La aritmética de los enteros

Ingeniería informática Curso: Álgebra

Fernando Chamizo https://matematicas.uam.es/~fernando.chamizo/

Comentarios

Trataremos ahora a temas mucho menos abstractos que recuerdan a la etapa escolar. Por supuesto, el enfoque será nuevo. Un gran protagonista es el algoritmo de Euclides que ocupa un papel muy relevante en muchas aplicaciones, sobre todo a la criptografía.

1. Divisibilidad

Ya hemos empleado en ejemplos anteriores implícitamente la noción de divisibilidad. Recordemos su significado: Dados $a \in \mathbb{Z}$ y $d \in \mathbb{Z}\setminus\{0\}$ decimos que d *divide* a a o que a es *múltiplo* de d o que d es *divisor* de a, si existe $q \in \mathbb{Z}$ tal que $a = dq$. También ha aparecido antes la notación básica al uso: se escribe $d \mid a$ para indicar que d divide a a. Para practicar con los símbolos, el significado de esta notación se resume en la expresión sintética

$$d \mid a \iff \exists q \in \mathbb{Z} \,:\, a = qd.$$

Se suele negar $d \mid a$ con $d \nmid a$. Por ejemplo, $7 \mid 21$, $-8 \mid 65536$, $7 \nmid 22$, $8 \nmid 1$. Según la definición, cualquier $d \in \mathbb{Z}\setminus\{0\}$ divide a 0, fuera de ese caso caso especial $|d| \le |a|$ cuando d divide a $a \in \mathbb{Z}\setminus\{0\}$, donde las barras indican el *valor absoluto* (el número sin signo).

A pesar de que no siempre podemos dividir en $\mathbb{Z}\setminus\{0\}$, sí que lo podemos hacer si admitimos una cantidad sobrante pequeña. El *teorema de la división* (o *lema de la división euclídea*) es un resultado básico que concreta esa afirmación:

> **Teorema de la división.** *Dados $a \in \mathbb{Z}$ y $b \in \mathbb{Z}\setminus\{0\}$ existen unos únicos números enteros q y r, llamados* cociente *y* resto*, respectivamente, tales que*
>
> $$a = bq + r \qquad y \qquad 0 \le r < |b|.$$

Por supuesto, $b \mid a$ si y solo si $r = 0$. La única diferencia con lo que sabes desde niño es que ahora también admitimos números negativos. Como indica el resultado, la política al respecto

es que el resto siempre debe ser mayor o igual que cero. Recuerda que en los cursos elementales se decía que a era el *dividendo* (lo que se va a dividir) y b el *divisor* (por lo que se divide).

Ejemplo. Calcular el cociente y el resto al dividir 17 y -17 entre -5.

En el primer caso, $17 = (-5)\cdot(-3)+2$ implica que el cociente y el resto son -3 y 2. En el segundo caso, $-17 = (-5)\cdot 4 + 3$ de modo que el cociente y el resto son 4 y 3.

Para la demostración de la existencia del cociente y el resto se introduce el conjunto

$$C = \{a - bq \,:\, q \in \mathbb{Z} \wedge a - bq \geq 0\}.$$

Nos limitamos a $b > 0$, el caso negativo es similar (ejercicio) porque $bq = (-b)(-q)$. Se tiene $C \neq \varnothing$ ya que, por ejemplo, $a - b\cdot 0 \in C$ si $a \geq 0$ y $a - b\cdot a \in C$ si $a < 0$. Sea r el menor elemento de C. Por definición, $r \geq 0$ y falta probar $r < b$. Procedemos por reducción al absurdo. Si $r = a - bq_0 > b$ entonces $r' = a - b(q_0+1) = r - b \geq 0$ también está en C, lo que contradice que r sea mínimo.

Ejemplo (Teórico). Demostrar la unicidad del cociente y el resto en el teorema de la división.

Digamos que $a = bq_1 + r_1$ y $a = bq_2 + r_2$ con $0 \leq r_1, r_2 < |b|$. Restando las igualdades se sigue $b(q_1 - q_2) = r_2 - r_1$. En particular, $b \mid r_1 - r_2$, pero como $|r_1 - r_2| < |b|$ esto solo puede darse si $r_1 = r_2$ que a su vez implica $q_1 = q_2$ empleando $b(q_1 - q_2) = r_1 - r_2$.

