El Máximo Común Divisor

Por Carlos Jacob Rubio Barrios y José Alejandro Lara Rodríguez

Nivel Intermedio

Divisibilidad

Si a y b son números enteros, se dice que a *divide* a b, denotado por $a \mid b$, si $b = ac$ para algún entero c. En este caso se dice que a es un *divisor* de b. Otras formas de decir que a divide a b son:

a es un factor de b,
b es un múltiplo de a,
b es divisible entre a.

Si a no divide a b, se escribe $a \nmid b$.
Si a y b son enteros, una *combinación lineal* de a y b es un entero de la forma $ax + by$ donde x, y son enteros.
En el siguiente teorema se presentan algunas propiedades útiles de la divisibilidad.

Teorema 1.

1. *Propiedad reflexiva: Para cualquier entero a, se tiene $a \mid a$.*
2. *Propiedad transitiva: Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.*
3. *Un entero c divide a los enteros a y b si y solamente si c divide a cualquier combinación lineal de a y b:*

   $$c \mid a \text{ y } c \mid b \Leftrightarrow c \mid (ax + by) \text{ para cualesquiera enteros } x, y.$$

4. *$a \mid b$ y $b \mid a$ si y solamente si $a = \pm b$.*
5. *Sea m un entero distinto de cero. Entonces $a \mid b$ si y solamente si $ma \mid mb$.*

Demostración. Todas las pruebas son inmediatas de la definición.

1. Es evidente que $a = a \cdot 1$.

2. Si $b = aq_1$ y $c = bq_2$, con q_1 y q_2 enteros, entonces $c = (aq_1)q_2 = a(q_1q_2)$.

3. $\Rightarrow$): Como $c \mid a$ y $c \mid b$, existen enteros q_1, q_2 tales que $a = cq_1$ y $b = cq_2$. Por lo tanto $ax = cq_1x$ y $by = cq_2y$. Sumando término a término y factorizando c se tiene que $ax + by = c(q_1x + q_2y)$, lo que demuestra que c siempre divide a $ax + by$.

   $\Leftarrow$): Como c divide a cualquier combinación lineal de a y b, en particular, $c \mid (a \cdot 1 + b \cdot 0)$ y $c \mid (a \cdot 0 + b \cdot 1)$; es decir, $c \mid a$ y $c \mid b$.

4. Supongamos primero que $a \mid b$ y $b \mid a$. Primero se observa que si $a = 0$ entonces $b = 0$ ya que $a \mid b$ y se cumple $0 = \pm 0$. Recíprocamente, si $b = 0$, entonces a es cero y también se cumple $a = \pm b$. Supongamos que ni a ni b son cero. De la hipótesis se sigue que existen enteros u_1, u_2 tales que $b = au_1$ y $a = bu_2$. Esto implica que $b = bu_2u_1$ y $a = au_1u_2$ y por tanto $u_1u_2 = 1$. Entonces $u_1 = u_2 = 1$ o $u_1 = u_2 = -1$. Luego $a = b$ o $a = -b$.

   Recíprocamente, supongamos que $a = \pm b$. Por definición se tiene $b \mid a$. También se tiene $b = \pm a$ y por lo $a \mid b$.

5. Si $a \mid b$, entonces $b = ac$ para algún entero c. Multiplicando ambos lados de la igualdad por m, se obtiene $mb = mac$ lo que indica que $ma \mid mb$ (observe que no importa que m sea cero o distinto de cero).

   Recíprocamente, si $ma \mid mb$, entonces existe algún entero c tal que $mb = mac$. Como $m \neq 0$, aplicando la ley de la cancelación se obtiene $b = ac$.

□

Algunos casos particulares del Teorema 1 se presentan en el siguiente

Corolario 1.

1. *Si $a \mid b$, entonces $a \mid bx$ para cualquier entero x.*

2. *Si $c \mid a$ y $c \mid b$, entonces $c \mid (\pm a \pm b)$.*

Demostración. 1. Por hipótesis $a \mid b$ y como siempre sucede que $a \mid 0$, entonces $a \mid (bx + 0y)$ para cualesquiera enteros x, y, esto es, $a \mid bx$.

2. De la hipótesis se sigue que c divide a cualquier combinación lineal de a y b, y cada uno de los enteros $a + b$, $a - b$, $-a + b$ y $-a - b$ es una combinación lineal de a y b.

□

Teorema 2. *Sean a y b números enteros.*

1. *$a \mid |a|$ y $|a| \mid a$.*

2. *Las siguientes condiciones son equivalentes:*

   a) $a \mid b$.

   b) $|a| \mid |b|$.

Demostración. 1. De acuerdo con la definición de valor absoluto se tiene

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

Es decir, $|a| = \pm a$. Esto prueba que $a \mid |a|$. También se tiene que $a = \pm|a|$. Por tanto, $|a| \mid a$.

2. Supongamos primero que $a \mid b$. Como $|a| \mid a$ y $a \mid b$ se sigue que $|a| \mid b$; ahora se tiene que $|a| \mid b$ y $b \mid |b|$; por tanto $|a| \mid |b|$.

   Recíprocamente, supongamos que $|a| \mid |b|$. Como $a \mid |a|$ y $|a| \mid |b|$ se obtiene que $a \mid |b|$. Como también se tiene que $|b| \mid b$, se llega a que $a \mid b$.

□

El Algoritmo de la división

Una propiedad muy útil que relaciona el orden en el conjunto de los números enteros con la divisibilidad es la siguiente.

