

Capítulo 1

Teoría elemental de números

Vas a pasar las próximas semanas con un conjunto que conoces desde los seis años: los números enteros. Y precisamente por eso este primer Tema es el más importante de todo el curso, aunque no sea el más vistoso. No vas a aprender *nuevos números*: vas a aprender a **demostrar** las cosas que ya dabas por sabidas, empezando por la más elemental de todas: qué significa que un número divida a otro. Todo lo que sostiene la Teoría de Números —desde la factorización única hasta la criptografía moderna— se construye sobre una sola idea, la de dividir con resto, aplicada una y otra vez.

1.1 Algoritmos de división y Euclides

💡 Motivación

Vamos a introducir las operaciones básicas de los números enteros: la diferencia, la divisibilidad y el orden. A partir de aquí estableceremos el algoritmo de la división, que garantiza que el cociente y el resto de dividir dos enteros son únicos. Con ese algoritmo como herramienta, definiremos el máximo común divisor y llegaremos al algoritmo de Euclides, que nos permitirá calcularlo de forma eficiente.

1.1.1 Divisibilidad, diferencia y orden

Antes de demostrar nada hace falta fijar el vocabulario. En esta primera definición vas a ver tres conceptos —diferencia, divisibilidad, orden— que parecen independientes pero que en realidad se construyen todos sobre la misma base: la suma y el producto de $\mathbb{Z}$. Fíjate en cómo cada uno se apoya en el anterior.

📖 Definición 1.1 — Diferencia, divisibilidad y orden

Sean a y b dos enteros.

1. Llamaremos **diferencia** $a - b$ de estos dos enteros a otro entero d que satisfaga la igualdad $a = b + d$.
2. Si $a \neq 0$ y $b = a \cdot q$ para algún q , diremos que a **divide** a b . Otras expresiones equivalentes son: a es un *divisor* de b , a es un *factor* de b , b es **múltiplo** de a . Si a divide a b , escribiremos $a \mid b$.
3. Diremos que $b > a$ si existe un número natural n tal que $b = a + n$. Diremos que $b \geq a$ si $b > a$ o $b = a$.

$a \mid b$ se lee « a divide a b »: existe $q \in \mathbb{Z}$ con $b = aq$. Es una afirmación (verdadera o falsa), no un número: no se opera con ella, se demuestra o se refuta.

Fíjate en un detalle que se pasa por alto fácilmente y que va a perseguirte todo el tema: la definición exige $a \neq 0$. El 0 no divide a nada, ni siquiera a sí mismo. Guarda esta observación, porque dentro de un par de páginas volverá a aparecer.

Tres ejemplos bastan para fijar la idea, y el tercero es tan importante como los otros dos: saber divisar también significa saber *no* dividir.

Ejemplo 1.1 — Primeros casos de divisibilidad

- a) $3 \mid 9$, puesto que $3 \cdot 3 = 9$.
- b) $4 \mid 24$, puesto que $4 \cdot 6 = 24$.
- c) $6 \nmid 21$, puesto que no existe ningún entero q tal que $6 \cdot q = 21$.

Los dos primeros apartados se prueban igual: basta exhibir el cociente. El tercero es de otra naturaleza, porque hay que descartar *todos* los candidatos a la vez, y el enunciado no te regala el argumento. Aquí tienes dos maneras de rematarlo, y conviene que te acostumbres a las dos, porque en el tema volverás a necesitarlas: por tamaño, $6 \cdot 3 = 18 < 21 < 24 = 6 \cdot 4$, así que ningún múltiplo de 6 cae exactamente en 21; o por paridad, $6q$ es siempre par y 21 es impar, así que no pueden coincidir.

¿Por qué funciona todo esto? El anillo $(\mathbb{Z}, +, \cdot)$

Recordemos que la suma y el producto de números enteros satisfacen las propiedades asociativa y conmutativa. Además, $(\mathbb{Z}, +)$ es un grupo abeliano. También se satisface la propiedad distributiva $a(b + c) = ab + ac$, por lo que $(\mathbb{Z}, +, \cdot)$ es un *anillo conmutativo con elemento unidad* (el 1) y *sin divisores de cero*, es decir, si $ab = 0$ entonces necesariamente $a = 0$ o $b = 0$. Todas las demostraciones que vienen a continuación usan solo estas reglas de los anillos conmutativos: ni una más.

Todo $a \neq 0$ divide a 0. El propio 0 no divide a nada: la condición $a \neq 0$ no es un tecnicismo.

Como todo entero no nulo divide a 0 (basta tomar $q = 0$ en la Definición 1.1, apartado 2), se sigue que **todo** $a \neq 0$ **divide a** 0. Sí, hace falta repetir la condición $a \neq 0$: es la misma que exige la definición, y aquí es donde de verdad se nota, porque «0 divide a 0» tentaría a cualquiera a escribirla sin pensar.

1.1.2 Propiedades básicas de la divisibilidad

Con la definición ya en la mano, el siguiente paso es cosechar sus consecuencias inmediatas. Las ocho propiedades que siguen no son una lista para memorizar: son ocho pequeños teoremas, cada uno con su propia demostración a partir de los axiomas de anillo. Tres de ellas te van a acompañar el resto de la carrera, así que léelas con calma la primera vez.

Proposición 1.1 — Propiedades básicas de la divisibilidad

Sean a, b, c números enteros.

1. $0 \cdot a = 0$.
2. $a(-b) = -ab$.
3. Si $a \neq 0$ y $ab = ac$, entonces $b = c$.
4. Si $a \neq 0$ y $a \mid b$, entonces $a \mid bx$ para cada entero x .

5. Sean $a \neq 0$ y $b \neq 0$. Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.
6. **Combinación lineal:** Sea $a \neq 0$. Si $a \mid b$ y $a \mid c$, se verifica que $a \mid (bx + cy)$ para cualquier par de enteros x e y .
Es decir, si a divide a b y a c , divide a *cualquier* $bx + cy$. Es la propiedad más usada de todo el tema. Recuérdala: reaparecerá al hablar del máximo común divisor.
7. Sean a y b positivos. Si $a \mid b$ entonces $a \leq b$.
8. Sean $a \neq 0$ y $b \neq 0$. Si $a \mid b$ y $b \mid a$, se tiene que $a = b$ o $a = -b$.

Demostración.

- Como $0 + 0 = 0$ tenemos que $0 \cdot a = (0 + 0)a$, que por la propiedad distributiva es $0 \cdot a + 0 \cdot a$. Restando $0 \cdot a$ en ambos miembros, $0 = 0 + 0 \cdot a$; y como 0 es el elemento neutro de la suma, concluimos que $0 = 0 \cdot a$.
- Por definición, $-ab$ es el elemento opuesto de ab respecto de la suma, y además es único. Así pues, $a(-b) + ab = a(-b + b) = a \cdot 0 = 0$. Luego $a(-b)$ es el opuesto de ab y, por tanto, igual a $-ab$.
- En la igualdad $ab = ac$ sumamos $-ac$ a ambos miembros: $ab + (-ac) = 0 \Rightarrow a[b + (-c)] = 0$. Como $a \neq 0$ y $\mathbb{Z}$ no tiene divisores de cero, necesariamente $b + (-c) = 0$. Sumando c a ambos miembros, $b = c$.
- Por definición, si $a \mid b$ existe un número q tal que $b = aq$. De aquí que $bx = aqx$. Sea $q' = qx$; entonces $bx = aq'$ y, por tanto, $a \mid bx$.
- Si $a \mid b$ existe q_1 tal que $b = aq_1$. Si $b \mid c$ existe q_2 tal que $c = bq_2$. Por tanto, $c = bq_2 = aq_1q_2$. Sea $q = q_1q_2$; se tiene que $c = aq$, luego $a \mid c$.
- Si $a \mid b$ y $a \mid c$ existen q_1 y q_2 tales que $b = aq_1$ y $c = aq_2$. Entonces,

$$bx + cy = aq_1x + aq_2y = a(q_1x + q_2y) = aq$$

donde $q = q_1x + q_2y$. Así pues, $a \mid (bx + cy)$.

- Si $a \mid b$ existe q tal que $b = aq$. Como a y b son positivos, q es positivo. Por tanto podemos escribir $b = \underbrace{a + a + \dots + a}_{q \text{ veces}} = a + s$, con $s \geq 0$ (pues $q - 1 \geq 0$). De $b = a + s$ se deduce que $a \leq b$.
- Como $a \mid b$ existe q_1 tal que $b = aq_1$. De $b \mid a$ existe q_2 tal que $a = bq_2$. Por tanto, $a = aq_1q_2$, de donde $q_1q_2 = 1$. Por la propiedad 7 aplicada a los valores absolutos, esto obliga a $q_1 = q_2 = 1$ o $q_1 = q_2 = -1$, por lo que $a = b$ o $a = -b$.



Detente un momento en la propiedad 6. Parece modesta —«las combinaciones lineales heredan los divisores comunes»— pero es, con diferencia, la herramienta que más vas a usar en lo que queda de tema: sostiene la demostración de la Identidad de Bézout y, más adelante, el criterio para resolver ecuaciones diofánticas. Cuando dentro de unas páginas te encuentres atascado en una demostración sobre el máximo común divisor, la primera pregunta que debes hacerte es: *¿puedo escribir lo que busco como $bx + cy$?*

Dos hipótesis que no puedes ignorar

La propiedad 7 exige a y b **positivos**, y no es un capricho: sin esa hipótesis, es falsa. Por ejemplo, $3 \mid -6$ (pues $-6 = 3 \cdot (-2)$) y sin embargo $3 > -6$. La versión que sí vale para enteros de cualquier signo llegará enseguida, con el valor absoluto.