Un concepto estrechamente ligado a la divisibilidad es el *máximo común divisor* de dos enteros a y b no simultáneamente nulos que, como sugiere su nombre, se define como el mayor $d \in \mathbb{N}$ tal que $d \mid a$ y $d \mid b$. Usaremos la notación $d = \mathrm{mcd}(a,b)$. Cuando $\mathrm{mcd}(a,b) = 1$ se dice que a y b son *coprimos* o *primos entre sí*.

Nótese que se ha definido el máximo común divisor de forma que sea siempre positivo. En relación con esto, es insensible a cambios de signo de los argumentos:

$$\mathrm{mcd}(a,b) = \mathrm{mcd}(a,|b|) = \mathrm{mcd}(|a|,b) = \mathrm{mcd}(|a|,|b|).$$

Otras propiedades muy sencillas son $\mathrm{mcd}(a,b) = \mathrm{mcd}(b,a)$ y $\mathrm{mcd}(a,0) = \mathrm{mcd}(0,a) = |a|$. Dejamos sin definir $\mathrm{mcd}(0,0)$ ya que, en cierto modo es ∞ pues 0 es divisible por números arbitrariamente grandes.

Ejemplo. Explicar por qué $\mathrm{mcd}(-10,25) = 5$.

Si comprobamos los números del 1 al 10 veremos que los divisores positivos de -10 son 1, 2, 5 y 10. De ellos solo 1 y 5 dividen a 25. El máximo común divisor es 5 porque es el mayor de los dos.

Ligado también a la divisibilidad, pero con una importancia menor en el desarrollo de la teoría, se define el *mínimo común múltiplo* de $a, b \in \mathbb{Z}\setminus\{0\}$ como el menor $c \in \mathbb{N}$ tal que $a \mid c$ y $b \mid c$. Escribiremos $c = \mathrm{mcm}(a,b)$.

Existe una relación sencilla entre el máximo común divisor y el mínimo común múltiplo:

$$\operatorname{mcm}(a,b) = \frac{|a||b|}{\operatorname{mcd}(a,b)} \qquad \text{para} \quad a,b \in \mathbb{Z} \setminus \{0\}.$$

Más adelante veremos cómo se prueba. Una consecuencia directa es que si a y b son coprimos, entonces $\operatorname{mcm}(a,b) = |a||b|$.

Ejemplo. Calcular $\operatorname{mcm}(-10, 25)$.

Usando la fórmula y el ejemplo anterior, $\operatorname{mcm}(-10,25) = 10 \cdot 25/5 = 50$.

De nuevo, el mínimo común múltiplo es invariante frente a cambios de signo de sus argumentos.

2. El algoritmo de Euclides

Seguramente ya tienes una idea acerca de cómo calcular a mano $\operatorname{mcd}(a,b)$ cuando a y b son números naturales pequeños. Ahora vamos a ver un método que aparentemente es más largo y complicado. Para justificar esta paradoja hay que apelar a tu corazón de informático en ciernes. Si tratases de implementar el algoritmo que conoces sería ineficiente para números enormes. Concretamente, ningún ordenador imaginable podría calcular el máximo común divisor de números que ocupan cientos o miles de bits en memoria. Sin embargo, con el método que vas a aprender, en cualquier ordenador actual el cálculo lleva una fracción de segundo.

Este método maravilloso de muchos siglos de antigüedad (aparece en los *Elementos* de Euclides de cerca del 300 a. C., obra importantísima en la historia de las matemáticas) es el *algoritmo de Euclides* que consiste en la aplicación sucesiva de

$$r_{n-1} = r_n c_{n-1} + r_{n+1} \qquad \text{para} \quad 1 \le n \le N$$

partiendo de $r_0 = a$, $r_1 = b$ con $a, b \in \mathbb{Z} \setminus \{0\}$ y donde c_{n-1} y r_{n+1} son, respectivamente, el cociente y el resto al dividir r_{n-1} entre r_n. El algoritmo termina cuando $r_{N+1} = 0$ (no podríamos dividir por cero) y se tiene $r_N = \operatorname{mcd}(a,b)$.

