Proposición.

(*i*) *La relación* $\mid$ *de divisibilidad en* $\mathbb{Z}$ *es reflexiva, transitiva y para cada* $a, b \in \mathbb{Z}$ *se tiene que*

$$a \mid b,\ b \mid a \implies a = b \text{ o } a = -b. \tag{1}$$

(*ii*) *La restricción de la relación* $\mid$ *de divisibilidad a* $\mathbb{N}$ *o a* $\mathbb{N}_0$ *es una relación de orden, es decir, es reflexiva, transitiva y anti-simétrica.*

Como se trata de una relación de orden en $\mathbb{N}$, podemos restringirla a cualquier subconjunto de $\mathbb{N}$ y obtener una relación de orden. En la Figura 6.1 en la página siguiente dibujamos el diagrama de Hasse de su restricción al conjunto de todos los divisores de 360.

Demostración. (*i*) Si a es un elemento de $\mathbb{Z}$, entonces $a = a \cdot 1$ y, por lo tanto, $a \mid a$: esto nos dice que la relación de divisibilidad es reflexiva. Por otro lado, si a, b y c son enteros y se tiene que $a \mid b$ y $b \mid c$, de manera que existen enteros x e y tales que $b = ax$ y $c = by$, entonces claramente $c = axy$ y esto nos dice que $a \mid c$: vemos así que la relación $\mid$ es transitiva.

Sean ahora a y b dos elementos de $\mathbb{Z}$ y supongamos que $a \mid b$ y que $b \mid a$, de manera que existen enteros c y d tales que $b = ac$ y $a = bd$. Tenemos entonces que $a = acd$, es decir, que

$$a(1 - cd) = 0. \tag{2}$$

Si $a = 0$, entonces $b = ac = 0c = 0$ y a y b son iguales. Si en cambio $a \neq 0$, entonces de la igualdad (2) se deduce que $1 - cd = 0$, esto es, que $cd = 1$ y, por lo tanto, que $c = 1$ o $c = -1$. Correspondiendo a esas dos posibilidades tenemos que $b = a \cdot 1 = a$ o que $b = a \cdot (-1) = -a$. Esto prueba la implicación (1).

(*ii*) La restricción de la relación $\mid$ a $\mathbb{N}$ o a $\mathbb{N}_0$ es reflexiva y transitiva porque la relación original en $\mathbb{Z}$ lo es, como acabamos de mostrar. Nos queda entonces probar que es anti-simétrica. Sean a y b dos elementos de $\mathbb{N}_0$ tales que $a \mid b$ y $b \mid a$. Como en $\mathbb{Z}$ vale la implicación (1), tenemos que $a = b$ o $a = -b$. Como a y b no negativo, esto solo puede ocurrir si son, de hecho, los dos nulos y, en particular, iguales. Esto prueba que la relación de divisibilidad en $\mathbb{N}_0$ es anti-simétrica, y esto implica inmediatamente que también lo es en $\mathbb{N}$. □

6.1.4. Usaremos muchas veces la siguiente observación, que establece una relación entre la relación de divisibilidad y la del orden usual de los números enteros:

Proposición. *Sean* a *y* b *dos enteros. Si* $b \mid a$ *y* $a \neq 0$*, entonces* $|b| \leq |a|$.

Notemos que la hipótesis de que el entero a no sea nulo es necesaria para alcanzar la conclusión de la proposición: por ejemplo, es $1 \mid 0$ pero ciertamente no vale que $1 \leq 0$.

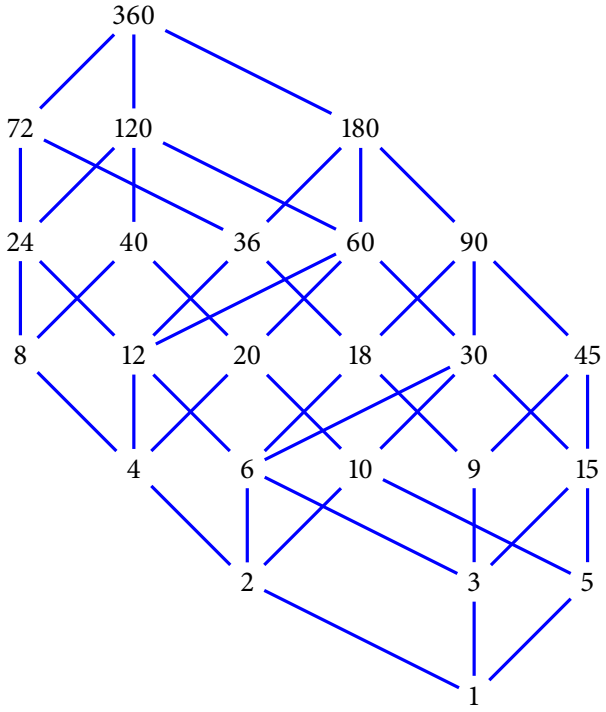


Figura 6.1. El diagrama de Hasse de la relación de divisibilidad restringida al conjunto de los divisores positivos de 360.

Demostración. Supongamos que b divide a a, de manera que hay un entero c tal que $a = bc$. De esto se sigue que $|a| = |b||c|$. Si $a \neq 0$, entonces tiene que ser $c \neq 0$ y, por lo tanto, como c es un entero, $|c| \geq 1$: tenemos entonces que $|a| = |b||c| \geq |b|$, como afirma la proposición. □

6.1.5. Otra propiedad básica de la divisibilidad es su compatibilidad con las operaciones aritméticas:

Proposición. *Sean a, b y c tres enteros.*
(*i*) *Si c divide a a y b, entonces también divide a $a + b$ y a $a - b$.*
(*ii*) *Si c divide a a, entonces también divide a ab.*

Las recíprocas de estas dos afirmaciones son falsas. Por ejemplo, 2 divide a $5 + 3$ y a $5 + 3$ pero no divide ni a 5 ni a 2. De manera similar, 6 divide a $4 \cdot 3$ pero no divide a ninguno de los dos factores. Hay, de todas formas, una situación importante en la que sí podemos garantizar que la implicación recíproca de la de (*ii*) vale: nos ocuparemos de eso en la Proposición 9.2.2 más adelante.

Demostración. (i) Supongamos que c divide a a y a b, de manera que hay enteros x e y tales que $a = cx$ y $b = cy$. En ese caso tenemos que $a + b = cx + cy = c(x + y)$ y $a - b = cx - cy = c(x - y)$: como claramente $x + y$ y $x - y$ son enteros, esto nos dice que c divide a $a + b$ y a $a - b$. La primera afirmación de la proposición queda así probada.

(i) Supongamos ahora que c divide a a, de manera que hay un entero x tal que $a = cx$. Por supuesto, esto implica que $ab = cbx$ y, por lo tanto, que c divide a ab. □

6.1.6. Muchas veces usaremos la Proposición 6.1.5 vía el siguiente corolario:

Corolario. *Sean a, b y c tres enteros. Si c divide a a y a $a + b$, entonces también divide a b.*

Demostración. En efecto, en ese caso de la proposición se sigue que c divide a $(a + b) - a = b$. □

§6.2. El algoritmo de la división

6.2.1. Si a y b son enteros y b divide a a, entonces hay otro entero c tal que $a = bc$. Cuando b *no* divide a a, esto no es cierto, por supuesto. La Proposición 6.2.3 que probaremos más abajo nos permite describir exactamente qué sucede en el caso general.

6.2.2. Antes de eso, hagamos una observación que nos será útil varias veces:

Lema. *Sea $b \in \mathbb{N}$ y sean $i, j \in \mathbb{Z}$. Si $0 \leq i, j < b$ y $b \mid i - j$, entonces $i = j$.*

Demostración. Supongamos que $0 \leq i, j < b$ y $b \mid i - j$. Tenemos entonces que

$$-b < 0 - j \leq i - j < b - j \leq b,$$

así que $|i - j| < b$. Por otro lado, como b divide a $i - j$, de la Proposición 6.1.4 sabemos que o bien $i - j = 0$ o bien $|b| \leq |i - j|$. La segunda de estas dos posibilidades no puede ocurrir, así que debe ocurrir la primera: esto nos dice que $i = j$, como afirma el lema. □

6.2.3. La siguiente proposición establece una propiedad fundamental de los números enteros:

Proposición. *Sean $a \in \mathbb{Z}$ y $b \in \mathbb{N}$. Hay enteros q y r tales que $a = qb + r$ y $0 \leq r < b$ y, más aún, estos enteros q y r están unívocamente determinados por a y b.*

Llamamos a q y a r el ***cociente*** y el ***resto*** de la ***división*** de a por b, respectivamente.

Demostración. Consideremos el conjunto

$$S \coloneqq \{a - kb : k \in \mathbb{Z}, a - kb \geq 0\}.$$

Este conjunto no es vacío: si $a \geq 0$, entonces $a - 0 \cdot b = a \geq 0$, así que $a \in S$, y si en cambio $a < 0$, entonces $a - (2a)b = (1 - 2b)a \geq 0$, así que $a - (2a)b \in S$. Como S está claramente contenido en $\mathbb{N}_0$, podemos considerar su mínimo $r \coloneqq \min S$.

Como r pertenece a S, es $r \geq 0$ y existe $q \in \mathbb{Z}$ tal que $r = a - qb$, es decir, tal que $a = qb + r$. Mostremos que $r < b$. Supongamos por un momento que esto no es así, de manera que $r \geq b$ y, por lo tanto, $a - (q+1)b = r - b \geq 0$. Como consecuencia de esto, tenemos que $r - b \in S$: esto es absurdo, ya que $r - b$ es estrictamente menor que r, porque b es positivo, y r es el menor elemento de S. Vemos así que $a = qb + r$ y que $0 \leq r < b$, y esto prueba la afirmación de existencia del enunciado. Veamos la de unicidad.

Supongamos que q, r, q' y r' son enteros tales que

$$a = qb + r, \qquad 0 \leq r < b, \tag{3}$$

y

$$a = q'b + r, \qquad 0 \leq r' < b. \tag{4}$$

Observemos que

$$qb + r = q'b + r' \tag{5}$$

y, por lo tanto, que $r - r' = (q' - q)b$. En particular, b divide a $r - r'$: como $0 \leq r, r' < b$, de acuerdo al Lema 6.2.2 tenemos entonces que $r = r'$. Usando esto en (5), concluimos que $qb = q'b$ y, en consecuencia, que $(q - q')b = 0$. Como $b \neq 0$, esto nos dice que $q - q' = 0$, esto es, que $q = q'$. Así, si se cumplen las condiciones (3) y (4) se tiene necesariamente que $q = q'$ y que $r = r'$: esto prueba la afirmación de unicidad de la proposición. □

6.2.4. El siguiente corolario de la proposición es casi inmediato y muestra que podemos ver al resto de la división de un número por otro, en cierta forma, como la única "obstrucción" a la divisibilidad.

Corolario. *Sean $a \in \mathbb{Z}$ y $b \in \mathbb{N}$. El resto de la división de a por b es 0 si y solamente si b divide a a.*

Demostración. Sean q y r el cociente y el resto, respectivamente, de la división de a por b, de manera que $a = qb + r$ y $0 \leq r < b$. Observemos que es $|r| < b$.

Si $r = 0$, entonces tenemos que $a = qb$ y, por lo tanto, que b divide a a. Supongamos, para probar la implicación recíproca, que b divide a a. Hay entonces un entero c tal que $a = bc$ y, por lo

tanto, $bc = qb + r$. De esta igualdad vemos que $r = (c - q)b$, así que, en particular, b divide a r y, de acuerdo a la Proposición 6.1.4, o bien $r = 0$ o bien $|b| \leq |r|$. Esta segunda posibilidad no ocurre — en efecto, sabemos que $|r| < b = |b|$ — así que necesariamente $r = 0$. Esto prueba el corolario. □

6.2.5. Una observación importante que debemos hacer es que si $a \in \mathbb{Z}$ y $b \in \mathbb{N}$ siempre podemos encontrar de manera efectiva al cociente q y al resto r de la división de a por b. En la base de esto esta la siguiente descripción alternativa de ese cociente:

Lema. *Sea a un entero no negativo. El conjunto $T \coloneqq \{k \in \mathbb{N}_0 : a - kb \geq 0\}$ es no vacío y finito, y su elemento máximo es el cociente de la división de a por b.*

Demostración. El conjunto T no es vacío, ya que contiene a 0. Por otro lado, si $k \in T$, entonces $a - kb \geq 0$ y, por lo tanto, $k \leq a/b$: esto nos dice que el conjunto T está contenido en $\{0, \ldots, \lfloor a/b \rfloor\}$ y, en particular, que es finito. Tiene entonces sentido considerar su elemento máximo $q \coloneqq \max T$. Pongamos además $r \coloneqq a - qb$.