Teorema 3. *Si a y b son enteros con $b \neq 0$ y $a \mid b$, entonces $|a| \leq |b|$.*

Demostración. La hipótesis $a \mid b$ implica que $|a| \mid |b|$. Entonces $|b| = |a|c$ para algún entero c. Como $b \neq 0$, tenemos que $a \neq 0$ y por lo tanto $|b| > 0$ y $|a| > 0$. De aquí, $c > 0$ o, de manera equivalente, $c \geq 1$. Luego, $|b| = |a|c \geq |a|$. □

Una consecuencia inmediata de este teorema es que todo entero distinto de cero tiene un número finito de divisores. En efecto, sea a un entero distinto de cero y sea $d \in \mathcal{D}$ donde $\mathcal{D}$ es el conjunto de los divisores de a. Entonces $d \mid a$ y por lo tanto $|d| \leq |a|$, o lo que es equivalente $-|a| \leq d \leq |a|$. Luego, $\mathcal{D}$ es subconjunto del conjunto

$$\{-|a|, -|a| + 1, \ldots, -1, 0, 1, \ldots, |a|\}$$

de donde se sigue que $\mathcal{D}$ es un conjunto finito.

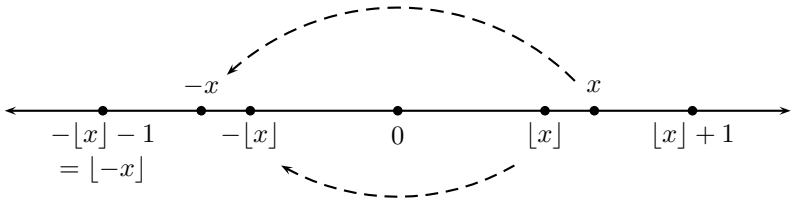
Si x es un número real, $\lfloor x \rfloor$ denota al mayor entero menor o igual que x:

$$\lfloor x \rfloor = \text{máx}\{k \in \mathbb{Z} \colon k \leq x\}.$$

El entero $\lfloor x \rfloor$ es el *piso* de x y de acuerdo con la definición es el único entero tal que

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1.$$

Si x es entero, $\lfloor x \rfloor = x$ y si x no es entero, $\lfloor x \rfloor$ es el primer entero a la izquierda de x en la recta real. Por ejemplo $\lfloor -3.5 \rfloor = -4$ y $\lfloor 3.8 \rfloor = 3$.
Si x no es entero, entonces $\lfloor -x \rfloor = -\lfloor x \rfloor - 1$. En efecto, $\lfloor x \rfloor$ es el entero inmediato anterior a x y $\lfloor x \rfloor + 1$ es el entero inmediato posterior x, de modo que el entero inmediato anterior a $-x$ es $-\lfloor x \rfloor - 1$ y el entero inmediato posterior a $-x$ es $-\lfloor x \rfloor$.



Teorema 4 (Algoritmo de la división)**.** *Si a y b son enteros y $b \neq 0$, entonces existen enteros q y r únicos tales que*

$$a = qb + r \quad con \quad 0 \leq r < |b|.$$

Se dice que q es el "cociente" y r es el "residuo".

Demostración. En primer lugar demostraremos la existencia de los enteros q y r, considerando dos casos.
Caso 1: $b > 0$. Haciendo $q = \lfloor \frac{a}{b} \rfloor$, tenemos que

$$q \leq \frac{a}{b} < q + 1 \Rightarrow qb \leq a < (q+1)b \Rightarrow 0 \leq a - qb < b.$$

Tomando $r = a - qb$, se sigue que las elecciones posibles para el entero r son 0, 1, $2, \ldots, b-1$.
Caso 2: $b < 0$. Como $-b > 0$, por el Caso 1, existen enteros q y r tales que $a = q(-b) + r = (-q)b + r$ con $0 \leq r < -b = |b|$. Luego, $-q$ y r son el cociente y residuo, respectivamente.
Para demostrar la unicidad, supongamos que q, r, q' y r' son tales que $a = qb + r$ con $0 \leq r < |b|$ y $a = q'b + r'$ con $0 \leq r' < |b|$. Si $r - r' \geq |b|$, se tendría que $r \geq |b| + r' \geq |b|$, lo que es una contradicción. Luego, $r - r' < |b|$ y también $r' - r < |b|$, así que $|r - r'| < |b|$.
Por otro lado se tiene que $b(q - q') = r' - r$ lo que indica que $b \mid r' - r$; por tanto también se tiene que $|b|$ divide a $|r - r'|$. Si $r' - r \neq 0$ se tendría $|b| \leq |r - r'|$ lo que sería una contradicción. Luego $r - r' = 0$, esto es, $r = r'$. Dado que $b \neq 0$, $bq + r = bq' + r'$ implica que $q = q'$. □

A continuación, veamos algunas aplicaciones del Algoritmo de la división.

Ejemplo 1. *Sea n un entero positivo tal que $3n + 1$ es un cuadrado. Demostrar que $n + 1$ es suma de tres cuadrados.*

Solución. Sea n un entero positivo tal que $3n + 1 = k^2$ para algún entero k. Por el algoritmo de la división, $k = 3q + r$ con $r = 0, 1$ o 2.
Si $k = 3q$, entonces $3n + 1 = 9q^2$ de donde 1 es múltiplo de 3, lo cual es un absurdo.
Si $k = 3q + 1$, entonces $3n + 1 = 9q^2 + 6q + 1$ de donde $n = 3q^2 + 2q$. Así, $n + 1 = q^2 + q^2 + (q+1)^2$ es suma de tres cuadrados.
Si $k = 3q + 2$, entonces $3n + 1 = 9q^2 + 12q + 4$ de donde $n = 3q^2 + 4q + 1$. Así, $n + 1 = q^2 + (q+1)^2 + (q+1)^2$ es suma de tres cuadrados.