Hay un caso excepcional muy tonto: Si $b \mid a$ entonces $N = 1$, en esta situación obviamente $\operatorname{mcd}(a,b) = |b|$ y $r_1 = b$ con lo que $r_1 = -\operatorname{mcd}(a,b)$ si $b < 0$.

Aunque el algoritmo suene lioso, en la práctica es mecánico y fácil de recordar.

Ejemplo. Calcular $\operatorname{mcd}(-24, 10)$ con el algoritmo de Euclides.

Sabemos que $\operatorname{mcd}(-24,10) = \operatorname{mcd}(24,10)$, aunque nada impide aplicar directamente el algoritmo de Euclides con a negativo. Los cálculos en este caso serían:

$$\begin{aligned}
n = 1 &\;\to\; -24 = 10 \cdot (-3) + 6 &&\to\; c_0 = -3,\ r_2 = 6 \\
n = 2 &\;\to\; 10 = 6 \cdot 1 + 4 &&\to\; c_1 = 1,\ r_3 = 4 \\
n = 3 &\;\to\; 6 = 4 \cdot 1 + 2 &&\to\; c_2 = 1,\ r_4 = 2 \\
N = n = 4 &\;\to\; 4 = 2 \cdot 2 + 0 &&\to\; c_3 = 2,\ r_5 = 0
\end{aligned}$$

El máximo común divisor buscado es $r_4 = 2$.

Incidiendo en un comentario anterior, ejemplos como este hacen poca propaganda de las virtudes del algoritmo de Euclides porque basta un momento de reflexión para convencerse de que $\mathrm{mcd}(-24, 10) = 2$ sin llevar a cabo prácticamente ninguna cuenta ya que los únicos divisores comunes de 24 y 10 son 1 y 2.

Practiquemos con otro ejemplo que sería mucho más difícil de hacer "de cabeza".

Ejemplo. Calcular $\mathrm{mcd}(9737, 1939)$ con el algoritmo de Euclides.

Esta vez solo indicaremos las cuentas del algoritmo en sí, sin recalcar los valores de n ni los cocientes y restos parciales:

$$\begin{aligned} 9737 &= 1939 \cdot 5 + 42, \\ 1939 &= 42 \cdot 46 + 7, \\ 42 &= 7 \cdot 6 + 0. \end{aligned}$$

Esta vez hemos terminado en $N = 3$ pasos. El máximo común divisor buscado es $r_3 = 7$, el último resto no nulo.

No utilizar la invariancia del máximo común divisor por cambios de signos en sus argumentos modifica los cálculos, incluso el número de pasos puede ser distinto.

Ejemplo. Calcular $\mathrm{mcd}(-3991, 1963)$ con el algoritmo de Euclides primero directamente y después usando que coincide con $\mathrm{mcd}(3991, 1963)$.

Las dos columnas siguientes recogen las dos versiones:

$$\begin{aligned} 3991 &= 1963 \cdot 2 + 65, \\ 1963 &= 65 \cdot 30 + 13, \\ 65 &= 13 \cdot 5 + 0; \end{aligned} \qquad \begin{aligned} -3991 &= 1963 \cdot (-3) + 1898, \\ 1963 &= 1898 \cdot 1 + 65, \\ 1898 &= 65 \cdot 29 + 13, \\ 65 &= 13 \cdot 5 + 0, \end{aligned}$$

De ambas maneras se obtiene que el máximo común divisor buscado es 13.

Comentario. Los ejemplos, aunque preparados, no hacen justicia a lo rápido que es el algoritmo de Euclies para números gigantescos. El número de pasos está acotado por cinco veces el número de dígitos (en base diez). De este modo, con el *software* adecuado, calcular el máximo común divisor de números con el tamaño mencionado al comienzo de este apartado es una trivialidad en un ordenador moderno.