Como $q \in T$, es $r \geq 0$. Tiene que ser $r < b$: si no fuese ese el caso, tendríamos que

$$a - (q + 1)b = a - qb - b = r - b \geq 0$$

y, por lo tanto, que $q + 1 \in T$: esto es absurdo, ya que elegimos a q como el mayor elemento de T. Concluimos de esta manera que $a = qb + r$ y que $0 \leq r < b$. De acuerdo a la Proposición 6.2.3, se sigue de esto que q y r son el cociente y el resto de la división de a por b y esto prueba el lema. □

6.2.6. Este lema nos dice cómo encontrar el cociente y el resto de la división de un entero cualquiera a por un entero positivo b.

- Si a es positivo, este lema nos dice que para buscar el cociente y el resto de la división de a por b podemos proceder de la siguiente manera: para cada número $i \in \mathbb{N}_0$ desde 0 en adelante, en orden, calculamos $a - (i + 1)b$ y paramos la primera vez que esa diferencia sea negativa: el cociente entonces es i y el resto es $a - ib$.
- Si en cambio a es negativo, podemos usar este procedimiento para encontrar el cociente q y el resto r de la división de $-a$ por b, de manera que $-a = qb + r$ y $0 \leq r < b$. Si $r = 0$, entonces tenemos que $a = (-q)b$, así que $-q$ y 0 son el resto y el cociente de dividir a a por b; si en cambio $r \neq 0$, entonces es $a = (-q - 1)b + (b - r)$ y $0 \leq b - r < b$, así que $-q - 1$ y $b - r$ son el resto y el cociente de esa división.

En la Figuras 6.1 y 6.2 damos implementaciones de este algoritmo en Haskell y en Python. Es de notar que virtualmente todos los lenguajes de programación proveen herramientas para calcular el cociente y el resto de la división entre dos enteros, usando algoritmos mucho más eficientes que este. Así, en Haskell, por ejemplo, tenemos las funciones `div` y `mod` que hacen precisamente

eso: las expresiones `div a b` y `mod a b` denotan, respectivamente, el cociente y el resto de dividir a `a` por `b` cuando `b` es positivo.

```haskell
division :: Integer -> Integer -> (Integer, Integer)
division a b
  | a >= 0   = buscar 0
  | a < 0    = let (q, r) = division (-a) b
               in if r == 0 then (-q, 0) else (-1 - q, b - r)
  where buscar i
          | a - (i + 1) * b >= 0   = buscar (i + 1)
          | otherwise              = (i, a - i * b)
```

Programa 6.1. Un implementación del algoritmo de la división en Haskell. La expresión `division a b` se evalúa a un par ordenado `(q, r)` en el que `q` y `r` son, respectivamente, el cociente y el resto de la división de `a` por `b`.

```python
def division(a, b):
    if a >= 0:
        i = 0
        while a - (i + 1) * b >= 0:
            i = i + 1
        return (i, a - i * b)
    else:
        q, r = division(-a, b)
        if r == 0:
            return (-q, 0)
        else:
            return (-1 - q, b - r)
```

Programa 6.2. Un implementación del algoritmo de la división en Python. La expresión `division(a, b)` se evalúa a un par ordenado `(q, r)` en el que `q` y `r` son, respectivamente, el cociente y el resto de la división de `a` por `b`.

§6.3. La notación posicional

6.3.1. Una aplicación simple pero importante de la Proposición 6.2.3 de la sección anterior es el siguiente resultado, que está en base de la forma en que escribimos normalmente los números.

Proposición. *Sea b un entero tal que $b \geq 2$. Si a es un entero positivo, entonces existen $k \in \mathbb{N}_0$ y $d_0, \ldots, d_k \in \{0, \ldots, b-1\}$ tales que*

$$a = d_0 + d_1 b + d_2 b^2 + \cdots + d_k b^k$$

y $d_k \neq 0$.

Demostración. Para cada entero positivo a sea $P(a)$ la afirmación

$$\text{existen } k \in \mathbb{N}_0 \text{ y } d_0, \ldots, d_k \in \{0, \ldots, b-1\} \text{ tales que } a = \textstyle\sum_{i=0}^{k} d_i b^i \text{ y } d_k \neq 0.$$

Probaremos haciendo inducción con respecto a a que $P(a)$ vale cualquiera sea $a \in \mathbb{N}$.

- Si $a = 1$, claramente podemos elegir $k = 0$ y $d_0 = 1$ para tener $a = \sum_{i=0}^{k} d_i b^i$, y esto prueba que vale la afirmación $P(1)$.
- Sea ahora a un elemento cualquiera de $\mathbb{N}$ y supongamos que cada una de las afirmaciones $P(1), P(2), \ldots, P(a)$ vale. De acuerdo a la Proposición 6.2.3, existen enteros q y r tales que $a+1 = qb + r$ y $0 \leq r < b$. Como $q = (a+1-r)/b \leq (a+1)/b$ y $b \geq 2$, tenemos que $q < a+1$.

  Si $q = 0$, entonces $a = r$ y podemos elegir $k = 0$ y $d_0 = r$ para ver que $P(a+1)$ vale. Supongamos entonces que $q > 0$. En ese caso, nuestra hipótesis inductiva nos dice que $P(q)$ vale, es decir, que existen $l \in \mathbb{N}_0$ y $e_0, \ldots, e_l \in \{0, \ldots, b-1\}$ tales que $q = \sum_{i=0}^{l} e_i b^i$ y $e_l \neq 0$. Como consecuencia de esto tenemos que

  $$a + 1 = r + qb = r + \left(\sum_{i=0}^{l} e_i b^i \right) b = r + \sum_{i=0}^{l} e_i b^{i+1} = r + \sum_{i=1}^{l+1} e_{i-1} b^i.$$

  Podemos entonces elegir $k = l+1$, $d_0 = r$ y $d_i = e_{i-1}$ para cada $i \in \{1, \ldots, k\}$ para tener $a + 1 = \sum_{i=0}^{k} d_i b^i$ y $d_k \neq 0$, y esto muestra que vale la afirmación $P(a+1)$ también en este caso.

La inducción queda así completa y eso prueba la proposición. □

6.3.2. Queremos probar ahora que los números k y $d_0, \ldots, d_k$ de la Proposición 6.3.1 están bien determinados por los números b y a con los que empezamos.

Proposición. *Sea b es un entero tal que $b \geq 2$. Si a es un entero positivo, entonces hay exactamente* una *forma de elegir $k \in \mathbb{N}$ y $d_0, \ldots, d_k \in \{0, \ldots, b-1\}$ de manera que se cumplan las dos condiciones de la Proposición 6.3.1.*

Demostración. Sean $k, l \in \mathbb{N}_0$ y $d_0, \ldots, d_k, e_0, \ldots, e_l \in \{0, \ldots, b-1\}$ tales que

$$d_0 + d_1 b + \cdots + d_k b^k = a = e_0 + e_1 b + \cdots + e_l b^l, \tag{6}$$

$d_k \neq 0$ y $e_l \neq 0$. Probaremos que en esta situación necesariamente se tiene que $k = l$ y que $d_i = e_i$ para todo $i \in \{0, \ldots, k\}$: la proposición es consecuencia inmediata de esto. Observemos que sin pérdida de generalidad podemos suponer que $k \leq l$.

De la igualdad (6) se deduce que

$$d_0 - e_0 = \sum_{i=1}^{l} e_i b^i - \sum_{i=1}^{k} d_i b^i = \left(\sum_{i=1}^{l} e_i b^{i-1} - \sum_{i=1}^{k} d_i b^{i-1} k \right) b,$$

así que $b \mid d_0 - e_0$. Como $0 \leq d_0, e_0 < b$, el Lema 6.2.2 nos permite concluir que $d_0 = e_0$.

Vemos así que el conjunto

$$S \coloneqq \left\{ i \in \{0, \ldots, k\} : d_j = e_j \text{ para cada } j \in \{0, \ldots, i\} \right\}$$

no es vacío y podemos, por lo tanto, considerar su máximo $m \coloneqq \max S$. Tenemos entonces que $m \in S$, de manera que

$$d_j = e_j \text{ para cada } j \in \{0, \ldots, m\},$$

y que o bien $m = k$ o bien $m < k$ y $d_{m+1} \neq e_{m+1}$.

Supongamos que estamos en el segundo de estos dos casos. De la igualdad (6), tenemos que

$$\begin{aligned} 0 &= \sum_{i=0}^{l} e_i b^i - \sum_{i=0}^{k} d_i b^i = \sum_{i=m+1}^{l} e_i b^i - \sum_{i=m+1}^{k} d_i b^i \\ &= e_{m+1} - d_{m+1} + b \left(\sum_{i=m+1}^{l} e_i b^{i-1} - \sum_{i=m+1}^{k} d_i b^{i-1} \right). \end{aligned}$$

Como la expresión entre paréntesis es un entero, esto nos dice que b divide a $d_{m+1} - e_{m+1}$. Como además $0 \leq d_{m+1}, e_{m+1} < b$, el Lema 6.2.2 nos dice que $d_{m+1} = e_{m+1}$: esto es absurdo, ya que contradice nuestra hipótesis.

Debe ser entonces necesariamente $m = k$. Así, todos los sumandos que aparecen a la izquierda de la igualdad (6) también aparecen a la derecha y, por lo tanto, esa igualdad implica que

$$0 = \sum_{i=k+1}^{l} e_i b^i.$$

Si $k < l$, en esta suma cada uno de los términos de esta última suma es no negativo y el último, $e_l b^l$, positivo: esto es imposible. Podemos concluir entonces que $k = l$. Ahora bien, que los tres números m, l y k sean iguales significa precisamente que vale lo que queremos, y esto completa la prueba de la proposición. □

6.3.3. Si b es un entero tal que $n \geq 2$ y a un entero positivo, las Proposiciones 6.3.1 y 6.3.2 nos dicen que hay exactamente una forma de elegir $k \in \mathbb{N}_0$ y $d_0, \ldots, d_k \in \{0, \ldots, b-1\}$ de manera que $a = \sum_{i=0}^{k} d_i b^i$ y $d_k \neq 0$. Escribimos en ese caso

$$a = (d_k, d_{k-1}, \ldots, d_1, d_0)_b.$$

Llamamos a esto la ***representación en base b*** del número a y a los números $d_k, \ldots, d_0$ los ***dígitos*** de a en base b. Cuando b es 10, 2, 8 o 16, decimos ***representación decimal***, ***binaria***, ***octal*** o ***hexadecimal*** en lugar de representación en base b. Así, por ejemplo, es fácil verificar que

$$1234 = (5, 4, 1, 4)_6 = (1, 6, 2, 1)_9 = (1, 18, 19)_{27} = (1, 0)_{1234} = (1234)_{10\,000}.$$

6.3.4. Notemos que solo hablamos de los dígitos en base b de un número cuando la base b es al menos 2. No tiene sentido hablar de los dígitos en base 1 de un número positivo a: de acuerdo a la definición, deberíamos podemos escribir a a en la forma

$$d_0 + d_1 \cdot 1 + \cdots + d_k \cdot 1^k$$

con $d_0, \ldots, d_k \in \{0\}$, pero esto es claramente imposible.

