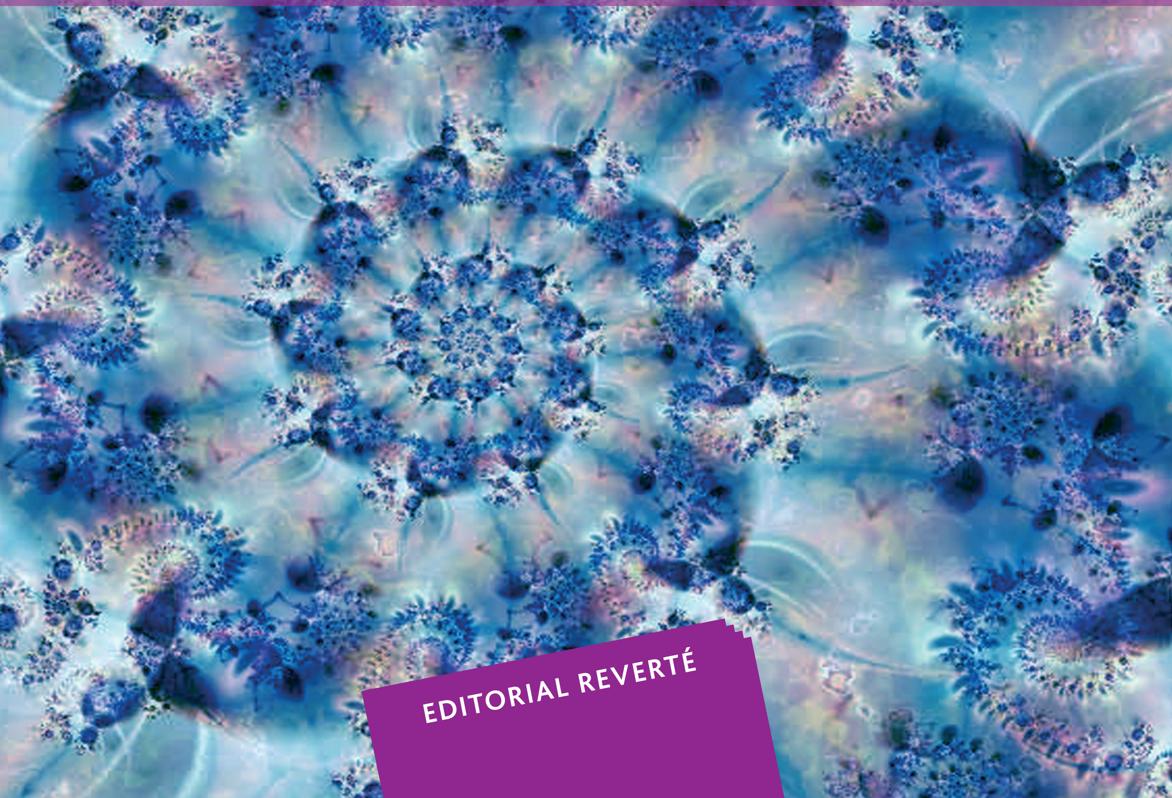
Álgebra Lineal y Geometría

Manuel Castellet \ Irene Llerena



EDITORIAL REVERTÉ

Álgebra lineal y Geometría

Manuel Castellet
Catedrático de la Universidad Autónoma de Barcelona

Irene Llerena
Profesora Titular de la Universidad de Barcelona

Con la colaboración de

Carlos Casacuberta
Profesor Titular de la Universidad de Barcelona

EDITORIAL
REVERTÉ

Barcelona · Bogotá · Buenos Aires · México

Titulo de la obra original:
Àlgebra Lineal i Geometria

Edición en lengua catalana publicada por:
Publicacions de la Universitat Autònoma de Barcelona

Revisado por los autores

Edición en papel
© Editorial Reverté, S. A., 2000
ISBN: 978-84-291-5009-4

Edición e-book (PDF)
© Editorial Reverté, S. A., 2020
ISBN: 978-84-291-9285-8

Propiedad de:
EDITORIAL REVERTE, S.A.
Loreto 13-15 Local B
08029 Barcelona, España
Tel.: 93 419 33 36
reverte@reverte.com
www.reverte.com

A Albert, Josep y Marc

Et surtout leurs adeptes y trouvent des jouissances analogues à celles que donnent la peinture et la musique. Ils admirent la délicate harmonie des nombres et des formes; ils s'émerveillent quand une découverte nouvelle leur ouvre une perspective inattendue; et la joie qu'ils éprouvent ainsi n'a-t-elle pas le caractère esthétique, bien que les sens n'y prennent aucune part?...

C'est pourquoi je n'hésite pas à dire que les mathématiques méritent d'être cultivées pour elles-mêmes et que les théories qui ne peuvent être appliquées à la physique doivent l'être comme les autres.

...Mais, le mathématicien pur qui oublierait l'existence du monde extérieur serait semblable à un peintre qui saurait harmonieusement combiner les couleurs et les formes, mais à qui les modèles, feraient défaut. Sa puissance créatrice serait bientôt tarie.

Henri Poincaré

Índice

XIII Espacios afines euclídeos

Introducción

La imagen de un gran roble que tiene por raíces el álgebra, la geometría plana, la trigonometría, la geometría analítica y los números irracionales, por tronco el análisis, y diversas ramas, ya no es aceptada actualmente. Hoy en día, a finales del siglo 20, la imagen adecuada para representar las matemáticas es, tal como dice H. Eves, la de un baniano, un árbol con varios troncos, que desarrolla siempre troncos nuevos: cada rama del baniano, por un crecimiento fibroso, se extiende hacia abajo hasta llegar al suelo. Entonces arraiga y con el tiempo ese filamento se va volviendo grueso y fuerte hasta convertirse en un nuevo tronco con muchas ramas, cada una de las cuales lanza sus filamentos hacia el suelo.