Por el teorema de la división sabemos que en el algoritmo de Euclides $r_n > r_{n+1} \geq 0$ y, por tanto, el algoritmo termina, el N con $r_{N+1} = 0$ está bien definido. La pregunta natural es por qué $r_N = \mathrm{mcd}(a, b)$, en suma, por qué funciona el algoritmo. De nuevo la respuesta está en el teorema de la división, del cual es fácil deducir con su notación (ejercicio), $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r)$. Aplicando esta relación en cada paso del algoritmo de Euclides se sigue $\mathrm{mcd}(a, b) = \mathrm{mcd}(r_n, r_{n+1})$ y para $n = N$ se deduce $\mathrm{mcd}(a, b) = \mathrm{mcd}(r_N, 0) = r_N$.

3. Ecuaciones diofánticas lineales

Una de las aplicaciones matemáticas principales del algoritmo de Euclides es la resolución de ecuaciones lineales (de grado uno) en enteros. A este respecto, un resultado fundamental es el siguiente:

> **Identidad de Bézout.** *Dados $a, b \in \mathbb{Z}$ no simultáneamente nulos existen $x, y \in \mathbb{Z}$ tales que $ax + by = d$ con $d = \mathrm{mcd}(a, b)$.*

Comentario. Sorprendentemente, el matemático del siglo XVIII que da nombre al resultado no tiene demasiado que ver con él. Parece que la atribución deriva de que se le llamó así en un libro de álgebra del siglo XX que tuvo gran impacto.

La identidad de Bézout con este enunciado es un resultado de existencia. Por ejemplo, partiendo de $\mathrm{mcd}(168, 77) = 7$ permite concluir que la ecuación $168x + 77y = 7$ tiene alguna solución $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, pero no nos da pistas acerca de cómo calcularla. Es ahí donde entra el algoritmo de Euclides, que da una prueba constructiva de la identidad de Bézout indicando un método para encontrar una solución. En pocas palabras, se despeja d de la penúltima ecuación y se van sustituyendo las anteriores hasta que todo queda en función de a y b.

Con más detalle: Sabemos que $r_N = d$, por tanto, tomando $n = N - 1$ en la recurrencia, $r_{N-2}x_{N-2} + r_{N-1}y_{N-2} = d$ con $(x_{N-2}, y_{N-2}) = (1, -c_{N-2})$. Por otro lado, tomando $n = N - 2$ se puede expresar r_{N-1} en términos de r_{N-2} y r_{N-3} para obtener, sustituyendo, $r_{N-3}x_{N-3} + r_{N-2}y_{N-3} = d$ para ciertos $x_{N-3}, y_{N-3} \in \mathbb{Z}$. Repitiendo el proceso, al final llegamos a $ax_0 + by_0 = d$ porque $r_0 = a$ y $r_1 = b$.

Ejemplo. Hallar x e y enteros tales que $168x + 77y = 7$.

El algoritmo de Euclides viene dado por

$$168 = 77 \cdot 2 + 14 \qquad 77 = 14 \cdot 5 + 7 \qquad 14 = 7 \cdot 2 + 0$$

y nos confirma que $\mathrm{mcd}(168, 77) = 7$. De la penúltima identidad se obtiene $7 = 77 - 14 \cdot 5$ Ahora sustituyendo el divisor, 14, utilizando la primera identidad y dejando todo en función de 168 y 77, se obtiene

$$\begin{aligned} 7 &= 77 - (168 - 77 \cdot 2) \cdot 5 \\ &= 77 - 168 \cdot 5 + 77 \cdot 10 \\ &= 168(-5) + 77 \cdot 11. \end{aligned}$$

Por tanto $(x, y) = (-5, 11)$ es una solución válida.

Ejemplo. Hallar x e y enteros tales que $29x + 8y = 1$.

Procediendo como antes,

$$\begin{array}{rcl} 29 &=& 8\cdot 3+5\\ 8 &=& 5\cdot 1+3\\ 5 &=& 3\cdot 1+2\\ 3 &=& 2\cdot 1+1\\ 1 &=& 1\cdot 2+0 \end{array} \quad\Longrightarrow\quad \begin{array}{rcl} (4^{\underline{\text{a}}}\text{ ecuación})\ 1 &=& 3-2\cdot 1\\ (3^{\underline{\text{a}}}\text{ ecuación})\ 1 &=& 3-(5-3\cdot 1)\cdot 1 = 5\cdot(-1)+3\cdot 2\\ (2^{\underline{\text{a}}}\text{ ecuación})\ 1 &=& 5\cdot(-1)+(8-5\cdot 1)\cdot 2 = 8\cdot 2+5\cdot(-3)\\ (1^{\underline{\text{a}}}\text{ ecuación})\ 1 &=& 8\cdot 2-(29-8\cdot 3)\cdot 3 = 29\cdot(-3)+8\cdot 11. \end{array}$$

Lo cual nos da la solución $(x, y) = (-3, 11)$.