De todas formas, en varios contextos — como la teoría de la computabilidad — es usual hablar de la «escritura en base 1» de un número». Por esto nos referimos a lo siguiente: si a es un entero positivo, entonces la escritura en base 1 de a es la expresión

$$\underbrace{111\cdots111}_{a \text{ veces}}$$

con a unos. Así, por ejemplo,

11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111

es la escritura en base 1 de 85. No es evidente que esto pueda llegar a tener alguna utilidad, ciertamente! Varios sistemas de escritura originalmente usaron ideas parecidas. Por ejemplo, los siguientes son los símbolos usados para escribir los números 1, 2 y 3 en chino, inclusive hoy en día, y en notación romana:

I II III

Es importante tener en cuenta, de todas formas, que esto no es un caso particular de la noción de «escritura en base b» que describimos arriba.

```haskell
digitos :: Integer -> Integer -> [Integer]
digitos a b
  | q == 0    = [r]
  | otherwise = r : digitos q b
  where q = a `div` b
        r = a `mod` b
```

Programa 6.3. Una implementación en HASKELL del algoritmo para obtener los dígitos de un entero positivo `a` en base `b`. El resultado es una lista de los dígitos, desde el menos significativo en adelante. Por ejemplo, `digitos 123 10` denota `[3, 2, 1]`.

6.3.5. Estudiando la demostración que dimos para la Proposición 6.3.1 se hace aparente que nos da método efectivo para encontrar los dígitos de un número entero positivo con respecto a una base. En efecto, supongamos que a y b son enteros positivos y que $b \geq 2$. Sean q y r el cociente y el resto de dividir a a por b. Si el cociente q es nulo, entonces $r \neq 0$ porque $a \neq 0$ y, por lo tanto, claramente es

$$a = (r)_b.$$

Si en cambio el cociente q no es nulo, y conocemos los dígitos de q en base b, de manera que conocemos $k \in \mathbb{N}_0$ y $d_0, \ldots, d_k \in \{0, \ldots, b-1\}$ de manera que $d_k \neq 0$ y

$$q = (d_k, d_{k-1}, \ldots, d_1, d_0)_b, \tag{7}$$

entonces

$$a = (d_k, d_{k-1}, \ldots, d_1, d_0, r)_b. \tag{8}$$

En efecto, la igualdad (7) nos dice que $q = d_0 + d_1 b + \cdots + d_k b^k$, así que

$$a = r + qb = r + (d_0 + d_1 b + \cdots + d_k b^k)b = r + d_0 b + d_1 b^2 + \cdots + d_k b^{k+1}$$

y, como $d_k \neq 0$, esto significa que la igualdad (8) vale.

En las Figuras 6.3 y 6.4 damos implementaciones de esta idea en HASKELL y en PYTHON, respectivamente. Todos los lenguajes de programación proveen alguna forma de imprimir números y todos usan exactamente este algoritmo para encontrar sus dígitos.

```
def digitos(a, b):
    q = a // b
    r = a % b
    if q == 0:
        return [r]
    else:
        return [r] + digitos(q, b)
```

Programa 6.4. Una implementación en PYTHON del algoritmo para obtener los dígitos de un entero positivo `a` en base `b`. Como antes, el resultado es una lista de los dígitos, desde el menos significativo en adelante.

§6.4. Máximo común divisor

6.4.1. Sean a y b dos enteros y supongamos que no son los dos nulos. Un ***divisor común*** de a y b es simplemente un entero d que es tanto un divisor de a como de b. Escribimos $D(a,b)$ al conjunto de todos los divisores comunes *positivos* de a y b.

Este conjunto $D(a,b)$ no es vacío: en efecto, el número 1 pertenece a $D(a,b)$. Por otro lado, si $d \in D(a,b)$, entonces de la Proposición 6.1.4 tenemos que o bien $a = 0$ o bien $d \leq |a|$, y que o bien $b = 0$ o bien $d \leq |b|$. Como a y b no son los dos nulos, se sigue de esto que $d \leq \max\{|a|,|b|\}$. En otras palabras, si ponemos $N \coloneqq \max\{|a|,|b|\}$, entonces $D(a,b) \subseteq \{1,\dots,N\}$. Vemos así que el conjunto $D(a,b)$ es finito y, en particular, que podemos considerar su elemento máximo: lo llamamos ***máximo común divisor*** de a y b y lo escribimos $\mathsf{mcd}(a,b)$.

Esto define el máximo común divisor de dos números que no son simultáneamente nulos. Si, por el contrario, es $a = b = 0$, entonces todo elemento de $\mathbb{N}$ es un divisor común positivo de a y b y, por lo tanto, no tiene sentido hablar en este caso del elemento máximo de $D(a,b)$. En este caso especial definimos $\mathsf{mcd}(0,0) \coloneqq 0$.

6.4.2. Decimos que dos enteros a y b son ***coprimos*** cuando $\mathsf{mcd}(a,b) = 1$. Esta condición significa, precisamente, que no son ambos nulos y que el único divisor común positivo que tienen es 1. Así, por ejemplo, 2 y 3 son números coprimos, mientras que 6 y 15 no lo son.

6.4.3. El máximo común divisor de dos enteros es un elemento de $\mathbb{N}_0$ y es nulo si y solamente si esos dos enteros son nulos: esto es consecuencia inmediata de la definición. Otras observaciones sencillas que podemos hacer son las siguientes:

Proposición. *Sean a y b dos enteros.*

(*i*) *Es* $\mathsf{mcd}(a,b) = \mathsf{mcd}(b,a)$.

(*ii*) *Es* $\mathsf{mcd}(a,b) = |a|$ *si y solamente si a divide a b.*

(*iii*) *En particular, cualquiera sea a se tiene que* $\mathsf{mcd}(a, 0) = |a|$.
(*iv*) *Se tiene que* $\mathsf{mcd}(a, b) = \mathsf{mcd}(-a, b) = \mathsf{mcd}(a, -b) = \mathsf{mcd}(-a, -b)$.

Demostración. (*i*) Si $a = b = 0$, entonces es evidente que $\mathsf{mcd}(a, b) = \mathsf{mcd}(b, a)$. Si en cambio alguno de a o b es no nulo, entonces los conjuntos $D(a, b)$ y $D(b, a)$ coinciden, así que tienen el mismo elemento máximo: esto significa, precisamente, que $\mathsf{mcd}(a, b) = \mathsf{mcd}(b, a)$ también en este caso.

(*ii*) Supongamos primero que a divide a b. Si $a = 0$, entonces también $b = 0$ y la igualdad $\mathsf{mcd}(a, b) = |a|$ es evidente. Supongamos entonces que $a \neq 0$. Si $d \in D(a, b)$, entonces d divide a a y, de acuerdo a la Proposición **6.1.4**, se tiene que $d \leq |a|$. Como además $|a| \in D(a, b)$, vemos que $|a|$ es el elemento máximo del conjunto $D(a, b)$, es decir, que $|a| = \mathsf{mcd}(a, b)$. Esto muestra que la condición del enunciado es suficiente.

Veamos que es necesaria. Supongamos que $\mathsf{mcd}(a, b) = |a|$. Si $b = 0$, entonces a divide a b independientemente de nuestra hipótesis, así que supongamos que $b \neq 0$. En ese caso, $\mathsf{mcd}(a, b)$ es el elemento máximo del conjunto $D(a, b)$, y esto significa que, en particular, $|a|$ divide a b, así que a divide a b.

(*iii*) Como $a \mid 0$, esto es consecuencia de (*ii*).

(*iv*) Si $a = b = 0$, lo que afirma el enunciado es evidente. Si en cambio alguno de a o b es no nulo, entonces los conjuntos $D(a, b)$, $D(-a, b)$, $D(a, -b)$ y $D(-a, -b)$ coinciden y, por lo tanto, tienen el mismo elemento máximo. □

6.4.4. La siguiente propiedad es fundamental:

Proposición. *Si a, b y c son tres enteros, entonces*

$$\mathsf{mcd}(a - cb, b) = \mathsf{mcd}(a, b), \qquad \mathsf{mcd}(a, b - ca) = \mathsf{mcd}(a, b).$$

Demostración. En vista de la Proposición **6.4.3**(*i*) es suficiente que mostremos la primera de las igualdades del enunciado. Sean a, b y c tres enteros. Si b es cero, entonces esa igualdad evidente. Supongamos entonces que $b \neq 0$. Afirmamos que

$$D(a, b) = D(a - cb, b). \tag{9}$$

En efecto, si $d \in D(a, b)$, entonces d es un entero positivo que divide a a y a b y, por lo tanto, divide a $a - bc$ y a b: esto significa que $d \in D(a - cb, b)$. Recíprocamente, si $d \in D(a - cb, b)$, entonces d es un entero positivo que divide a $a - cb$ y a b, y por lo tanto divide a $a = (a - cb) + cb$ y a b, así que pertenece a $D(a, b)$.

De la igualdad (9) se deduce que

$$\mathsf{mcd}(a, b) = \mathsf{máx}\, D(a, b) = \mathsf{máx}\, D(a - cb, b) = \mathsf{mcd}(a - cb, b)$$

y esto prueba la proposición. □

6.4.5. Una de las razones por las que la Proposición 6.4.4 es importante es que está en la base de un algoritmo para calcular el máximo común divisor de dos enteros.

En vista de la Proposición 6.4.3(*iv*), es suficiente que veamos cómo hacer esto cuando los dos enteros son no negativos. Supongamos entonces que a y b son dos enteros no negativos y que, por ejemplo, $a \geq b$. Si $b = 0$, entonces sabemos que $\mathsf{mcd}(a, b) = a$ y no es necesario hacer más nada. Si en cambio $b > 0$, entonces podemos dividir a a por b. Sean q y r el cociente y el resto, respectivamente. Como $a = qb + r$, la Proposición 6.4.4 nos dice que

$$\mathsf{mcd}(a, b) = \mathsf{mcd}(a - qb, b) = \mathsf{mcd}(r, b).$$

Notemos que r y b son dos enteros no negativos y que $a + b > r + b$, ya que $a \geq b > r$. De esta forma redujimos el cálculo del máximo común divisor de dos números no negativos al del máximo común divisor de otros dos cuya suma es menor que la de los originales. Podemos repetir este procedimiento: cada vez que lo hacemos la suma de los dos números decrece y es positiva, así que el proceso tiene que terminar.

Veamos un ejemplo. Para calcular $\mathsf{mcd}(385, 150)$, observamos que el cociente y el resto de la división de 385 por 150 son 2 y 85, respectivamente, de manera que $385 = 2 \cdot 150 + 85$ y entonces

$$\mathsf{mcd}(385, 150) = \mathsf{mcd}(385 - 2 \cdot 150, 150) = \mathsf{mcd}(85, 150).$$

Tenemos que calcular ahora $\mathsf{mcd}(85, 150)$. Es $150 = 1 \cdot 85 + 65$, así que

$$\mathsf{mcd}(85, 150) = \mathsf{mcd}(85, 150 - 1 \cdot 85) = \mathsf{mcd}(85, 65).$$

Otra vez, dividiendo vemos que $85 = 1 \cdot 65 + 20$ y, por lo tanto, que

$$\mathsf{mcd}(85, 65) = \mathsf{mcd}(85 - 1 \cdot 65, 65) = \mathsf{mcd}(20, 65).$$

Finalmente, como $65 = 3 \cdot 20 + 5$,

$$\mathsf{mcd}(20, 65) = \mathsf{mcd}(20, 65 - 3 \cdot 20) = \mathsf{mcd}(20, 5)$$

y, como 5 divide a 20, este último máximo común divisor es 5. Concluimos así que

$$\mathsf{mcd}(385, 150) = 5.$$

Este procedimiento funciona en todos los casos, como veremos más abajo. Se lo conoce como el *algoritmo de Euclides*, porque Euclides lo describe en el Libro 7 de sus *Elementos*, publicados aproximadamente 300 años a.e.c. — aunque es probable que el algoritmo haya sido conocido desde mucho tiempo antes. En la Figura 6.2 reproducimos el pasaje relevante.