La propiedad 8, por su parte, da un signo, no una igualdad. Con $a = 3$ y $b = -3$ se cumple $3 \mid -3$ y $-3 \mid 3$, y en efecto $3 = -(-3)$: la conclusión « $a = b$ o $a = -b$ » se cumple, pero sería un error leerla como « $a = b$ » sin más.

1.1.3 Dos ejemplos de manejo algebraico

Cerramos esta sección con dos ejemplos que no introducen ideas nuevas, pero que son el mejor entrenamiento posible para el método que vas a repetir sin descanso en las páginas siguientes: *desenrollar* una hipótesis de divisibilidad hasta convertirla en una igualdad con un cociente, operar con esa igualdad, y volver a *empaquetarla* como una divisibilidad nueva.

Ejemplo 1.2 — Distributividad y signos

Pruébese que, dados a, b, c, d enteros, entonces:

- a) $(a + b)(c + d) = ac + bc + ad + bd$.
- b) $(-a)(-b) = ab$.

Demostración.

a. Por la propiedad distributiva,

$$(a + b)(c + d) = (a + b)c + (a + b)d$$

aplicándola de nuevo a cada sumando,

$$(a + b)c + (a + b)d = ac + bc + ad + bd$$

b. Por la propiedad 2 de la Proposición 1.1,

$$(-a)(-b) = -[(-a)b] = -[-(ab)] = ab$$

■

El segundo ejemplo del bloque es el primero de verdad exigente: encadena dos veces el método de «desenrollar y volver a empaquetar», y en el apartado b) añade un ingrediente nuevo, la cancelación por ausencia de divisores de cero.

Ejemplo 1.3 — Producto y cancelación en la divisibilidad

Sean a, b, c, d enteros con $a \neq 0$ y $c \neq 0$. Demuéstrese que:

- a) Si $a \mid b$ y $c \mid d$, entonces $ac \mid bd$.
- b) Si $ac \mid bc$, entonces $a \mid b$.

Demostración.

a. De $a \mid b$ y $c \mid d$ sabemos que existen q_1 y q_2 tales que $b = aq_1$ y $d = cq_2$. Por tanto,

$$bd = aq_1cq_2 = ac(q_1q_2)$$

Llamando $q = q_1q_2$, resulta $ac \mid bd$.

b. Si $ac \mid bc$ existe q tal que $bc = acq$. Entonces $bc - acq = 0$, y por la propiedad distributiva, $c(b - aq) = 0$. Como $c \neq 0$ y $\mathbb{Z}$ no tiene divisores de cero, deducimos $b - aq = 0$, es decir $b = aq$, y así $a \mid b$. ■

Un recíproco que no es cierto

Del apartado a) te puede tentar pensar que $a \mid bc$ implica $a \mid b$ o $a \mid c$. Es falso en general:

$$6 \mid 4 \cdot 9 = 36$$

pero $6 \nmid 4$ y $6 \nmid 9$.

Cuando a es *primo* sí es cierto, y se llama **Lema de Euclides**; lo verás en la Sección 2.2.

Lo esencial de este bloque

- Divisibilidad, diferencia y orden se definen unos a partir de otros, todos apoyados en la suma y el producto de $\mathbb{Z}$. La condición $a \neq 0$ en $a \mid b$ no es accesorio: sin ella, ni « $0 \mid 0$ » ni la propia definición tendrían sentido.
- Las ocho propiedades básicas son consecuencias directas de los axiomas de anillo. La propiedad 6 —las combinaciones lineales heredan los divisores comunes— es la más importante: la volverás a usar en Bézout y en las ecuaciones diofánticas.
- Dos hipótesis frágiles que conviene memorizar: la propiedad 7 exige positividad, y la propiedad 8 solo da el signo, no la igualdad.
- El método de trabajo de todo el tema ya está aquí en miniatura: desenrollar la hipótesis de divisibilidad como una igualdad con cociente, operar, y volver a empaquetar el resultado como una nueva divisibilidad.

1.2 Valor absoluto

Con la divisibilidad ya formalizada, nos falta una herramienta antes de poder enunciar el Algoritmo de la División: una manera de comparar *tamaños* de enteros que funcione igual de bien con signos negativos que con positivos. La propiedad 7 de la Proposición 1.1 — $a \mid b \Rightarrow a \leq b$ — solo servía para a, b positivos, y en el bloque anterior ya viste un contraejemplo en cuanto un signo se colaba en la historia. El valor absoluto es exactamente el remedio: una aplicación que «olvida» el signo y deja solo el tamaño.

Definición 1.2 — Valor absoluto

Llamaremos *valor absoluto* a la aplicación $|\cdot| : \mathbb{Z} \rightarrow \mathbb{Z}$, definida por

$$|n| = \begin{cases} n & \text{si } n \geq 0, \\ -n & \text{si } n < 0. \end{cases}$$

Aplicación bien definida

Toda aplicación debe asignar a cada elemento del dominio **exactamente una** imagen: ni ninguna, ni más de una. Comprobar esto —que no falte ningún caso y que no se solapen— se llama comprobar que la aplicación está *bien definida*. Lo volverás a hacer, y no pocas veces, especialmente con operaciones sobre clases de equivalencia.

Observa que la propia definición de valor absoluto, por sus dos casos « $n \geq 0$ » y « $n < 0$ », ya reparte todo $\mathbb{Z}$ sin solapamientos ni huecos: todo entero cae en uno de los dos casos, y en uno solo. Esto es precisamente lo que hace falta comprobar para que una definición por casos tenga derecho a llamarse *aplicación*.

¿Por qué merece la pena decirlo explícitamente?

Parece una perogrullada —claro que $|n|$ tiene un único valor para cada n — pero la costumbre de comprobarlo es la que te va a salvar más adelante, cuando definas una operación *a partir de un representante* de una clase y tengas que verificar que el resultado no depende de qué representante hayas elegido. Esa comprobación tiene el mismo nombre —bien definida— y exactamente el mismo espíritu que la que acabas de hacer aquí, casi sin darte cuenta.

El valor absoluto hereda de la suma y el producto de $\mathbb{Z}$ un puñado de propiedades que lo hacen manejable. La demostración es más larga de lo habitual, pero no porque sea difícil: es que la propia definición está partida en dos casos, así que cada propiedad que involucre una suma o un producto obliga, en principio, a repasar todas las combinaciones de signos. Es un buen momento para poner a prueba tu paciencia con el álgebra elemental.

Proposición 1.2 — Propiedades del valor absoluto

Sean $a, b, n \in \mathbb{Z}$ unos números enteros.

1. $|n| \geq 0$.
2. $|n| = 0$ si y solo si $n = 0$.
3. $|a \cdot b| = |a| \cdot |b|$.
4. $|a + b| \leq |a| + |b|$.
5. Si $a \neq 0$, $b \neq 0$ y $a \mid b$, entonces $|a| \leq |b|$.

Demostración.

1 y 2. Se siguen trivialmente de la definición de valor absoluto.

3. Por definición, $|ab| = ab$ si $ab \geq 0$, y $|ab| = -ab$ si $ab < 0$. Distinguimos casos según el signo de a y de b .

- Si $a \geq 0$ y $b \geq 0$, entonces $ab \geq 0$; por tanto $|ab| = ab = |a| |b|$.
- Si $a \geq 0$ y $b < 0$, entonces $ab \leq 0$. Además $|a| = a$ y $|b| = -b$. Tenemos entonces $|ab| = -ab = (-b)a = |b| |a| = |a| |b|$.
- El caso $a < 0$ y $b \geq 0$ se estudia análogamente, intercambiando los papeles de a y b .
- Si $a < 0$ y $b < 0$, entonces $ab > 0$, y además $|a| = -a$ y $|b| = -b$. Por tanto $|ab| = ab = (-|a|)(-|b|) = |a| |b|$.

4. De la definición de valor absoluto, $|a+b| = a+b$ si $a+b \geq 0$, y $|a+b| = -(a+b)$ si $a+b < 0$.

- Si $a \geq 0$ y $b \geq 0$, entonces $a+b \geq 0$, y $|a+b| = a+b = |a| + |b|$.
- Si $a \geq 0$, $b < 0$ y $a \geq -b$, entonces $a+b \geq 0$, luego $|a+b| = a+b = |a| + b$. Como $b < 0$ tenemos $|b| = -b$, así que $|a+b| = |a| - |b| \leq |a| + |b|$.
- Si $a \geq 0$, $b < 0$ y $a < -b$, entonces $a+b < 0$. De la definición, $|a+b| = -(a+b) = (-a) + (-b) = -|a| + |b| \leq |a| + |b|$.
- El caso $a < 0$, $b \geq 0$ se trata análogamente.
- Si $a < 0$ y $b < 0$, entonces $a+b < 0$, y además $|a| = -a$, $|b| = -b$. Por tanto $|a+b| = -(a+b) = (-a) + (-b) = |a| + |b|$.

En cada uno de los cinco casos se obtiene $|a+b| \leq |a| + |b|$, con igualdad exactamente cuando a y b no tienen signos opuestos (incluido el caso en que alguno de los dos es 0).