Al igual que el gran roble, esos banianos son hermosos y tienen una larga vida. Se dice que el baniano de la India bajo el cual meditaba Buda todavía vive y sigue creciendo.

Se puede ascender al árbol por diferentes troncos, empezando por los fundamentos, que representan las raíces del tronco elegido. Todos los troncos están, evidentemente, interconectados por el complicado sistema de ramaje del árbol.

Nosotros hemos escogido tres troncos del baniano: la aritmética, el álgebra lineal y la geometría. De cada uno de estos troncos hemos presentado algunas raíces que han de permitir al estudiante ir subiendo por el árbol y, junto con los conocimientos adquiridos en otros troncos (análisis, álgebra, topología, etc.), poder moverse seguro por una parcela del gran baniano.

El presente texto es el fruto de la experiencia de varios años de los autores impartiendo las asignaturas "Geometría I" en la Universidad de Barcelona y "Álgebra I" en la Universidad Autónoma de Barcelona, y está fuertemente influenciado por el constante intercambio de ideas con Josep Vaquer.

El libro se puede dividir en tres partes: Aritmética y Álgebra (capítulos 1, 2 y 3), Álgebra lineal (capítulos 4, 5, 6, 7, 8, 11 y 12) y Geometría (capítulos 9, 10 y 13). Aunque cada parte tiene interés propio, todas ellas están íntimamente relacionadas dando unidad al texto. Si $A \to B$ significa que para estudiar el capítulo B se necesita una parte esencial del A, los capítulos del texto pueden ordenarse así:

$$
\begin{tikzcd}
 & & 3 \arrow[d] & 1 \arrow[r] & 2 \arrow[d] & & & \textit{Aritmética y Álgebra} \\
4 \arrow[r] & 5 \arrow[r] & 6 \arrow[r] & 7 \arrow[r] \arrow[d] & 8 \arrow[r] \arrow[d] & 11 \arrow[r] & 12 \arrow[d] & \textit{Álgebra lineal} \\
 & & & 9 \arrow[r] & 10 \arrow[rr] & & 13 & \textit{Geometría}
\end{tikzcd}
$$

Hemos procurado que el lenguaje sea llano y que el texto pueda servir tanto al profesor como al alumno que lo lea por su cuenta. Al final de cada capítulo hemos incluido una breve nota histórica, que solamente pretende ser lo que su nombre indica.

Junto con una lista cuidadosamente elaborada de ejercicios clásicos, hemos incluido en cada capítulo una serie de ejercicios para programar. Para la resolución de esos ejercicios, suponemos que el estudiante es capaz de programar en algún lenguaje y pretendemos que con ellos profundice en la teoría y al mismo tiempo trabaje personalmente métodos de cálculo.

El libro está especialmente pensado para estudiantes de primer curso de las Facultades de Matemáticas, Física e Informática y de las Escuelas de Ingeniería y Arquitectura. Una selección de los capítulos puede ser adecuada también para los restantes estudios científicos, técnicos y socioeconómicos.

La colaboración de Carles Casacuberta ha sido decisiva para la confección de este libro. La lectura atenta que ha hecho del texto, sus sugerencias y la elaboración de la mayoría de los ejercicios para programar han significado una contribución inestimable que agradecemos de todo corazón.

La realización material del libro se ha visto facilitada por la aportación de Jordi Saludes, quien, gracias a su dominio del programa de edición TEX, ha hecho posible que el texto tenga este aspecto tan agradable.

M. CASTELLET – I. LLERENA

Capítulo I

Divisibilidad en los números enteros

I.1 División entera. Ideales

Designaremos por $\mathbf{Z}$ el conjunto de los números enteros. La teoría de la divisibilidad en $\mathbf{Z}$ es consecuencia de la siguiente importante propiedad.

Teorema 1.1 (de la división entera) *Dados $a, b \in \mathbf{Z}$, $b \neq 0$, existen dos únicos números enteros q y r que cumplen $a = bq + r$, $0 \leq r < |b|$. Estos números q y r se llaman el* cociente *y el* resto *de la división entera de a por b.*

Ejemplo:

$$-8 = 3 \cdot (-3) + 1, \qquad 3 = (-8) \cdot 0 + 3.$$

Si el resto de la división entera de a por b es 0, se dice que a es un *múltiplo* de b (escribiremos $a = \dot{b}$), que b es un *divisor* de a (escribiremos $b \mid a$), o que *a es divisible por b*. Indicaremos por (b) el conjunto de los múltiplos de b. Observemos que (b) cumple las dos propiedades siguientes:

- es cerrado por la suma; es decir, $a, c \in (b) \Rightarrow a + c \in (b)$;
- si $a \in (b)$ y c es cualquier entero, entonces $ac \in (b)$.

Proposición 1.2 *Si el subconjunto $I \subset \mathbf{Z}$ cumple*

1. $a, b \in I \Rightarrow a + b \in I$,
2. $a \in I$, $c \in \mathbf{Z} \Rightarrow ac \in I$,

entonces existe un $b \in I$ tal que $I = (b)$.