Δύο ἀριθμῶν δοθέντων μὴ πρώτων πρὸς ἀλλήλους τὸ μέγιστον αὐτῶν κοινὸν μέτρον εὑρεῖν. Ἔστωσαν οἱ δοθέντες δύο ἀριθμοὶ μὴ πρῶτοι πρὸς ἀλλήλους οἱ ΑΒ, ΓΔ. δεῖ δὴ τῶν ΑΒ, ΓΔ τὸ μέγιστον κοινὸν μέτρον εὑρεῖν. Εἰ μὲν οὖν ὁ ΓΔ τὸν ΑΒ μετρεῖ, μετρεῖ δὲ καὶ ἑαυτόν, ὁ ΓΔ ἄρα τῶν ΓΔ, ΑΒ κοινὸν μέτρον ἐστίν. καὶ φανερόν, ὅτι καὶ μέγιστον: οὐδεὶς γὰρ μείζων τοῦ ΓΔ τὸν ΓΔ μετρήσει. Εἰ δὲ οὐ μετρεῖ ὁ ΓΔ τὸν ΑΒ, τῶν ΑΒ, ΓΔ ἀνθυφαιρουμένου ἀεὶ τοῦ ἐλάσσονος ἀπὸ τοῦ μείζονος λειφθήσεταί τις ἀριθμός, ὃς μετρήσει τὸν πρὸ ἑαυτοῦ. μονὰς μὲν γὰρ οὐ λειφθήσεται: εἰ δὲ μή, ἔσονται οἱ ΑΒ, ΓΔ πρῶτοι πρὸς ἀλλήλους: ὅπερ οὐχ ὑπόκειται. λειφθήσεταί τις ἄρα ἀριθμός, ὃς μετρήσει τὸν πρὸ ἑαυτοῦ. καὶ ὁ μὲν ΓΔ τὸν ΒΕ μετρῶν λειπέτω ἑαυτοῦ ἐλάσσονα τὸν ΕΑ, ὁ δὲ ΕΑ τὸν ΔΖ μετρῶν λειπέτω ἑαυτοῦ ἐλάσσονα τὸν ΖΓ, ὁ δὲ ΓΖ τὸν ΑΕ μετρείτω. ἐπεὶ οὖν ὁ ΓΖ τὸν ΑΕ μετρεῖ, ὁ δὲ ΑΕ τὸν ΔΖ μετρεῖ, καὶ ὁ ΓΖ ἄρα τὸν ΔΖ μετρήσει: μετρεῖ δὲ καὶ ἑαυτόν: καὶ ὅλον ἄρα τὸν ΓΔ μετρήσει. ὁ δὲ ΓΔ τὸν ΒΕ μετρεῖ: καὶ ὁ ΓΖ ἄρα τὸν ΒΕ μετρεῖ: μετρεῖ δὲ καὶ τὸν ΕΑ: καὶ ὅλον ἄρα τὸν ΒΑ μετρήσει: μετρεῖ δὲ καὶ τὸν ΓΔ: ὁ ΓΖ ἄρα τοὺς ΑΒ, ΓΔ μετρεῖ. ὁ ΓΖ ἄρα τῶν ΑΒ, ΓΔ κοινὸν μέτρον ἐστίν. λέγω δή, ὅτι καὶ μέγιστον. εἰ γὰρ μή ἐστιν ὁ ΓΖ τῶν ΑΒ, ΓΔ μέγιστον κοινὸν μέτρον, μετρήσει τις τοὺς ΑΒ, ΓΔ ἀριθμοὺς ἀριθμὸς μείζων ὢν τοῦ ΓΖ. μετρείτω, καὶ ἔστω ὁ Η. καὶ ἐπεὶ ὁ Η τὸν ΓΔ μετρεῖ, ὁ δὲ ΓΔ τὸν ΒΕ μετρεῖ, καὶ ὁ Η ἄρα τὸν ΒΕ μετρεῖ: μετρεῖ δὲ καὶ ὅλον τὸν ΒΑ: καὶ λοιπὸν ἄρα τὸν ΑΕ μετρήσει. ὁ δὲ ΑΕ τὸν ΔΖ μετρεῖ: καὶ ὁ Η ἄρα τὸν ΔΖ μετρήσει: μετρεῖ δὲ καὶ ὅλον τὸν ΔΓ: καὶ λοιπὸν ἄρα τὸν ΓΖ μετρήσει ὁ μείζων τὸν ἐλάσσονα: ὅπερ ἐστὶν ἀδύνατον: οὐκ ἄρα τοὺς ΑΒ, ΓΔ ἀριθμοὺς ἀριθμός τις μετρήσει μείζων ὢν τοῦ ΓΖ: ὁ ΓΖ ἄρα τῶν ΑΒ, ΓΔ μέγιστόν ἐστι κοινὸν μέτρον: [ὅπερ ἔδει δεῖξαι].

Figura 6.2. La proposición 2 del Libro 7 de los Elementos de Euclides, en el que enuncia el problema de encontrar el máximo común divisor de dos números y lo resuelve, presentando el algoritmo que lleva su nombre. Empieza con «Dados dos números no primos uno al otro, encontrar su medida más grande. Sean AB y CD los dos números dados no primos uno al otro. Si CD mide a AB, y también se mide a sí mismo, entonces CD es una medida común de AB, CD. Y es manifiesto que es la más grande. Pero si CD no mide a AB, entonces, el menos de los números AB, CD se puede restar varias veces del más grande, y algún número sera el resto, que medirá al que está antes de él. Etc».

6.4.6. Describamos precisamente el algoritmo de Euclides en una forma conveniente para probar que funciona. Empezamos como arriba con dos números enteros no negativos a y b, suponemos que $a \geq b$ y definimos una sucesión

$$r_0, r_1, r_2, r_3, \ldots$$

de enteros no negativos de la siguiente manera. Ponemos $r_0 \coloneqq a$, $r_1 \coloneqq b$ y, para cada $i \geq 2$,

$$r_i \coloneqq \begin{cases} \text{el resto de dividir } r_{i-2} \text{ por } r_{i-1}, & \text{si } r_{i-1} \neq 0; \\ 0, & \text{en caso contrario.} \end{cases} \tag{10}$$

El algoritmo de Euclides para determinar el máximo común divisor de a y de b consiste en calcular las componentes de esta sucesión y quedarse con la última no nula. Por ejemplo, si $a = 385$ y $b = 150$, entonces la sucesión $(r_i)_{i\geq 0}$ es

$$385,\ 150,\ 85,\ 65,\ 20,\ 5,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ \ldots$$

y, por lo tanto, $\mathsf{mcd}(385, 150) = 5$.

6.4.7. Proposición. *Sean a y b dos enteros no negativos tales que $a \geq b$ y sea $(r_i)_{i\geq 0}$ la sucesión que acabamos de describir.*

(*i*) *Existe $N \in \mathbb{N}_0$ tal que $r_i \neq 0$ para todo $i \leq N$ y $r_i = 0$ para todo $i > N$.*

(*ii*) *Para todo $i \in \mathbb{N}$ tal que $i \leq N + 1$ se tiene que $\mathsf{mcd}(a, b) = \mathsf{mcd}(r_{i-1}, r_i)$.*

(*iii*) *Es $\mathsf{mcd}(a, b) = r_N$.*

Este resultado nos dice que el algoritmo de Euclides, cuando empezamos con dos enteros no negativos a y b, se detiene después de un número finito de pasos — el número N — y el último número que produce es precisamente el máximo común divisor de a y b. En otros palabras, nos dice que el algoritmo funciona, como queríamos.

Demostración. Observemos que

$$r_i \geq 0 \text{ para todo } i \in \mathbb{N}. \tag{11}$$

En efecto, se tiene que $r_1 = b \geq 0$ y para todo $i \geq 2$ se tiene que $r_i \geq 0$ ya que r_i es, de acuerdo a la definición (10), o bien el resto de una división, que es siempre un número no negativo, o bien 0.

Por otro lado, se tiene que

$$\text{para todo } i \in \mathbb{N} \text{ o bien } r_i = 0 \text{ o bien } r_i > r_{i+1}. \tag{12}$$

Para verlo, basta notar que si $i \in \mathbb{N}$ y $r_i \neq 0$, entonces r_{i+1} es el resto de dividir a un número por r_i, que es necesariamente menor que r_i.

Supongamos por un momento que $r_i \neq 0$ para todo $i \in \mathbb{N}$. De acuerdo a (11), el conjunto $R \coloneqq \{r_i : i \in \mathbb{N}\}$ está contenido en $\mathbb{N}_0$, así que tiene un menor elemento: esto es, existe $i \in \mathbb{N}$ tal que $r_i \leq r_j$ para todo $j \in \mathbb{N}$. Esto es absurdo, ya que como $r_i \neq 0$ por nuestra hipótesis, de (12) sabemos que $r_i > r_{i+1}$.

Esta contradicción implica que tiene que existir $i \in \mathbb{N}$ tal que $r_i = 0$ y, por lo tanto, que el conjunto $S \coloneqq \{i \in \mathbb{N} : r_{i+1} = 0\}$ no es vacío. Como está contenido en $\mathbb{N}$, sabemos que él también tiene tiene un menor elemento. Llamémoslo N. Se tiene, claro, que $r_i \neq 0$ si $i \leq N$ y $r_{N+1} = 0$. Más aún, en vista de la forma en que está definida la sucesión $(r_i)_{i\geq 0}$, es claro que como $r_{N+1} = 0$ se tiene que $r_i = 0$ para todo entero $i > N$. Esto prueba que vale la parte (i) de la proposición.

Para cada $i \in \mathbb{N}$ sea $P(i)$ la afirmación

$$i > N+1 \;\; o \;\; \mathsf{mcd}(a,b) = \mathsf{mcd}(r_{i-1}, r_i)$$

y mostremos que $P(i)$ vale para todo $i \in \mathbb{N}$: esto probará la parte (ii) de la proposición.

Que $P(1)$ vale es evidente, ya que $r_0 = a$ y $r_1 = b$. Supongamos que $j \in \mathbb{N}$ y que la afirmación $P(j)$ vale, es decir, que $j > N+1$ o

$$\mathsf{mcd}(a,b) = \mathsf{mcd}(r_{j-1}, r_j). \tag{13}$$

Si $j > N+1$, entonces por supuesto es $j+1 > N+1$ y, por lo tanto, la afirmación $P(j+1)$ vale. Consideremos el caso en que $j \leq N$, de manera que vale la igualdad (13). La forma en que elegimos el número N implica que $r_j \neq 0$, así que la definición de la sucesión $(r_i)_{i\geq 0}$ nos dice que r_{j+1} es el resto de dividir a r_{j-1} por r_j. Si q es el cociente de esa división, entonces que $r_{j+1} = r_{j-1} - qr_j$ y, por lo tanto,

$$\mathsf{mcd}(r_{j-1}, r_j) = \mathsf{mcd}(r_{j-1} - qr_k, r_j) = \mathsf{mcd}(r_{j+1}, r_j) = \mathsf{mcd}(r_j, r_{j+1}).$$

Junto con (13) esto nos dice que $\mathsf{mcd}(a,b) = \mathsf{mcd}(r_j, r_{j+1})$ y, en definitiva, que $P(j+1)$ también vale en este caso. La inducción queda así completa.

Finalmente, tomando $i = N+1$ en la igualdad de la parte (ii), vemos que

$$\mathsf{mcd}(a,b) = \mathsf{mcd}(r_N, r_{N+1}) = \mathsf{mcd}(r_N, 0) = r_N,$$

como se afirma en la parte (iii) de la proposición. □

6.4.8. Es inmediato implementar este algoritmo en Haskell y en Python. En las Figuras 6.3 y 6.4 damos una forma de hacerlo. Este algoritmo es extremadamente importante en las aplicaciones, así que hay toda una literatura dedicada a su estudio y mejora — el código que presentamos es la implementación más sencilla posible. El libro [Knu1969] de Donald Knuth tiene una discusión detallada de este algoritmo.

```haskell
module MCD where

mcd :: Integer -> Integer -> Integer
mcd a 0 = abs a
mcd a b = mcd b (a `mod` b)
```

Figura 6.3. Un implementación en Haskell del algoritmo de la Euclides. Esto es casi exactamente el algoritmo que describimos en 6.4.6, salvo que esta modificado para que cualquiera de `a` o `b` pueda ser negativo en la expresión `mcd a b`.

```python
def mcd(a, b):
    if b == 0:
        return abs(a)
    else:
        return mcd(b, a % b)
```

Figura 6.4. Un implementación en Python del algoritmo de la Euclides.

