3

DIVISIBILIDAD

3.1 COCIENTE Y RESTO

Cuando somos chicos aprendemos que 6 “cabe” cuatro veces en 27 y el resto es 3, o sea

$$27 = 6 \cdot 4 + 3.$$

Un punto importante es que el resto debe ser menor que 6. Aunque, también es verdadero que, por ejemplo

$$27 = 6 \cdot 3 + 9,$$

debemos tomar el menor valor para el resto, de forma que “lo que queda” sea un número no negativo lo más chico posible. El hecho de que el conjunto de posibles “restos” tenga un mínimo es una consecuencia del axioma del buen orden.

Teorema 3.1.1. *Sean* a *y* b *números enteros cualesquiera con* $b \in \mathbb{N}$, *entonces existen enteros únicos* q *y* r *tales que*

$$a = b \cdot q + r \qquad y \qquad 0 \leqslant r < b.$$

Demostración. Debemos aplicar el axioma del buen orden al conjunto de los “restos”

$$R = \{x \in \mathbb{N}_0 | a = by + x \text{ para algún } y \in \mathbb{Z}\}.$$

Primero demostraremos que R no es vacío. Si $a \geqslant 0$ la igualdad

$$a = b \cdot 0 + a$$

demuestra que $a \in R$, mientras que si $a < 0$ la igualdad

$$a = b \cdot a + (1 - b) \cdot a$$

demuestra que $(1 - b) \cdot a \in R$ (en ambos casos es necesario controlar que el elemento es no negativo.)

Ahora, como R es un subconjunto no vacío de $\mathbb{N}_0$, tiene un mínimo r, y como r esta en R se sigue que $a = bq + r$ para algún q en $\mathbb{Z}$. Además

$$a = bq + r \Rightarrow a = b(q + 1) + (r - b)$$

de manera que si $r \geqslant b$ entonces $r - b$ esta en R. Pero $r - b$ es menor que r, contradiciendo la definición de r como el menor elemento de R. Como la suposición $r \geqslant b$ nos lleva a una contradicción, solo puede ocurrir que $r < b$, como queríamos demostrar.

Es fácil ver que el cociente q y el resto r obtenidos en el teorema son únicos. Supongamos que q' y r', también satisfacen las condiciones, esto es

$$a = bq' + r' \qquad \text{y} \qquad 0 \leqslant r' < b.$$

Si $q > q'$, entonces $q - q' \geqslant 1$ y tenemos que

$$r' = a - bq' = (a - bq) + b(q - q') \geqslant r + b.$$

Como $r + b \geqslant b$, se sigue que $r' \geqslant b$ contradiciendo la segunda propiedad de r'. Por lo tanto la suposición $q' > q$ es falsa. El mismo argumento con q y q' intercambiados demuestra que $q < q'$ también es falsa. Entonces debemos tener $q = q'$, y en consecuencia $r = r'$, puesto que

$$r = a - bq = a - bq' = r'.$$

□

Ejemplo.

- Si $a = 10$ y $b = 3$, entonces $10 = 3 \cdot 3 + 1$. Es decir $q = 3$, $r = 1$.
- Si $a = 2$ y $b = 5$, entonces $2 = 5 \cdot 0 + 2$. Es decir $q = 0$, $r = 2$.
- Si $a = -10$ y $b = 3$, entonces $-10 = 3 \cdot (-4) + 2$. Es decir $q = -4$, $r = 2$. En algunos viejos compiladores del lenguaje C, la división entera estaba mal definida, pues consideraban, por ejemplo, $-10 = 3 \cdot (-3) - 1$. Es decir, si el número a ser dividido era negativo, tomaban el resto también como un número negativo, lo cual no está de acuerdo al teorema 3.1.1.
- Si $a = -2$ y $b = 3$, entonces $-2 = 3 \cdot (-1) + 1$. Es decir $q = -1$, $r = 1$.

§ *Desarrollos en base* b, *(*$b \geqslant 2$*)*

Una consecuencia importante del teorema 3.1.1 es que justifica nuestro método usual de representación de enteros. Desde chicos aprendimos que nuestro sistema de numeración es *decimal*, es decir hay 10 dígitos, del 0 al 9, y todo número se escribe como combinación de esos dígitos.

¿Cuáles son estos 10 dígitos? 0 y 1 vienen dados por los axiomas, el símbolo 2 representa $1 + 1$, el símbolo 3 representa $1 + 1 + 1$, etc. Todo número natural puede ser escrito con la notación posicional como combinación de estos diez dígitos. Por ejemplo, el número 407 se puede escribir como

$$407 = 4 \cdot 10^2 + 0 \cdot 10^1 + 7 \cdot 10^0,$$

y el número 23827 se puede escribir como

$$23827 = 2 \cdot 10^4 + 3 \cdot 10^3 + 8 \cdot 10^2 + 2 \cdot 10^1 + 7 \cdot 10^0.$$

Más formalmente.

Teorema 3.1.2. *Todo número natural* m *puede ser escrito de una única forma como*

$$m = r_n 10^n + r_{n-1} 10^{n-1} + \cdots + r_1 10 + r_0$$

con $r_n \neq 0$ *y* $0 \leqslant r_i < 10$ *para* $i = 0, 1, \ldots, n$.

Podemos decir entonces que

x *se representa como la cadena* $r_n r_{n-1} \ldots r_1 r_0$ *en notación decimal.*

o también que

$$x = (r_n r_{n-1} \ldots r_1 r_0)_{10}.$$

La representación decimal de un número también el llamada *representación en base* 10.

Este teorema es una consecuencia importante del algoritmo de división y es el que justifica nuestro método usual de representación de enteros. También podemos desarrollar en potencias de b con b cualquier entero $\geqslant 2$ (y vale el teorema anterior reemplazando 10 por b).

Ejemplo. Deseamos escribir el número 407 con una expresión de la forma

$$407 = r_n 5^n + r_{n-1} 5^{n-1} + \cdots + r_1 5 + r_0,$$

con $0 \leqslant r_i < 5$. Veamos que esto es posible y se puede hacer de forma algorítmica. La forma de hacerlo es, primero, dividir el número original y los sucesivos cocientes por 5:

$$407 = 5 \cdot 81 + 2 \tag{3.1.1}$$
$$81 = 5 \cdot 16 + 1 \tag{3.1.2}$$
$$16 = 5 \cdot 3 + 1 \tag{3.1.3}$$
$$3 = 5 \cdot 0 + 3. \tag{3.1.4}$$

Observar entonces que

$$\begin{aligned} 407 &= 5 \cdot 81 + 2 && \text{por } (3.1.1) \\ &= 5 \cdot (5 \cdot 16 + 1) + 2 && \text{por } (3.1.2) \\ &= 5^2 \cdot 16 + 5 \cdot 1 + 2 && \\ &= 5^2 \cdot (5 \cdot 3 + 1) + 5 \cdot 1 + 2 && \text{por } (3.1.3) \\ &= 5^3 \cdot 3 + 5^2 \cdot 1 + 5 \cdot 1 + 2. && \end{aligned}$$

En este caso diremos que el desarrollo en base 5 de 407 es 3112 o, resumidamente, $407 = (3112)_5$. Observar que el desarrollo en base 5 de 407 viene dado por los restos de las divisiones sucesiva, leídos en forma ascendente.

Sea $b \geqslant 2$ un número entero, llamado *base* para los cálculos. Para cualquier entero positivo x tenemos, por la aplicación repetida del teorema 3.1.1,

$$\begin{aligned} x &= bq_0 && + r_0 \\ q_0 &= bq_1 && + r_1 \\ &\dots && \\ q_{n-2} &= bq_{n-1} && + r_{n-1} \\ q_{n-1} &= bq_n && + r_n. \end{aligned}$$

Aquí cada resto es uno de los enteros $0, 1, \dots, b-1$, y paramos cuando $q_n = 0$. Reemplazando sucesivamente los cocientes q_i, como lo hicimos en el ejemplo, obtenemos

$$x = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b + r_0.$$

Hemos representado x (con respecto a la base b) por la secuencia de los restos, y escribimos $x = (r_n r_{n-1} \dots r_1 r_0)_b$. Convencionalmente $b = 10$ es la base para los cálculos hechos "a mano" y omitimos ponerle el subíndice, entonces tenemos la notación usual

$$1984 = 1 \cdot 10^3 + 9 \cdot 10^2 + 8 \cdot 10 + 4.$$

Esta notación posicional requiere símbolos solo para los enteros $0, 1, \dots, b-1$. La base $b = 2$ es particularmente adaptable para los cálculos en computadoras porque los símbolos 0 y 1 pueden representarse físicamente por la ausencia o presencia de un pulso de electricidad o luz.