5. Si $a \mid b$ entonces $b = aq$ para algún q . Como $b \neq 0$, también $q \neq 0$. Por las propiedades 1 y 2 de esta misma proposición, $|q| \geq 1$; y por la propiedad 3, $|b| = |a| |q|$. Así pues $|a|$ divide a $|b|$, y como ambos son positivos, la propiedad 7 de la Proposición 1.1 da $|a| \leq |b|$. ■

Nota

Un comentario sobre la Propiedad 5. Si $a \neq 0$, $b \neq 0$ y $a \mid b$, entonces $|a| \leq |b|$. Guárdala: es la pieza esencial que va a necesitar para demostrar, en la próxima sección, otra propiedad clave: que el cociente y el resto de dividir dos enteros son únicos.

Antes de seguir, un aviso sobre la propiedad 4 que rompe una tentación muy extendida.

$|a-b|$ **no es** $|a| - |b|$

Con $a = 1$ y $b = -1$: $|a-b| = |2| = 2$, mientras que $|a| - |b| = 1 - 1 = 0$.

La propiedad 4, aplicada a a y $-b$, sí te da una desigualdad correcta y útil: $|a-b| = |a+(-b)| \leq |a| + |-b| = |a| + |b|$.

Lo que *no* es cierto en general es la igualdad, y tampoco lo es « $|a-b| \geq |a| - |b|$ » sin más precauciones: la versión correcta:

$$||a| - |b|| \leq |a-b|$$

la demostrarás tú mismo como ejercicio al cierre de la Sección.

El último resultado de este bloque no añade ninguna propiedad nueva: te da una forma de manejar la desigualdad $|a| < b$ sin tener que arrastrar la definición por casos. Vas a usarla constantemente, así que merece la pena verla demostrada con calma.

Ejemplo 1.4 — Una desigualdad con valor absoluto, sin casos

Demuéstrese que si $a, b \in \mathbb{Z}$ y $b > 0$, entonces

$$|a| < b \quad \text{si y solo si} \quad a < b \quad \text{y} \quad -a < b.$$

Demostración.

($\Rightarrow$) Sabemos que $|a|$ es a si $a \geq 0$, y $-a$ si $a < 0$. Si $a \geq 0$, como $|a| = a$ se tiene $a < b$, y entonces $-a \leq a < b$. Si $a < 0$, entonces $a < -a = |a| < b$. En ambos casos, $a < b$ y $-a < b$.

($\Leftarrow$) Supongamos $a < b$ y $-a < b$. Por la definición de valor absoluto, $|a| = a$ o $|a| = -a$; en cualquiera de los dos casos, $|a| < b$. ■

Vuelta atrás: la propiedad 4 sin casos

El Ejemplo 1.4 tiene una hermana no escrita, con la misma demostración cambiando « $<$ » por « $\leq$ »: para $c \geq 0$,

$$|x| \leq c \quad \Longleftrightarrow \quad -c \leq x \leq c.$$

Con esta equivalencia, la propiedad 4 se demuestra en dos líneas y sin distinguir un solo caso. De la propia definición de valor absoluto, para cualquier entero n se cumple $-|n| \leq n \leq |n|$ (es exactamente el caso $c = |n|$). Aplicándolo a a y b por separado y sumando las dos cadenas de desigualdades,

$$-(|a| + |b|) \leq a + b \leq |a| + |b|,$$

y por la equivalencia anterior, con $x = a + b$ y $c = |a| + |b|$, se concluye $|a + b| \leq |a| + |b|$.

Guarda esta idea con el mismo cariño que la demostración por casos del libro: en matemáticas, cuando una prueba se llena de casos, merece la pena preguntarse si no habrá una desigualdad —como esta $-|n| \leq n \leq |n|$ — que los estaba escondiendo a todos a la vez.

Lo esencial de este bloque

- El valor absoluto es una aplicación bien definida $|\cdot| : \mathbb{Z} \rightarrow \mathbb{Z}$, partida en dos casos que cubren $\mathbb{Z}$ sin solaparse: exactamente lo que hace falta para que merezca llamarse aplicación.
- Sus cinco propiedades básicas se demuestran caso a caso a partir de la propia definición. La propiedad 4, la desigualdad triangular, admite además una demostración sin casos a partir de $-|n| \leq n \leq |n|$.
- La propiedad 5 — $a \mid b$ con $a, b \neq 0$ implica $|a| \leq |b|$ — es la pieza que estabas esperando desde el bloque anterior: con ella, y solo con ella, demostrarás la unicidad del Algoritmo de la División.
- Cuidado con $|a - b|$: no es $|a| - |b|$. La desigualdad correcta, $||a| - |b|| \leq |a - b|$, queda como ejercicio.

1.3 El Algoritmo de la División

Llegamos al resultado que da nombre a la Sección, y no es una exageración decir que todo lo que vas a estudiar en las próximas semanas cuelga de él. Vas a demostrar algo que sabes hacer desde primaria —dividir dos números y quedarte con un cociente y un resto— pero esta vez con dos exigencias que la escuela nunca te pidió: que el resultado exista siempre, sin excepción, y que sea el único posible. La divisibilidad te ha dado el vocabulario; el valor absoluto, en particular su propiedad 5, te ha dado la herramienta para medir distancias sin que los signos estorben. Con eso basta.

Pero antes de enunciar el teorema hace falta confesar algo: su demostración necesita un principio que ni hemos enunciado ni hemos demostrado. Es el momento de presentarlo.

Buen Orden: Todo subconjunto no vacío de $\mathbb{N} \cup \{0\}$ tiene mínimo. Parece obvio, pero sostiene media Teoría de Números: hoy, la existencia del resto; más adelante, Bézout y Euclides.

El Principio del Buen Orden

La propiedad (no demostrada pero verdadera) de que el conjunto $\mathbb{N}$ está **bien ordenado** se enuncia como:

Todo subconjunto no vacío de $\mathbb{N} \cup \{0\}$ tiene un elemento mínimo.

Dicho de otro modo: si vas escogiendo números enteros no negativos de un conjunto no vacío, por muchos que haya, en algún momento tropiezas con el más pequeño de todos —nunca puedes seguir bajando indefinidamente—.

Vamos a aceptar este principio como herramienta de trabajo; en la Sección 1-3 verás que es, de hecho, *equivalente* al Principio de Inducción que ya conoces del bachillerato, y lo demostrarás con todo rigor.

La demostración que sigue tiene una estrategia que conviene que identifiques desde ya, porque la vas a ver repetirse: en vez de *construir* el resto r a mano, lo vamos a definir como *el mínimo de un conjunto bien elegido*. Elegir bien ese conjunto es todo el truco.

Teorema 1.1 — Algoritmo de la División

Sean $a \in \mathbb{Z}$ y $b \in \mathbb{N}$. Existen enteros q y r tales que

$$a = bq + r, \quad 0 \leq r < b.$$

Además, q y r son únicos.

Mínimo de un conjunto: Construir r como mínimo de $\{a - bk \geq 0\}$ es el mismo truco que usarás para Bézout: el mínimo positivo de un conjunto bien elegido tiene justo la propiedad que buscas.

Demostración.

Existencia. Sea el conjunto $S = \{a - bk : k \in \mathbb{Z}, a - bk \geq 0\}$.

Veamos primero que $S \neq \emptyset$. Tomando $k = -|a|$ obtenemos $a - bk = a + b|a|$; como $b \geq 1$, se tiene $b|a| \geq |a| \geq -a$, así que $a + b|a| \geq a + (-a) = 0$. Por tanto $a + b|a| \in S$.

Como S es un subconjunto no vacío de $\mathbb{N} \cup \{0\}$, por el Principio del Buen Orden tiene un elemento mínimo; llamémoslo r , y sea q el entero tal que $r = a - bq$. Por construcción $r \in S$, así que $r \geq 0$.

Veamos que además $r < b$. Si fuera $r \geq b$, el número $r - b = a - b(q + 1)$ cumpliría $r - b \geq 0$, luego $r - b \in S$; pero $r - b < r$, lo que contradice que r sea el mínimo de S . Así pues $r < b$. En consecuencia, $a = bq + r$ con $0 \leq r < b$.

Unicidad. Supongamos que $a = bq_1 + r_1 = bq_2 + r_2$ con $0 \leq r_1 < b$, $0 \leq r_2 < b$ y $r_1 \neq r_2$. Entonces $b(q_2 - q_1) = r_1 - r_2$, luego $b \mid (r_1 - r_2)$; y como $r_1 - r_2 \neq 0$, la propiedad 5 de la Proposición 1.2 da $|b| \leq |r_1 - r_2|$, es decir, $b \leq |r_1 - r_2|$ (pues $b > 0$). Pero de $0 \leq r_1 < b$ y $0 \leq r_2 < b$ se sigue $-b < r_1 - r_2 < b$, es decir $|r_1 - r_2| < b$, lo que contradice la desigualdad anterior. Por tanto $r_1 = r_2$, y de $b(q_2 - q_1) = 0$ con $b \neq 0$ se obtiene $q_1 = q_2$. ■

A los números a , b , q y r del teorema se les suele llamar, respectivamente, *dividendo*, *divisor*, *cociente* y *resto*.