Casi todos los lenguajes de programación cuentan con muy buenas implementaciones de este algoritmo — Haskell tiene la función `gcd` en su preludio y Python a la función `gcd` en el módulo `math` de la librería estándar — y en general uno debería usarlas.

6.4.9. El máximo común divisor de dos números que no son los dos nulos es, por definición, el máximo de un conjunto. Nuestro siguiente resultado da una descripción alternativa de él como el *mínimo* de otro conjunto.

Proposición. *Sean a y b dos enteros no simultáneamente nulos. El conjunto*

$$S(a,b) \coloneqq \{xa + yb : x, y \in \mathbb{Z},\ xa + yb > 0\}$$

es un subconjunto no vacío de $\mathbb{N}$ y su elemento mínimo es $\mathsf{mcd}(a,b)$.

Demostración. Alguno de los cuatro números a, $-a$, b o $-b$ es positivo y, por lo tanto, pertenece a $S(a,b)$: esto muestra que este conjunto no es vacío. Como está contenido en $\mathbb{N}$, podemos considerar su elemento mínimo $d \coloneqq \mathsf{mín}\, S$. Como d pertenece a $S(a,b)$, es claro que $d \geq 1$ y que existen $u, v \in \mathbb{Z}$ tales que $d = ua + vb$.

Sean q y r el cociente y el resto de la división de a por d, de manera que $a = qd + r$ y $0 \leq r < d$.

Si $r > 0$, entonces como

$$(1 - qu)a - qvb = r$$

y $1 - qu$ y $-qv$ son enteros, se tiene que $r \in S(a, b)$: esto es imposible ya que $r < d$. Vemos así que tiene que ser $r = 0$ y, por lo tanto, d divide a a. Un argumento similar muestra que d divide a b y, por lo tanto, d es un divisor común de a y b.

Sea ahora e un elemento de $D(a, b)$, de manera que e divide a a y a b. Como $d = ua + vb$, es claro que e divide también a d y, como $d \neq 0$, la Proposición 6.1.4 nos dice que $e \leq d$. Esto muestra que d es el mayor elemento de $D(a, b)$ y, por lo tanto, que $d = \mathsf{mcd}(a, b)$, como afirma la proposición. □

6.4.10. Una consecuencia inmediata e importante de esta proposición es el siguiente corolario:

Corolario. *Si a y b son dos enteros y $d = \mathsf{mcd}(a, b)$, entonces hay enteros x e y tales que $d = xa + yb$.*

Llamamos a esta igualdad la ***identidad de Bézout***, por Étienne Bézout, que probó un análogo de este resultado para polinomios.

Demostración. Si $a = b = 0$, entonces $d = 0$ y eligiendo $x = y = 0$ es evidente que vale la igualdad del enunciado. Si en cambio a y b no son simultáneamente nulos, la Proposición 6.4.9 nos dice que el número d pertenece al conjunto $S(a, b)$ allí descripto y, por lo tanto, existen enteros x e y tales que $d = xa + yb$. □

6.4.11. Para muchas aplicaciones, necesitamos no solamente poder calcular el máximo común divisor de dos enteros sino que también queremos encontrar números x e y para los que valga la identidad de Bézout. Veamos cómo podemos hacer esto.

Supongamos como en 6.4.6 que tenemos dos enteros no negativos a y b tales que $a \geq b$, sea $d \coloneqq \mathsf{mcd}(a, b)$ y definamos la sucesión $(r_i)_{i \geq 0}$ como allí, esto es, poniendo $r_0 \coloneqq a$, $r_1 \coloneqq b$ y, para cada $i \geq 2$,

$$r_i \coloneqq \begin{cases} \text{el resto de dividir } r_{i-2} \text{ por } r_{i-1}, & \text{si } r_{i-1} \neq 0; \\ 0, & \text{en caso contrario.} \end{cases}$$

Sea N el número que nos provee la Proposición 6.4.7, de manera que $r_i \neq 0$ si $i \leq N$, $r_i = 0$ si $i > N$ y $r_N = d$. Estamos buscando enteros x e y tales que $xa + yb = r_N$. Busquemos, más generalmente, pares de enteros $x_0, y_0, x_1, y_1, \ldots, x_N, y_N$ tales que para cada $i \in \{0, \ldots, N\}$ se tenga $x_i a + y_i b = r_i$.

Observemos que cuando $i = 0$ o $i = 1$ esto es fácil: basta poner $x_0 \coloneqq 1$, $y_0 \coloneqq 0$, $x_1 \coloneqq 0$, $y_1 \coloneqq 1$, ya que $r_0 = a$ y $r_1 = b$. Ahora bien, supongamos que $2 \leq i \leq N$ y que ya encontramos enteros $x_{i-1}, y_{i-1}, x_i, y_i$ de manera tal que $x_{i-1}a + y_{i-1}b = r_{i-1}$ y $x_i a + y_i b = r_i$. Si llamamos q_{i+1} al cociente

de la división de r_{i-1} por r_i, de manera que $r_{i-1} = q_{i+1}r_i + r_{i+1}$, tenemos entonces que

$$\begin{aligned} r_{i+1} &= r_{i-1} - q_{i+1}r_i = (x_{i-1}a + y_{i-1}b) - q_{i+1}(x_i a + y_i b) \\ &= (x_{i-1} - q_{i+1}x_i)a + (y_{i-1} - q_{i+1}y_i)b \end{aligned}$$

y, por lo tanto, basta que pongamos

$$x_{i+1} \coloneqq x_{i-1} - q_{i+1}x_i \tag{14}$$

e

$$y_{i+1} \coloneqq y_{i-1} - q_{i+1}y_i \tag{15}$$

para que se tenga que $x_{i+1}a + y_{i+1}b = r_{i+1}$.

De esta manera vamos determinando enteros x_i e y_i para cada i de 0 hasta N, hasta finalmente encontrar x_N e y_N: estos satisfacen la condición de que $x_N a + y_N b = r_N = d$, que es la identidad de Bézout.

Veamos un ejemplo de cómo funciona este proceso. Determinemos los coeficientes de la identidad de Bézout para $a = 385$ y $b = 150$. Como en **6.4.6**, calculamos las componentes de la sucesión $(r_i)_{i\geq 0}$ pero en cada paso a partir del segundo no solamente calculamos el resto r_i de dividir r_{i-2} por r_{i-1} sino también el cociente q_i. La primera componente nula de la sucesión de restos es r_6, así que sabemos que $r_5 = \mathsf{mcd}(a, b)$.

i	0	1	2	3	4	5	6
r_i	385	150	85	65	20	5	0
q_i			2	1	1	3	
x_i	1	0	1	−1	2	−7	
y_i	0	1	−2	3	−5	18	

(16)

Ahora calculamos en orden los números x_i e y_i: empezamos poniendo $x_0 = 1$, $y_0 = 0$, $x_1 = 0$ e $y_1 = 1$, y a todos los otros los determinamos usando las fórmulas (14) y (15). Encontramos de esta forma que

$$(-7) \cdot 385 + 18 \cdot 150 = 5,$$

que es la identidad de Bézout para 385 y 150, como queríamos.

Este procedimiento es conocido como el *algoritmo de Euclides extendido* y es la forma en que se determinan los coeficientes de la identidad de Bézout en la práctica. Todos los programas de álgebra computacional tienen implementaciones de este algoritmo. En la Figura 6.5 en la página siguiente damos una posible implementación en Haskell.

```
module EMCD where

emcd :: Integer -> Integer -> (Integer, Integer, Integer)
emcd a b = (d, signum a * x, signum b * y)
  where (d, x, y) = paso 1 0 0 1 (abs a) (abs b)

paso x y x' y' a 0 = (a, x, y)
paso x y x' y' a b = paso x' y' x'' y'' b (a `mod` b)
  where q = a `div` b
        x'' = x - q * x'
        y'' = y - q * y'
```

Programa 6.5. Un implementación en HASKELL del algoritmo de Euclides extendido. Con estas definiciones. `emcd a b` es una terna `(d, x, y)` tal que `d` es el máximo común divisor de `a` y `b`, y `x` e `y` son tales que $ax + by = 1$. Este algoritmo difiere del que describimos en 6.4.11. La función `paso` se ocupa de hacer cada paso del algoritmo: la vez i-ésima que es llamada recibe como argumentos a los números x_{i-1}, y_{i-1}, x_i, y_i, r_{i-1} y r_i, en ese orden.

```
module EMCD where

emcd :: Integer -> Integer -> (Integer, Integer, Integer)
emcd a 0 = (abs a, signum a, 0)
emcd a b = (d, y, x - (a `div` b) * y)
  where (d, x, y) = emcd b (a `mod` b)
```

Programa 6.6. Una implementación de la versión del algoritmo de Euclides extendido descripta en 6.4.13. Otra vez, el valor de `emcd a b` es una terna `(d, x, y)` tal que `d` es el máximo común divisor de `a` y `b`, y `x` e `y` son tales que $ax + by = 1$. Esta versión difiere de la anterior en que los coeficientes `x` e `y` se obtienen «hacia atrás». Este código es bastante más sencillo que el de la Figura 6.5 pero aquel tiene la ventaja de que usa lo que se llama *recursión de cola* y es, por lo tanto, más eficiente.

6.4.12. Probemos que este algoritmo funciona en todos los casos:

Proposición. *Sean a y b dos enteros no negativos y supongamos que $a \geq b$. Sea $(r_i)_{i\geq 0}$ la sucesión construida en 6.4.6 a partir de a y b, y sea $N \in \mathbb{N}_0$ como en la Proposición 6.4.7, de manera que $r_i \neq 0$ si $i \leq N$, $r_i = 0$ para todo $i > N$ y $r_N = \mathsf{mcd}(a, b)$. Sean $x_0, x_1, \ldots, x_N$ y $y_0, y_1, \ldots, y_N$ las secuencias de enteros tales que*

$$x_0 = 1, \qquad y_0 = 0, \tag{17}$$

$$x_1 = 0, \qquad y_1 = 1, \tag{18}$$

y, para cada $i \in \{2, \ldots, N\}$,

$$x_i = x_{i-2} - q_i x_{i-1}, \qquad y_i = y_{i-2} - q_i y_{i-1} \tag{19}$$

con q_i el cociente de dividir a r_{i-2} por r_{i-1}. Se tiene entonces que

$$r_i = x_i a + y_i b \tag{20}$$

para cada $i \in \{0, \ldots, N\}$ y, en particular, que

$$\mathsf{mcd}(a, b) = x_N a + y_N b.$$

Demostración. Es suficiente que mostremos que para cada $i \in \{0, \ldots, N\}$ vale la igualdad (20), ya que cuando i es N ésta nos dice que $x_N a + y_N b = r_N = \mathsf{mcd}(a, b)$.

Sea $P(i)$, para cada $i \in \mathbb{N}_0$, la afirmación «o bien $i > N$ o bien $r_i = x_i a + y_i b$» y mostremos que $P(i)$ vale para todo $i \in \mathbb{N}_0$ haciendo inducción. Las afirmaciones $P(0)$ y $P(1)$ valen: esto es consecuencia inmediata de las igualdades (17) y (18). En efecto, $x_0 a + y_0 b = a = r_0$ y $x_1 a + y_1 b = b = r_1$.