DEMOSTRACIÓN: Si $I = \{0\}$, entonces $I = (0)$. Si I contiene un elemento no nulo a, también contiene $-a = a \cdot (-1)$, y o bien a o bien $-a$ es positivo. Por tanto, I contiene enteros positivos. Sea b el menor de los positivos contenidos en I. Por 2, I contiene todos los múltiplos de b: $(b) \subset I$. Vamos a ver que $I \subset (b)$ y, por tanto, $I = (b)$. En efecto, dado $a \in I$ cualquiera, por (1.1),

$$a = bq + r.$$

Por 1 y 2, $r = a - bq = a + b(-q) \in I$; pero $0 \leq r < |b| = b$, y b es el menor de los positivos de I; así pues, $r = 0$ y, por tanto, $a = bq \in (b)$. □

Un subconjunto I que cumple las condiciones 1 y 2 de (1.2) se llama un *ideal* de $\mathbf{Z}$. El elemento b tal que $I = (b)$ se denomina *base* del ideal.

Ejercicio:

$(b) = (c)$ si y sólo si $c = \pm b$.

Observación:

$(a) \subset (b)$ si y sólo si $b \mid a$. Las cuestiones de divisibilidad equivalen, por tanto, a cuestiones sobre inclusiones entre ideales.

I.2 Mínimo común múltiplo y máximo común divisor

Dados números enteros $a_1, \ldots, a_n$, la intersección $(a_1) \cap \ldots \cap (a_n)$ es el conjunto de los números enteros múltiplos comunes de todos ellos. Este conjunto cumple las dos condiciones de (1.2) y, por tanto, $(a_1) \cap \ldots \cap (a_n) = (m)$ para un m conveniente. Este m está caracterizado por las dos propiedades siguientes:

- m es múltiplo común de $a_1, \ldots, a_n$;
- cualquier otro múltiplo común de $a_1, \ldots, a_n$ es múltiplo de m.

Diremos que m es el *mínimo común múltiplo* de $a_1, \ldots, a_n$ y escribiremos

$$m = \text{m.c.m.}(a_1, \ldots, a_n).$$

¡Atención!:

Observemos que también $-m$ es mínimo común múltiplo de $a_1, \ldots, a_n$.

Consideremos ahora la unión $(a_1) \cup \ldots \cup (a_n)$. Este conjunto, en general, no cumple las condiciones de (1.2). Por ejemplo, $(2) \cup (3)$ no contiene el $5 = 2 + 3$. Formemos a partir de $(a_1) \cup \ldots \cup (a_n)$ un subconjunto I de $\mathbf{Z}$ que cumpla las condiciones de (1.2). Por la condición 1, I debe contener todas las sumas de múltiplos de $a_1, \ldots, a_n$: $a_1c_1 + \ldots + a_nc_n$. No hace falta ampliar más; el conjunto

$$I = \{a_1c_1 + \ldots + a_nc_n \mid c_1, \ldots, c_n \in \mathbf{Z}\}$$

cumple ya las condiciones de (1.2) y, por tanto, existe un entero d tal que $I = (d)$. Denotaremos I por $(a_1, \ldots, a_n)$. Así pues, $I = (a_1, \ldots, a_n) = (d)$. Este número d está caracterizado por las dos propiedades siguientes:

- d es divisor común de $a_1, \ldots, a_n$, ya que ello equivale a afirmar que $a_i \in (d)$ para $i = 1, \ldots, n$. $(a_i = a_1 \cdot 0 + \ldots + a_i \cdot 1 + \ldots + a_n \cdot 0 \in I)$.
- Cualquier otro divisor d' común a $a_1, \ldots, a_n$ divide a d. En efecto, que d' sea divisor de $a_1, \ldots, a_n$ significa que $a_i \in (d')$, $i = 1, \ldots, n$. Por tanto, $\{a_1c_1 + \ldots + a_nc_n \mid c_i \in \mathbf{Z}\} \subset (d')$, es decir, $(d) \subset (d')$, lo cual implica que d' es un divisor de d.

Diremos que d es el *máximo común divisor* de $a_1, \ldots, a_n$ y escribiremos

$$d = \text{m.c.d.}(a_1, \ldots, a_n).$$

¡Atención!:

También $-d$ es máximo común divisor de $a_1, \ldots, a_n$.

Observemos que el máximo común divisor d es una suma de múltiplos de $a_1, \ldots, a_n$,

$$d = a_1r_1 + \ldots + a_nr_n.$$

Esta expresión es conocida como *identidad de Bézout.*

Acabaremos este apartado con un método práctico de cálculo del máximo común divisor y de la identidad de Bézout. El método se basa en el siguiente resultado:

Proposición 2.1 *Sea $a = bq + r$ la división entera de a por b. Entonces*

$$\text{m.c.d.}(a, b) = \text{m.c.d.}(b, r).$$

DEMOSTRACIÓN: El resultado es consecuencia de que $(a, b) = (b, r)$. En efecto, todo elemento $ac_1 + bc_2 \in (a, b)$ satisface $ac_1 + bc_2 = b(qc_1 + c_2) + rc_1 \in (b, r)$ y, recíprocamente, todo elemento $bn_1 + rn_2 \in (b, r)$ satisface $bn_1 + rn_2 = an_2 + b(n_1 - qn_2) \in (a, b)$. □

Si aplicamos reiteradamente esta proposición, obtenemos

$$\begin{array}{lll} a = bq + r, & (a,b) = (b,r), & r < |b|, \\ b = rq_1 + r_1, & (b,r) = (r,r_1), & r_1 < r, \\ r = r_1q_2 + r_2, & (r,r_1) = (r_1,r_2), & r_2 < r_1. \end{array}$$

Los sucesivos restos van disminuyendo y obtendremos, por tanto, en un momento dado resto cero:

$$\begin{array}{lll} r_{k-2} = r_{k-1}q_k + r_k, & (r_{k-2}, r_{k-1}) = (r_{k-1}, r_k), & r_k < r_{k-1}, \\ r_{k-1} = r_k q_{k+1} + 0, & (r_{k-1}, r_k) = (r_k, 0) = (r_k). & \end{array}$$

Así pues, $(a, b) = (r_k)$; es decir, $r_k = \text{m.c.d.}(a, b)$.