Si tuvieras que programar este procedimiento, posiblemente te llevaría un rato. Además, al hacer los cálculos a mano hay que poner cierto cuidado identificando qué números hay que operar y cuáles no.

Existe una manera alternativa de proceder con la que es difícil perderse y permite una implementación rápida y eficiente, pues no hay que almacenar todo el algoritmo para ir sustituyendo las ecuaciones, se puede llevar a cabo al tiempo que el algoritmo de Euclides sin ningún gasto de memoria. Se basa en una tabla del tipo

	c_0	c_1	c_2	$\dots$	c_{N-1}	
1	0	a_1	a_2	$\dots$	a_{N-1}	$*$
0	-1	b_1	b_2	$\dots$	b_{N-1}	$*$

donde los c_n son los cocientes sucesivos del algoritmo de Euclides y los a_n y b_n se construyen con la regla

$$a_{n+1} = a_n c_n + a_{n-1}, \qquad b_{n+1} = b_n c_n + b_{n-1}.$$

Es decir, cada elemento de una fila se multiplica por el cociente que está encima y se suma el resultado al elemento anterior. La última columna, marcada con asteriscos, no es necesaria, pero nos puede servir como comprobación, pues siempre debe dar b/d, $-a/d$ con $d = \text{mcd}(a, b)$. La columna que nos interesa es la penúltima porque $(x, y) = (a_{N-1}, b_{N-1})$ es una solución de $ax + by = \pm d$. Es fácil ajustar el signo a ojo. De todas formas, se cumple que para obtener una solución de $ax + by = d$ hay que tomar (a_{N-1}, b_{N-1}) si N (el número de pasos en el algoritmo de Euclides) es par y $(-a_{N-1}, -b_{N-1})$ si es impar.

Si estás interesado en saber por qué funciona esto, toma $n = N - 1$ en el siguiente ejemplo.

Ejemplo (Teórico). Con la notación anterior completada con $a_0 = 0$, $b_0 = -1$, probar por inducción $aa_n + bb_n = (-1)^{n+1} r_{n+1}$ para $0 \le n < N$.

Para $n = 0$ se reduce a sustituir las definiciones. Por otro lado, las recurrencias para a_n y b_n implican $aa_{n+1} + bb_{n+1} = (aa_n + bb_n)c_n + aa_{n-1} + bb_{n-1}$. Por la hipótesis de inducción, esto coincide con $(-1)^{n+1} r_{n+1} c_n + (-1)^n r_n$. La fórmula del algoritmo de Euclides asegura $r_{n+1} c_n = r_n - r_{n+1}$ y, sustituyendo, se obtiene $(-1)^{n+2} r_{n+2}$, completando el paso de inducción.

Ejemplo. Hallar, esta vez con la tabla, una solución entera de $168x + 77y = 7$.

El algoritmo de Euclides nos había dado los cocientes $c_0 = 2$, $c_1 = 5$, $c_2 = 2$. La tabla se construye en dos pasos:

	2	5	2
1	0	1	
0	−1	−2	

y

	2	5	2	
1	0	1	5	
0	−1	−2	−11	

y se tiene $168 \cdot 5 + 77(-11) = -7$, por tanto, $(-5, 11)$ es solución de la ecuación buscada (según lo dicho, el cambio de signo responde a que hay tres pasos, un número impar, en el algoritmo). Si completamos la última columna, obtenemos 11, -24 que coincide con $77/7$, $-168/7$ en consonancia con la comprobación antes indicada.

Los posibles signos de a y b no introducen complicaciones adicionales.

Ejemplo. Hallar con la tabla una solución entera de $-29x + 34y = 1$.