Veamos ahora el paso inductivo. Sea j un entero tal que $j \geq 2$ y supongamos que las afirmaciones $P(j-1)$ y $P(j-2)$ valen. Si $j > N$, entonces claramente la afirmación $P(j)$ vale. Consideremos el caso en que $j \leq N$. Que $P(j-1)$ y $P(j-2)$ valgan, entonces, nos dice que $r_{j-1} = x_{j-1} a + y_{j-1} b$ y que $r_{j-2} = x_{j-2} a + y_{j-2} b$. Si q_j es el resto de dividir a r_{j-2} por r_{j-1}, tenemos que

$$\begin{aligned} r_j &= r_{j-2} - q_i r_{j-1} \\ &= (x_{j-2} a + y_{j-2} b) - q_i (x_{j-1} a + y_{j-1} b) \\ &= (x_{j-2} - q_i x_{j-1}) a + (y_{j-2} - q_i y_{j-1}) b \end{aligned}$$

y, de acuerdo a las ecuaciones (19), esto es

$$= x_j a + y_j b.$$

Vemos así que $P(j)$ vale también en este caso y esto completa la inducción. □

6.4.13. Hay una forma alternativa de obtener los coeficientes de la identidad de Bézout que es a veces más conveniente y que los encuentra «hacia atrás». Supongamos que empezamos con dos enteros positivos a y b tales que $a \geq b$, construyamos como en **6.4.6** la sucesión $(r_i)_{i\geq 0}$, y sea N el número cuya existencia asegura la Proposición 6.4.7, de manera que, en particular, $r_N = \mathsf{mcd}(a,b)$ y $r_{N+1} = 0$. Construimos ahora una secuencia de enteros $z_0, z_1, \ldots, z_N$ poniendo $z_0 \coloneqq 0$, $z_1 \coloneqq 1$ y, para cada i desde 2 hasta N,

$$z_i \coloneqq z_{i-2} - q_{N+2-i} z_{i-1},$$

con q_i el cociente de dividir a r_{i-2} por r_{i-1}. Al terminar, ponemos $x \coloneqq z_{N-1}$ e $y \coloneqq z_N$ y vale que $xa + yb = \mathsf{mcd}(a,b)$, así que encontramos la identidad de Bézout.

Por ejemplo, si $a = 385$ y $b = 150$ en primer lugar construimos la tabla

i	0	1	2	3	4	5	6
r_i	385	150	85	65	20	5	0
q_i			2	1	1	3	

(21)

de manera que aquí $N = 5$, y usando esa información una segunda tabla

i	0	1	2	3	4	5
z_i	0	1	−3	4	−7	18

En este caso es $x = -7$ e $y = 18$ y $385x + 150y = 5$ es el máximo común divisor de 385 y 150.

Proposición. *Sean a y b dos enteros positivos a y b tales que $a \geq b$ y sean N y $r_0, r_1, \ldots, r_N$ los números construidos en la Proposición 6.4.7. Si $z_0, z_1, \ldots, z_N$ es la secuencia de números construida arriba, entonces*

$$z_{N-1}a + z_N b = \mathsf{mcd}(a,b).$$

Esta proposición nos dice que el algoritmo descripto en **6.4.13** funciona, esto es, que los da coeficientes que hacen cierta la identidad de Bézout. En la Figura 6.6 damos una implementación en Haskell. La diferencia fundamental entre este y el anterior es que cuando llevamos a cabo el de **6.4.11** es suficiente que en todo momento tengamos las últimas dos columnas de la tabla (16), mientras que cuando llevamos a cabo el procedimiento de **6.4.13** es necesario guardar completa la tabla de (21) para poder empezar a calcular los enteros z_i.

Demostración. Supongamos que el conjunto

$$S \coloneqq \{i \in \{0, \ldots, N-1\} : z_i r_{N-i-1} + z_{i+1} r_{N-i} \neq \mathsf{mcd}(a,b)\}$$

no es vacío, y sea j su mínimo. Notemos que cuando $i = 0$ es

$$z_i r_{N-i-1} + z_{i+1} r_{N-i} = z_0 r_{N-1} + z_1 r_N = r_N = \mathsf{mcd}(a, b)$$

y esto nos dice que 0 no pertenece al conjunto S y, por lo tanto, que $j > 0$. Ahora bien, como j es es el menor elemento de S y $0 \leq j - 1 \leq N - 1$, la diferencia $j - 1$ tiene que pertenecer a S, y esto significa que

$$\begin{aligned} \mathsf{mcd}(a, b) &= z_{j-1} r_{N-j} + z_j r_{N-j+1} \\ &= (z_{j+1} + q_{N+1-j} z_j) r_{N-j} + z_j r_{N-j+1} \qquad \text{porque } z_{j+1} = z_{j-1} - q_{N+1-j} z_j \\ &= z_{j+1} r_{N-j} + z_j (q_{N+1-j} r_{N-j} + r_{N+1-j}) \\ &= z_{j+1} r_{N-j} + z_j r_{N-1-j} \end{aligned}$$

porque $r_{N+1-j} = q_{N-1-j} r_{N+1-j} + r_{N+2-j}$, de acuerdo a la definición de la sucesión $(r_i)_{i \geq 0}$. Esto es absurdo porque j no pertenece al conjunto S, y esta contradicción provino de haber supuesto que S no es vacío. Esto significa que sí lo es y, en particular, que $N - 1$ no pertenece a S, esto es, que

$$\mathsf{mcd}(a, b) = z_{N-1} r_0 + z_N r_1 = z_{N-1} a + z_N b.$$

Esto es lo que queríamos probar. □

§6.5. Algunas aplicaciones de la identidad de Bézout

6.5.1. Vamos a usar la identidad de Bézout varias veces en todo lo que sigue. La primera aplicación es la siguiente caracterización del máximo común divisor de dos enteros que es extremadamente útil:

Proposición. *Sean a y b dos enteros. El máximo común divisor de a y b es el único elemento d de $\mathbb{N}_0$ que tiene las siguientes dos propiedades:*

- *d es un divisor común de a y b, y*
- *todo elemento de $\mathbb{N}_0$ que es un divisor común de a y b también divide a d.*

Demostración. Sea $d \coloneqq \mathsf{mcd}(a, b)$ y sean x e y enteros tales que $d = xa + yb$. Si e es un divisor positivo común de a y b, entonces e también divide a $d = xa + yb$. Como d es un divisor común de a y b, vemos así que d tiene las dos propiedades del enunciado.

Supongamos ahora que tenemos otro entero no negativo d' que tiene esas dos propiedades. Como d' es un divisor común de a y b y d tiene la segunda propiedad del enunciado, tenemos que $d \mid d'$. Por otro lado, como d es un divisor común de a y de b y d' tiene la segunda propiedad del enunciado, tenemos que $d' \mid d$. Podemos concluir entonces que $d = d'$, ya que tanto d como d' son enteros no negativos. Esto prueba la proposición. □

6.5.2. La caracterización del máximo común divisor de dos enteros que nos da la Proposición 6.5.1 es extremadamente útil. Veamos algunos ejemplos de cómo podemos usarla.

Corolario. *Si a, a', b y b' son enteros tales que $a \mid a'$ y $b \mid b'$, entonces*

$$\mathsf{mcd}(a, b) \mid \mathsf{mcd}(a', b').$$

Demostración. Sean a, a', b y b' enteros y supongamos que $a \mid a'$ y que $b \mid b'$. Sea además $d \coloneqq \mathsf{mcd}(a, b)$. Como d divide a a y a divide a a', vemos que d divide a a'. De manera similar, d divide a b': como d es entonces un divisor común de a' y b', la Proposición 6.5.1 nos dice que d divide a $\mathsf{mcd}(a', b')$. Esto es lo que afirma el corolario. □

6.5.3. Otra aplicación sencilla y útil de la proposición es el siguiente resultado que nos permite simplificar expresiones que involucran la función mcd.

Proposición. *Si a, b y c son enteros, entonces*

$$\mathsf{mcd}(ac, bc) = \mathsf{mcd}(a, b) \cdot c.$$

Demostración. Escribamos $d \coloneqq \mathsf{mcd}(a, b)$ y $e \coloneqq \mathsf{mcd}(ac, bc)$. De acuerdo a la identidad de Bézout 6.4.10, hay enteros x e y tales que $d = xa + yb$. Como $dc = xac + ybc$ y e divide a ac y a bc, vemos entonces que e divide a dc.

Por otro lado, como d divide a a y a b, es claro que dc divide a bc y a bd, así que la Proposición 6.5.1 nos dice que dc divide a e. Como d y e son enteros no negativos, podemos concluir de todo esto que $d = e$, que es lo que afirma la proposición. □

6.5.4. Usando la Proposición 6.5.3 podemos dar una nueva caracterización del máximo común divisor de dos números:

Corolario. *Sean a y b dos enteros y sea $d \coloneqq \mathsf{mcd}(a, b)$.*

(*i*) *Los enteros a' y b' tales que $a = da'$ y $b = db'$ son coprimos.*

(*ii*) *Si e es un entero no negativo tal que existen dos enteros coprimos u y v para los que se tiene que $a = eu$ y $a = ev$, entonces $e = d$.*

Demostración. (*i*) En la situación del enunciado, tenemos que

$$d = \mathsf{mcd}(a, b) = \mathsf{mcd}(da', db') = d \cdot \mathsf{mcd}(a', b'),$$

así que necesariamente $\mathsf{mcd}(a', b') = 1$.

(*ii*) Si $e \in \mathbb{N}_0$ y $u, v \in \mathbb{Z}$ son tales que $a = eu$, $b = ev$ y $\mathsf{mcd}(u, v) = 1$, entonces

$$\mathsf{mcd}(a, b) = \mathsf{mcd}(eu, ev) = e \cdot \mathsf{mcd}(u, v) = e$$

y esto es lo que queremos. □

6.5.5. Nuestro siguiente resultado nos da mas posibilidades de manipulación de expresiones que contienen la función mcd.

Proposición. *Sean a, b y c tres enteros y supongamos que a y b son coprimos.*

(*i*) *Si* $a \mid bc$, *entonces* $a \mid c$.
(*ii*) *Si* $a \mid c$ *y* $b \mid c$, *entonces* $ab \mid c$.
(*iii*) *Es* $\mathsf{mcd}(a, bc) = \mathsf{mcd}(a, c)$.
(*iv*) *Es* $\mathsf{mcd}(ab, c) = \mathsf{mcd}(a, c) \cdot \mathsf{mcd}(b, c)$.

Demostración. Como a y b son coprimos, existen enteros x e y tales que $xa + yb = 1$.

(*i*) Supongamos primero que a divide a bc. Como $xac + ybc = c$ y a divide a los dos sumandos del lado izquierdo, también divide al lado derecho.

(*ii*) Supongamos ahora que $a \mid c$ y que $b \mid c$. De eso se sigue que ab divide a bc y a ac, así que también divide a c, porque este número es igual a $xac + ybc$.

(*iii*) Sean $d \coloneqq \mathsf{mcd}(a, c)$ y $e \coloneqq \mathsf{mcd}(a, bc)$. Como d divide a a y a c, divide a a y a bc: de acuerdo a la Proposición 6.5.1, tenemos entonces que d divide a e. Por otro lado, como e divide a a y a bc, vemos que e divide a $c = (xa + yb)c = xac + ybc$. Esto nos dice que e es un divisor común positivo de a y c, así que e divide a d. Como d y e se dividen mutuamente y son no negativos, concluimos de esta forma que $d = e$, que es lo que queremos.

(*iv*) Pongamos $d \coloneqq \mathsf{mcd}(a, c)$, $e \coloneqq \mathsf{mcd}(b, c)$ y $f \coloneqq \mathsf{mcd}(ab, c)$. Como $d \mid a$ y $e \mid b$, se tiene que $de \mid ab$. Por otro lado, como $d \mid a$ y $e \mid c$, tenemos que $de \mid ac$, y como $d \mid c$ y $e \mid b$ que $de \mid bc$: usando esto y la igualdad $c = xac + ybc$, podemos concluir que $de \mid c$. Vemos así que de es un divisor común de ab y de c, así que $de \mid f$.