Este método para hallar el máximo común divisor se llama *algoritmo de Euclides.*

Para calcular el máximo común divisor de más de dos enteros, aplicamos:

Ejercicio:

$$\text{m.c.d.}(a_1, a_2, a_3) = \text{m.c.d.}[\text{m.c.d.}(a_1, a_2), a_3] \text{ y, en general,}$$
$$\text{m.c.d.}(a_1, \ldots, a_n) = \text{m.c.d.}[\text{m.c.d.}(a_1, \ldots, a_{n-1}), a_n].$$

Las divisiones enteras efectuadas en el algoritmo de Euclides nos permiten expresar $d = r_k = \text{m.c.d.}(a, b)$ como suma de un múltiplo de a y un múltiplo de b. En efecto, en

$$d = r_k = r_{k-2} - r_{k-1}q_k$$

d se expresa como suma de un múltiplo de r_{k-2} y un múltiplo de r_{k-1}. Ahora bien, $r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}$, y sustituyendo en la igualdad anterior obtenemos una expresión de d como suma de un múltiplo de r_{k-3} y un múltiplo de r_{k-2}. Volviendo a sustituir convenientemente, podemos expresar d como suma de múltiplos de r_{k-4} y r_{k-3}; y así sucesivamente hasta obtener la identidad de Bézout

$$d = ar + bs.$$

En el próximo apartado (3.2) demostraremos que si $m = \text{m.c.m.}(a, b)$ y $d = \text{m.c.d.}(a, b)$, entonces $md = \pm ab$. Esto nos permite calcular m si conocemos d. Para el cálculo del mínimo común múltiplo de más de dos números utilizamos:

Ejercicio:

m.c.m.$(a_1, a_2, a_3) =$ m.c.m.[m.c.m.$(a_1, a_2), a_3]$ y, en general,
m.c.m.$(a_1, \ldots, a_n) =$ m.c.m.[m.c.m.$(a_1, \ldots, a_{n-1}), a_n]$.

I.3 Números primos entre sí y números primos

Se dice que a y b son *primos entre sí* si m.c.d.$(a, b) = 1$.

Ejemplos:

1. m.c.d.$(3, 8) = 1$. Observemos que $1 = 3 \cdot 3 + 8 \cdot (-1)$.
2. Si $d =$ m.c.d.(a, b) y $a = da'$, $b = db'$, entonces m.c.d.$(a', b') = 1$. En efecto, si d' fuera un divisor común de a' y b', entonces dd' sería divisor común de a y b y, por tanto, un divisor de d. Esto sólo es posible si $d' = \pm 1$.

Teorema 3.1 (de Euclides) *Si $a \mid bc$ y* m.c.d.$(a, b) = 1$, *entonces $a \mid c$.*

DEMOSTRACIÓN: Si $1 =$ m.c.d.(a, b), podemos expresar el 1 como $1 = ar + bs$. Multiplicando por c obtenemos $c = acr + bcs$. Pero a divide a los dos sumandos y, por tanto, $a \mid c$. □

Proposición 3.2 *Si $m =$* m.c.m.(a, b) *y $d =$* m.c.d.(a, b), *entonces se cumple $md = \pm ab$.*

DEMOSTRACIÓN: Pongamos $a = da'$ y $b = db'$. Se trata de ver que $m = \pm da'b'$ es un mínimo común múltiplo de a y b. Es evidente que $da'b'$ es múltiplo común de a y b. Sea n otro múltiplo común de a y b; es decir, $n = ar = bs$. Entonces $a'dr = b'ds$, de donde $a'r = b's$ con a', b' primos entre sí. Entonces, por (3.1), a' divide a s, es decir, $s = a'h$ y $n = bs = db'a'h$. Así resulta que n es múltiplo de $db'a'$. □

Cualquier número entero p es divisible por ± 1 y por $\pm p$. Diremos que p es *primo* si estos son sus únicos divisores. El 1 y el -1 no se consideran números primos.

Proposición 3.3 *El conjunto de los números primos es infinito.*

DEMOSTRACIÓN: Lo demostraremos viendo que, dado un conjunto finito de números primos $N = \{p_1, \ldots, p_m\}$, siempre hay un número primo fuera de N. En efecto, consideremos $a = p_1 \cdots p_m + 1$. Si $b \mid a$, también $-b \mid a$; por tanto, a tiene siempre divisores positivos. Sea p el menor de los divisores positivos de a diferentes de 1. Claramente, p es primo. Si p fuera uno de los p_i, dividiría a $p_1 \cdots p_m$ y, por tanto, dividiría a $a - p_1 \cdots p_m = 1$. Esto es imposible, ya que $p \neq 1$. De ahí que $p \notin N$. □

Proposición 3.4 *Todo número entero a no nulo, $a \neq \pm 1$, es producto de números primos.*