Un paso que se te puede escapar

En la unicidad, fíjate en el orden exacto de los pasos: primero se supone $r_1 \neq r_2$ —es la hipótesis de la que se parte para llegar a una contradicción— y *solo entonces* se invoca la propiedad 5, que exige precisamente que la cantidad sobre la que se aplica sea distinta de cero. Invocar esa propiedad antes de justificar $r_1 - r_2 \neq 0$ sería un salto en el vacío, aunque la conclusión final sea correcta. Es un patrón que te va a perseguir toda la carrera: antes de usar una propiedad que exige « $\neq 0$ », demuestra primero que el « $\neq 0$ » se cumple.

El teorema anterior exige $b \in \mathbb{N}$, es decir, $b > 0$. El siguiente resultado, con la misma estrategia que ya usamos en el Corolario 1-1.10 original, extiende el algoritmo a cualquier divisor no nulo, **sin repetir la demostración desde cero**: basta reducir el caso $b < 0$ al caso $b > 0$ que ya tenemos resuelto, cambiando b por $-b$.

Corolario 1.1 — División con divisor negativo

Dados $a, b \in \mathbb{Z}$ con $b \neq 0$, existen enteros q y r , únicos, tales que

$$a = bq + r, \quad 0 \leq r < |b|.$$

Reducir al caso resuelto: Cuando un caso nuevo se deja transformar en uno que ya has demostrado —aquí, cambiando b por $-b$ — no hace falta repetir el argumento entero. Es una economía que vas a usar continuamente.

Demostración. Si $b > 0$, estamos en las hipótesis del Teorema 1.1 y no hay nada más que probar. Supongamos entonces $b < 0$; así $-b > 0$, y por el Teorema anterior existen q' y r únicos tales que $a = (-b)q' + r$ con $0 \leq r < -b$. Llamando $q = -q'$, esta igualdad se reescribe como $a = bq + r$ con $0 \leq r < -b = |b|$. La unicidad de q y r se sigue de la de q' y r . ■

Nada mejor para fijar un teorema de existencia que verlo funcionar con números concretos, y en particular con divisores y dividendos negativos, que es donde más fácil resbala.

✏ Ejemplo 1.5 — División con distintos signos

- a) Dados 3 y 7: $3 = 7 \cdot 0 + 3$, con $0 \leq 3 < 7$.
- b) Dados 7 y 3: $7 = 3 \cdot 2 + 1$, con $0 \leq 1 < 3$.
- c) Dados -15 y 8: $-15 = 8 \cdot (-2) + 1$, con $0 \leq 1 < 8$.
- d) Dados -23 y -17: $-23 = (-17) \cdot 2 + 11$, con $0 \leq 11 < |-17| = 17$.

e) Dados $b = -7$ y $a = 1, -2, 61, -59$:

$$1 = (-7) \cdot 0 + 1, \quad -2 = (-7) \cdot 1 + 5, \quad 61 = (-7) \cdot (-8) + 5, \quad -59 = (-7) \cdot 9 + 4.$$

El resto negativo que tienta a escribirse

En c), la igualdad $-15 = 8 \cdot (-1) - 7$ también es cierta, pero *no* es la división del teorema: el resto tendría que ser -7 , que no cumple $0 \leq r < 8$. El Algoritmo de la División no admite restos negativos bajo ningún concepto, por negativo que sea el dividendo.

El Algoritmo de la División no es solo una herramienta de cálculo: es, sobre todo, una herramienta de *demonstración*. El siguiente ejemplo muestra el patrón que más vas a repetir con ella —la *disección por restos*—: para probar algo sobre **todos** los enteros, se dividen entre un módulo bien elegido y se comprueba la propiedad en cada uno de los, ahora sí, finitos restos posibles.

✍ Ejemplo 1.6 — El cuadrado de un impar tiene la forma $8k + 1$

Demuéstrese, a partir del Algoritmo de la División, que el cuadrado de todo número entero impar se puede escribir en la forma $8k + 1$.

Demostración. Por el Algoritmo de la División, para todo entero a se tiene $a = 4q + r$ con $0 \leq r < 4$, así que r solo puede tomar los valores 0, 1, 2, 3. Por tanto, todo entero a es de una de las formas $4q, 4q + 1, 4q + 2$ o $4q + 3$.

Los números $4q = 2 \cdot (2q)$ y $4q + 2 = 2(2q + 1)$ son pares, así que solo hace falta considerar los impares, es decir los de la forma $4q + 1$ y $4q + 3$. Elevándolos al cuadrado,

$$(4q + 1)^2 = 16q^2 + 8q + 1 = 8(2q^2 + q) + 1 = 8k + 1,$$

$$(4q + 3)^2 = 16q^2 + 24q + 9 = 8(2q^2 + 3q + 1) + 1 = 8k + 1.$$

■

El último ejemplo del bloque exige un paso más de cuidado que el anterior: dos números que comparten valor —porque son, a la vez, un cuadrado y un cubo— pueden repartirse en restos *distintos* al dividirlos entre 7 como enteros x e y separados. Lo que hay que comparar no es x con y , sino x^2 con y^3 .

✍ Ejemplo 1.7 — Un número que es cuadrado y cubo a la vez

Demuéstrese que si un número entero es a la vez un cuadrado y un cubo, entonces se puede escribir en la forma $7k$ o $7k + 1$.

Demostración. Veamos primero un caso particular: el número 64 es un cuadrado, 8^2 , y un cubo, 4^3 , y en efecto es de la forma $7k + 1$, pues $64 = 7 \cdot 9 + 1$. Veamos ahora el caso general.

Sea $a = x^2 = y^3$ para ciertos enteros x, y . Por el Algoritmo de la División, $x = 7q + r$ con $0 \leq r < 7$. Desarrollando,

$$x^2 = (7q + r)^2 = 49q^2 + 14qr + r^2 = 7(7q^2 + 2qr) + r^2,$$

así que el resto de x^2 al dividir entre 7 coincide con el resto de r^2 . Haciendo $r = 0, 1, \dots, 6$, los restos de r^2 son, respectivamente, 0, 1, 4, 2, 2, 4, 1. Por tanto, x^2 **solo puede dejar resto** 0, 1, 2 o 4 al dividir entre 7.

Análogamente, $y = 7q' + r'$ con $0 \leq r' < 7$, y

$$y^3 = (7q' + r')^3 = (7q')^3 + 3(7q')^2r' + 3(7q')r'^2 + r'^3 = 7k' + r'^3,$$

así que el resto de y^3 coincide con el de r'^3 . Haciendo $r' = 0, 1, \dots, 6$, los restos de r'^3 son $0, 1, 1, 6, 1, 6, 6$. Por tanto, y^3 **solo puede dejar resto** $0, 1$ o 6 al dividir entre 7 .

Como $a = x^2 = y^3$, el resto de a al dividir entre 7 tiene que pertenecer a la vez a $\{0, 1, 2, 4\}$ (las posibilidades de x^2) y a $\{0, 1, 6\}$ (las de y^3). La intersección de ambos conjuntos es $\{0, 1\}$. Por tanto, a es de la forma $7k$ o $7k + 1$. ■

Fe de erratas: así cerraba el argumento el texto original

Qué dice el texto. Tras calcular los mismos restos de arriba, algunas ediciones concluyen: «como $a = x^2 = y^3$, vemos que las formas de x^2 e y^3 solo coinciden para $r = r' = 0$ y $r = r' = 1$, que son, respectivamente, $7k$ y $7k + 1$ ».

Por qué falla. Lo que tiene que coincidir es el *resto de a* —que es único, por la propia unicidad del Algoritmo de la División—, no el resto r de x con el resto r' de y . No hay ningún motivo para que $r = r'$: el propio caso particular de arriba lo refuta. En $64 = 8^2 = 4^3$, el resto de $x = 8$ entre 7 es $r = 1$, y el resto de $y = 4$ entre 7 es $r' = 4$: son distintos, y aun así 64 cae en la forma correcta, $7k + 1$.

Corrección. La que has visto arriba: se comparan los conjuntos de restos posibles de x^2 y de y^3 —no los restos de x y de y — y se toma su intersección.

Moraleja. Una conclusión verdadera no certifica que el argumento que la produce sea correcto. Es una distinción que un examen de test no te va a perdonar, y que un examen de demostración te va a exigir explícitamente.

Lo esencial de este bloque

- El Algoritmo de la División es el teorema central del tema: garantiza que el cociente y el resto de dividir a entre $b > 0$ existen y son únicos, con $0 \leq r < b$.
- La existencia se construye tomando r como el *mínimo* de un conjunto bien elegido, apoyándose en el Principio del Buen Orden. La unicidad se apoya en la propiedad 5 del valor absoluto —y exige justificar primero que $r_1 \neq r_2$ antes de aplicarla.
- El Corolario extiende el resultado a cualquier divisor $b \neq 0$ ($0 \leq r < |b|$), reduciendo el caso $b < 0$ al caso ya demostrado.
- La disección por restos —dividir entre un módulo bien elegido y agotar los casos— es el método de demostración que más vas a repetir con esta herramienta. Al aplicarla a expresiones como x^2 o y^3 , lo que hay que comparar son los restos de esas expresiones, nunca los restos de las variables originales.

1.4 El operador MOD

El Algoritmo de la División te ha dado un resto único para cada par (a, b) . Eso significa que «tomar el resto de dividir a entre b » es, en toda regla, una *operación*: metes dos enteros y sale un único entero. Le vamos a poner nombre y notación propios, porque la vas a usar sin parar —y porque es, literalmente, el operador % o mod que ya conoces si has programado algo alguna vez.