Por otro lado, existen enteros u, v, r y s tales que $d = ua + vc$ y $e = rb + sc$, así que

$$de = (ua + vc)(rb + sc) = urab + (usa + vrb + vsc)c.$$

Como f divide a ab y a c, vemos entonces que también divide a de. Como f y de son enteros no

negativos que se dividen mutuamente, tenemos en definitiva que $de = f$, que es lo que queríamos probar. □

6.5.6. La última parte de la proposición que acabamos de probar tiene la siguiente generalización:

Corolario. *Sea $r \in \mathbb{N}$. Si $a_1, \ldots, a_r$ son enteros coprimos dos a dos y $b \in \mathbb{Z}$, entonces*

$$\mathsf{mcd}(a_1 \cdots a_r, b) = \mathsf{mcd}(a_1, b) \cdots \mathsf{mcd}(a_r, b).$$

Demostración. Procedamos por inducción con respecto a r, notando que cuando r es 1 la afirmación es evidente. Sea entonces $s \in \mathbb{N}$, supongamos que la afirmación del enunciado vale cuando r es s y mostremos que entonces vale también cuando r es $s+1$.

Sean entonces $a_1, \ldots, a_{s+1}$ enteros coprimos dos a dos y sea b otro entero. Como los s enteros $a_1, \ldots, a_s$ son coprimos dos a dos, la hipótesis inductiva nos dice que

$$\mathsf{mcd}(a_1 \cdots a_s, a_{s+1}) = \mathsf{mcd}(a_1, a_{s+1}) \cdots \mathsf{mcd}(a_s, a_{s+1}) = 1,$$

así que los números $a_1 \cdots a_s$ y a_{s+1} son coprimos. La Proposición **6.5.5**(*iv*) nos dice entonces que

$$\mathsf{mcd}(a_1 \cdots a_{s+1}, b) = \mathsf{mcd}(a_1 \cdots a_s \cdot a_{s+1}, b) = \mathsf{mcd}(a_1 \cdots a_s, b) \cdot \mathsf{mcd}(a_{s+1}, b)$$

y usando otra vez la hipótesis inductiva vemos que esto es igual a

$$\mathsf{mcd}(a_1, b) \cdots \mathsf{mcd}(a_s, b) \cdot \mathsf{mcd}(a_{s+1}, b).$$

Esto completa la inducción. □

6.5.7. El resultado del siguiente ejercicio describe qué ocurre en la situación del Corolario 6.5.6 si la hipótesis no se cumple.

Ejercicio. Sea $r \in \mathbb{N}$. Muestre que si $a_1, \ldots, a_r$ y b son enteros arbitrarios, entonces

$$\mathsf{mcd}(a_1 \cdots a_r, b) \mid \mathsf{mcd}(a_1, b) \cdots \mathsf{mcd}(a_r, b).$$

y, dando un ejemplo, muestre que estos dos números no son necesariamente iguales.

6.5.8. De manera similar, podemos generalizar la parte (*ii*) de la Proposición **6.5.5** al caso en que tenemos varios divisores:

Corolario. *Sea $r \in \mathbb{N}$. Si $a_1, \ldots, a_r$ son enteros coprimos dos a dos y cada uno de ellos divide a un entero b, entonces el producto $a_1 \cdots a_r$ también divide a b.*

Si los r enteros $a_1, \ldots, a_r$ no son dos a dos coprimos la concluimos en general no vale. Por ejemplo, 6 y 15 dividen a 30 pero su producto no lo hace.

Demostración. De acuerdo al Corolario 6.5.6, tenemos que

$$\mathsf{mcd}(a_1 \cdots a_r, b) = \mathsf{mcd}(a_1, b) \cdots \mathsf{mcd}(a_r, b)$$

y, de acuerdo a la Proposición 6.4.3(*ii*) y la hipótesis de que cada uno de los enteros $a_1, \ldots, a_r$ divide a b, tenemos que $\mathsf{mcd}(a_i, b) = |a_i|$ para cada $i \in \{1, \ldots, r\}$ y, por lo tanto, tenemos que

$$\mathsf{mcd}(a_1 \cdots a_r, b) = |a_1 \cdots a_r|.$$

Esa misma Proposición 6.4.3(*ii*) nos dice entonces que $a_1 \cdots a_r$ divide a b. □

6.5.9. Nuestro siguiente resultado afirma que si dos enteros son coprimos entonces dos potencias de ellos también lo son.

Proposición. *Sean a y b dos enteros y sean k, $l \in \mathbb{N}$. Si $\mathsf{mcd}(a, b) = 1$, entonces $\mathsf{mcd}(a^k, b^l) = 1$.*

Demostración. Supongamos que $\mathsf{mcd}(a, b) = 1$, de manera que existen enteros x e y tales que $1 = xa + yb$. Se sigue de esto y de la fórmula de Newton que

$$\begin{aligned} 1 = 1^{k+l} = (xa + yb)^{k+l} &= \sum_{i=0}^{k+l} \binom{k+l}{i} x^{k+l-1} y^i a^{k+l-i} b^i \\ &= \left(\sum_{i=0}^{l} \binom{k+l}{i} x^{k+l-i} y^i a^{l-i} b^i \right) a^k + \left(\sum_{i=l+1}^{k+l} \binom{k+l}{i} x^{k+l-i} y^i a^{k+l-i} b^{i-l} \right) b^l, \end{aligned}$$

y las dos expresiones encerradas entre paréntesis son enteros. Sea $d \coloneqq \mathsf{mcd}(a^k, b^l)$. Como d divide a a^k y a b^l, esa igualdad implica que d divide a 1. Por supuesto, esto nos dice que $d = 1$, como queremos. □

6.5.10. Otra propiedad útil al calcular máximos comunes divisores es la siguiente:

6.5.11. Corolario. *Si a y b son enteros y $k \in \mathbb{N}$, entonces $\mathsf{mcd}(a^k, b^k) = \mathsf{mcd}(a, b)^k$.*

Demostración. Sea $d \coloneqq \mathsf{mcd}(a, b)$. Como d divide a a y a b, hay enteros u y v tales que $a = du$ y $b = dv$. De acuerdo a la Proposición 6.5.3, tenemos que

$$d \cdot \mathsf{mcd}(u, v) = \mathsf{mcd}(du, dv) = \mathsf{mcd}(a, b) = d,$$

de manera que $\mathsf{mcd}(u, v) = 1$. La Proposición 6.5.9 nos dice entonces que también $\mathsf{mcd}(u^k, v^k) = 1$

y usando esto podemos concluir que

$$\mathsf{mcd}(a^k, b^k) = \mathsf{mcd}(d^k u^k, d^k v^k) = d^k \cdot \mathsf{mcd}(u^k, v^k) = d^k,$$

que es lo que afirma el corolario. □

§6.6. Ejercicios

Fracciones reducidas

6.6.1. Ejercicio. Muestre que todo número racional puede escribirse de una única forma como un cociente a/b con $a \in \mathbb{Z}$, $b \in \mathbb{N}$ y $\mathsf{mcd}(a, b) = 1$. Decimos que esta es la ***forma reducida*** de ese número.

Una definición uniforme para el máximo común divisor

6.6.2. Ejercicio. Si a y b son dos enteros cualesquiera, entonces $\mathsf{mcd}(a, b)$ es el único elemento d de $\mathbb{N}_0$ tal que el conjunto $\{xa + yb : x, y \in \mathbb{Z}\}$ coincide con $\{zd : z \in \mathbb{Z}\}$.

Podríamos haber usado esta caracterización del máximo común divisor de dos números para definirlo: tiene la ventaja de que no nos fuerza a considerar por separado en caso en el que los dos números a y b son nulos.

El máximo común divisor de un conjunto finito de números

6.6.3. Ejercicio. Sean $k \in \mathbb{N}$ y $a_1, \ldots, a_k \in \mathbb{Z}$.

(*a*) Si los enteros $a_1, \ldots, a_k$ no todos simultáneamente nulos, el conjunto $D(a_1, \ldots, a_k)$ de los enteros positivos que dividen a cada uno de ellos es finito y no vacío. Tiene sentido entonces considerar su elemento máximo, al que llamamos el ***máximo común divisor*** de los enteros $a_1, \ldots, a_k$ y escribimos $\mathsf{mcd}(a_1, \ldots, a_k)$. Si en cambio todos los enteros $a_1, \ldots, a_k$ son nulos, definimos $\mathsf{mcd}(0, \ldots, 0) = 0$.

(*b*) Si $k \geq 3$, entonces

$$\mathsf{mcd}(a_1, \ldots, a_k) = \mathsf{mcd}(\mathsf{mcd}(a_1, a_2), a_3, \ldots, a_k). \tag{22}$$

(*c*) Existen enteros $x_1, \ldots, x_k$ tales que

$$x_1 a_1 + \cdots + x_k a_k = \mathsf{mcd}(a_1, \ldots, a_k). \tag{23}$$

(*d*) El entero $\mathsf{mcd}(a_1, \ldots, a_k)$ es el único que tiene las siguientes dos propiedades:

- es un divisor común positivo de los números $a_1, \ldots, a_k$, y
- divide a cada divisor común de los números $a_1, \ldots, a_k$.

(*e*) El entero $\mathsf{mcd}(a_1, \ldots, a_k)$ es el único entero no negativo d tal que el conjunto

$$\{x_1 a_1 + x_2 a_2 + \cdots + x_k a_k : x_1, x_2, \ldots, x_k \in \mathbb{Z}\}$$

coincide con $\{yd : y \in \mathbb{Z}\}$.

(*f*) Describa un algoritmo basado en la igualdad (22) y el algoritmo de Euclides para encontrar tanto a $\mathsf{mcd}(a_1, \ldots, a_k)$ como a enteros $x_1, \ldots, x_k$ para los que vale la igualdad (23).

El mínimo común múltiplo de dos enteros

6.6.4. Ejercicio. Sean a y b dos enteros.

(*a*) Sea $M(a, b)$ el conjunto de los múltiplos positivos comunes de a y de b, es decir, de los números enteros positivos m tales que $a \mid m$ y $b \mid m$. Si a y b no son simultáneamente nulos, entonces el conjunto $M(a, b)$ no es vacío y podemos entonces considerar su mínimo elemento: lo llamamos el ***mínimo común múltiplo*** de a y b, y lo escribimos $\mathsf{mcm}(a, b)$. Si en cambio alguno de a o b es nulo definimos $\mathsf{mcm}(a, b) = 0$.

(*b*) El entero no negativo $\mathsf{mcm}(a, b)$ es el único que tiene las siguientes dos propiedades:

- es un múltiplo común de a y de b, y
- divide a todo múltiplo común de a y de b.

(*c*) Si a y b son no negativos, entonces $ab = \mathsf{mcd}(a, b) \cdot \mathsf{mcm}(a, b)$. En particular, es $\mathsf{mcm}(a, b) = ab$ si y solamente si $\mathsf{mcd}(a, b) = 1$.

(*d*) Si a, b y c son enteros, entonces

$$\mathsf{mcm}(ac, bc) = \mathsf{mcm}(a, b) \cdot c.$$

Si además a y b son coprimos, entonces

$$\mathsf{mcm}(ab, c) \cdot c = \mathsf{mcd}(a, c) \cdot \mathsf{mcd}(b, c).$$

(*e*) Dé una definición del mínimo común múltiplo de un conjunto finito de enteros, en el espíritu del Ejercicio 6.6.3, y pruebe sus propiedades básicas. En particular, muestre que si

$n \in \mathbb{N}$ es al menos 3 y $a_1, \ldots, a_n$ son enteros, entonces

$$\mathsf{mcm}(\mathsf{mcm}(a_1, a_2), a_3, \ldots, a_n) = \mathsf{mcm}(a_1, a_2, a_3, \ldots, a_n).$$

Algunas propiedades del máximo común divisor y del mínimo común múltiplo

6.6.5. Ejercicio.

(*a*) Si a, b y c son enteros, entonces

$$\mathsf{mcd}(\mathsf{mcd}(a, b), c) = \mathsf{mcd}(a, \mathsf{mcd}(b, c))$$

y

$$\mathsf{mcm}(\mathsf{mcm}(a, b), c) = \mathsf{mcm}(a, \mathsf{mcm}(b, c)).$$

En otras palabras, las operaciones $\mathsf{mcd}(\cdot, \cdot)$ y $\mathsf{mcm}(\cdot, \cdot)$ son asociativas.