Ejemplo. ¿Cuál es la representación en base 2 de $(109)_{10}$?

Demostración. Dividiendo repetidamente por 2 obtenemos

$$\begin{aligned}
109 &= 2 \cdot 54 + 1\\
54 &= 2 \cdot 27 + 0\\
27 &= 2 \cdot 13 + 1\\
13 &= 2 \cdot 6 + 1\\
6 &= 2 \cdot 3 + 0\\
3 &= 2 \cdot 1 + 1\\
1 &= 2 \cdot 0 + 1
\end{aligned}$$

Por lo tanto

$$(109)_{10} = (1101101)_2.$$

La base 16 también es usada en computación pues se utiliza el byte como unidad básica de memoria y debido a que un byte puede tomar 2^8 posibles valores, podemos representar un byte en base 2 por ternas de 0 y 1 , o por un símbolo en base 16. Es claro que los dígitos disponibles (del 0 al 9) no nos alcanzan para representar un número en base 16, pues se requieren 16 símbolos. La convención usada es

$$\mathsf{A} = 10, \quad \mathsf{B} = 11, \quad \mathsf{C} = 12, \quad \mathsf{D} = 13, \quad \mathsf{E} = 14, \quad \mathsf{F} = 15.$$

Ejemplo. Representemos 12488 en base 16.

$$\begin{aligned}
12488 &= 16 \cdot 780 + 8\\
780 &= 16 \cdot 48 \ \ + 12\\
48 &= 16 \cdot 3 \quad + 0\\
3 &= 16 \cdot 0 \quad + 3.
\end{aligned}$$

Luego $12488 = (30\mathsf{C}8)_{16}$.

□

§ *Ejercicios*

1) Encontrar q y r que satisfagan el teorema 3.1.1 cuando

   a) $a = 1001, \qquad b = 11;$

   b) $a = 12345, \qquad b = 234.$

2) Encontrar las representaciones de $(1985)_{10}$ en:

   a) Base 2, *b)* Base 5, *c)* Base 11.

3) Encontrar las representación usual (base 10) de:

   a) $(11011101)_2$, *b)* $(4165)_7$.

3.2 DIVISIBILIDAD

Definición 3.2.1. Dados dos enteros x e y decimos que y es un *divisor* de x, y escribimos $y|x$, si

$$x = yq \quad \text{para algún} \quad q \in \mathbb{Z}.$$

También decimos que y es un *factor* de x, que y *divide* a x, que x es *divisible* por y, y que x es *múltiplo* de y.

Cuando $y|x$ podemos usar el símbolo $\frac{x}{y}$ (o x/y) para denotar el entero q tal que $x = yq$. Cuando y no es un divisor de x tenemos que asignar un nuevo significado a la fracción x/y, puesto que este número no es un entero. El lector indudablemente, esta familiarizado con las reglas para manejar fracciones, y usaremos esas reglas de tanto en tanto, pero es importante recordar que las fracciones no han sido aún formalmente definidas en el contexto de este apunte. Y es aún más importante recordar que x/y no es un elemento de $\mathbb{Z}$ a menos que y divida a x.

Veamos ahora alguna propiedades básicas de la relación "divide a".

Proposición 3.2.2. *Sean a, b, c enteros, entonces*

a) $1|a$, $\quad a|0$, $\quad a|\pm a$;

b) *si* $a|b$, *entonces* $a|bc$ *para cualquier* c;

c) *si* $a|b$ *y* $a|c$, *entonces* $a|(b+c)$;

d) *si* $a|b$ *y* $a|c$, *entonces* $a|(rb+sc)$ *para cualesquiera* $r, s \in \mathbb{Z}$.

e) *si* $a, b > 0$ *y* $a|b$, *entonces* $a \leqslant b$.

Demostración. La demostración de estos hechos es sencilla, por ejemplo *c)*: como $a|b$, existe q tal que $b = aq$. Análogamente, como $a|c$, existe q' tal que $c = aq'$. Entonces $b + c = aq + aq' = a(q + q')$, luego $a|(b + c)$. Las demás demostraciones, excepto la última, se dejan como ejercicio para el lector.

Demostración de *e)*: como $a|b$ existe $q \in \mathbb{Z}$ tal que $b = aq$, como $a, b > 0$, entonces, por la compatibilidad de $>$ con el producto, $q > 0$. Luego $q - 1 \geqslant 0$ y, de nuevo por la compatibilidad, $a(q-1) \geqslant 0$. Ahora bien, $b = aq = a + a(q-1)m$ luego $b - a = a(q-1) \geqslant 0$, por lo tanto $b \geqslant a$. $\square$

Ejemplo. Demostremos que si c, d y n son enteros tales que, $d|n$ y $c\,\middle|\,\frac{n}{d}$, entonces

$$c|n \quad \text{y} \quad d\,\Big|\,\frac{n}{c}$$

Demostración. Como $d|n$ existe un entero s tal que $n = ds$, y n/d denota al entero s. Puesto que $c|(n/d)$ existe un entero t tal que

$$s = \frac{n}{d} = ct.$$

Se sigue que

$$n = ds = d(ct) = c(dt)$$

entonces $c|n$ y n/c denota al entero dt. Finalmente, como $n/c = dt$ tenemos $d|(n/c)$, como queríamos demostrar. □

Proposición 3.2.3. *Sean a y b enteros.*

a) *Si $ab = 1$ entonces $a = b = 1$ o $a = b = -1$.*

b) *Si x e y son enteros tales que $x|y$ e $y|x$, entonces $x = y$ o $x = -y$.*

Demostración.

a) Si a o b valen 0, entonces $ab = 0 \neq 1$. Luego a y b son distintos de 0. Si $a > 0$ y $b < 0$ por los axiomas de compatibilidad del orden con el producto $ab < 0$. Lo mismo ocurre si $a < 0$ y $b > 0$.

Es decir podemos suponer que o bien $a > 0$ y $b > 0$, o bien $a < 0$ y $b < 0$.

Si $a > 0$ y $b > 0$, entonces $a \geqslant 1$ y $b \geqslant 1$. Si $a = 1$, como $ab = 1$, tenemos que $b = 1 \cdot b = 1$. Si $a > 1$, como $b > 0$ por compatibilidad de $<$ con el producto tenemos que $ab > 1$, lo cual no es cierto. Es decir, hemos probado que si $a > 0$ y $b > 0$, entonces $a = 1$ y $b = 1$.

Si $a < 0$ y $b < 0$, entonces $-a > 0$ y $-b > 0$ y $(-a)(-b) = ab = 1$. Luego, por el párrafo de arriba, $-a = -b = 1$ y en consecuencia $a = b = -1$.

b) Sean x, y tales que $x|y$ e $y|x$. Como $x|y$, existe $q \in \mathbb{Z}$ tal que $y = qx$. Análogamente, como $y|x$ existe q' tal que $x = q'y$. Luego

$$y = qx = q(q'y) = (qq')y.$$

Por el axioma de cancelación (cancelando y) obtenemos que $1 = qq'$. Por lo demostrado más arriba tenemos que, o bien $q = q' = 1$ y en consecuencia $x = y$, o bien $q = q' = -1$ y en consecuencia $x = -y$. □

§ *Ejercicios*

1) Usar el principio de inducción para demostrar que, para todo $n \geqslant 0$ se cumplen;

   a) $n^2 + 3n$ es divisible por 2,

   b) $n^3 + 3n^2 + 2n$ es divisible por 6.