El algoritmo de Euclides señalando los cocientes es:

$$\begin{aligned} -29 = 34 \cdot (-1) + 5 &\quad \to \quad c_0 = -1, \\ 34 = 5 \cdot 6 + 4 &\quad \to \quad c_1 = 6, \\ 5 = 4 \cdot 1 + 1 &\quad \to \quad c_2 = 1, \\ 4 = 1 \cdot 4 + 0 &\quad \to \quad c_3 = 4. \end{aligned}$$

La tabla asociada a estos cocientes resulta

	−1	6	1	4
1	0	1	6	7
0	−1	1	5	6

de donde $(x, y) = (7, 6)$ es una solución de $-29x + 34y = 1$. Esta vez no hay que cambiar el signo porque el número de pasos ha sido 4 que es par.

Cuando uno considera en una ecuación solo las soluciones enteras (o a veces racionales) se dice que está tratando una *ecuación diofántica*, en honor a Diofanto de Alejandría que en el siglo III planteó problemas de este tipo. Las ecuaciones diofánticas lineales en dos variables $ax + by = c$ con $a, b, c \in \mathbb{Z}$ generalizan la que aparece en la identidad de Bézout y surge el problema de saber si tienen solución y, en caso afirmativo, cómo hallar todas ellas. La respuesta es el contenido del siguiente resultado:

> *Sean $a, b, c \in \mathbb{Z}$ con a y b no simultáneamente nulos y $d = \mathrm{mcd}(a, b)$. La ecuación $ax + by = c$ tiene solución $x, y \in \mathbb{Z}$ si y solo si $d \mid c$. En ese caso, todas las soluciones (que son infinitas) vienen parametrizadas por*
>
> $$x = \frac{cx_0 + bt}{d}, \quad y = \frac{cy_0 - at}{d} \qquad \text{con} \quad t \in \mathbb{Z}$$
>
> *donde x_0 e y_0 son enteros fijados cualesquiera que cumplen $ax_0 + by_0 = d$.*

En términos prácticos, si nos piden resolver $ax + by = c$ en enteros debemos aplicar el algoritmo de Euclides para hallar (x_0, y_0) y después usar las fórmulas para x e y. En realidad, simplificando $ax + by = c$ por d basta considerar el caso con coeficientes a y b coprimos.

Ejemplo. Halla todas las soluciones enteras de $102x + 75y = 6$.

Dividiendo entre 3 se tiene $34x + 25y = 2$. El problema está bien propuesto porque $\mathrm{mcd}(34, 25) = 1$, que divide a 2. El algoritmo de Euclides confirma que este es el caso:

$$\begin{aligned} 34 &= 25 \cdot 1 + 9 \quad \to \quad c_0 = 1, \\ 25 &= 9 \cdot 2 + 7 \quad \to \quad c_1 = 2, \\ 9 &= 7 \cdot 1 + 2 \quad \to \quad c_2 = 1, \\ 7 &= 2 \cdot 3 + 1 \quad \to \quad c_3 = 3, \\ 2 &= 1 \cdot 2 + 0 \quad \to \quad c_4 = 2. \end{aligned}$$

La tabla que corresponde a los cocientes c_j es:

	1	2	1	3	2	
1	0	1	2	3	11	~~25~~
0	−1	−1	−3	−4	−15	~~−34~~

donde la última columna es solo para la comprobación. Por tanto una solución de $34x+25y = 1$ es $(11, -15)$ o su negativa. En este caso, es $(x_0, y_0) = (-11, 15)$ porque el número de pasos del algoritmo de Euclides es impar (cinco). Aplicando la fórmula, obtenemos la solución general de $34x + 25y = 2$, que coincide con la de $102x + 75y = 6$,

$$x = \frac{2 \cdot (-11) + 25t}{1} = -22 + 25t, \quad y = \frac{2 \cdot 15 - 34t}{1} = 30 - 34t \qquad \text{con} \quad t \in \mathbb{Z}.$$

Por ejemplo, para $t = 10$ se obtiene que $(x, y) = (228, -310)$ satisface $102x + 75y = 6$, lo cual no es nada obvio a simple vista.

El resultado sobre la solución de las ecuaciones diofánticas lineales en dos variables es una consecuencia bastante directa de la identidad de Bézout, .