DEMOSTRACIÓN: Tal como hemos visto en la demostración de (3.3), a tiene sempre un divisor primo $p_1 \neq \pm 1$. Así pues, tenemos $a = p_1 a_1$. Si $a_1 \neq \pm 1$, elijamos un divisor primo de a_1, $p_2 \neq \pm 1$, y tendremos $a_1 = p_2 a_2$. Luego $a = p_1 p_2 a_2$. Repitamos el mismo proceso si $a_2 \neq \pm 1$, y así sucesivamente. Ahora bien, $|a| > |a_1| > |a_2| > \ldots$. Llegará pues un momento en que tendremos $a = p_1 \cdots (p_n a_n)$ con $a_n = \pm 1$. Esto es una descomposición de a en números primos. □

La descomposición de un entero en producto de primos no es exactamente única. Por ejemplo,

$$12 = 2 \cdot 2 \cdot 3 = 2 \cdot (-2) \cdot (-3) = (-2) \cdot 3 \cdot (-2).$$

Hay, sin embargo, una cierta unicidad. Concretamente,

Proposición 3.5 *Si $p_1 \cdots p_n = q_1 \cdots q_m$ y todos los factores p_i, q_j son números primos, $i = 1, \ldots, n$, $j = 1, \ldots, m$, entonces $n = m$ y los números $\{p_1, \ldots, p_n\}$ son los mismos que los $\{q_1, \ldots, q_m\}$, salvo el signo (y el orden).*

DEMOSTRACIÓN: Observemos que si p, q son números primos, entonces o bien m.c.d.$(p, q) = 1$ o bien $p = \pm q$. Pero p_1 divide a $p_1 \cdots p_n = q_1(q_2 \cdots q_m)$. Por el teorema de Euclides (3.1), o bien $p_1 \mid q_2 \cdots q_m$, cuando m.c.d.$(p_1, q_1) = 1$, o bien $p_1 = \pm q_1$. En el primer caso, $p_1 \mid q_2(q_3 \cdots q_m)$; aplicando nuevamente el teorema de Euclides, obtenemos que $p_1 \mid q_3 \cdots q_m$, o $p_1 = \pm q_2$. Repitamos el proceso tantas veces como sea necesario. O bien hallaremos que p_1 es uno de los $q_j, j = 1, \ldots, m-2$, salvo el signo, o bien concluiremos que $p_1 \mid q_{m-1} q_m$, de donde $p_1 = \pm q_{m-1}$ o $p_1 = \pm q_m$.

Así pues, p_1 coincide, salvo el signo, con uno de los q_j. Cambiando el orden si es necesario, podemos suponer que $p_1 = \pm q_1$. Entonces $p_2 \cdots p_n = (\pm q_2) q_3 \cdots q_m$. El mismo razonamiento prueba que p_2 es igual, salvo el signo, a uno de los q_j, $j = 2, \ldots, m$, y así sucesivamente. Si $n < m$, llegaremos a la situación $1 = \pm q_{n+1} \cdots q_m$, y esto no es posible porque todos los q_j son diferentes de ± 1. Si $m > n$, llegaremos a $\pm p_{m+1} \cdots p_n = 1$, igualmente imposible. Por tanto, $n = m$. □

I.4 Congruencias

Fijemos $0 \neq m \in \mathbf{Z}$. Diremos que dos números enteros a y b son *congruentes módulo* m si $a - b \in (m)$. Esto equivale a decir que las divisiones enteras de a y b por m tienen el mismo resto. En efecto,

$$\left.\begin{array}{l} a = mq + r \\ b = mq_1 + r_1 \end{array}\right\} \Rightarrow a - b = m(q - q_1) + (r - r_1) \;\; \text{con} \;\; |r - r_1| < |m|.$$

Por tanto, $a - b \in (m)$ si y sólo si $r = r_1$. Si a y b son congruentes módulo m, escribiremos $a \equiv b\,(m)$.

Es muy fácil ver que se cumplen las siguientes condiciones:

1. Para todo $a \in \mathbf{Z}$, $a \equiv a\,(m)$.
2. $a \equiv b\,(m) \Rightarrow b \equiv a\,(m)$.
3. $a \equiv b\,(m)$, $b \equiv c\,(m) \Rightarrow a \equiv c\,(m)$.

Formemos ahora subconjuntos de $\mathbf{Z}$ de la siguiente manera: cada subconjunto está formado por todos los números enteros que dan el mismo resto al efectuar la división entera por m. Obtenemos m subconjuntos:

- $(m) =$ conjunto de enteros que dan resto 0,
- $\{\dot{m} + 1\} =$ conjunto de enteros que dan resto 1,
- ....
- $\{\dot{m} + (|m| - 1)\} =$ conjunto de enteros que dan resto $|m| - 1$.

Estos conjuntos se llaman *clases de restos módulo m*. Designaremos por $\mathbf{Z}/(m)$ el conjunto de las clases de restos módulo m. Cada entero está en una de estas clases y sólo en una. Una clase queda, por tanto, bien determinada al dar uno cualquiera de sus elementos. Diremos que ese elemento es un *representante* de la clase.

Nota:

El proceso que acabamos de llevar a cabo es un caso particular de un proceso general muy usual en matemáticas. Se trata de lo siguiente: sea A un conjunto; una *relación* en A es un criterio que nos permite decidir si dos elementos cualesquiera de A, a y b, "satisfacen la relación" o no. Más exactamente: dar una relación en A es dar una colección de pares ordenados de elementos de A (que serán los elementos que "satisfacen la relación"); es decir, dar un subconjunto del producto cartesiano $A \times A$. Indicaremos por $a \sim b$ el hecho de que a esté relacionado con b. Ejemplos de relaciones son

- $a \sim b \Leftrightarrow a \mid b$.
- $a \sim b \Leftrightarrow a < b$.
- $a \sim b \Leftrightarrow a - b \in (m)$.