3.3 El máximo común divisor y el mínimo común múltiplo

Recordemos que por la proposición 3.2.2 *e)*, si $x|y$ y ambos son mayores que 0, entonces $x \leqslant y$. En consecuencia, el conjunto de divisores de un número positivo está compuesto por números menores o iguales al número.

Definición 3.3.1. Si a y b son enteros algunos de ellos no nulo, decimos que un entero positivo d es el *máximo común divisor*, o *mcd*, de a y b si

a) $d|a$ y $d|b$;

b) si $c|a$ y $c|b$ entonces $c \leqslant d$.

Denotaremos al máximo común divisor de a y b por $\mathrm{mcd}(a, b)$ o, en caso de no haber confusión, por el par ordenado (a, b).

La condición *a)* nos dice que d es un común divisor de a y b y la condición *b)* nos dice que cualquier divisor común de a y b es menor igual que d. Podemos resumir la definición en una frase, diciendo: *el máximo común divisor de* a *y* b *es el mayor divisor común a ambos números.*

Ejemplo. Los divisores positivos comunes de 60 y 84 son 1, 2, 3, 6 y 12, luego, por ejemplo, 6 es un divisor común y por lo tanto satisface *a)*. Sin embargo, no satisface *b)* de la definición, pues $12|60$ y $12|84$ pero $12 > 6$. En este caso, 12 claramente es el máximo común divisor.

Ejemplo. Hallar $\mathrm{mcd}(174, 72)$.

Solución.

Divisores de 174: 1, 2, 3, 6, 29, 58, 87, 174

Divisores de 72: 1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72

Luego, los divisores comunes de 174 y 72 son $1, 2, 3, 6$, y claramente 6 es el mayor divisor común. Por lo tanto $\mathrm{mcd}(174, 72) = 6$. □

En los ejemplos anteriores usamos dos enteros pequeños y no tuvimos problemas en encontrar el máximo común divisor. Pero, ¿qué pasaría si consideráramos dos enteros “muy grandes”? En ese caso nos es factible calcular los divisores comunes y por lo tanto no podemos calcular el mcd de sea manera. En el desarrollo de esta sección veremos el *algoritmo de Euclides*, un método muy eficiente para calcular el máximo común divisor de dos números, incluso donde cada uno con varios cientos de dígitos.

Observación 3.3.2. Sean a, b enteros, alguno de ellos no nulo, y a', b' otro par de enteros tal que se cumple la propiedad:

$$c|a \ \wedge \ c|b \quad \Leftrightarrow \quad c|a' \ \wedge \ c|b',$$

es decir, c es divisor de a y b si y solo si es divisor de a' y b'. Entonces, $\mathrm{mcd}(a, b) = \mathrm{mcd}(a', b')$. Esto es obvio a partir de la definición del mcd.

Podemos enunciar las propiedades más sencillas del mcd en la siguiente proposición.

Proposición 3.3.3. *Sean* a, b *enteros con* $a \neq 0$, *entonces*

(1) $\mathrm{mcd}(b, a) = \mathrm{mcd}(a, b) = \mathrm{mcd}(\pm a, \pm b)$,

(2) *si* $a > 0$, $\mathrm{mcd}(a, 0) = a$ *y* $\mathrm{mcd}(a, a) = a$,

(3) $\mathrm{mcd}(1, b) = 1$.

Demostración. Estas propiedades son de demostración casi trivial, por ejemplo para demostrar que $\mathrm{mcd}(1, b) = 1$ comprobamos que 1 cumple con la definición:

a) $1|1$ y $1|b$;

b) si $c|1$ y $c|b$ entonces $c \leqslant 1$,

propiedades que son obviamente verdaderas.

1. y 2. se dejan a cargo del lector. □

La siguiente propiedad no es tan obvia y resulta muy importante.

Propiedad 3.3.4. *Si* $a \neq 0, b \in \mathbb{Z}$, *entonces* $\mathrm{mcd}(a, b) = \mathrm{mcd}(a, b - a)$.

Demostración. Sea $d = \mathrm{mcd}(a, b - a)$, luego

a) $d|a$ y $d|b - a$;

b) si $c|a$ y $c|b - a$ entonces $c \leqslant d$.

Ahora bien, como $d|a$ y $d|b - a$, entonces $d|a + (b - a) = b$. Es decir, para recalcar,

a') $d|a$ y $d|b$.

Por otro lado, si $c|a$ y $c|b$, entonces $c|b - a$, luego por *b)* tenemos que $c \leqslant d$. Es decir,

b') si $c|a$ y $c|b$, entonces $c \leqslant d$.

Luego, por *a')* y *b')* tenemos que d satisface la definición del mcd de a y b, es decir $d = \text{mcd}(a, b)$. □

La propiedad anterior nos provee un método práctico para encontrar el máximo común divisor entre dos números. Veamos su aplicación en el siguiente ejemplo.

Ejemplo. Encontrar el mcd entre 72 y 174.

Solución. Observar que

$$\begin{aligned}\text{mcd}(72, 174) &= \text{mcd}(72, 174 - 72) = \text{mcd}(72, 102) = \text{mcd}(72, 30)\\ &= \text{mcd}(42, 30) = \text{mcd}(12, 30) = \text{mcd}(12, 18) = \text{mcd}(12, 6)\\ &= \text{mcd}(6, 6) = 6.\end{aligned}$$

□

En general no es sencillo encontrar todos los divisores de un número entero. Por ejemplo, para los números de más de cien dígitos no es posible, en general, calcular sus divisores ni con las computadoras más poderosas de la actualidad. Por lo tanto, no es factible calcular el mcd de números con más de cien dígitos revisando todos los divisores comunes. El algoritmo que nos provee la propiedad 3.3.4 nos da un método práctico y relativamente eficiente para calcular el mcd. Veremos a continuación un método similar pero mucho más eficiente para calcular el mcd de dos enteros no negativos a, b con $b \neq 0$. Este método esta basado en el algoritmo de división y el siguiente resultado.

Proposición 3.3.5. *Sean* a, b *enteros no negativos con* $b \neq 0$, *entonces*

$$a = bq + r \quad \Rightarrow \quad \text{mcd}(a, b) = \text{mcd}(b, r). \tag{3.3.1}$$

Demostración. Se puede demostrar por definición directamente y en ese caso la demostración es similar a la de la propiedad 3.3.4.

Sin embargo, para mostrar que un problema se puede encarar de forma diferente, haremos la demostración utilizando la observación 3.3.2. Es decir probaremos que los divisores comunas de a y b son los mismos que los divisores comunes de b y r.

Para demostrar esto debemos observar que si c divide a y b, entonces también divide a $a - bq$; y como $a - bq = r$, tenemos que $c|r$. De este modo cualquier divisor común de a y b es también divisor común de b y r. Por otro lado si c divide b y r también divide a $a = bq + r$. Es decir, c es divisor común de a y b si y sólo si c es divisor común de b y r. Por lo tanto, por observación 3.3.2, obtenemos que $d = \text{mcd}(b, r)$. □

La aplicación repetida de este simple resultado, en combinación con el algoritmo de división, nos da un método para calcular el mcd.

Ejemplo. Encuentre el mcd de 2406 y 654.