Ejemplo. Demostrar que, con la notación anterior, $ax + by = c$ tiene solución si y solo si $d \mid c$.

La implicación directa "tiene solución $\implies$ $d \mid c$" se sigue fácilmente ya que en $ax + by = c$ el primer miembro es divisible por d (porque a y b lo son) y entonces el segundo debe serlo también.

La otra implicación "$d \mid c$ $\implies$ tiene solución" proviene de que la identidad de Bezout asegura que existen $x_0, y_0 \in \mathbb{Z}$ con $ax + by = d$ y entonces $x = x_0/d$, $y = cy_0/d$ son enteros que satisfacen $ax + by = c$.

Para el resto de la demostración, es muy sencillo comprobar que las soluciones anunciadas realmente lo son. Solo restaría probar que no falta ninguna deduciendo a partir de $ax_1 +$

$by_1 = c = ax_2 + by_2$ que existe un $n \in \mathbb{Z}$ tal que $x_1 - x_2 = bn/d$, $y_2 - y_1 = an/d$. Si te gustan las matemáticas, supondrá un reto completar los detalles por ti mismo o buscarlos en la bibliografía. En el primer caso te conviene leer antes el primer párrafo del siguiente apartado.

4. El teorema fundamental de la aritmética

Un resultado de divisibilidad que se deduce de la identidad de Bézout es que para $a, b, c \in \mathbb{Z}$

$$a \text{ y } b \text{ coprimos} \wedge a \mid bc \implies a \mid c.$$

La manera de obtenerlo es notar que la identidad de Bézout asegura que $ax + by = 1$ con ciertos $x, y \in \mathbb{Z}$, lo que implica $a\big(cx + \frac{bc}{a}y\big) = c$ y se concluye $a \mid c$.

La razón para resaltar esta propiedad de divisibilidad es que participa en la prueba de algunos resultados importantes. Su aplicación más famosa es en la demostración de que todo entero mayor que 1 se descompone en factores primos. Recordemos que un *número primo* es un número natural distinto de 1 que solo es divisible por sí mismo y por 1.

> **Teorema fundamental de la aritmética.** *Cada $n > 1$ entero se puede descomponer de forma única como*
>
> $$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \qquad \textit{con} \quad \alpha_j \in \mathbb{N} \quad \textit{y} \quad p_1 < \cdots < p_k \textit{ primos.}$$

Comentario. Actualmente se excluye el 1 de los primos, aunque en siglos pasados se incluía. Por otro lado, en algunos contextos es natural admitir primos negativos, aunque nosotros no lo haremos aquí.

Una vez que conocemos el resultado inicial y el teorema fundamental de la aritmética, no es difícil deducir (ejercicio) que dados $n, m > 1$ enteros si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ y $m = p_1^{\beta_1} \cdots p_k^{\beta_k}$ entonces

$$\mathrm{mcd}(n, m) = p_1^{\mathrm{mín}(\alpha_1, \beta_1)} \cdots p_k^{\mathrm{mín}(\alpha_k, \beta_k)} \qquad \text{y} \qquad \mathrm{mcm}(n, m) = p_1^{\mathrm{máx}(\alpha_1, \beta_1)} \cdots p_k^{\mathrm{máx}(\alpha_k, \beta_k)}$$

y que estas igualdades siguen siendo válidas incluso si admitimos que algunos α_j o β_j sean nulos. La conclusión es que es posible calcular $\mathrm{mcd}(n, m)$ y $\mathrm{mcm}(n, m)$ factorizando. Este es el método que seguramente ya conocías. Es importante recalcar que no suele ser adecuado para números grandes. Por ejemplo, si $n = 2^{512} + 40$ y $m = 2^{512} + 1$ la factorización de estos números llevaría a un esfuerzo computacional considerable, sin embargo, un paso del algoritmo de Euclides nos dice $\mathrm{mcd}(n, m) = \mathrm{mcd}(n, 39)$ Más adelante estudiaremos métodos que permiten concluir con muy pocos cálculos que al dividir n entre 39 el resto es 23, así pues, $\mathrm{mcd}(n, m) = \mathrm{mcd}(23, 39)$ y se concluye que n y m son coprimos. Incluso sin conocer estos métodos, el esfuerzo para hallar $2^{512} + 1$ con un ordenador y dividirlo entre 39 es menor que el necesario para factorizarlo.