Ejemplo 2. *Sean a, d y n enteros positivos con $a > 1$. Si $a^d - 1$ divide a $a^n - 1$, demostrar que d divide a n.*

Solución. Por el algoritmo de la división, existen enteros (únicos) q y r tales que $n = dq + r$ con $0 \leq r < d$. Entonces,

$$a^n - 1 = (a^{dq+r} - a^r) + (a^r - 1) = a^r(a^{dq} - 1) + (a^r - 1).$$

Si $a^d - 1$ divide a $a^n - 1$, entonces $a^d - 1$ divide a $a^r - 1$, pues $a^d - 1$ también divide a $a^{dq} - 1$ (observe que $a^{dq} - 1 = (a^d)^q - 1 = (a^d - 1)(a^{d(q-1)} + a^{d(q-2)} + \cdots + a^d + 1)$). Luego, si $a^r - 1 > 0$, tendríamos que $a^d - 1 \leq a^r - 1$ (por el Teorema 3) de donde $d \leq r$, lo cual no es posible. Por lo tanto, $a^r - 1 = 0$ lo cual implica que $r = 0$ y $n = dq$. Así, $d \mid n$.

El máximo común divisor

Como vimos antes, el número de divisores de un entero distinto de cero es finito, de modo que podemos definir el *máximo común divisor* de los enteros a y b como el máximo de los divisores comunes de a y b, esto es,

$$\text{máx}\{d \in \mathbb{Z} \colon d \mid a \text{ y } d \mid b\},$$

suponiendo que $a \neq 0$ o $b \neq 0$, donde $\mathbb{Z}$ denota el conjunto de los números enteros. Denotaremos a este número por $\text{mcd}(a, b)$. Se extiende la definición estableciendo que $\text{mcd}(0, 0) = 0$.

El máximo común divisor de a y b cuando $a \neq 0$ o $b \neq 0$, es por definición el elemento máximo de la intersección del conjunto de divisores de a con el conjunto de divisores de b:

$$\text{mcd}(a, b) = \text{máx}\{d \in \mathbb{Z} \colon d \mid a \text{ y } d \mid b\} = \text{máx}(\{d \in \mathbb{Z} \colon d \mid a\} \cap \{d \in \mathbb{Z} \colon d \mid b\}).$$

De la definición también es inmediato que $\text{mcd}(a, b) = \text{mcd}(b, a)$.

Dado que el conjunto de divisores de un entero a es el mismo que el conjunto de divisores de $-a$ se sigue directamente de la definición que

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

Ejemplo 3. *El máximo común divisor de 6 y 10 es 2, ya que*

$$\{d \in \mathbb{Z} \colon d \mid 6 \text{ y } d \mid 10\} = \{\pm 1, \pm 2, \pm 3, \pm 6\} \cap \{\pm 1, \pm 2, \pm 5, \pm 10\} = \{-2, -1, 1, 2\}.$$

También se tiene $mcd(-4, 6) = 2$ puesto que

$$mcd(-4, 6) = \text{máx}(\{\pm 1, \pm 2, \pm 4\} \cap \{\pm 1, \pm 2, \pm 3, \pm 6\}) = \text{máx}\{-2, -1, 1, 2\} = 2.$$

Por otro lado, $mcd(3, 0) = 3$ ya que

$$\text{máx}(\{-3, -1, 1, 3\} \cap \mathbb{Z}) = \text{máx}\{-3, -1, 1, 3\} = 3.$$

En general, $mcd(a, 0) = mcd(0, a) = |a|$ para cualquier entero a.

Teorema 5. *Si a y b son enteros, entonces*

$$mcd(a, b) = mcd(a, b - a) = mcd(b, a - b) = mcd(a, a + b).$$

Demostración. Si $a = b = 0$, el resultado es inmediato. Supondremos que $a \neq 0$ o $b \neq 0$. Para probar la primera igualdad de izquierda a derecha, bastará probar que el conjunto de divisores de a y b es el mismo que el conjunto de divisores de a y $b - a$ (pues el conjunto de divisores de un entero distinto de cero es un conjunto finito, y si dos conjuntos finitos son iguales necesariamente tienen el mismo elemento máximo.) Sea d un divisor común de a y b, es decir, $d \mid a$ y $d \mid b$. De acuerdo con el Corolario 1, se sigue que $d \mid (b - a)$. Recíprocamente, si $d \mid a$ y $d \mid b - a$, entonces $d \mid a$ y $d \mid a + (b - a)$, i.e., $d \mid a$ y $d \mid b$.
Las pruebas de que $\text{mcd}(a, b) = \text{mcd}(b, a - b)$ y $\text{mcd}(a, b) = \text{mcd}(a, b + a)$ son análogas y se dejan de ejercicio al lector. □

Una consecuencia inmediata del teorema anterior y que será de gran utilidad para el cálculo del máximo común divisor es la siguiente.

Corolario 2. *Sean a, b y n enteros. Entonces, $mcd(a, b) = mcd(a, b - an)$.*

Demostración. Si $n = 0$, el resultado es inmediato. Si $n > 0$, aplicando repetidamente el teorema anterior se tiene

$$\text{mcd}(a, b) = \text{mcd}(a, b - a) = \text{mcd}(a, b - a - a) = \cdots = \text{mcd}(a, b - na)$$

y si $n < 0$ se tiene

$$\begin{aligned}\text{mcd}(a, b) &= \text{mcd}(a, a + b) = \text{mcd}(a, a + a + b) = \cdots = \text{mcd}(a, |n|a + b) \\ &= \text{mcd}(a, -na + b).\end{aligned}$$

□

Se pueden usar repetidamente el Algoritmo de la división junto con el Teorema 5 para calcular el máximo común divisor. Ilustramos esto con un ejemplo.