Solución. Tenemos

$$\begin{aligned} \operatorname{mcd}(2406, 654) &= \operatorname{mcd}(654, 444) && \text{porque} \quad 2406 = 654 \cdot 3 + 444, \\ &= \operatorname{mcd}(444, 210) && \text{porque} \quad 654 = 444 \cdot 1 + 210, \\ &= \operatorname{mcd}(210, 24) && \text{porque} \quad 444 = 210 \cdot 2 + 24, \\ &= \operatorname{mcd}(24, 18) && \text{porque} \quad 210 = 24 \cdot 8 + 18, \\ &= \operatorname{mcd}(18, 6) && \text{porque} \quad 24 = 18 \cdot 1 + 6, \\ &= \operatorname{mcd}(6, 0) = 6 && \text{porque} \quad 18 = 6 \cdot 3 + 0 \end{aligned}$$

Por lo tanto, $\operatorname{mcd}(2406, 654) = 6$. □

Algoritmo de Euclides

Por lo general, para calcular el mcd de enteros a y b, con $b > 0$, definimos r_i recursivamente de la siguiente manera: $r_0 = a$, $r_1 = b$, y

$$\begin{array}{lll} (e_1) & r_0 = r_1 q_1 + r_2 & (0 < r_2 < r_1) \\ (e_2) & r_1 = r_2 q_2 + r_3 & (0 < r_3 < r_2) \\ (e_3) & r_2 = r_3 q_3 + r_4 & (0 < r_4 < r_3) \\ \dots & & \\ (e_i) & r_{i-1} = r_i q_i + r_{i+1} & (0 < r_{i+1} < r_i) \\ \dots & & \\ (e_{k-1}) & r_{k-2} = r_{k-1} q_{k-1} + r_k & (0 < r_k < r_{k-1}) \\ (e_k) & r_{k-1} = r_k q_k + 0, & \end{array}$$

Cuadro 1: Algoritmo de Euclides

Este ejemplo es un caso particular o una aplicación del algoritmo que nos permite calcular el máximo común divisor: sean a y b enteros con $b > 0$, sea $r_0 = a$, $r_1 = b$ y suponiendo definidos r_{i-1} y r_i definimos recursivamente r_{i+1} por la siguiente ecuación

$$r_{i-1} = r_i q + r_{i+1} \quad \text{con} \quad 0 < r_{i+1} < r_i.$$

Observar que r_{i+1} está bien definido por el algoritmo de división. Detenemos el proceso cuando uno de los restos r_i es igual a 0. Ahora bien, cada resto no nulo es positivo y estrictamente menor que el anterior. Entonces, queda claro que el proceso se va a detener. El proceso se explica esquemáticamente en el cuadro 1.

Este procedimiento es conocido como el *algoritmo de Euclides*, debido al matemático griego Euclides (300 a. c.). Es extremadamente útil en la práctica, y tiene importantes consecuencias.

Teorema 3.3.6. *Sean a y b enteros con $b > 0$, entonces el máximo común divisor es el último resto no nulo obtenido en el algoritmo de Euclides (con la notación del cuadro 1 es r_k).*

Demostración. Observar que aplicando repetidas veces la fórmula (3.3.1) obtenemos

$$\begin{aligned} r_k = \operatorname{mcd}(r_k, 0) = \operatorname{mcd}(r_{k-1}, r_k) = \operatorname{mcd}(r_{k-2}, r_{k-1}) = \cdots \\ \cdots = \operatorname{mcd}(r_2, r_3) = \operatorname{mcd}(r_1, r_2) = \operatorname{mcd}(r_0, r_1) = \operatorname{mcd}(a, b) \end{aligned}$$

□

Observación (*). El algoritmo de Euclides es fácilmente implementable en un lenguaje de programación. A continuación una versión del mismo en pseudocódigo.

ALGORITMO DE EUCLIDES

```
# pre: a y b son números positivos
# post: Obtenemos d = mcd(a,b)
i, j = a, b
while j != 0:
    # invariante: mcd(a, b) = mcd(i, j)
    resto = i % j   # i = q * j + resto
    i, j = j, resto
d = i
```

La expresión $i\,\%\,j$ representa el resto de dividir i por j. Observar que en el ciclo `while` los valores que se obtienen en cada repetición son $i' = j$, $j' = i\,\%\,j$, luego

$$i = q \cdot j + j' \;\Rightarrow\; \operatorname{mcd}(i, j) = \operatorname{mcd}(j, j') = \operatorname{mcd}(i', j').$$

Luego, al terminar el ciclo `while`, es decir cuando $j = 0$, tenemos que

$$\operatorname{mcd}(a, b) = \operatorname{mcd}(i, 0) = i.$$

Definición 3.3.7. Sean a, b enteros, entonces dados $s, t \in \mathbb{Z}$ diremos que

$$sa + tb$$

es una *combinación lineal entera* de a y b.

Observación. Sean $a, b \in \mathbb{Z}$, alguno de ellos no nulo, y d un máximo común divisor de a y b. Entonces, d divide a cualquier combinación lineal entera de a y b. Esto es una consecuencia directa de la proposición 3.2.2 *d)*.

Teorema 3.3.8. *Sean* $a, b \in \mathbb{Z}$*, alguno de ellos no nulo. Entonces, existen* $s, t \in \mathbb{Z}$ *tal que*

$$\mathrm{mcd}(a, b) = sa + tb.$$

Es decir $\mathrm{mcd}(a, b)$ *es combinación lineal entera de* a *y* b*.*

Demostración. Supongamos que $b > 0$ (los otros casos se deducen fácilmente) y sea $d = \mathrm{mcd}(a, b)$. La idea es calcular s y t tales que

$$d = sa + tb.$$

De acuerdo con la notación que utilizamos para explicar el algoritmo de Euclides, $d = r_k$ y usando la ecuación (e_{k-1}) tenemos

$$r_k = r_{k-2} - r_{k-1}q_{k-1}.$$

Así, d puede escribirse en la forma $d = s_k r_{k-2} + t_k r_{k-1}$, donde $s_k = 1$ y $t_k = -q_{k-1}$. Usando la ecuación (e_{k-2}), sustituyendo r_{k-1} en términos de r_{k-3} y r_{k-2} obtenemos

$$d = s_k(r_{k-3} - r_{k-2}q_{k-2}) + t_k r_{k-3} = s_{k-1}r_{k-3} + t_{k-1}r_{k-2}$$

donde $s_{k-1} = s_k + t_k$ y $t_{k-1} = -s_k q_{k-2}$. Aplicando repetidas veces las ecuaciones del algoritmo de Euclides obtenemos, en general que

$$d = s_i r_{i-2} + t_i r_{i-1}$$

con $s_i, t_i \in \mathbb{Z}$, para $2 \leqslant i \leqslant k$. En particular

$$d = s_2 r_0 + t_2 r_1 = s_2 a + t_2 b.$$

$\square$

Ejemplo. Encontrar usando el algoritmo de Euclides $d = \mathrm{mcd}(470, 55)$ y expresar d como combinación lineal entera entre 470 y 55.

Solución.

$$\begin{aligned}
470 &= 55 \cdot 8 + 30 & \Rightarrow \quad & 30 = 470 + (-8) \cdot 55 & \quad (1)\\
55 &= 30 \cdot 1 + 25 & \Rightarrow \quad & 25 = 55 + (-1) \cdot 30 & \quad (2)\\
30 &= 25 \cdot 1 + 5 & \Rightarrow \quad & 5 \;= 30 + (-1) \cdot 25 & \quad (3)\\
25 &= 5 \cdot 5 + 0. & & &
\end{aligned}$$

Luego, el máximo común divisor de 470 y 55 es 5 y de las fórmulas anteriores obtenemos:

$$\begin{aligned}
5 &= 30 + (-1) \cdot 25 & \text{(por (3))}\\
&= 30 + (-1) \cdot (55 + (-1) \cdot 30) = 2 \cdot 30 + (-1) \cdot 55 & \text{(por (2))}\\
&= 2 \cdot (470 + (-8) \cdot 55) + (-1) \cdot 55 = 2 \cdot 470 + (-17) \cdot 55 & \text{(por (1))}
\end{aligned}$$

De este modo, la expresión requerida $d = sa + tb$ es

$$5 = 2 \cdot 470 + (-17) \cdot 55.$$

□

Corolario 3.3.9. *Sean* a *y* b *enteros, unos de ellos no nulo y sea* $d = \mathrm{mcd}(a, b)$. *Sea* $c \in \mathbb{Z}$ *tal que* $c|a$ *y* $c|b$, *entonces* $c|d$.