Definición 1.3 — Operador MOD

Sean $a, b \in \mathbb{Z}$ con $b \neq 0$, y sea $a = bq + r$ con $0 \leq r < |b|$ (el Corolario 1.1 garantiza que q y r existen y son únicos). Definimos el operador *módulo*, $a \bmod b$, por

$$a \bmod b = r.$$

Operador, no relación

$a \bmod b$ es un **número**: el resto. Más adelante, en la Sección 1-5, escribirás $a \equiv b \pmod{m}$, que es una **afirmación** (verdadera o falsa) sobre otra pareja de números. Se parecen en la notación y no tienen nada que ver en la gramática: no confundas «vale r » con «es cierto que».

Como el operador MOD no es más que el resto del Algoritmo de la División leído con otro nombre, no hay nada que demostrar para calcularlo: basta reciclar lo que ya sabes.

Ejemplo 1.8 — Cálculo directo del operador MOD

Retomando los datos del Ejemplo 1.5:

$$\begin{aligned} 3 \bmod 7 &= 3, & 7 \bmod 3 &= 1, & (-15) \bmod 8 &= 1, & (-23) \bmod (-17) &= 11, \\ 1 \bmod (-7) &= 1, & (-2) \bmod (-7) &= 5, & 61 \bmod (-7) &= 5, & (-59) \bmod (-7) &= 4. \end{aligned}$$

Lo interesante del operador MOD no es que exista, sino una propiedad casi milagrosa que tiene: puedes sustituir cualquier número por otro que deje el mismo resto, sumar o multiplicar con el sustituto, y el resultado seguirá dejando el mismo resto que si hubieras operado con los números originales. Antes de verlo en general, compruébalo con un caso concreto: para calcular $(9^5 + 13 \cdot 20) \bmod 7$ no hace falta calcular $9^5 = 59049$. Como $9 \bmod 7 = 2$ y $20 \bmod 7 = 6$, basta calcular $(2^5 + 13 \cdot 6) \bmod 7$, y de hecho $13 \bmod 7 = 6$ también, así que se reduce a $(2^5 + 6 \cdot 6) \bmod 7 = (32 + 36) \bmod 7 = 68 \bmod 7 = 5$ —el mismo resultado que se obtiene operando con los números originales, pero sin manejar números de cinco cifras.

Proposición 1.3 — Propiedades del operador MOD

Sean a, b, c, d, m enteros con $m \neq 0$. Si $a \bmod m = c \bmod m$ y $b \bmod m = d \bmod m$, entonces:

- 1) $(a + b) \bmod m = (c + d) \bmod m$.
- 2) $(ab) \bmod m = (cd) \bmod m$.

Reducir antes de operar

Esta proposición es la que te permite sustituir un número por otro que deja el mismo resto, sumar o multiplicar, y llegar al mismo sitio. Es el germen de toda la aritmética modular que verás en la Sección 1-5: congruencias, el Teorema de Fermat, el de Euler.

Demostración. De las hipótesis se sigue que $a = mq_1 + r$, $b = mq_3 + r'$, $c = mq_2 + r$, $d = mq_4 + r'$, para el mismo resto r en a y en c , y el mismo resto r' en b y en d .

1. Se tiene $a + b = m(q_1 + q_3) + (r + r')$ y $c + d = m(q_2 + q_4) + (r + r')$. Si $r + r' < |m|$, esto ya es la división de $a + b$ y de $c + d$ entre m , así que $(a + b) \bmod m = (c + d) \bmod m = r + r'$. Si $r + r' \geq |m|$, entonces por el Corolario 1.1 —aplicado a $r + r'$ y a m , que puede ser negativo— existen q^* y r^* con $r + r' = mq^* + r^*$ y $0 \leq r^* < |m|$; sustituyendo,

$$a + b = m(q_1 + q_3 + q^*) + r^*, \quad c + d = m(q_2 + q_4 + q^*) + r^*,$$

así que $(a + b) \bmod m = (c + d) \bmod m = r^*$.

2. Operando,

$$ab = (mq_1 + r)(mq_3 + r') = m^2q_1q_3 + mq_1r' + mq_3r + rr' = mk + rr',$$

$$cd = (mq_2 + r)(mq_4 + r') = m^2q_2q_4 + mq_2r' + mq_4r + rr' = mk' + rr',$$

donde $k = mq_1q_3 + q_1r' + q_3r$ y $k' = mq_2q_4 + q_2r' + q_4r$. Razonando sobre rr' exactamente igual que en el apartado 1 —dividiendo rr' entre m si hiciera falta—, se concluye $(ab) \bmod m = (cd) \bmod m$. ■

Lo que sí puedes hacer, y lo que no

No se puede cancelar un factor común sin más. $(2 \cdot 3) \bmod 4 = 6 \bmod 4 = 2$ y $(2 \cdot 1) \bmod 4 = 2 \bmod 4 = 2$: coinciden. Pero $3 \bmod 4 = 3$ y $1 \bmod 4 = 1$ no coinciden. Es decir, $(ac) \bmod m = (bc) \bmod m$ **no** permite concluir $a \bmod m = b \bmod m$, aunque la Proposición sí te deje ir en la otra dirección (de $a \bmod m = b \bmod m$ a multiplicar ambos por c). Cuándo sí se puede cancelar es algo que aprenderás en la Sección 1-5, y la respuesta pasa —cómo no— por el máximo común divisor.

Tampoco se reducen los exponentes. La Proposición habla de sumar y multiplicar, no de elevar a una potencia *variable*. Por ejemplo, $2^{10} \bmod 7 = 1024 \bmod 7 = 2$, mientras que $2^{(10 \bmod 7)} \bmod 7 = 2^3 \bmod 7 = 1$: son distintos. Lo que sí puedes reducir, y con toda tranquilidad, es la *base*: $2^{10} = (2 \bmod 7)^{10} \bmod 7$ sigue valiendo, porque eso es aplicar la propiedad 2 varias veces seguidas sobre el mismo factor. Reducir la base es gratis; reducir el exponente, no —al menos, no todavía.

Con esta propiedad de compatibilidad ya puedes atacar un tipo de problema que vas a ver una y otra vez: demostrar que *ningún* entero cumple tal cosa, agotando los restos posibles.

✎ Ejemplo 1.9 — Tres enteros consecutivos y un múltiplo de 3

Demuéstrese que, dado un entero a , alguno de los números a , $a + 1$ o $a + 2$ es múltiplo de 3.

Demostración. $a \bmod 3$ solo puede ser 0, 1 o 2.

- Si $a \bmod 3 = 0$, entonces $a = 3q$, y a es múltiplo de 3.

- Si $a \bmod 3 = 1$, entonces $a = 3q + 1$, así que $a + 2 = 3q + 3 = 3(q + 1)$, y $a + 2$ es múltiplo de 3.
- Si $a \bmod 3 = 2$, entonces $a = 3q + 2$, así que $a + 1 = 3q + 3 = 3(q + 1)$, y $a + 1$ es múltiplo de 3.

En particular, hemos demostrado algo un poco más fuerte: de tres enteros consecutivos cualesquiera, uno y solo uno es múltiplo de 3 —basta tomar como a el menor de los tres. ■

Ejemplo 1.10 — Ningún $n^2 + 1$ es múltiplo de 7

Demuéstrese que, para ningún entero n , el número $n^2 + 1$ es múltiplo de 7.

Demostración. Supongamos, para llegar a una contradicción, que $n^2 + 1$ es múltiplo de 7 para algún n ; es decir, $n^2 + 1 = 7q$, así que $n^2 = 7(q - 1) + 6$, o lo que es lo mismo, $n^2 \bmod 7 = 6$. Por la Proposición 1.3 aplicada a $n \cdot n$, y usando que $n \bmod 7 = n \bmod 7$ trivialmente, se tiene $n^2 \bmod 7 = (n \bmod 7)^2 \bmod 7$. Así que basta comprobar los siete restos posibles de $n \bmod 7$, elevarlos al cuadrado y reducir otra vez módulo 7, y ver que el 6 no aparece nunca:

$$0^2 \bmod 7 = 0, \quad 1^2 \bmod 7 = 1, \quad 2^2 \bmod 7 = 4, \quad 3^2 \bmod 7 = 2,$$

$$4^2 \bmod 7 = 2, \quad 5^2 \bmod 7 = 4, \quad 6^2 \bmod 7 = 1.$$

Como 6 no está entre los valores posibles, ningún $n^2 + 1$ es múltiplo de 7. ■

Lo esencial de este bloque

- El operador $a \bmod b$ no es más que el resto del Algoritmo de la División, con nombre propio. No lo confundas con la relación de congruencia $a \equiv b \pmod{m}$ que verás en la Sección 1-5: una es un número, la otra una afirmación.
- Su propiedad clave es la *compatibilidad*: puedes sustituir un número por otro que deje el mismo resto antes de sumar o multiplicar, y llegar al mismo resultado. Es lo que te permite trabajar con números pequeños en vez de gigantescos.
- Dos límites de esa propiedad que no debes olvidar: no se pueden cancelar factores comunes sin más hipótesis, y no se pueden reducir exponentes variables —solo la base.
- La disección por restos, ya conocida del bloque anterior, se combina de maravilla con el operador MOD: agotar los restos posibles de $n \bmod m$ basta para descartar una propiedad para *todo* entero.