Ejemplo 4. *Calcular $mcd(4655, 1309)$.*

Solución. Al dividir 4655 entre 1309 hallamos que $4655 = 1309 \cdot 3 + 728$, es decir, $q = 3$ y $r = 728$. De acuerdo con el Teorema 5, se tiene

$$\text{mcd}(1309, 4665) = \text{mcd}(1309, 4665 - 1309 \cdot 3) = \text{mcd}(1309, 728).$$

Esto reduce el problema, pues ahora se debe hallar el mcd de números más pequeños. Repitiendo el proceso encontramos que $1309 = 728 \cdot 1 + 581$, de tal manera que $\text{mcd}(1309, 728) = \text{mcd}(728, 581)$. Continuando de esta manera:

$$\begin{aligned}
728 &= 581 \cdot 1 + 147, & \text{mcd}(728, 581) &= \text{mcd}(581, 147), \\
581 &= 147 \cdot 3 + 140, & \text{mcd}(581, 147) &= \text{mcd}(147, 140), \\
147 &= 140 \cdot 1 + 7, & \text{mcd}(147, 140) &= \text{mcd}(140, 7), \\
140 &= 7 \cdot 20 + 0, & \text{mcd}(140, 7) &= \text{mcd}(7, 0) = 7.
\end{aligned}$$

De esta forma se tiene que $\text{mcd}(4665, 1309) = 7$.
Aunque el procedimiento puede resultar largo y quizá tedioso por las divisiones sucesivas, este es un método que no requiere la factorización de números, la cual puede no ser fácil de realizar, sobre todo cuando se trata de números grandes. De hecho, se sabe que el número de pasos requeridos para encontrar el máximo común divisor de los enteros a y b es, en el peor de los casos, 5 veces el número de dígitos (en base 10) del más pequeño de los números. En el ejemplo anterior, los dos números tienen 4 dígitos, así que en el peor de los casos hubiera sido necesario realizar 20 divisiones o 20 algoritmos de la división.

Algoritmo Euclidiano. *Dados los enteros a y b, mediante la aplicación repetida del Algoritmo de la división se obtiene una sucesión de cocientes y residuos*

$$\begin{aligned}
a &= bq_0 + r_0, & 0 \le r_0 < |b|, \quad &(0)\\
b &= r_0q_1 + r_1, & 0 \le r_1 < r_0, \quad &(1)\\
r_0 &= r_1q_2 + r_2, & 0 \le r_2 < r_1, \quad &(2)\\
&\vdots & &\\
r_{n-2} &= r_{n-1}q_n + r_n, & 0 \le r_n < r_{n-1}, \quad &(n)\\
r_{n-1} &= r_nq_{n+1}, & &(n+1)
\end{aligned}$$

donde r_n es el último residuo distinto de cero. Entonces, r_n es el máximo común divisor de a y b.

Es importante enfatizar la existencia de r_n. Dado que $|b| > r_0 > r_1 > \cdots > r_n$ es una sucesión estrictamente decreciente de números enteros no negativos, la sucesión no puede continuar de manera indefinida.

Ejemplo 5. *Sean a, b y c enteros con $a > 1$. Demostrar que*

$$mcd(a^b - 1, a^c - 1) = a^{mcd(b,c)} - 1.$$

Solución. Por el algoritmo de la división, podemos escribir $b = cq + r$ con $0 \le r < c$. Luego,

$$\begin{aligned}
a^b - 1 &= (a^{cq} - 1)a^r + a^r - 1\\
&= (a^c - 1)(a^{c(q-1)} + a^{c(q-2)} + \cdots + a^c + 1)a^r + (a^r - 1).
\end{aligned}$$

Aplicando el Corolario 2 con los enteros $a^c - 1$, $a^b - 1$ y $n = (a^{c(q-1)} + a^{c(q-2)} + \cdots + a^c + 1)a^r$, tenemos que

$$\begin{aligned}
\text{mcd}(a^b - 1, a^c - 1) &= \text{mcd}(a^c - 1, a^{b-1} - (a^{c(q-1)} + a^{c(q-2)} + \cdots + a^c + 1)a^r(a^c - 1))\\
&= \text{mcd}(a^c - 1, a^r - 1).
\end{aligned}$$

De manera análoga, nuevamente por el Algoritmo de la división tenemos que $c = rq_1 + r_1$ con $0 \le r_1 < r$ y $\text{mcd}(a^c - 1, a^r - 1) = \text{mcd}(a^r - 1, a^{r_1} - 1)$. Continuando de

esta forma, si $r, r_1, r_2, \ldots, r_n$ son los residuos obtenidos en la aplicación del Algoritmo Euclidiano y r_n es el máximo común divisor de b y c obtenemos

$$(a^b-1, a^c-1) = (a^c-1, a^r-1) = (a^r-1, a^{r_1}-1) = \cdots = (a^{r_{n-1}}-1, a^{r_n}-1)$$
$$= (a^{r_n}-1, 0) = a^{r_n}-1 = a^{mcd(b,c)}-1.$$

El siguiente teorema establece que el máximo común divisor de los números a y b es combinación lineal de a y b. Es un resultado muy útil en problemas de la olimpiada.