Demostración. Por la proposición anterior d es combinación lineal entera de a y b. Como $c|a$ y $c|b$, entonces divide a d que es una combinación lineal entera de a y b (proposición 3.2.2 *d)*). □

Observación. El corolario anterior nos permite, después de cierto trabajo, cambiar la condición *b)* de la definición de máximo común divisor por una condición equivalente:

b') si $c|a$ y $c|b$ entonces $c|d$.

En alguna literatura puede encontrarse la definición de mcd con la condición *b')*.

Definición 3.3.10. Si $(a, b) = 1$ entonces decimos que a y b son *coprimos*.

Corolario 3.3.11. *Sean* a *y* b *enteros uno de ellos no nulo, entonces*

$$(a, b) = 1 \Leftrightarrow \textit{existen } s, t \in \mathbb{Z} \textit{ tales que } 1 = sa + tb.$$

Demostración. $(\Rightarrow)$ Es consecuencia trivial del teorema 3.3.8.

$(\Leftarrow)$ Sea $d = (a, b)$, entonces $d|a$ y $d|b$ y por lo tanto $d|sa + tb$ para cualesquiera $s, t \in \mathbb{Z}$. En particular, la hipótesis implica que $d|1$ y, en consecuencia $d = 1$. □

Ejemplo. Sean a y b enteros coprimos y $c \in \mathbb{Z}$, entonces,

$$a|c \ \wedge \ b|c \quad \Rightarrow \quad ab|c.$$

Solución. como a y b son coprimos, existen $s, t \in \mathbb{Z}$ tales que $1 = sa + tb$. Por lo tanto, multiplicando por c la ecuación, obtenemos $c = csa + ctb$. Como $a|c$ y $b|c$, existen $m, n \in \mathbb{Z}$ tal que $c = am$ y $c = bn$, luego:

$$c = csa + ctb = bnsa + amtb = ab(ns + mt).$$

Por lo tanto $ab|c$. □

El hecho de que el máximo común divisor de dos enteros a y b puede ser escrito como una combinación lineal entera de a y b (proposición 3.3.8) es una herramienta de suma utilidad para trabajar en problemas relacionados con el mcd. Por ejemplo, todos estamos familiarizados con la idea de que una fracción puede reducirse al "mínimo término", o sea a la forma a/b con a y b coprimos. El siguiente ejemplo establece que esta forma es única, y como veremos, el hecho clave de la demostración es que podemos expresar a 1 como $sa + tb$.

Ejemplo. Supongamos que a, a', b, b' son enteros positivos que satisfacen

a) $ab' = a'b$; *b)* $\text{mcd}(a, b) = \text{mcd}(a', b') = 1$.

Entonces $a = a'$ y $b = b'$.

(La condición *a)* podría escribirse como $a/b = a'/b'$, pero preferimos usar esta forma que no asume ningún conocimiento sobre fracciones.)

Demostración. Como por *b)* el $\text{mcd}(a, b) = 1$ existen enteros s y t tales que $sa + tb = 1$. En consecuencia

$$b' = (sa + tb)b' = sab' + tbb' \overset{a)}{=} sa'b + tb'b = (sa' + tb')b,$$

y por lo tanto $b|b'$. Por un argumento similar y usando el hecho de que el $\text{mcd}(a', b') = 1$ deducimos que $b'|b$, por lo tanto $b = b'$ o $b = -b'$ y como b y b' son ambos positivos debemos tener $b = b'$. Ahora de *a)* deducimos que $a = a'$ y el resultado esta demostrado. □

Observación (*). El algoritmo explicado anteriormente para obtener el $\text{mcd}(a, b)$ como combinación lineal entera $sa + tb$ no es muy sencillo de programar. Más aún, requiere terminar el cálculo del mcd usando el algoritmo de Euclides, para comenzar a calcular los coeficientes enteros s, t. Veremos a continuación un algoritmo que calcula usando el algortimo de Euclides simultáneamente los coeficientes enteros s y t y el máximo común divisor. El algoritmo se basa en el siguiente resultado, que es una forma más precisa de enunciar el teorema 3.3.8 .

Proposición 3.3.12. *Sean,* a, b *enteros,* $b > 0$*, y* r_i, q_i *los restos y cocientes obtenidos en el algoritmo de Euclides (ver tabla 1). Entonces,*

a) para $0 \leqslant i \leqslant k$*, existen* $s_i, t_i \in \mathbb{Z}$ *tal que*

$$r_i = s_i a + t_i b. \tag{3.3.2}$$

b) Más precisamente, si $s_0, t_0 = 1, 0$ *,* $s_1, t_1 = 0, 1$ *y*

$$s_i = s_{i-2} - q_{i-1}s_{i-1}, \qquad t_i = t_{i-2} - q_{i-1}t_{i-1}, \tag{3.3.3}$$

para $i \geqslant 2$*. Entonces* s_i*,* t_i *satisfacen (3.3.2).*

Demostración. *a)* Lo haremos por inducción sobre i.

Como r_i se define con una recursión que se basa en los dos casos anteriores, el caso base debe hacerse en dos valores: $i = 0$ e $i = 1$, pero como $r_0 = a$ (en este caso $s_0 = 1, s_1 = 0$) y $r_1 = b$ (en este caso $s_0 = 0, s_1 = 1$), se cumple el enunciado para el caso base.

Paso inductivo. Si $i > 1$, tenemos

$$\begin{aligned} r_i &= r_{i-2} + (-q_{i-1})r_{i-1} \\ &= s_{i-2}a + t_{i-2}b + (-q_{i-1})(s_{i-1}a + t_{i-1}b) \qquad \text{(hipótesis inductiva)} \\ &= (s_{i-2} - q_{i-1}s_{i-1})a + (t_{i-2} - q_{i-1}t_{i-1})b. \end{aligned}$$

b) Es claro por la demostración de *a)*. □

Con el uso de *b)* de la proposición anterior, podemos escribir el algoritmo para obtener s, t tal $\text{mcd}(a, b) = sa + tb$ con el siguiente pseudocódigo.

ALGORITMO DE EUCLIDES 2

```
# pre: a y b son números positivos
# post: Obtenemos s y t tal que mcd(a,b) = a*s + b*t
r[0], r[1] = a, b
s[0], t[0], s[1], t[1] = 1, 0, 0, 1
i = 1
while r[i] != 0:
    # invariante: r[i-1] = a * s[i-1] + b * t[i-1]
    #             y  mcd(a, b) = mcd(r[i-1], r[i])
    q, r[i+1] = r[i-1] // r[i], r[i-1] % r[i]
    s[i+1] = s[i-1] - s[i] * q
    t[i+1] = t[i-1] - t[i] * q
    i = i+1
s, t  = s[i-1], t[i-1]
```

Sin embargo, este algoritmo no es muy conveniente, a nivel de eficiencia de memoria, pues las variables r, s y t van guardando series de valores en forma innecesaria.

Una versión mejorada, aunque menos legible, es la siguiente.

Algoritmo de Euclides 2 (versión 2)

```
# pre: a y b son números positivos
# post: Obtenemos s y t tal que mcd(a,b) = a*s + b*t
r0, r1 = a, b
s0, t0, s1, t1 = 1, 0, 0, 1
while r1 != 0:
    # invariante: r0 = a * s0 + b * t0  y
    #              mcd(a, b) = mcd(r0, r1)
    resto = r0 % r1
    q, r0, r1 = r0 // r1, r1, resto
    s1p, t1p = s1, t1
    s0, t0, s1, t1 =  s1p, t1p, s0 - s1 * q, t0 - t1 * q
s, t  = s0, t0
```

Este último código y el de la página 56 son códigos válidos en Python 3 y pueden ser incorporados a un programa escrito en ese lenguaje.

§ *Mínimo común múltiplo*

Definición 3.3.13. Sean a y b enteros no nulos. Decimos que un entero positivo m es el *mínimo común múltiplo*, o *mcm*, de a y b si

a) $a|m$ y $b|m$;

b) si $a|n$ y $b|n$ entonces $m|n$.