Una relación es *relación de equivalencia* si cumple

- Propiedad reflexiva: para todo $a \in A$, $a \sim a$.
- Propiedad simétrica: $a \sim b \Rightarrow b \sim a$.
- Propiedad transitiva: $a \sim b$, $b \sim c \Rightarrow a \sim c$.

De los ejemplos anteriores, sólo la congruencia módulo m es una relación de equivalencia. Toda relación de equivalencia nos permite dividir el conjunto A en subconjuntos disjuntos (*clases de equivalencia*) de la siguiente manera: cada clase está formada por todos los elementos relacionados entre sí. Las tres propiedades anteriores aseguran que todo elemento está en una y sólo en una clase. En efecto, designemos por $[a]$ la clase de todos los elementos relacionados con a. Claramente, $a \in [a]$. Supongamos que a está también en otra clase: $a \in [c]$. Entonces $a \sim c$ y las propiedades transitiva y simétrica nos dicen que todo elemento relacionado con a está también relacionado con c y viceversa. Es decir, $[a] = [c]$.

Una *partición* de A es una serie de subconjuntos de A tales que todo $a \in A$ está en uno y sólo en uno de esos subconjuntos. Una *clasificación* de los elementos de A no es otra cosa que una partición de A. Por ejemplo, clasificamos $\mathbf{Z}$ en pares e impares, o clasificamos las personas por su nacionalidad. Las clases de equivalencia forman una partición de A. Recíprocamente, una partición de A determina una relación de equivalencia: $a, b \in A$ son "equivalentes" si están en el mismo subconjunto de la partición. Por tanto, clasificar es lo mismo que formar clases por una relación de equivalencia. Esta relación viene a ser el criterio según el cual clasificamos. Por ejemplo, si queremos clasificar los números enteros, tendremos que fijar con qué criterio lo hacemos. Si lo hacemos según su paridad, situaremos dos enteros en la misma clase si ambos son pares o ambos son impares. Lo que hemos hecho no es sino dar una relación de equivalencia.

El conjunto de las clases de equivalencia se llama *conjunto cociente* y se denota por $A/\!\sim$.

I.5 Los anillos $\mathbf{Z}/(m)$

Queremos ahora definir unas operaciones en $\mathbf{Z}/(m)$ que desempeñen el papel de la suma y el producto en $\mathbf{Z}$. La manera más natural de hacerlo es definir

$$[a] + [b] = [a + b], \qquad [a] \cdot [b] = [ab].$$

Sin embargo, hay un problema. Consideremos unos representantes distintos de las clases $[a]$ y $[b]$: sean $[a_1] = [a], [b_1] = [b]$. Las mismas definiciones dan $[a_1] + [b_1] = [a_1 + b_1]$, $[a_1] \cdot [b_1] = [a_1 b_1]$. Las clases $[a_1 + b_1]$, $[a_1 b_1]$ que ahora obtenemos, ¿coinciden con las clases $[a + b]$, $[ab]$ antes obtenidas? En otras palabras, la suma y el producto definidos, ¿dependen de los representantes elegidos? La respuesta es no; en efecto,

$$\left.\begin{array}{l} [a_1] = [a] \Rightarrow a_1 = a + \dot{m} \\ [b_1] = [b] \Rightarrow b_1 = b + \dot{m} \end{array}\right\} \Rightarrow \left\{\begin{array}{l} a_1 + b_1 = a + b + \dot{m} \Rightarrow [a_1 + b_1] = [a + b] \\ a_1 b_1 = ab + \dot{m} \Rightarrow [a_1 b_1] = [ab]. \end{array}\right.$$

Un conjunto A con dos operaciones ($a + b$, $a \cdot b$) es un *anillo* si cumple:

- Propiedades de $+$:
  - Asociativa: $(a + b) + c = a + (b + c) \quad \forall a, b, c \in A$.
  - Conmutativa: $a + b = b + a \quad \forall a, b \in A$.
  - Existe un elemento, que denominaremos *cero* y designaremos por 0, tal que
  $$a + 0 = 0 + a = a \quad \forall a \in A.$$
  - Para cada $a \in A$ hay un elemento, que denominaremos el *opuesto* de a y denotaremos por $-a$, tal que $a + (-a) = 0$.
- Propiedad de $\cdot$:
  - Asociativa: $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in A$.
- Propiedades que relacionan $+$ y $\cdot$:
  - Distributivas:
  $$a \cdot (b + c) = a \cdot b + a \cdot c,$$
  $$(a + b) \cdot c = a \cdot c + b \cdot c \quad \forall a, b, c \in A.$$

Si, además, se cumple que la operación $\cdot$ es conmutativa ($a \cdot b = b \cdot a$ para todo $a, b \in A$), se dice que A es un *anillo conmutativo*. Si existe un elemento $e \in A$ tal que $a \cdot e = e \cdot a = a$ para todo $a \in A$, se dice que A *tiene unidad*. El elemento e se llama la *unidad* de A y generalmente se designa por 1. Un elemento $a^{-1} \in A$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$ se llama un *inverso* de a.

Observemos que en un anillo se cumple $a \cdot 0 = 0 \cdot a = 0$ para todo a. En efecto, $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$. Por tanto, sumando $-(a \cdot 0)$ a ambos lados, obtenemos $0 = a \cdot 0$. Resulta, pues, que en un anillo A el 0 no puede tener inverso. Un anillo conmutativo con unidad en el cual todo elemento distinto de cero posee inverso se llama un *cuerpo.* $\mathbf{Z}$ es un anillo conmutativo con unidad. El conjunto de los racionales $\mathbf{Q}$, el conjunto de los reales $\mathbf{R}$ y el conjunto de los complejos $\mathbf{C}$ son cuerpos.