Teorema 6. *Si a y b son enteros, entonces existen enteros x, y tales que*

$$mcd(a,b) = ax + by.$$

Demostración. Se tiene $\text{mcd}(a,0) = |a| = a \cdot u + 0 \cdot 0$, donde $u = 1$ o -1. Análogamente, $\text{mcd}(0,b) = |b| = 0 \cdot 0 + b \cdot u'$, con $u' = 1$ o -1, y $\text{mcd}(0,0) = 0 \cdot 0 + 0 \cdot 1$. Se puede suponer que $ab \neq 0$. En el Algoritmo Euclidiano, primero se usa la ecuación (n), para escribir r_n en términos de los dos residuos inmediatos anteriores, $r_n = r_{n-2} - q_n r_{n-1}$. Después se usa la ecuación $(n-1)$ para escribir r_{n-1} en términos de r_{n-2} y r_{n-3}, etc. Al final de este proceso recursivo, r_n estará escrito en términos de a y b. □

Hay más de una manera de escribir $\text{mcd}(a,b)$ como combinación lineal de a y b. De hecho, hay una infinidad, pues si $\text{mcd}(a,b) = ax + by$, también se tiene $\text{mcd}(a,b) = a(x+b) + b(y-a)$. Sin embargo, en muchos problemas basta considerar una.

Ejemplo 6. *De acuerdo con el Ejemplo 4, se tiene $mcd(4655, 1309) = 7$. Además,*

$$4655 = 1309 \cdot 3 + 728, \quad (0)$$
$$1309 = 728 \cdot 1 + 581, \quad (1)$$
$$728 = 581 \cdot 1 + 147, \quad (2)$$
$$581 = 147 \cdot 3 + 140, \quad (3)$$
$$147 = 140 \cdot 1 + 7, \quad (4)$$
$$140 = 7 \cdot 20. \quad (5)$$

Despejando 7 en la ecuación (4), se tiene $7 = 147 - 140 \cdot 1$. Ahora se despeja 140 en la ecuación (3) y se sustituye en la ecuación anterior

$$7 = 147 - (581 - 147 \cdot 3) = 147 \cdot 4 - 581 \cdot 1.$$

A continuación se despeja 147 en la ecuación (2) y se sustituye quedando

$$7 = (728 - 581) \cdot 4 - 581 \cdot 1 = 728 \cdot 4 - 581 \cdot 5.$$

Se sustituye ahora 581

$$7 = 728 \cdot 4 - (1309 - 728) \cdot 5 = 728 \cdot 9 - 1309 \cdot 5.$$

Finalmente, se despeja 728 en la ecuación (0):

$$7 = (4655 - 1309 \cdot 3) \cdot 9 - 1309 \cdot 5 = 4655 \cdot 9 - 1309 \cdot 32.$$

Es decir, $mcd(4655, 1309) = 4655(9) + 1309(-32)$. También se tiene $mcd(4655, 1309) = 4655(9 + 1309) + 1309(-32 - 4655)$.

Una consecuencia inmediata del teorema anterior es que un entero c es combinación lineal de dos enteros a y b si y solamente si $\text{mcd}(a, b) \mid c$. En otras palabras, el conjunto de enteros que son combinación lineal de a y b coincide con el conjunto de los múltiplos de $\text{mcd}(a, b)$. En efecto, supongamos que $d = \text{mcd}(a, b)$. Como $d \mid a$ y $d \mid b$, entonces d divide a cualquier combinación lineal de a y b; en particular d divide a c. Recíprocamente, si $d \mid c$, entonces $c = dq$ para algún entero q. De acuerdo con el Teorema 6, existen enteros r, s tales que $d = ar + bs$. Luego $c = dq = a(rq) + b(sq)$.

Según el Teorema 6, $\text{mcd}(a, b)$ es combinación lineal de a y b. El recíproco no es cierto, es decir, si c es combinación lineal de a y b, c no necesariamente es el máximo común divisor de a y b. Como el máximo común divisor de dos números distintos de cero es positivo, estamos interesados en combinaciones lineales que den por resultado un número positivo. Resulta que de entre todas las combinaciones lineales que dan por resultado un número positivo, la más pequeña de todas, es el máximo común divisor. Dado que $\text{mcd}(a, b) = \text{mcd}(|a|, |b|)$, con frecuencia nos podemos restringir al caso $a > 0, b > 0$.

Teorema 7. *Si a y b son enteros positivos y $d = ax + by$ es su combinación lineal positiva mínima, entonces $d = mcd(a, b)$.*

Demostración. Se debe probar que d es un divisor común de a y b y que además es el máximo entre todos los divisores comunes. De acuerdo con el Algoritmo de la división, se tiene $a = dq + r$ con $0 \leq r < d$. Como $d = ax + by$, se obtiene que $a = (ax + by)q + r$, de donde $r = a(1 - xq) + b(-yq)$. Dado que $r < d$ y d es la combinación lineal positiva mínima de a y b, no es posible que $r > 0$; entonces $r = 0$ y $d \mid a$. De manera análoga se muestra que $d \mid b$.
Como $d \mid a$ y $d \mid b$, entonces d divide a cualquier combinación lineal de a y b (Teorema 1); en particular $d \mid \text{mcd}(a, b)$. De acuerdo con el Corolario 2 se tiene que $d \leq \text{mcd}(a, b)$. Por otro lado, como $\text{mcd}(a, b) \mid a$ y $\text{mcd}(a, b) \mid b$, se tiene que $\text{mcd}(a, b) \mid d$. Luego $\text{mcd}(a, b) \leq d$. Las dos desigualdades implican que $d = \text{mcd}(a, b)$. □

Ejemplo 7. *Los números $10, 20$ y 30 son combinaciones lineales positivas de $a = 2210$ y $b = 980$:*

$$10 = a \cdot (-47) + b \cdot 106, \quad 20 = a \cdot 4 + b \cdot (-9), \quad 30 = a \cdot (-43) + b \cdot 97$$

Con base en el teorema anterior podemos afirmar que el máximo común divisor de a y b no es ni 20 ni 30, pues 10 es combinación lineal positivia de a y b que es menor que 20 y 30. Para poder asegurar que 10 es el máximo común divisor de a y b necesitamos más información.