La condición *a)* nos dice que m es múltiplo común de a y b, la condición *b)* nos dice que cualquier otro múltiplo de a y b también debe ser múltiplo de m. Por ejemplo hallemos el mínimo común múltiplo entre 8 y 14. Escribamos los múltiplos de ambos números y busquemos el menor común a ambos. Los primeros múltiplos de 8 son: $8, 16, 24, 32, 40, 48, 56, \ldots$. Los primeros múltiplos de 14 son: $14, 28, 42, 56, 72, \ldots$. Luego se tiene $\text{mcm}(8, 14) = 56$. Nos faltaría comprobar que cualquier múltiplo de 8 y 14 es múltiplo de 56, pero eso se deduce fácilmente de los resultados que veremos a continuación.

El siguiente teorema garantiza la existencia del mcm.

Teorema 3.3.14. *Sean a y b enteros no nulos, entonces*

$$\mathrm{mcm}(a,b) = \frac{ab}{\mathrm{mcd}(a,b)}.$$

Demostración. Demostraremos que

$$m = \frac{ab}{\mathrm{mcd}(a,b)}$$

es el mínimo común múltiplo de a, b.

Como

$$m = \frac{ab}{\mathrm{mcd}(a,b)} = \frac{a}{\mathrm{mcd}(a,b)}b = a\frac{b}{\mathrm{mcd}(a,b)}$$

resulta que m es múltiplo de a y b, y por lo tanto se satisface *a)* de la definición de mínimo común múltiplo. Veamos ahora *b)*: sea $n \in \mathbb{Z}$ tal que $a|n$ y $b|n$. Como existen enteros r, s tales que

$$\mathrm{mcd}(a,b) = ra + sb, \tag{3.3.4}$$

dividiendo la ecuación (3.3.4) por $\mathrm{mcd}(a,b)$ y multiplicando por n, obtenemos la siguiente ecuación:

$$n = r\frac{a}{\mathrm{mcd}(a,b)}n + s\frac{b}{\mathrm{mcd}(a,b)}n. \tag{3.3.5}$$

Escribiendo $n = b'b = a'a$ (a', b' en $\mathbb{Z}$) y haciendo los reemplazos en (3.3.5), resulta finalmente

$$n = rb'\frac{ab}{\mathrm{mcd}(a,b)} + sa'\frac{ab}{\mathrm{mcd}(a,b)} = (rb' + sa')m,$$

lo cual demuestra que m divide a n. □

En particular este resultado implica que si a y b son enteros coprimos, entonces $\mathrm{mcm}(a,b) = ab$.

Ejemplo. Encontrar el mcm de 8 y 14.

Solución. Es claro que $2 = \mathrm{mcd}(8,14)$, luego $\mathrm{mcm}(8,14) = 8 \cdot 14/2 = 56$. □

§ *Ejercicios*

1) Encontrar el mcd de 721 y 448 y expresarlo en la forma $721m + 448n$ con $m, n \in \mathbb{Z}$.

2) Usar proposición 3.3.8 para demostrar que si a, b y n son enteros no nulos, entonces $\operatorname{mcd}(na, nb) = n \operatorname{mcd}(a, b)$.

3) Usar el Ej. 2 para demostrar que si el $\operatorname{mcd}(a, b) = d$, entonces

$$\operatorname{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

4) Sean a y b enteros positivos y sea $d = \operatorname{mcd}(a, b)$. Probar que existen enteros x e y que satisfacen la ecuación $ax + by = c$ si y solo si $d|c$.

5) Encontrar enteros x e y que satisfagan $966x + 685y = 70$.

3.4 factorización en primos

Definición 3.4.1. Se dice que un entero positivo p es *primo* si $p \geqslant 2$ y los únicos enteros positivos que dividen p son 1 y p mismo.

Luego si un entero $m \geqslant 2$ no es un primo si y sólo si existe m_1 divisor de m tal que $m_1 \neq 1, m$, es decir con $1 < m_1 < m$. Sea m_2 el cociente de m por m_1: es claro que $m_2 \neq 1, m$ y por lo tanto $1 < m_2 < m$. Concluyendo,

un entero $m \geqslant 2$ no es un primo si y sólo si $m = m_1 m_2$ donde m_1 y m_2 son enteros estrictamente entre 1 y m.

Enfaticemos que de acuerdo a la definición, 1 *no* es primo.

Los primeros primos (los menores que 100) son

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 \text{ y } 97.$$

Observación (Criba de Eratóstenes *). Un forma de encontrar números primos es con la *criba de Eratóstenes.* Es un algoritmo que permite hallar todos los números primos menores que un número natural dado n. Se forma una lista con todos los números naturales comprendidos entre 2 y n, y se van tachando los números que no son primos de la siguiente manera: comenzando por el 2, se tachan todos sus múltiplos; comenzando de nuevo, cuando se encuentra un número entero que no ha sido tachado, ese número es declarado primo, y se procede a tachar todos sus múltiplos y así sucesivamente. El proceso termina cuando alcanzamos n.

Podemos expresar el algoritmo en pseudocódigo:

Criba de Eratóstenes

```
# pre: n número natural
# post: se obtiene ''primos'' la lista de números primos hasta n
primos = [] # lista vacía
tachados = [] # lista de números tachados
for i = 2 to n:
    if i not in tachados:
        primos.append(i) # agregar i a primos
        k = 2
        while k * i <= n:
            tachados.append(k * i) # agrega k*i a tachados
            k = k + 1
```

Este código en si no es eficiente, pero muestra una forma sencilla de obtener primos con el uso de la criba de Eratóstenes. El código puede ser mejorado y su rendimiento aumenta enormemente, como en la siguiente implementación.

Criba de Eratóstenes 2

```
# pre: n número natural
# post: primos[i] = True si y solo si i <= n es primo.
primos = lista de longitud n con todas las coordenadas True
for i = 2 to [n^0.5]:
    if primos[i] == True:
        for j = i**2 to n+1 step i:
            primos[j] = False
```

En el algoritmo `[n^0.5]` denota la parte entera de la raíz cuadrada de `n`. Por otro lado, `for j = k to m step t` simboliza que comenzamos un contador `j` en `k` y lo vamos incrementando en `t` hasta llegar a `m`.

El lector debe estar casi totalmente familiarizado con la idea de que cualquier entero positivo puede expresarse como producto de primos: por ejemplo

$$825 = 3 \cdot 5 \cdot 5 \cdot 11.$$

La existencia de esta factorización en primos para cualquier entero positivo es una consecuencia del axioma del buen orden.

Teorema 3.4.2. *Todo entero mayor que* 1 *es producto de números primos.*

Demostración. Sea B el conjunto de enteros positivos que no tienen una factorización en primos.

Si B no es vacío entonces, por el axioma del buen orden, tiene un mínimo m. Si m fuera un primo p entonces tendríamos la factorización trivial

$m = p$; por lo tanto m no es primo y existen m_1, m_2 enteros positivos con $1 < m_1 < m$ y $1 < m_2 < m$ tal que $m = m_1 m_2$.

Como estamos suponiendo que m es el menor entero ($\geqslant 2$) que no tiene factorización en primos, entonces m_1 y m_2 tienen factorización en primos. Pero entonces la ecuación $m = m_1 m_2$ produce una factorización en primos de m, contradiciendo la suposición de que m era un elemento de B. Por lo tanto B debe ser vacío, y la afirmación esta probada. $\square$

Ejemplo. Encontremos la factorización en números primos de 201 000. Esto se hace dividiendo sucesivamente los números hasta llegar a factores primos:

$$\begin{aligned} 201\,000 = 201 \cdot 1000 &= 3 \cdot 67 \cdot 10 \cdot 10 \cdot 10 \\ &= 3 \cdot 67 \cdot 2 \cdot 5 \cdot 2 \cdot 5 \cdot 2 \cdot 5 \\ &= 2^3 \cdot 3 \cdot 5^3 \cdot 67. \end{aligned}$$

Como vimos más arriba $2, 3, 5$ y 67 son números primos y por lo tanto hemos obtenido la descomposición prima de 201 000.

Veamos ahora algunas propiedades básicas de los números primos.