1.5 Máximo común divisor e Identidad de Bézout

Tienes ya todas las piezas —divisibilidad, valor absoluto, el Algoritmo de la División— para el resultado que da sentido a todo lo que hemos construido hasta ahora. Vamos a definir el máximo común divisor, y vamos a demostrar algo que a primera vista parece un capricho: que ese máximo común divisor siempre puede escribirse como $ax+by$, una combinación lineal de a y b con coeficientes enteros. No es un capricho. Es la propiedad que vas a usar para resolver ecuaciones diofánticas, para invertir números módulo m , y —dentro de dos bloques— para calcular el propio máximo común divisor con el Algoritmo de Euclides.

Antes de la definición formal merece la pena preguntarse algo que casi nunca se pregunta: ¿por qué tendría que existir «el» máximo común divisor de dos enteros? La respuesta corta es más sencilla de lo que esperarías, aunque no cuenta toda la historia. El 1 divide a cualquier entero, así que el conjunto de divisores comunes de a y b nunca es vacío. Y si, por ejemplo, $a \neq 0$, todo divisor común d cumple $d \mid a$ con $d \neq 0$ y $a \neq 0$, así que por la propiedad 5 de la Proposición 1.2, $|d| \leq |a|$: solo hay un número finito de enteros candidatos. Un conjunto finito y no vacío de enteros positivos tiene máximo, así que «el mayor divisor común», en el sentido numérico, siempre existe.

Pero fíjate en lo que *no* hemos probado: que ese máximo numérico sea, además, divisible por **todos** los demás divisores comunes. Esa propiedad más fuerte —no solo ser el mayor, sino que todos los demás lo dividan— es la que de verdad importa, y es la que exige la definición formal.

Definición 1.4 — Divisor común y máximo común divisor

Sean $a, b \in \mathbb{Z}$. Un entero $d \neq 0$ es un *divisor común* de a y b si $d \mid a$ y $d \mid b$. Un divisor común d de a y b es el *máximo común divisor* de a y b —y se denota $\text{m.c.d.}(a, b)$ — si $d > 0$ y todo divisor común de a y b divide también a d . Por convenio, $\text{m.c.d.}(0, 0) = 0$.

«Máximo», con matiz

La condición que de verdad define $d = \text{m.c.d.}(a, b)$ no es «ser el mayor número» sino «ser divisible por todos los demás divisores comunes». Ambas nociones de máximo coinciden, pero solo la segunda es la que se usa en las demostraciones —fíjate bien en cuál invocas cada vez.

Ejemplo 1.11 — Cálculo de m.c.d. por listado de divisores

- a) Los divisores de 8 son $\pm 1, \pm 2, \pm 4, \pm 8$; los de 6 son $\pm 1, \pm 2, \pm 3, \pm 6$. Los divisores comunes son $\pm 1, \pm 2$, así que $\text{m.c.d.}(6, 8) = 2$.
- b) Si $a \in \mathbb{Z}$ y $a \neq 0$, entonces $\text{m.c.d.}(a, 0) = |a|$.
- c) Los divisores de -21 son $\pm 1, \pm 3, \pm 7, \pm 21$; los de 12 son $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$. El mayor divisor común es 3, así que $\text{m.c.d.}(-21, 12) = 3$.

Definición 1.5 — Máximo común divisor de n enteros

Sean $a_1, a_2, \dots, a_n$ enteros. Llamaremos *máximo común divisor* de $a_1, \dots, a_n$ al divisor común $d > 0$ tal que cualquier otro divisor común de $a_1, \dots, a_n$ divide también a d . Se denota $\text{m.c.d.}(a_1, \dots, a_n)$.

Vale la pena detenerse un momento en el apartado c) del Ejemplo 1.11. Observa que $-21 \cdot 1 + 12 \cdot 2 = 3 = \text{m.c.d.}(-21, 12)$. Y si calculas $\text{m.c.d.}(-30, 50)$ por el mismo método de listar divisores obtienes 10, que también se deja escribir como combinación lineal: $50 \cdot 2 + (-30) \cdot 3 = 10$. Dos

casos particulares no demuestran nada, pero sí sugieren una pregunta: ¿será verdad *siempre* que el máximo común divisor de a y b se puede escribir como $ax + by$? El siguiente teorema contesta que sí —y de paso resuelve, sin que lo hayamos pedido, la pregunta que dejamos abierta hace un momento: que ese máximo numérico es divisible por todos los demás divisores comunes.

Teorema 1.2 — Identidad de Bézout

Sean a y b enteros distintos de 0. Existe un único d máximo común divisor de a y b . Además, d es el entero positivo más pequeño que puede expresarse en la forma $ax + by$, con $x, y \in \mathbb{Z}$.

Buen Orden, otra vez

Esta es la segunda de las tres veces que el Buen Orden hace el trabajo pesado en este tema: ya lo usaste para el Algoritmo de la División, y lo volverás a usar para que el Algoritmo de Euclides termine. El patrón es siempre el mismo: tomar el mínimo de un conjunto bien elegido.

Demostración.

Veamos primero que d existe, y después que es único.

Existencia. Sea $M = \{ax + by > 0 : x, y \in \mathbb{Z}\}$, el conjunto de las combinaciones lineales positivas de a y b . El conjunto M no es vacío, ya que $|a| = (\pm 1)a + 0b \in M$ (con el signo adecuado según el de a). Por el Principio del Buen Orden, M tiene un elemento mínimo; llamémoslo d . Como $d \in M$, existen $x_1, y_1 \in \mathbb{Z}$ tales que $d = ax_1 + by_1$.

Veamos que $d \mid a$. Supongamos que no; entonces, por el Algoritmo de la División, existen q, r con $a = dq + r$ y $0 < r < d$ (nótese $r \neq 0$, precisamente porque $d \nmid a$). Así pues,

$$r = a - dq = a - (ax_1 + by_1)q = a(1 - x_1q) + b(-y_1q),$$

así que r es una combinación lineal de a y b ; y como $r > 0$, se tiene $r \in M$. Pero $r < d$, lo que contradice que d sea el mínimo de M . Por tanto $d \mid a$. Un argumento completamente análogo, cambiando a por b , prueba que $d \mid b$.

Veamos ahora que d es efectivamente el máximo común divisor. Sea d' cualquier otro divisor común de a y b ; entonces $a = d'p_1$ y $b = d'p_2$ para ciertos $p_1, p_2 \in \mathbb{Z}$. Sustituyendo,

$$d = ax_1 + by_1 = d'p_1x_1 + d'p_2y_1 = d'(p_1x_1 + p_2y_1),$$

así que $d' \mid d$. Junto con $d > 0$, esto es exactamente la Definición 1.4.

Unicidad. Supongamos que d_1 y d_2 son ambos máximo común divisor de a y b . Por la Definición 1.4 aplicada a cada uno, $d_1 \mid d_2$ y $d_2 \mid d_1$; y como $d_1, d_2 \neq 0$, la propiedad 5 de la Proposición 1.2 da $|d_1| \leq |d_2|$ y $|d_2| \leq |d_1|$, es decir $|d_1| = |d_2|$. Como además $d_1 > 0$ y $d_2 > 0$ por definición, se concluye $d_1 = d_2$. ■

El recíproco de Bézout es falso

El Teorema dice que el mínimo positivo de $\{ax + by\}$ es el máximo común divisor. No dice que *cualquier* combinación lineal positiva lo sea. Por ejemplo, $2 = 2 \cdot 1 + 3 \cdot 0$ es una combinación lineal de 2 y 3, y sin embargo $\text{m.c.d.}(2, 3) = 1 \neq 2$. Antes de afirmar que un número es un máximo común divisor solo porque lo has escrito como $ax + by$, comprueba que además es divisor de a y de b —o, mejor aún, que es el *menor* positivo de esa forma. Esta es, con diferencia, la trampa más frecuente en los exámenes sobre este tema.

Corolario 1.2 — Coprimalidad y Bézout

Sean a y b enteros distintos de 0. Entonces $\text{m.c.d.}(a, b) = 1$ si y solo si existen enteros s, t tales que $as + bt = 1$.

La herramienta del resto del tema

Este Corolario es el que vas a invocar constantemente de aquí en adelante: para resolver ecuaciones diofánticas, para decidir cuándo un número tiene inverso módulo m , y para demostrar el Teorema Chino del Resto en la Sección 1-5.

Demostración.

($\Rightarrow$) Si $\text{m.c.d.}(a, b) = 1$, entonces $d = 1$ es, por el Teorema 1.2, el menor entero positivo de la forma $ax + by$; en particular, es *alguna* de esa forma, así que existen s, t con $as + bt = 1$.

($\Leftarrow$) Supongamos que $as + bt = 1$ para ciertos $s, t \in \mathbb{Z}$. Sea c un divisor común cualquiera de a y b . Por la propiedad 6 de la Proposición 1.1, $c \mid (as + bt)$, es decir $c \mid 1$; por tanto $c = \pm 1$. Así pues, el único divisor común positivo de a y b es 1, y en consecuencia $\text{m.c.d.}(a, b) = 1$. ■

Ejemplo 1.12 — Coprimalidad y producto

Demuéstrese que si $\text{m.c.d.}(a, b) = 1$ y $\text{m.c.d.}(a, c) = 1$, entonces $\text{m.c.d.}(a, bc) = 1$.