El siguiente teorema es de gran importancia pues da algunas caracterizaciones para el máximo común divisor.

Teorema 8. *Sean a, b y $d > 0$ enteros. Las siguientes afirmaciones son equivalentes:*

1. $d = mcd(a, b)$.
2. *d es la combinación lineal positiva mínima de a y b.*

3. $d \mid a$, $d \mid b$, *y si* $c \mid a$ *y* $c \mid b$, *entonces* $c \mid d$.

4. $d \mid a$, $d \mid b$, *y* d *es combinación lineal de* a *y* b.

Demostración. El teorema anterior muestra que $2)$ implica $1)$. Recíprocamente, si $d = \text{mcd}(a, b)$ y d_1 es combinación lineal positiva de a y b, entonces $d \mid d_1$ ya que d divide a cualquier combinación lineal de a y b. Luego $d \leq d_1$ y d es la combinación lineal positiva mínima de a y b. Esto muestra que $1)$ y $2)$ son equivalentes.
Ahora bien, $1)$ implica $3)$, pues cualquier divisor de a y b divide a cualquier combinación lineal de a y b, en particular, divide a $\text{mcd}(a, b)$. Supongamos ahora que d satisface $3)$; dado que $\text{mcd}(a, b)$ es un divisor común de a y b, se sigue que $\text{mcd}(a, b) \mid d$ y por lo tanto $\text{mcd}(a, b) \leq d$. Por otro lado, como $d \mid a$ y $d \mid b$, entonces $d \mid \text{mcd}(a, b)$, ya que $\text{mcd}(a, b)$ es combinación lineal de a y b. Así, $d \leq \text{mcd}(a, b)$, y queda probado que $d = \text{mcd}(a, b)$. Esto muestra que $1)$ y $3)$ son equivalentes.
Finalmente, veamos que $2) \Leftrightarrow 4)$. Si d satisface la condición $2)$, entonces por el teorema anterior, $d = \text{mcd}(a, b)$ y por lo tanto se satisface la condición $4)$. Supongamos ahora que d satisface la condición $4)$ y sea c un entero tal que $c \mid a$ y $c \mid b$. Como d es combinación lineal de a y b, tenemos que $c \mid d$. Luego, se satisface la condición $3)$ y por lo tanto se satisface la condición $2)$ (pues las condiciones $1)$, $2)$ y $3)$ son equivalentes). Esto muestra que las condiciones $2)$ y $4)$ son equivalentes. □

De acuerdo con el Ejemplo 7, los números $10, 20$ y 30 son combinaciones lineales positivas de 2210 y 980. Dado que 10 es combinación lineal de 2210 y 980, y 10 es divisor común de 2210 y 980, con base en el teorema anterior se concluye que 10 es el máximo común divisor de 2210 y 980.

El Ejemplo 5 se puede resolver de otra manera utilizando el Teorema 8. En efecto, sea $d = \text{mcd}(b, c)$. Entonces, $b = sd$ y $c = td$ para algunos enteros s, t. Tenemos que $a^b - 1 = (a^d)^s - 1$ y $a^c - 1 = (a^d)^t - 1$ son divisibles por $a^d - 1$, de modo que por el Teorema 8 $a^d - 1$ divide a $\text{mcd}(a^b - 1, a^c - 1)$. De aquí, $a^d - 1 \leq \text{mcd}(a^b - 1, a^c - 1)$. Por otra parte, tenemos que $d = bx + cy$ para algunos enteros x, y. Además, x e y deben tener signos opuestos (claramente no pueden ser ambos negativos, ya que d es positivo. Tampoco pueden ser ambos positivos, ya que si lo fueran se tendría que $d \geq b + c$ lo que es una contradicción, pues $d \leq b$ y $d \leq c$). Asumamos, sin pérdida de generalidad, que $x > 0$, $y \leq 0$ y sea $t = \text{mcd}(a^b - 1, a^c - 1)$. Entonces, $t \mid (a^{bx} - 1)$ y $t \mid (a^{-cy} - 1)$, lo cual implica que t divide a $((a^{bx} - 1) - a^d(a^{-cy} - 1)) = a^d - 1$, y por lo tanto $t \leq a^d - 1$. En conclusión, tenemos que $t = \text{mcd}(a^b - 1, a^c - 1) \leq a^d - 1 \leq \text{mcd}(a^b - 1, a^c - 1)$, esto es, $\text{mcd}(a^b - 1, a^c - 1) = a^d - 1 = a^{mcd(b,c)} - 1$.

Una consecuencia inmediata del Teorema 8 es que si a y b son enteros y $1 = ax + by$ para algunos enteros x, y, entonces el máximo común divisor de a y b es 1, pues en este caso, 1 es la combinación lineal positiva mínima de a y b.
Se dice que dos enteros a y b son *primos relativos*, *primos entre sí* o *coprimos*, si su máximo común divisor es 1.

