de Euler nos dice que  $a^{\varphi(p)} \equiv 1$  (mód  $p$ ). Pero  $\varphi(p) = p - 1$ . Multiplicando ambos miembros por  $a$  tenemos el resultado buscado.  $\square$

El teorema de Fermat proporciona un *criterio de número compuesto*: Sea  $n$  un número del que queremos averiguar si es primo o compuesto. Tomamos un  $a$  primo relativo con  $n$  (por ejemplo,  $a = 2$ ) y calculamos  $b \equiv a^{n-1}$  (mód  $n$ ). Si  $b \neq 1$ , el número  $n$  es compuesto. Pero si  $b = 1$  no sabemos si el número  $n$  es primo o compuesto. Naturalmente podemos probar con otra base  $a$  distinta, pero aunque para varios  $a$  se verifique que  $a^{n-1} \equiv 1$  (mód  $n$ ), no podemos concluir que  $n$  sea primo. De hecho existen números  $n$  tales que  $a^{n-1} \equiv 1$  (mód  $n$ ) para todo  $a$  primo relativo con  $n$ . Tales números se llaman *números de Carmichael*, hay 2163 entre 1 y  $25 \cdot 10^9$  y el mas pequeño es  $561 = 3 \cdot 11 \cdot 17$ .

El criterio anterior se puede afinar (véase cualquier libro sobre teoría de números), pero aún los criterios mejorados no son concluyentes (existen números compuestos que los pasan). Para finalizar vamos a ver un *criterio de primalidad* de interés teórico, aunque poco práctico.

**Lema 2.83.** *Sea  $p$  un primo. Entonces  $a^2 \equiv 1 \pmod{p}$  si y sólo si  $a \equiv 1 \pmod{p}$  o  $a \equiv -1 \pmod{p}$*

*Demostración.* La hipótesis es que  $p \mid (a^2 - 1) = (a - 1)(a + 1)$ . Por ser  $p$  primo tiene que dividir a uno de los factores.  $\square$

En términos de clases de restos este lema dice que  $[a]_p^{-1} = [a]_p$  si y sólo si  $[a]_p = \pm[1]$ .

**Teorema 2.84** (Teorema de Wilson). *Un entero positivo  $p$  es primo si y sólo si  $(p - 1)! \equiv -1 \pmod{p}$*

*Demostración.* Supongamos que  $(p - 1)! \equiv -1 \pmod{p}$ . Entonces existe un entero  $q$  tal que  $qp - (p - 1)! = 1$ , así que m. c. d.( $p, (p - 1)!$ ) = 1 y  $p$  no es divisible por ningún entero menor que  $p$  y mayor que 1 (todos ellos dividen a  $(p - 1)!$ ). Luego  $p$  es primo.

A la inversa sea  $p$  primo distinto de 2 (el caso  $p = 2$  se comprueba fácilmente). Multiplicamos todas las clases  $[1]_p \cdot [2]_p \cdots [p - 1]_p$ . Por el lema 2.83, para cada clase  $[a]_p$  en este producto, salvo la primera y la última, también  $[a]_p^{-1}$  está en el producto. Y el producto vale  $[a]_p[a]_p^{-1} = 1$ . Luego  $[(p - 1)!]_p = [p - 1]_p = [-1]_p$ . Pero este es el resultado buscado.  $\square$

## Referencias

- [1] J. A. Beachy and W. D. Blair, *Abstract Algebra*, Waveland Press 1996
- [2] P. M. Cohn, *Algebra I*, Wiley and sons 1977
- [3] D. S. Dummit and R. M. Foote, *Abstract Algebra*, Prentice-Hall 1991
- [4] O. Ore, *Number Theory and its History*, Academic Press