(*b*) Si a, b, c son enteros, entonces

$$\mathsf{mcd}(a, \mathsf{mcm}(b, c)) = \mathsf{mcm}(\mathsf{mcd}(a, b), \mathsf{mcd}(a, c))$$

y

$$\mathsf{mcm}(a, \mathsf{mcd}(b, c)) = \mathsf{mcd}(\mathsf{mcm}(a, b), \mathsf{mcm}(a, c)).$$

(*c*) Si a y b no son simultáneamente nulos, entonces

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

(*d*) Si a, b y c son enteros, entonces

$$\mathsf{mcm}(a, b, c) \cdot \mathsf{mcd}(a, b) \cdot \mathsf{mcd}(b, c) \cdot \mathsf{mcd}(c, a) = abc \cdot \mathsf{mcd}(a, b, c).$$

Este ejercicio fue uno de los tomados en la primera Olimpíada de Matemáticas de Moscú en 1935.

La sucesión $(a^n - 1)_{n\geq 0}$

6.6.6. Ejercicio. Sea a un entero distinto de 0 y de 1.

(*a*) Si x e y son enteros y $n \in \mathbb{N}$, entonces

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1})$$

y, en particular, $x - y$ divide a $x^n - y^n$.

(*b*) Si $n, m \in \mathbb{N}$ y n divide a m, entonces $a^n - 1$ divide a $a^m - 1$.

(*c*) Si $n, m \in \mathbb{N}$ y r es el resto de la división de n por m, entonces

$$\mathsf{mcd}(a^n - 1, a^m - 1) = \mathsf{mcd}(a^r - 1, a^m - 1).$$

(*d*) Si $n, m \in \mathbb{N}$, entonces $\mathsf{mcd}(a^n - 1, a^m - 1) = a^{\mathsf{mcd}(n,m)} - 1$.

Los números de Fibonacci

6.6.7. Ejercicio. Sea $(F_n)_{n\geq 0}$ la sucesión de los números de Fibonacci.

(*a*) Muestre que para todo $n \in \mathbb{N}$ se tiene que $\mathsf{mcd}(F_n, F_{n+1}) = 1$ y encuentre enteros x e y tales que $xF_n + yF_{n+1} = 1$.

(*b*) Si $n, m \in \mathbb{N}$ y n divide a m, entonces F_n divide a F_m.

(*c*) Si $n, m \in \mathbb{N}$ y r es el resto de la división de n por m, entonces

$$\mathsf{mcd}(F_n, F_m) = \mathsf{mcd}(F_r, F_m).$$

(*d*) Si $n, m \in \mathbb{N}_0$, entonces

$$\mathsf{mcd}(F_n, F_m) = F_{\mathsf{mcd}(n,m)}.$$

Sugerencia: Para probar la parte (*b*) es útil recordar el Lema 5.4.7 del Capítulo 5.

6.6.8. Ejercicio. Sea $n \in \mathbb{N}$.

(*a*) El algoritmo de Euclides necesita $n + 1$ pasos para calcular $\mathsf{mcd}(F_{n+3}, F_{n+2})$.

(*b*) Si a y b son dos enteros positivos tales $a > b$ y para los cuales el algoritmo de Euclides necesita $n + 1$ pasos para calcular $\mathsf{mcd}(a, b)$, entonces $a \geq F_{n+3}$ y $b \geq F_{n+2}$.

Observemos que la conjunción de estas dos afirmaciones nos dice que el peor caso — en el sentido de que tarda la máxima cantidad de pasos — para el algoritmo de Euclides es aquél en el que sus datos de partida son dos números de Fibonacci consecutivos.

(*c*) Si a y b son enteros tales que $1 < b, a < N$, entonces el número de pasos que algoritmo de Eu-

clides requiere para calcular $\mathsf{mcd}(a,b)$ no excede a $\lceil \log_\varphi(\sqrt{5}N)\rceil - 2$. Aquí $\varphi = (1+\sqrt{5})/2$, $\log_\varphi$ denota el logaritmo en base φ y para cada número real u escribimos $\lceil u\rceil$ el menor entero mayor que u.

Este resultado es conocido como *Teorema de Lamé*, por Gabriel Lamé, quien lo obtuvo en 1844. Puede encontrarse una discusión detallada del algoritmo de Euclides desde el punto de vista de la complejidad en el libro [Knu1969].

Los números de la forma $2^{2^n}+1$

6.6.9. Ejercicio. Para cada $n \in \mathbb{N}_0$ sea $F_n := 2^{2^n}+1$.

(*a*) Muestre que para todo $n \in \mathbb{N}_0$ y todo $k \in \mathbb{N}$ vale $F_n \mid F_{n+k} - 2$.

(*b*) Deduzca de eso que los números $F_0, F_1, F_2, \ldots$ son coprimos dos a dos.

El desarrollo en fracción continua finita de un número racional

6.6.10. Ejercicio. Sea a/b un número racional positivo escrito de manera irreducible, de manera que a y b son enteros positivos y $\mathsf{mcd}(a,b) = 1$. Sea $(r_i)_{i\geq 0}$ la sucesión construida por el algoritmo de Euclides para calcular el máximo común divisor de a y b, como en 6.4.6, y sea N el número que nos da la Proposición 6.4.7, de manera que $r_i \neq 0$ si $i \leq N$, $r_N = \mathsf{mcd}(a,b) = 1$ y $r_i = 0$ si $i > N$. Sean, finalmente, $q_2, \ldots, q_{N+1}$ la sucesión de los cocientes que encontramos al llevar a cabo el algoritmo: esto es, tales que $r_{i-2} = q_i r_{i-1} + r_i$ para cada $i \in \{2, \ldots, N+1\}$.

Muestre que

$$\frac{a}{b} = q_2 + \frac{r_2}{r_1} = q_2 + \cfrac{1}{q_3 + \cfrac{r_3}{r2}} = q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cfrac{r_4}{r_3}}} = q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cfrac{1}{q_5 + \cfrac{r_5}{r_4}}}} = \cdots$$

y que se puede continuar así hasta obtener la expresión

$$\frac{a}{b} = q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cfrac{1}{\ddots + \cfrac{1}{q_{N+1}}}}}.$$

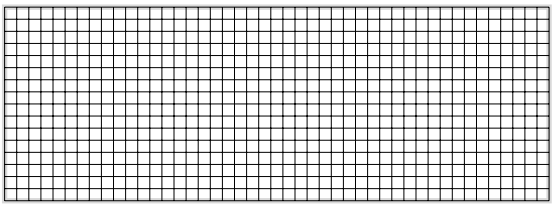
Esta escritura para el número a/b se llama su expresión como ***fracción continua finita***. Así, por

ejemplo, tenemos que

$$\frac{77}{30} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4}}}},$$

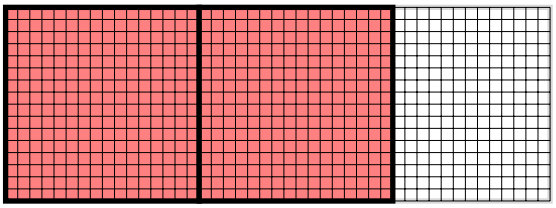
$$\frac{81\,201}{56\,660} = 1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{5 + \cfrac{1}{6 + \cfrac{1}{7 + \cfrac{1}{8}}}}}}}.$$

6.6.11. Sean a y b dos enteros positivo tales que $a \geq b$ y supongamos que tenemos una cuadrícula de a por b. Por ejemplo, si $a = 45$ y $b = 16$, tenemos el siguiente diagrama



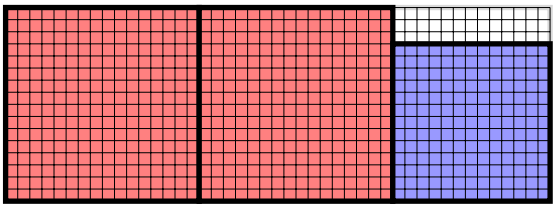
Nuestro objetivo es cubrir esta cuadrilla con cuadrados de tamaños enteros. Es claro que esto es posible: basta usar $45 \cdot 16 = 720$ cuadrados de 1 por 1. Lo que queremos, sin embargo, es usar la menor cantidad posible de cuadrados. Una estrategia posible que podemos probar es la de usar la mayor cantidad posible de cuadrados lo más grandes que podamos.

En este ejemplo concreto, es claro que el tamaño máximo de un cuadrado de lados enteros que entra en el diagrama es 16. Además, como el cociente de dividir 45 por 16 es 2, el número máximo de cuadrados de lado 16 que podemos poner es 2.

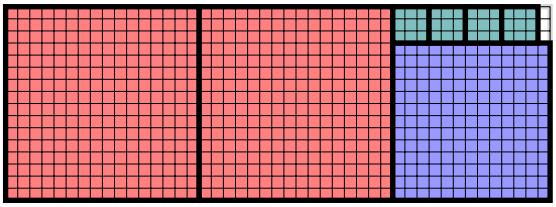


Después de poner esos dos rectángulos, nos queda sin cubrir una región de 13 por 16. El lado del

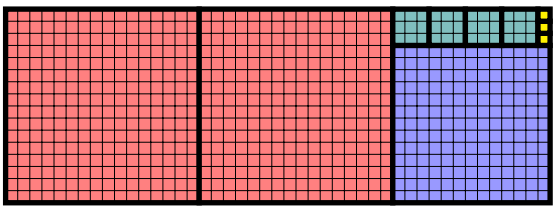
cuadrado más grande que entra en ella es 13 y claramente entra uno solo: si lo ponemos, queda



Quedó libre una región de 13 por 3: el cuadrado más grande que entra ahí es de 3 por 3 y entran 4 de ellos.



Finalmente, es claro que la región que nos queda sólo la podemos cubrir con 3 cuadrados de 1 por 1. Al terminar, entonces, tenemos la siguiente situación:

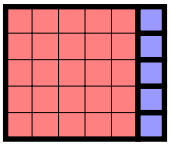


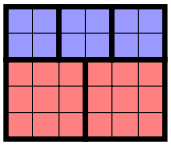
6.6.12. Ejercicio. Sean a y b dos enteros positivos tales que $a \geq b$ y sean $(r_i)_{i\geq 0}$, N y $q_2, \ldots, q_{N+1}$ como en el Ejercicio 6.6.10. Se tiene que

$$ab = q_2 r_1^2 + q_3 r_3^2 + \cdots + q_{N+1} r_N^2$$

y es posible cubrir un rectángulo de a por b con $q_2 + q_3 + \cdots + q_{N+1}$ cuadrados de lados de longitud entera.

Observemos que no es claro que la estrategia que describimos arriba para hacer cubrir el rectángulo sea una que minimice el número de cuadrados y, de hecho, esto no es cierto. El menor ejemplo de esto aparece cuando consideramos un rectángulo de 6 por 5: de los siguientes dos diagramas el de la izquierda fue construido usando la estrategia anterior y usa en total 6 cuadrados, mientras que el de la derecha usa solamente 5.





Si a y b son enteros positivos tales que $a \geq b$ y $\mathsf{mcd}(a, b)$, escribamos $\sigma(a, b)$ al menor número de cuadrados de lados enteros con los que es posible cubrir un rectángulo de a por b. Richard Kenyon mostró en su trabajo [Ken1996] que hay una constante positiva C tal que

$$\mathsf{máx}\left\{\frac{a}{b}, \log_2 a\right\} \leq \sigma(a, b) \leq \frac{a}{b} + C \log_2 b$$

cada vez que a y b son enteros coprimos y $a \geq b > 0$.

En el contexto de este problema, es interesante recordar el siguiente teorema clásico de Max Dehn [Deh1903] y Roland Sprague [Spr1940], que tiene una demostración sorprendentemente difícil: un rectángulo puede ser cubierto con finitos cuadrados sin que estos se superpongan si y solamente si el cociente de las longitudes de sus lados es un número racional. Una demostración muy simplificada y más conceptual de este resultado — en el que el problema se reduce a un problema sobre el flujo de electricidad en un circuito eléctrico que es luego resuelto usando la Ley de Kirchoff — puede encontrarse en [BSST1940].