Corolario 3. *Si* a *y* b *son enteros tales que mcd*$(a, b) = d$, *entonces mcd* $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Demostración. Tenemos que $d = ax + by$ para algunos enteros x, y. Como $d \mid a$ y $d \mid b$, resulta que $\frac{a}{d}$ y $\frac{b}{d}$ son enteros, y por lo tanto $1 = (\frac{a}{d})x + (\frac{b}{d})y$. Se sigue que $\text{mcd}(\frac{a}{d}, \frac{b}{d}) = 1$. □

Ejemplo 8. *Si a y b son enteros con mcd$(a, b) = 1$, demostrar que mcd$(a^2, b^2) = 1$.*

Solución. Tenemos que existen enteros x, y tales que $ax+by = 1$. Elevando al cuadrado obtenemos que $1 = a^2x^2 + b(2axy + by^2)$, y por lo tanto $\text{mcd}(a^2, b) = 1$. Esto muestra que si $\text{mcd}(a, b) = 1$, entonces $\text{mcd}(a^2, b) = 1$. Usando esto, concluimos que $\text{mcd}(a^2, b^2) = 1$.

Teorema 9 (Propiedad Multiplicativa del Máximo Común Divisor)**.** *Sean a, b y n enteros positivos. Entonces, mcd$(na, nb) = n \cdot$ mcd(a, b).*

Demostración. Sea $d = \text{mcd}(a, b)$. Sabemos que existen enteros x, y tales que $d = ax + by$. Como $d \mid a$ y $d \mid b$, tenemos que $nd \mid na$, $nd \mid nb$ y $nd = (an)x + (bn)y$. Luego, nd, na y nb satisfacen la condición $4)$ del Teorema 8, y por lo tanto $nd = \text{mcd}(na, nb)$ (por la equivalencia de $1)$ con $4)$ de dicho teorema). □

Ejemplo 9. *Sean a y b enteros tales que mcd$(a, b) = 1$. Demostrar que*

$$\textit{mcd}(a + b, a^2 - ab + b^2) = 1 \textit{ o } 3.$$

Solución. Sea $d = \text{mcd}(a + b, a^2 - ab + b^2)$. Tenemos que d es divisor de $(a + b)^2 - a^2 + ab - b^2 = 3ab$. Luego, d divide a $3b(a + b) - 3ab = 3b^2$ y también a $3a(a+b)-3ab = 3a^2$. Luego, por el Teorema 8 se sigue que d divide a $\text{mcd}(3a^2, 3b^2)$. Esto es, d divide a $3 \cdot \text{mcd}(a^2, b^2)$ por la propiedad multiplicativa del máximo común divisor. Como $\text{mcd}(a, b) = 1$, el ejemplo anterior implica que $\text{mcd}(a^2, b^2) = 1$, y por lo tanto $d \mid 3$. Así, $d = 1$ o 3.

Ejemplo 10. *Sea $n \geq 5$ un entero. Determinar el máximo común divisor de $a = n^3 - n^2 - 12n$ y $b = 2n^2 - 7n - 4$ en términos de n.*

Solución. Observemos primero que $a = n(n - 4)(n + 3)$ y $b = (n - 4)(2n + 1)$. Aplicando la propiedad multiplicativa del máximo común divisor, tenemos que

$$\text{mcd}(a, b) = (n - 4) \cdot \text{mcd}(n(n + 3), 2n + 1).$$

Como n y $2n + 1$ son primos relativos (pues $1 = (-2)n + 1(2n + 1)$), es fácil ver que $\text{mcd}(n(n + 3), 2n + 1) = \text{mcd}(n + 3, 2n + 1)$ (ejercicio). Luego, basta calcular $\text{mcd}(n + 3, 2n + 1)$.
Sean $A = 2n + 1$, $B = n + 3$ y $d = \text{mcd}(A, B)$. Como $d \mid A$ y $d \mid B$, tenemos que $d \mid (2B - A)$, esto es, $d \mid 5$. De aquí, $d = 1$ o 5. Supongamos que $d = 5$; entonces, $5 \mid A$ y $5 \mid B$. De aquí, $5 \mid (A - B)$, esto es, $5 \mid (n - 2)$. Recíprocamente, si $5 \mid (n - 2)$ entonces $n = 5k + 2$ para algún entero k. Luego, $A = 2n + 1 = 5(1 + 2k)$ y $B = n + 3 = 5(k + 1)$, lo que significa que A y B son múltiplos de 5. Por lo tanto, tenemos que $5 \mid A$ y $5 \mid B$ si y sólo si $5 \mid (n - 2)$. Esto implica que si $d = 5$, entonces $5 \mid (n - 2)$. Recíprocamente, si $5 \mid (n - 2)$ entonces $5 \mid A$ y $5 \mid B$, y por el Teorema 8

se sigue que $5 \mid d$. Como $d = 1$ o 5, debemos tener que $d = 5$. En conclusión, $d = 5$ si y sólo si $5 \mid (n-2)$, y por lo tanto, $d = 1$ si y sólo si $5 \nmid (n-2)$. Luego,

$$\text{mcd}(a,b) = \begin{cases} 5(n-4) & \text{si} \quad 5 \mid (n-2), \\ n-4 & \text{si} \quad 5 \nmid (n-2). \end{cases}$$

Si un entero a divide a un producto bc, no necesariamente divide a alguno de los factores. Por ejemplo, $4 \mid 2 \cdot 10$, pero $4 \nmid 2$ y $4 \nmid 10$. Sin embargo, si el divisor es primo relativo con alguno de los factores, es posible concluir que el divisor divide al factor con el cual no es primo relativo.