Observación 3.4.3. Sea $a \in \mathbb{Z}$ y p primo. Entonces

a) Si $p \not| a$, entonces $\operatorname{mcd}(a, p) = 1$.

b) Si p y p' son primos y $p | p'$ entonces $p = p'$.

Demostración.

a) Como los únicos divisores de p son p y 1, y $p \not| a$, el único divisor común de p y a es 1.

b) p' es primo, por lo tanto tiene sólo dos divisores positivos 1 y p'. Como p no es 1, tenemos que $p = p'$. $\square$

Para encontrar una descomposición prima de un número, digamos n, debemos ir tomando todos los números menores a n y comprobando si estos lo dividen o no. En lo que sigue veremos el criterio de la raíz, que se utiliza para comprobar si un número es primo en menos pasos que la comprobación directa.

Lema 3.4.4. *Si $n > 0$ no es primo, entonces existe $m > 0$ tal que $m | n$ y $m \leqslant \sqrt{n}$.*

Demostración. Si n no es primo, entonces $n = m_1 m_2$ con $1 < m_1, m_2 < n$. Supongamos que $m_1, m_2 > \sqrt{n}$, entonces $n = m_1 m_2 > \sqrt{n}\sqrt{n} = n$, lo cual es una contradicción. Por lo tanto, m_1 o m_2 debe ser menor o igual que $\sqrt{n}$ y por consiguiente encontramos un divisor de n menor o igual a $\sqrt{n}$. $\square$

Proposición 3.4.5 (Criterio de la raíz)**.** *Sea* $n \geqslant 2$*. Si para todo* m *tal que* $1 < m \leqslant \sqrt{n}$ *se cumple que* $m \not| n$*, entonces* n *es primo.*

Demostración. Supongamos que n no es primo, luego, por el lema anterior, existe m tal que $m|n$ y $1 < m \leqslant \sqrt{n}$ y esto contradice nuestras hipótesis. La contradicción se produce al suponer que n no es primo, por lo tanto n es primo. □

Este criterio reduce enormemente la cantidad de pruebas que debemos hacer para verificar si un número es primo.

Ejemplo. Verifiquemos si 467 es primo o no.

Solución. Observar primero que si no utilizamos el criterio de la raíz deberíamos hacer 465 divisiones: deberíamos comprobar si $m|467$ con $1 < m < 467$.

Como $\sqrt{467} < 22$, por el criterio de la raíz, sólo debemos comprobar si $m|467$ para $2 \leqslant m \leqslant 21$. Un sencilla comprobación (dividiendo) muestra que los números $2, 3, \cdots, 20, 21$ no dividen a 467 y por lo tanto 467 es primo. □

La facilidad con la que establecemos la existencia de la factorización de primos conlleva dos dificultades importantes. Primero el problema de encontrar los factores primos no es de ningún modo directo; y segundo no es obvio que exista una *única* factorización en primos para todo entero dado $n \geqslant 2$. El siguiente resultado es un paso clave en la demostración de la unicidad.

Teorema 3.4.6. *Sea* p *un número primo.*

a) *Si* $p|xy$ *entonces* $p|x$ *o* $p|y$.

b) $x_1, x_2, \ldots, x_n$ *son enteros tales que*

$$p|x_1x_2\ldots x_n$$

entonces $p|x_i$ *para algún* x_i *(*$1 \leqslant i \leqslant n$*).*

Demostración.

a) Si $p|x$ ya está probado el resultado. Si $p \not| x$ entonces tenemos $\text{mcd}(x, p) = 1$. Por proposición 3.3.8, existen enteros r y s tales que $rp + sx = 1$. Por lo tanto tenemos

$$y = 1 \cdot y = (rp + sx)y = (ry)p + s(xy).$$

Como $p|p$ y $p|xy$, entonces divide a ambos términos y se sigue que $p|y$.

b) Usemos el principio de inducción. El resultado es obviamente verdadero cuando $n = 1$ (base inductiva).

Ahora, supongamos que el resultado es verdadero cuando $n = k$, es decir si $p|x_1x_2\ldots x_k$, entonces $p|x_i$ para algún i con $1 \leqslant i \leqslant k$ (hipótesis inductiva).

Debemos probar que si $p|x_1x_2\ldots x_kx_{k+1}$, entonces $p|x_i$ para algún x_i $(1 \leqslant i \leqslant k+1)$.

Supongamos $p|x_1x_2\ldots x_kx_{k+1}$ y sea $x = x_1x_2\ldots x_k$. Si $p|x$ entonces, por la hipótesis inductiva, $p|x_i$ para algún x_i en el rango $1 \leqslant i \leqslant k$. Si $p \not| x$ entonces, por 1), se sigue que $p|x_{k+1}$. De este modo, en ambos casos p divide uno de los x_i $(1 \leqslant i \leqslant k+1)$. □

Un error común es asumir que el teorema 3.4.6 se mantiene verdadero cuando reemplazamos el primo p por un entero arbitrario . Pero esto claramente falso: por ejemplo

$$6|3 \cdot 8 \quad \text{pero} \quad 6 \not| 3 \quad \text{y} \quad 6 \not| 8.$$

Ejemplos como éste nos ayudan a entender que el teorema 3.4.6 expresa una propiedad muy significativa de los números primos. Además veremos que esta propiedad juega un papel crucial en el siguiente resultado, que a veces es llamado el *Teorema Fundamental de la Aritmética*.

Teorema 3.4.7. *La factorización en primos de un entero positivo $n \geqslant 2$ es única, salvo el orden de los factores primos.*

Demostración. Por el axioma del buen orden, si existe un entero para el cual el teorema es falso, entonces hay un entero mínimo $n_0 \geqslant 0$ con esta propiedad. Supongamos entonces que

$$n_0 = p_1p_2\ldots p_k \quad \text{y} \quad n_0 = p'_1p'_2\ldots p'_l,$$

donde los p_i $(1 \leqslant i \leqslant k)$ son primos, no necesariamente distintos, y los p'_i $(1 \leqslant i \leqslant l)$ son primos, no necesariamente distintos. La primera ecuación implica que $p_1|n_0$, y la segunda ecuación implica que $p_1|p'_1p'_2\ldots p'_l$. Por consiguiente por teorema 3.4.6 tenemos que $p_1|p'_j$ para algún j $(1 \leqslant j \leqslant l)$. Reordenando la segunda factorización podemos asumir que $p_1|p'_1$, y puesto que p_1 y p'_1 son primos, se sigue que $p_1 = p'_1$ (observación 3.4.3 *b)*). Luego por el axioma (**I7**), podemos cancelar los factores p_1 y p'_1, y obtener

$$p_2p_3\ldots p_k = p'_2p'_3\ldots p'_l,$$

y llamemos a este número n_1. Pero supusimos que n_0 tenía dos factorizaciones diferentes, y hemos cancelado el mismo número $(p_1 = p'_1)$ en ambas factorizaciones, luego n_1 tiene también dos factorizaciones primas diferentes. Esto contradice la definición de n_0 como el mínimo entero sin factorización única. Por lo tanto el teorema es verdadero para $n \geqslant 2$. □

En la práctica a menudo reunimos los primos iguales en la factorización de n y escribimos

$$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r},$$

donde $p_1, p_2, \dots, p_r$ son primos distintos y $e_1, e_2, \dots, e_r$ son enteros positivos. Por ejemplo $7000 = 2^3 \cdot 5^3 \cdot 7$.

La unicidad de la factorización prima de cualquier entero mayor que 1 nos permite hacer la siguiente definición.

Definición 3.4.8. Se n entero mayor o igual a 2 y

$$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r},$$

donde p_i primo para todo i $(1 \leqslant i \leqslant r)$ y $e_1, e_2, \dots, e_r$ son enteros positivos. Entonces, diremos que $p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ es la *factorización prima de* n y que p_i es un *factor primo de* n $(1 \leqslant i \leqslant r)$.