$\mathbf{Z}/(m)$ es un anillo conmutativo con unidad, [1]. $\mathbf{Z}/(m)$ tiene, sin embargo, propiedades que no tenía $\mathbf{Z}$. Por ejemplo, el producto de dos elementos diferentes de [0] puede ser [0]. Así, en $\mathbf{Z}/(6)$, $[2] \cdot [3] = [0]$. A estos elementos se les llama *divisores de cero.* Por otro lado, hay elementos que tenen inverso. Por ejemplo, en $\mathbf{Z}/(8)$, $[3] \cdot [3] = [1]$. Observemos que, en un anillo, si un elemento es divisor de cero no puede tener inverso. En efecto, sea $a \cdot b = 0$ con $a \neq 0$ y $b \neq 0$. Si existe el inverso de a, resulta que $b = 1 \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0$, en contra de lo que hemos supuesto.

Proposición 5.1 *Si* m.c.d.$(a, m) = 1$, *$[a]$ tiene un inverso en $\mathbf{Z}/(m)$. Si* m.c.d.$(a, m) = d \neq \pm 1, \pm m$, *entonces $[a]$ es un divisor de cero en $\mathbf{Z}/(m)$.*

DEMOSTRACIÓN: Si m.c.d.$(a, m) = 1$ podemos poner $1 = ar + ms$, de donde $[1] = [ar] = [a][r]$ y $[r]$ es inverso de $[a]$. Si $d =$ m.c.d.(a, m), pongamos $a = da'$, $m = dm'$. Entonces $am' = a'm \in [0]$, de donde $[a][m'] = [0]$ y $[m'] \neq 0$, ya que $0 < m' < |m|$. □

Corolario 5.2 *El anillo $\mathbf{Z}/(p)$ es un cuerpo si y sólo si p es primo.*

DEMOSTRACIÓN: Si p es primo, (5.1) nos dice que $\mathbf{Z}/(p)$ es un cuerpo. Si $\mathbf{Z}/(p)$ es un cuerpo, no puede tener divisores de cero (véase la observación hecha antes de (5.1)). Entonces (5.1) nos dice que p debe ser primo. □

I.6 Ecuaciones diofánticas lineales

Nuestro objetivo en este apartado es estudiar las soluciones enteras de la ecuación

$$ax + by = c,$$

donde $a, b, c \in \mathbf{Z}$. La primera proposición se refiere a la existencia de soluciones.

Proposición 6.1 *La ecuación diofántica $ax + by = c$, $a, b, c \in \mathbf{Z}$, tiene solución si y sólo si el máximo común divisor de a y b divide a c.*

Ejercicio:

Demostrar esta proposición.

Supongamos, pues, que $ax + by = c$ tiene solución. Dividiendo por $d =$ m.c.d.(a, b), obtenemos una ecuación con las mismas soluciones, $a'x + b'y = c'$, en la cual m.c.d.$(a', b') = 1$. Multipliquemos la identidad de Bézout $1 = a'r + b's$ por c':

$$c' = a'rc' + b'sc'.$$

$x = rc'$, $y = sc'$ es, por tanto, una solución de la ecuación $a'x + b'y = c'$.

Por otro lado, restando las dos expresiones anteriores obtenemos

$$a'(x - rc') + b'(y - sc') = 0.$$

Por el Teorema de Euclides (3.1)

$$a' \mid y - sc' \qquad \text{y} \qquad b' \mid x - rc'.$$

Es decir, existen t y u tales que

$$\begin{array}{rcl} y & = & sc' + ta' \\ x & = & rc' + ub'. \end{array}$$

Sustituyendo en la ecuación inicial,

$$c' = a'x + b'y = a'rc' + a'ub' + b'sc' + b'ta' = c' + a'b'(u + t),$$

ya que rc', sc' es una solución. Por tanto, $u + t = 0$. La solución general de la ecuación dada es, pues,

$$\begin{array}{rcl} x & = & rc' - tb' \\ y & = & sc' + ta'. \end{array}$$

I.7 Nota histórica

La aritmética, que se inició con los babilonios hacia el año 2000 a. C. y se desarrolló entre los años 600 y 300 a. C. en las escuelas griegas de Pitágoras, Euclides y Diofanto, es todavía hoy una rama de intensa y atractiva actividad investigadora. Las propiedades de los números enteros y las relaciones entre ellos, los conceptos y propiedades de múltiplo, divisor, número primo, la descomposición de un entero (positivo) en producto de primos, el teorema de Euclides, etc., formaron ya parte del cuerpo de doctrina de los libros VII, VIII y IX de los *Elementos* de Euclides. Pierre de Fermat (1601?–1665), un hombre de letras que leía matemáticas por afición (la *Aritmética* de Diofanto de Alejandría) es una de las figuras clave de la aritmética moderna; él fue quien se planteó el resolver la mayoría de los problemas aritméticos dando algunos criterios, demostrando teoremas, estableciendo conjeturas y asegurando haber demostrado un resultado (conocido ahora como el *último teorema de Fermat*) que, pese a los esfuerzos de los más ilustres matemáticos, sigue siendo una cuestión abierta: la ecuación $x^n + y^n = z^n$ con x, y, z enteros y $n > 2$, no tiene ninguna solución no trivial. Es el gran reto (o la gran espina) que tienen los investigadores en teoría de números. Sin pasar por alto la contribución de Leonhard Euler (1707–1783) que, entre otros, demostró en 1736 el *pequeño teorema de Fermat*: $a^p \equiv a\,(p)$, p primo, y la de Carl Friedrich Gaus (1777–1855), que en sus *Disquisitiones Arithmeticae* sistematizó las congruencias y desarrolló su teoría tal com la usamos hoy en día, conviene mencionar también a Ernst Eduard Kummer (1810–1893), Julius Wilhelm Richard Dedekind (1831–1916) y Leopold Kronecker (1823–1891), los cuales, en sus trabajos sobre números algebraicos, utilizan ya los conceptos de anillo, ideal y cuerpo, aunque las teorías abstractas no se han desarrollado hasta el siglo 20.