Teorema 10. *Si $a \mid bc$ y $mcd(a,b) = 1$, entonces $a \mid c$.*

Demostración. De acuerdo con la hipótesis, existen enteros x, y tales que $1 = ax + by$. Multiplicando por c, se obtiene que $c = acx + bcy$. Como $a \mid bc$, existe un entero q tal que $bc = aq$. Luego $c = acx + aqy = a(cx + qy)$, de donde $a \mid c$. □

Ejemplo 11. *Sean a y b enteros positivos primos relativos tales que $ab = c^n$ para algún entero positivo c y algún entero positivo n. Demostrar que existen enteros x, y tales que $a = x^n$ y $b = y^n$.*

Solución. Sea $d = \text{mcd}(a,c)$. Tenemos que $a = du$ y $c = dv$ con $u = \frac{a}{d}$ y $v = \frac{c}{d}$ primos relativos (ver Corolario 3). Entonces,

$$ab = dub = (dv)^n = c^n \Rightarrow ub = d^{n-1}v^n \Rightarrow u \mid d^{n-1}v^n.$$

Como u y v^n son primos relativos (pues u y v lo son), el teorema anterior implica que $u \mid d^{n-1}$. Sea $k = \frac{d^{n-1}}{u}$. Como $1 = \text{mcd}(a,b) = \text{mcd}(du, kv^n)$ existen enteros r, s tales que $1 = dur + kv^n s$. Luego, d y k son primos relativos, y en consecuencia d^{n-1} y k también lo son. De aquí, $1 = \text{mcd}(d^{n-1}, k) = \text{mcd}(ku, k) = k \cdot \text{mcd}(u, 1) = k$ y por lo tanto, $d^{n-1} = u$, $a = du = d^n$ y $b = kv^n = v^n$.

Para finalizar, dejamos unos ejercicios para el lector.

Ejercicios

1. Sean a y b enteros positivos impares tales que $a \nmid b$. Demuestra que existen enteros q y r tales que $b = aq + r$ donde r es impar y $-a < r < a$.

2. Sean a y b enteros tales que $b < 0$ y $b \nmid a$. Si $a = bq + r$ con $0 \leq r < |b|$, demuestra que $q = \lfloor \frac{a}{b} \rfloor + 1$.

3. Sean a, b y c enteros y sea $d = \text{mcd}(a,b)$. Si $a \mid c$ y $b \mid c$, demuestra que $\frac{ab}{d}$ también divide a c.

4. Sean a y b enteros primos relativos. Demuestra que $\text{mcd}(a+b, a-b) = 1$ o 2.

5. Se dice que una fracción $\frac{a}{b}$ es irreducible si los enteros a y b son primos relativos. Demuestra que la fracción $\frac{21n+4}{14n+3}$ es irreducible para todo entero positivo n.

6. Los números de la sucesión $101, 104, 109, 116, \ldots$ son de la forma $a_n = 100 + n^2$, $n = 1, 2, \ldots$. Para cada entero positivo n sea $d_n = \text{mcd}(a_n, a_{n+1})$. Determina el valor $\max\limits_{n\geq 1} d_n$.

7. Sean m y n enteros positivos con m impar. Demuestra que $2^m - 1$ y $2^n + 1$ son primos relativos.

8. Sean m y n enteros positivos con $m \neq n$. Determina $\text{mcd}(a^{2m}+1, a^{2n}+1)$ para cualquier entero a. (Sugerencia: si $A_n = a^{2n} + 1$, demuestra que $A_n \mid (A_m - 2)$ si $m > n$).

9. Sean a y b enteros positivos y sea d su máximo común divisor. Si $\frac{a+1}{b} + \frac{b+1}{a}$ es un entero, demuestra que $d \leq \sqrt{a+b}$.

10. Para cualesquiera enteros positivos $a > b > 1$, una sucesión $x_1, x_2, \ldots$ está definida por $x_n = \frac{a^n-1}{b^n-1}$. Determina el menor entero d tal que para cualesquiera a y b, esta sucesión no contiene d términos consecutivos que son números primos.

11. Sean $a = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ y $b = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ donde $m_i \geq 0$ y $n_i \geq 0$ son enteros y los p_i son primos distintos para $1 \leq i \leq r$. Si $t_i = \text{mín}\{m_i, n_i\}$ denota el valor mínimo de m_i y n_i, demuestra que

$$\text{mcd}(a, b) = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r}.$$

12. Usa el ejercicio anterior para demostrar la siguiente propiedad multiplicativa del máximo común divisor.

$$(ah, bk) = (a, b)(h, k) \left(\frac{a}{(a, b)}, \frac{k}{(h, k)}\right) \left(\frac{b}{(a, b)}, \frac{h}{(h, k)}\right)$$

para cualesquiera enteros a, b, h y k. Aquí, hemos abreviado la notación $\text{mcd}(a, b)$ por (a, b). Esta propiedad muestra en particular, que si $(a, b) = (h, k) = 1$, entonces $(ah, bk) = (a, k)(b, h)$.

13. Dados tres enteros a, b y c, se define su máximo común divisor como

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

   a) Demuestra que $\text{mcd}(a, b, c) = \text{mcd}(a, \text{mcd}(b, c))$.

   b) Demuestra que existen enteros x, y, z tales que $ax+by+cz = \text{mcd}(a, b, c)$.

Bibliografía

1. Ana Rechtman Bulajich, Carlos Jacob Rubio Barrios. *Divisibilidad y congruencias*. Tzaloa No. 2, 2009.

2. José Alejandro Lara Rodríguez, Carlos Jacob Rubio Barrios. *Álgebra Superior (notas de curso)*. Universidad Autónoma de Yucatán, 2014.