Demostración. Por el Corolario 1.2, existen $s, t, s', t' \in \mathbb{Z}$ tales que

$$1 = as + bt, \quad 1 = as' + ct'.$$

Multiplicando ambas igualdades,

$$1 = (as + bt)(as' + ct') = a(ass' + cst' + bts') + bc(tt').$$

Llamando $s'' = ass' + cst' + bts'$ y $t'' = tt'$, tenemos $1 = as'' + (bc)t''$, así que, otra vez por el Corolario 1.2 —ahora aplicado a a y bc —, se concluye $\text{m.c.d.}(a, bc) = 1$. ■

Lo esencial de este bloque

- El máximo común divisor $\text{m.c.d.}(a, b)$ no se define como «el mayor divisor común» sin más, sino como el divisor común que es, además, divisible por todos los demás. Que ambas nociones coincidan es parte de lo que demuestra la Identidad de Bézout.
- La Identidad de Bézout es el segundo de los tres resultados centrales del tema: $\text{m.c.d.}(a, b)$ existe, es único, y es el menor entero positivo de la forma $ax + by$. Su demostración es, otra vez, el mínimo de un conjunto bien elegido —el Buen Orden aplicado a las combinaciones lineales positivas.
- Cuidado con el recíproco: que $d = ax + by$ no implica que d sea el máximo común divisor.
- El Corolario — $\text{m.c.d.}(a, b) = 1 \iff \exists s, t : as + bt = 1$ — es la herramienta que más vas a usar de aquí en adelante, dentro y fuera de esta Sección.

1.6 El Algoritmo de Euclides

La Identidad de Bézout te ha dicho que $\text{m.c.d.}(a, b)$ existe y que se puede escribir como $ax + by$. Lo que no te ha dicho es *cómo calcularlo*. El método del Ejemplo 1.11 —listar todos los divisores de a y de b — funciona, pero se vuelve inviable en cuanto los números crecen un poco. Vamos a ver un método muchísimo más eficiente, que además, como subproducto, te va a dar los coeficientes x e y de Bézout sin tener que adivinarlos.

💡 Motivación

El método que viene a continuación se llama Algoritmo de Euclides porque aparece desarrollado en el Libro VII de los *Elementos*. De Euclides, matemático griego del siglo III a.C., apenas se sabe nada aparte de que vivió en Alejandría; sin embargo, los *Elementos* recopilaron el saber de Geometría y Teoría de Números de su época, y se usaron como libro de texto hasta comienzos del siglo XX. Euclides partió de un conjunto de definiciones y axiomas explícitos —el mismo método que, con otro lenguaje, estás aprendiendo tú en este tema— y ese estilo ha servido de modelo a los matemáticos desde entonces.

Antes de enunciar el algoritmo necesitamos dos resultados previos, que juntos dicen algo muy simple: dividir no cambia el máximo común divisor, solo lo traslada a números más pequeños.

Proposición 1.4 — Divisores comunes de una división

Dados dos enteros a y b , con $b \neq 0$, y sea r el resto de dividir a entre b . Entonces:

1. Los divisores comunes de a y b son divisores de r .
2. Los divisores comunes de b y r son divisores de a .

Demostración. Sea $a = bq + r$. Sea c un divisor común de a y b ; entonces $a = cq_1$ y $b = cq_2$ para ciertos $q_1, q_2 \in \mathbb{Z}$. Sustituyendo, $cq_1 = cq_2q + r$, de donde $r = c(q_1 - q_2q)$; así pues $c \mid r$, lo que prueba 1.

Supongamos ahora que $c \mid b$ y $c \mid r$; entonces $b = cq'_1$ y $r = cq'_2$ para ciertos q'_1, q'_2 . Sustituyendo en $a = bq + r$, $a = cq'_1q + cq'_2 = c(q'_1q + q'_2)$, así que $c \mid a$, lo que prueba 2. ■

Teorema 1.3 — El m.c.d. del dividendo y del divisor es el del divisor y el resto

Sean $a, b \in \mathbb{Z}$, $b \neq 0$, y sea r el resto de dividir a entre b . Entonces

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

El invariante

Este Teorema es el corazón del método: al pasar de (a, b) a (b, r) , el máximo común divisor **no cambia**, pero los números sí se hacen más pequeños ($r < b$). Repetir esto una y otra vez es todo el Algoritmo de Euclides.

Demostración. Por la Proposición 1.4, los divisores comunes de a y b son exactamente los mismos que los divisores comunes de b y r —el mismo conjunto—. Dos pares con el mismo conjunto de divisores comunes tienen, en particular, el mismo máximo común divisor. ■

Con esto ya tenemos todo lo necesario. La idea es repetir el Teorema anterior las veces que haga falta: de (a, b) pasamos a (b, r_1) , de ahí a (r_1, r_2) , y así sucesivamente, sin que el máximo

común divisor cambie nunca, hasta que uno de los dos números sea 0 —momento en el que el máximo común divisor es, simplemente, el otro número—.

Teorema 1.4 — Algoritmo de Euclides

Sean $a, b \in \mathbb{Z}$, no ambos nulos. Como $\text{m.c.d.}(a, b) = \text{m.c.d.}(|a|, |b|)$, podemos suponer sin pérdida de generalidad que $a \geq b > 0$. Se dividen sucesivamente:

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b;$$

$$b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1 \quad (\text{si } r_1 \neq 0);$$

$$r_1 = r_2q_3 + r_3, \quad 0 \leq r_3 < r_2 \quad (\text{si } r_2 \neq 0);$$

y así sucesivamente. El proceso termina en un número finito de pasos, y $\text{m.c.d.}(a, b)$ es el último resto no nulo de la sucesión.

Buen Orden, la tercera y última vez

Esta es la tercera y última de las apariciones del Buen Orden en este tema: garantiza que los restos, siendo naturales y estrictamente decrecientes, no pueden bajar para siempre. Ya lo viste en el Algoritmo de la División y en la Identidad de Bézout: es, con diferencia, el principio que más trabajo hace en toda la Sección.

Demostración. Corrección. Si $r_1 = 0$, entonces $a = bq_1$, así que $b \mid a$, y $\text{m.c.d.}(a, b) = b$. Si $r_1 \neq 0$, por el Teorema 1.3 aplicado a a y b , $\text{m.c.d.}(a, b) = \text{m.c.d.}(b, r_1)$. Si a su vez $r_2 = 0$, entonces $\text{m.c.d.}(b, r_1) = r_1$ y hemos terminado; si no, aplicamos otra vez el mismo Teorema a b y r_1 , y obtenemos $\text{m.c.d.}(b, r_1) = \text{m.c.d.}(r_1, r_2)$. Repitiendo este argumento,

$$\text{m.c.d.}(a, b) = \text{m.c.d.}(b, r_1) = \text{m.c.d.}(r_1, r_2) = \text{m.c.d.}(r_2, r_3) = \dots,$$

en cada paso con el mismo máximo común divisor, hasta llegar a un resto nulo.

Terminación. Los restos sucesivos forman una cadena

$$b > r_1 > r_2 > r_3 > \dots \geq 0$$

de números naturales estrictamente decreciente. Por el Principio del Buen Orden, no puede existir una sucesión infinita estrictamente decreciente de enteros no negativos —si el conjunto $\{b, r_1, r_2, \dots\}$ fuera infinito, no tendría mínimo, ya que para cualquier candidato a mínimo el siguiente resto sería todavía menor—. Así pues, en algún paso n se alcanza $r_n = 0$, y por la parte de corrección, $\text{m.c.d.}(a, b) = r_{n-1}$, el último resto no nulo. ■

Nada aclara más un algoritmo que verlo funcionar. Los tres ejemplos que siguen van de menos a más: cálculo directo, cálculo con los coeficientes de Bézout, y un caso con bastantes más pasos de los habituales.

Ejemplo 1.13 — Cálculo directo

Calcúlese $\text{m.c.d.}(280, 30)$.

Demostración. Dividiendo 280 entre 30: $280 = 30 \cdot 9 + 10$, con $r_1 = 10 \neq 0$. Dividiendo 30 entre 10: $30 = 10 \cdot 3 + 0$, con $r_2 = 0$. Por tanto, $\text{m.c.d.}(280, 30) = \text{m.c.d.}(30, 10) = 10$. ■

Ejemplo 1.14 — Euclides extendido

Calcúlese $d = \text{m.c.d.}(3120, 270)$ y encuéntrase $x, y \in \mathbb{Z}$ tales que $d = 3120x + 270y$.

Demostración. Dividiendo sucesivamente,

$$3120 = 270 \cdot 11 + 150, \quad r_1 = 150 \neq 0; \quad (\text{i})$$

$$270 = 150 \cdot 1 + 120, \quad r_2 = 120 \neq 0; \quad (\text{ii})$$

$$150 = 120 \cdot 1 + 30, \quad r_3 = 30 \neq 0; \quad (\text{iii})$$

$$120 = 30 \cdot 4 + 0, \quad r_4 = 0. \quad (\text{iv})$$

Así pues, $d = \text{m.c.d.}(3120, 270) = r_3 = 30$.