I.8 Ejercicios

1. Calcular m.c.d.$(28n + 5, 35n + 2)$ para todo $n \geq 1$.

2. Probar que en la sucesión de Fibonacci 0, 1, 1, 2, 3, 5, 8, 13, ... $(a_n = a_{n-1} + a_{n-2})$ dos términos consecutivos son siempre primos entre sí.

3. Demostrar que, si p es primo, $(p-1)! \equiv -1\,(p)$ (*congruencia de Wilson*).

4. Demostrar que, si p es primo, $a^p \equiv a\,(p)$ para todo a (*pequeño teorema de Fermat*).

5. Calcular 2001^{2001} módulo 17.

6. Demostrar los criterios de divisibilidad por 3, 4, 5, 9, 11, 13 y 19.

7. Resolver las ecuaciones diofánticas $111x+36y = 15$, $10x+26y = 1224$, $6x + 10y = 20$, $6x + 10y = 3$.

8. A una isla desierta —sólo habitada por un mono y muchos cocoteros— llegan cinco náufragos; recogen tantos cocos como pueden y se echan a descansar. A medianoche, un marinero desconfiado, temiendo que los otros se despierten y coman algún coco, se levanta, hace cinco partes iguales del total de cocos, separa su parte y deja el resto; pero le ha

sobrado un coco, que da al mono. Al cabo de una hora, un segundo marinero tiene la misma idea: hace cinco partes iguales del total de cocos (¡de los que quedan, por supuesto!), se guarda una parte, deja el resto y da al mono un coco que ha sobrado. Al cabo de otra hora, ... Cada uno de los cinco marineros efectúa la misma operación.

Al día siguiente por la mañana, al levantarse, deciden repartir los cocos (los del montón final) entre los cinco, cada uno de ellos disimulando la risa. Sobra un coco, que dan al mono. Pregunta: ¿cuántos cocos habían recogido como mínimo? (The Saturday Evening Post, $\simeq$ 1925).

9. Oliana Molls trabaja cuatro días consecutivos y descansa uno. Betty trabaja dos y descansa uno. Sólo se ven los días de luna llena (uno de cada veintiocho días). Betty tuvo fiesta ayer, Oliana la tendrá pasado mañana y hace diez días había luna llena. ¿Cuántos días faltan para que se vean? ¿Cuántos días libres comunes habrán perdido mientras tanto por falta de luna llena?

10. a) Encontrar las soluciones de la ecuación lineal $6x \equiv 14\,(16)$, y de la ecuación de segundo grado $x^2 - 3x - 3 \equiv 0\,(7)$.

b) Estudiar en general la resolución de las ecuaciones $ax \equiv b\,(m)$, $ax^2 + bx + c \equiv 0\,(p)$ con p primo.

11. (*Teorema chino del resto*) Demostrar que si $(m,n) = 1$ las ecuaciones $x \equiv a\,(m)$ y $x \equiv b\,(n)$ tienen una única solución módulo mn.

12. Determinar los $a \in \mathbf{Z}/(8)$ tales que el sistema $7x+5y = 2$, $5x+ay = 16$ tiene solución en $\mathbf{Z}/(8)$.

13. a) Demostrar que, si $(a,n) = (b,n) = 1$, la ecuación $ax + by = c$ tiene exactamente n soluciones en $\mathbf{Z}/(n)$.

b) Encontrar las soluciones de $3x+4y = 1$ en $\mathbf{Z}/(7)$ y de $3x+7y = 2$ en $\mathbf{Z}/(8)$.

14. Demostrar que en cualquier solución entera x, y, z de la ecuación $x^2 + y^2 = z^2$ (*terna pitagórica*),

a) x, y o z es múltiplo de 5,

b) x o y es múltiplo de 3,

c) x o y es múltiplo de 4.

15. Demostrar que las únicas relaciones de equivalencia en $\mathbf{Z}$ compatibles con la suma y el producto son las congruencias.

I.9 Ejercicios para programar

16. Cálculo del máximo común divisor y del mínimo común múltiplo de dos números enteros. (Indicación: utilizar las proposiciones I.2.1 y I.3.2.)

17. Resolución de la ecuación diofántica $ax + by = c$. (Indicación: utilizar como subprograma el ejercicio I.16 y seguir el proceso del apartado I.6.)

18. Factorización de un número entero en producto de primos.

19. Construcción de la tabla de los números primos más pequeños que 100.000. (Indicación: ir guardando los primos más pequeños o iguales que 313 en una variable dimensionada. Así estarán disponibles para ir efectuando las sucesivas divisiones.)

20. Cálculo de $1/a$ en $\mathbf{Z}/(p)$, $a \neq 0$, p primo.

21. Cálculo de $\sqrt{a}$ en $\mathbf{Z}/(p)$, p primo, si existe.