La factorización prima nos dice que los números primos son los "ladrillos" esenciales para "construir" los números enteros usando multiplicaciones. Ahora bien, podría ocurrir que haya un número finitos de ellos y que podamos escribir cada número como producto de primos en forma muy sintética. Pero este no es el caso.

Proposición 3.4.9 (Teorema de Euclides)**.** *Existen infinitos números primos.*

Demostración. Haremos la demostración por el absurdo: supongamos que existen en total r números primos $p_1, p_2, \dots, p_r$. Sea $n = p_1 p_2 \dots p_r + 1$. Sea p primo tal que $p|n$. Como la lista de primos es exhaustiva, existe i con $1 \leqslant i \leqslant r$ tal que $p = p_i$. Ahora bien $p_i|n$ y $p_i|p_1 p_2 \dots p_r$, luego $p_i|n - p_1 p_2 \dots p_r = 1$, lo cual es un absurdo que vino de suponer que el número de primos es finito. □

Ejemplo. Probemos que si m y n son enteros tales que $m \geqslant 2$ y $n \geqslant 2$, entonces $m^2 \neq 2n^2$.

Demostración. Supongamos que la factorización prima de n contiene al 2 elevado a la x (donde x es cero si 2 no es factor primo de n). Entonces $n = 2^x h$, donde h es producto de primos más grandes que 2, luego

$$2n^2 = 2(2^x h)^2 = 2^{2x+1} h^2.$$

Por lo tanto 2 está elevado a una potencia *impar* en la factorización prima de $2n^2$.

Por otro lado, si $m = 2^y g$, donde g es producto de primos mayores que 2, entonces

$$m^2 = (2^y g)^2 = 2^{2y} g^2,$$

luego 2 está elevado a una potencia *par* (posiblemente cero) en la factorización prima de m^2. se sigue entonces que de ser $m^2 = 2n^2$ deberíamos tener dos factorizaciones primas diferentes del mismo número entero, contradiciendo al teorema 3.4.7. Entonces $m^2 \neq 2n^2$. □

Es claro que la conclusión del ejemplo vale también si nosotros permitimos que alguno de los enteros m o n valga 1. Luego podemos expresar el resultado diciendo que no hay enteros positivos m y n que cumplan

$$\left(\frac{m}{n}\right)^2 = 2$$

o equivalentemente, diciendo que la raíz cuadrada de 2 no puede ser expresada como una fracción m/n.

Una notación conveniente para nuestros propósitos será la siguiente: sean m y n dos enteros positivos, a veces es conveniente escribir la factorización prima de ambos números usando los mismos primos, y los primos que usamos son los que se encuentran en la factorización prima de ambos. Es decir escribimos

$$m = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}, \qquad n = p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}.$$

con $e_i, f_i \geqslant 0$ para $i = 1, \dots, r$ y e_i o f_i distinto de cero.

Veremos ahora un resultado que se puede deducir fácilmente del Teorema Fundamental de la Aritmética (TFA).

Proposición 3.4.10. *Sean* $m, n \geqslant 2$ *con*

$$m = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}, \qquad n = p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}.$$

donde p_i *primo y* $e_i, f_i \geqslant 0$ *para* $i = 1, \dots, r$.

Entonces $m|n$ *si y sólo si* $e_i \leqslant f_i$ *para todo* i.

Demostración.

($\Rightarrow$) Por la descomposición de m es claro que $p^{e_i}|m$. Como $m|n$ entonces $p^{e_i}|n$. Es decir $n = p^{e_i}u$. Es claro por TFA entonces que $e_i \leqslant f_i$.

($\Leftarrow$) Como $e_i \leqslant f_i$, tenemos que $p^{e_i}|p^{f_i}$, para $1 \leqslant i \leqslant r$. Luego

$$p_1^{e_1} p_2^{e_2} \dots p_r^{e_r} | p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}.$$

Es decir $m|n$. □

Corolario 3.4.11. *Sea* $n \geqslant 2$ *y* p *un número primo, entonces* $p|n$ *si y solo si* p *es un factor primo de* n. □

Ahora veremos que es posible calcular el mcd y el mcm de un par de números sabiendo sus descomposiciones primas.

Proposición 3.4.12. *Sean* m *y* n *enteros positivos cuyas factorizaciones primas son*

$$m = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}, \qquad n = p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}.$$

a) El mcd de m *y* n *es* $d = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ *donde, para cada* i *en el rango* $1 \leqslant i \leqslant r$, k_i *es el mínimo entre* e_i *y* f_i.

b) El mcm de m *y* n *es* $u = p_1^{h_1} p_2^{h_2} \dots p_r^{h_r}$ *donde, para cada* i *en el rango* $1 \leqslant i \leqslant r$, h_i *es el máximo entre* e_i *y* f_i.

Demostración.

a) Sea c tal que $c|n$ y $c|m$, entonces los primos que intervienen en la factorización de c son $p_1, \dots, p_r$ y por lo tanto $c = p_1^{t_1} p_2^{t_2} \dots p_r^{t_r}$. Además, como $c|n$ y $c|m$ tenemos que $t_i \leqslant e_i, f_i$ y por lo tanto $t_i \leqslant k_i = \mathrm{mín}(e_i, f_i)$. De esto se deduce que $c|p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = d$. Por otro lado, es claro que $p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ divide a m y n y se deduce el resultado.

b) Se deja como ejercicio. □

Observación. La proposición anterior nos puede llevar a pensar que una forma sencilla de encontrar el mcd y mcm es usando la descomposición en factores primos de los números involucrados. Esto, en general, no es así para números grandes: no hay un método eficiente para encontrar la descomposición prima de un número grande. Esencialmente, el mejor método para encontrar un divisor de un número grande es el criterio de la raíz, es decir probando si algún número menor que la raíz del número original lo divide. El criterio de la raíz baja el número de comprobaciones de n a $\sqrt{n}$ y eso no ayuda mucho cuando n es grande.

Ahora bien, ¿qué es un "número grande"? En la actualidad, por ejemplo, con todos los recursos computacionales de que se disponen, no es posible factorizar números de 200 dígitos o más. Por lo tanto, no podríamos encontrar el mcd de dos números de 200 dígitos o más a partir de la factorización prima de ambos. Sin embargo, con el algoritmo de Euclides el mcd de estos números se obtendría en pocos segundos.

Ejemplo. Encontremos el mcd y el mcm de 825 y 385 utilizando las factorizaciones primas de ambos.

Solución. Como $825 = 3 \cdot 5^2 \cdot 11$ y $385 = 5 \cdot 7 \cdot 11$, tenemos que

$$\mathrm{mcd}(825, 385) = 5 \cdot 11 = 55, \qquad \mathrm{mcm}(825, 385) = 3 \cdot 5^2 \cdot 7 \cdot 11 = 5775.$$

□

§ *Ejercicios*

1) Sean m, n enteros con $m, n \geqslant 2$. Probar que, m y n son coprimos si y sólo si no comparten ningún primo en la factorización.

   En otras palabras, sean

   $$m = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}, \qquad n = q_1^{f_1} q_2^{f_2} \ldots q_s^{f_s},$$

   las descomposiciones primas de m y n con $e_i, f_j > 0$. Entonces $\mathrm{mcd}(m, n) = 1$ si y sólo si con $p_i \neq q_j$ para todos los i, j.

2) Probar que si m y n son enteros positivos, tales que $m \geqslant 2$ y $n \geqslant 2$, y $m^2 = kn^2$, entonces k es el cuadrado de un entero.

3) Usar la identidad

   $$2^{rs} - 1 = (2^r - 1)(2^{(s-1)r} + 2^{(s-2)r} + \cdots + 2^r + 1)$$

   para probar que si $2^n - 1$ es primo, entonces n es primo.

4) Encontrar el mínimo n para el cual la recíproca del ejercicio anterior es falsa: esto es, n es primo pero $2^n - 1$ no lo es.

5) Para $n \in \mathbb{N}$ sea q_n el factor primo más pequeño de $n! + 1$.

   a) Probar que $q_n > n$.

   b) Probar, usando el resultado del item anterior, que existen infinitos números primos (demostración de Hermite).