Para los coeficientes de Bézout, deshacemos los pasos. De (iii), $30 = 150 - 120 \cdot 1$. Despejando 120 de (ii) —es decir, $120 = 270 - 150 \cdot 1$ — y sustituyendo,

$$30 = 150 - (270 - 150 \cdot 1) = 150 \cdot 2 - 270.$$

Despejando ahora 150 de (i) —es decir, $150 = 3120 - 270 \cdot 11$ — y sustituyendo,

$$30 = (3120 - 270 \cdot 11) \cdot 2 - 270 = 3120 \cdot 2 + 270 \cdot (-23).$$

Por tanto, $x = 2$ e $y = -23$. ■

Una tabla en vez de sustituciones hacia atrás

Deshacer los pasos a mano, como acabamos de hacer, es la fuente de error de signo más frecuente de todo el tema. Una alternativa más segura es arrastrar los coeficientes *hacia delante*: cada fila mantiene la identidad $r_i = 3120 s_i + 270 t_i$, y se calcula con $r_{i+1} = r_{i-1} - q_i r_i$, igual para s y para t .

i	r_i	q_i	s_i	t_i
0	3120	—	1	0
1	270	11	0	1
2	150	1	1	-11
3	120	1	-1	12
4	30	4	2	-23
5	0			

La tabla se autocomprueba en cada fila: basta verificar que $r_i = 3120 s_i + 270 t_i$. Y el resultado, claro, es el mismo que por sustitución hacia atrás: $d = 30$, $x = 2$, $y = -23$.

Ejemplo 1.15 — Un caso con más pasos de lo habitual

Hállese $\text{m.c.d.}(12384, 4720)$.

Demostración.

$$\begin{aligned}
 12384 &= 4720 \cdot 2 + 2944, & r_1 &= 2944, & 4720 &= 2944 \cdot 1 + 1776, & r_2 &= 1776, \\
 2944 &= 1776 \cdot 1 + 1168, & r_3 &= 1168, & 1776 &= 1168 \cdot 1 + 608, & r_4 &= 608, \\
 1168 &= 608 \cdot 1 + 560, & r_5 &= 560, & 608 &= 560 \cdot 1 + 48, & r_6 &= 48, \\
 560 &= 48 \cdot 11 + 32, & r_7 &= 32, & 48 &= 32 \cdot 1 + 16, & r_8 &= 16, \\
 32 &= 16 \cdot 2 + 0, & r_9 &= 0.
 \end{aligned}$$

Por tanto, $\text{m.c.d.}(12384, 4720) = r_8 = 16$. ■

¿Cuántos pasos hacen falta como mucho?

El matemático francés Gabriel Lamé (1795–1870) demostró que el número de divisiones que exige el Algoritmo de Euclides nunca supera cinco veces el número de cifras del menor de los dos números. En el ejemplo anterior, 4720 tiene cuatro cifras, así que hacían falta como mucho 20 divisiones —y solo se han necesitado 9—.

La cota de Lamé es, además, ajustada: para cada número natural n existen enteros a_n, b_n para los que el algoritmo necesita *exactamente* n divisiones, y el peor caso posible son dos términos consecutivos de la sucesión de Fibonacci. Por ejemplo, $\text{m.c.d.}(89, 55)$ necesita 9 divisiones —en todas ellas, salvo la última, el cociente es 1—, y 89, 55 son los términos octavo y séptimo de Fibonacci. No es casualidad: es la razón por la que el Algoritmo de Euclides sigue siendo, hoy, la base de la aritmética con enteros de cientos de cifras en criptografía.

Cerramos el bloque —y la Sección— con una propiedad de escalado del máximo común divisor, y tres aplicaciones que la ponen a prueba.

Teorema 1.5 — Escalado del m.c.d.

Si $k > 0$, entonces $\text{m.c.d.}(ka, kb) = k \cdot \text{m.c.d.}(a, b)$.

Demostración. Dividiendo ka entre kb : $ka = (kb)q_1 + r$ con $0 \leq r < kb$. Entonces $r = ka - kbq_1 = k(a - bq_1)$, así que $k \mid r$, y podemos escribir $r = kr_1$ con $0 \leq r_1 < b$; es decir,

$$ka = (kb)q_1 + kr_1, \quad 0 \leq r_1 < b.$$

Esta es exactamente la primera división del Algoritmo de Euclides aplicado a a y b , multiplicada por k . Repitiendo el argumento sobre kb y kr_1 —y, en general, en cada paso siguiente—, el Algoritmo de Euclides aplicado a ka y kb reproduce paso a paso el aplicado a a y b , con cada igualdad multiplicada por k . En particular, ambos procesos terminan en el mismo número de pasos, y el último resto no nulo de uno es k veces el del otro:

$$kr_{n-1} = (kr_n)q_{n+1} + 0.$$

Por tanto, $\text{m.c.d.}(ka, kb) = k \cdot \text{m.c.d.}(a, b)$. ■

Una demostración por repetición es, en el fondo, una inducción

El argumento anterior —«repitiendo el proceso»— es intuitivamente convincente, pero fíjate en que es, en realidad, una inducción encubierta sobre el número de pasos del algoritmo, del tipo que formalizarás en la Sección 1-3. Si quieres un reto: existe también una demostración de este mismo Teorema a partir de la Identidad de Bézout, sin apoyarse en «repetir pasos» en absoluto. Inténtalo antes de seguir leyendo.

Corolario 1.3 — Escalado del m.c.d., con k de cualquier signo

Para cada entero $k \neq 0$, $\text{m.c.d.}(ka, kb) = |k| \cdot \text{m.c.d.}(a, b)$.

Demostración. Si $k > 0$, es el Teorema 1.5. Si $k < 0$, entonces $-k > 0$, y como $\text{m.c.d.}(x, y) = \text{m.c.d.}(|x|, |y|)$ para cualesquiera x, y —el máximo común divisor solo depende de los divisores, y x y $-x$ tienen los mismos—, se tiene $\text{m.c.d.}(ka, kb) = \text{m.c.d.}(-ka, -kb)$. Aplicando el Teorema 1.5 a $-k > 0$, $\text{m.c.d.}(-ka, -kb) = (-k) \cdot \text{m.c.d.}(a, b)$. Como $k < 0$, $-k = |k|$, y así $\text{m.c.d.}(ka, kb) = |k| \cdot \text{m.c.d.}(a, b)$. ■

✎ Ejemplo 1.16 — Aprovechar un divisor común evidente

Calcúlese $\text{m.c.d.}(36, 90)$.

Demostración. Por simple inspección, $18 \mid 36$ y $18 \mid 90$: en efecto, $36 = 18 \cdot 2$ y $90 = 18 \cdot 5$. Por el Teorema 1.5,

$$\text{m.c.d.}(36, 90) = \text{m.c.d.}(18 \cdot 2, 18 \cdot 5) = 18 \cdot \text{m.c.d.}(2, 5) = 18 \cdot 1 = 18.$$

■

✎ Ejemplo 1.17 — Suma y diferencia de coprimos

Demuéstrese que si $\text{m.c.d.}(a, b) = 1$, entonces $\text{m.c.d.}(a + b, a - b) = 1$ o 2 .

Demostración. Sea $d = \text{m.c.d.}(a + b, a - b)$. Entonces $d \mid (a + b)$ y $d \mid (a - b)$, así que, por la propiedad 6 de la Proposición 1.1, d divide a $(a + b) + (a - b) = 2a$ y a $(a + b) - (a - b) = 2b$. Por tanto, d divide a cualquier divisor común de $2a$ y $2b$, en particular a $\text{m.c.d.}(2a, 2b)$, que por el Teorema 1.5 vale $2 \cdot \text{m.c.d.}(a, b) = 2$. Como $d \mid 2$ y $d > 0$, se concluye $d = 1$ o $d = 2$. ■

✎ Ejemplo 1.18 — Reducción a coprimos

Demuéstrese que $d = \text{m.c.d.}(a, b)$ si y solo si $d \mid a$, $d \mid b$ y $\text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Demostración. ($\Rightarrow$) Sea $d = \text{m.c.d.}(a, b)$. Como $d \mid a$ y $d \mid b$, podemos escribir $a = d \cdot \frac{a}{d}$ y $b = d \cdot \frac{b}{d}$, con $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$. Por el Corolario 1.3,

$$d = \text{m.c.d.}(a, b) = \text{m.c.d.}\left(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}\right) = d \cdot \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right),$$

y como $d \neq 0$, se sigue $\text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

($\Leftarrow$) Supongamos $d \mid a$, $d \mid b$ y $\text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Por el mismo Corolario,

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

■

Lo esencial de este bloque

- El Algoritmo de Euclides calcula $\text{m.c.d.}(a, b)$ dividiendo sucesivamente: el máximo común divisor es el último resto no nulo. Su corrección se apoya en que dividir no cambia el máximo común divisor ($\text{m.c.d.}(a, b) = \text{m.c.d.}(b, r)$); su terminación, en que los restos forman una sucesión decreciente de naturales —el Buen Orden, por tercera y última vez en este tema.
- Deshacer los pasos del algoritmo da los coeficientes de Bézout. La sustitución hacia atrás es propensa a errores de signo; la tabla hacia delante es una alternativa más segura y autocomprobable.
- La cota de Lamé —a lo sumo cinco divisiones por cada cifra del menor número— explica por qué el algoritmo sigue siendo práctico con números de cientos de cifras, y el peor caso son números de Fibonacci consecutivos.
- El máximo común divisor escala: $\text{m.c.d.}(ka, kb) = |k| \cdot \text{m.c.d.}(a, b)$. Combinado con la Identidad de Bézout, permite reducir cualquier problema sobre a, b a uno sobre $a/d, b/d$, que son coprimos.

Con esto termina la Sección 1-1 al completo. Has recorrido el camino entero: de la definición más elemental de divisibilidad a los tres resultados que sostienen toda la Teoría de Números que viene después —el Algoritmo de la División, la Identidad de Bézout y el Algoritmo de Euclides—, los tres contruidos, en el fondo, con la misma herramienta: el mínimo de un conjunto bien elegido.