Comentario. La factorización de $2^{512}+1$ no se consiguió hasta los años 90 del siglo pasado y dio lugar a algunos titulares en periódicos. Se necesitaron 700 *workstations* de la época trabajando en paralelo durante meses y un superordenador. Este cálculo está todavía muy lejos de lo que puede hacerse en un ordenador personal actual. No hay buenos algoritmos para factorizar en primos números de cientos de dígitos (sobre todo si se escogen "con mala idea"). Algunos esquemas criptográficos comunes se basan en que multiplicar primos enormes es trivial para un ordenador, mientras que recuperarlos a partir del producto es muy difícil.

A este nivel, nuestro único método para descomponer en primos es la *división sucesiva* que consiste en ir probando la divisibilidad por primos cada vez mayores.

Ejemplo. Descomponer 1274 y 3809 en factores primos y utilizar el resultado para calcular su máximo común divisor y su mínimo común múltiplo.

Los primeros primos son 2, 3, 5, 7, 11, 13, 17, 19... Como 1274 es par, es divisible por 2, el primer primo, obteniéndose $1274 = 2 \cdot 637$. Ahora nos ocupamos de descomponer 637. Ya no es par y probando sucesivamente con primos mayores que 2, vemos que $637 = 7 \cdot 91$. Seguimos ahora probando a dividir 91 por primos mayores o iguales que 7 para obtener $91 = 7 \cdot 13$ que lleva a la factorización $1274 = 2 \cdot 7^2 \cdot 13$. Cuando hacemos lo mismo con 3809, el primer primo que lo divide es 13 que da $3809 = 13 \cdot 293$. La cuestión es decidir si 293 es primo o no. Para ello no hace falta prolongar nuestra tabla, porque si fuera producto de varios primos, uno de ellos debería ser como mucho $\sqrt{293} = 17{,}11\ldots$ y habría aparecido ya.

Tras las factorizaciones $1274 = 2 \cdot 7^2 \cdot 13$ y $3809 = 13 \cdot 293$, las fórmulas muestran que $2^0 \cdot 7^0 \cdot 13^1 \cdot 293^0 = 13$ es el máximo común divisor y que $2^1 \cdot 7^2 \cdot 13^1 \cdot 293^1 = 373282$ es el mínimo común múltiplo.

A pesar de que la demostración del teorema fundamental de la aritmética es asequible con lo que conocemos, seguramente te resultaría tediosa. El estudiante interesado puede encontrarla fácilmente en la bibliografía. A cambio, veamos la prueba de la relación entre el máximo común divisor y el mínimo común múltiplo. Nos limitamos a enteros positivos, porque cualquier combinación de signos se trataría de forma similar. Procederemos desde primeros principios. Si diéramos por supuesto el teorema fundamental de la aritmética, con las fórmulas anteriores, todo se reduciría a la igualdad $\min(\alpha,\beta) + \max(\alpha,\beta) = \alpha + \beta$.

Ejemplo (Teórico). Demostrar la fórmula $\operatorname{mcm}(a,b)\operatorname{mcd}(a,b) = ab$ para $a, b \in \mathbb{Z}^+$.

Escribiendo $d = \operatorname{mcd}(a,b)$ es fácil ver que $a = a'd$ y $b = b'd$ con a' y b' coprimos. Con esta notación, queremos demostrar $\operatorname{mcm}(a,b) = a'b'd^2/d$. Obviamente, $a'b'd$ es un múltiplo de a y de b. Sea M cualquier múltiplo común. Por ser divisible por b, $M = d'b'd$ y utilizando que también lo es por a, se tiene la cadena de implicaciones:

$$a'd \mid M \implies a'd \mid b'dd' \implies a' \mid b'd' \implies a' \mid d' \implies d' \geq a' \implies M \geq a'b'd.$$

En definitiva, hemos probado que $a'b'd$ es un múltiplo común de a y b y que cualquier otro es mayor o igual que él, por tanto, $\operatorname{mcm}(a,b) = a'b'd$.