# Máximo común divisor

## Algoritmo de Euclides e Igualdad de Bézout

Anteriormente nos enfocamos en estudiar el concepto de divisibilidad y los divisores de un número $a \in \mathbb{Z}$ dado. Ahora, nos enfocaremos en estudiar los divisores comunes de dos números $a, b \in \mathbb{Z}$ dados.

Definición: Dados $a, b \in \mathbb{Z}$, diremos que $c \in \mathbb{Z}$ es un divisor común de a y b si

$$c \mid a \quad y \quad c \mid b.$$

Denotaremos por $Div(a,b)$ al conjunto de divisores comunes de a y b.

Observaciones:

① $Div(a,b) \neq \emptyset$, ya que $1 \mid a$ y $1 \mid b$.

② $Div(a,b) = \{\text{divisores de } a\} \cap \{\text{divisores de } b\}$.

③ Si $b = 0$, entonces

$$Div(a,0) = \{\text{divisores de } a\}.$$

④ $c \in Div(a,b)$ si y solamente si $-c \in Div(a,b)$.

⑤ Si $a = b = 0$, entonces $Div(0,0) = \mathbb{Z}$.

En este caso, $Div(0,0)$ es un conjunto infinito

⑥ Si $a \neq 0$ o $b \neq 0$, entonces $Div(a,b)$ es un conjunto finito, y por lo tanto tiene un elemento maximal.

Ejemplos:

① Hallar los divisores comunes de $a = 45$ y $b = -40$.

Divisores de a: $\pm 1, \pm 3, \pm 5, \pm 9, \pm 15, \pm 45$

Divisores de b: $\pm 1, \pm 2, \pm 4, \pm 5, \pm 8, \pm 10, \pm 20, \pm 4$

$Div(45,-40) = \{\pm 1, \pm 5\}$

② Hallar los divisores comunes de $a = 100$ y $b = 441$

Divisores de 100: $\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20, \pm 25, \pm 50, \pm 100$

Divisores de 441: $\pm 1, \pm 3, \pm 7, \pm 9, \pm 21, \pm 49, \pm 147, \pm 441$

$Div(100, 441) = \{\pm 1\}$.

De las observaciones 5 y 6, se tiene el siguiente concepto:

**Definición:** Sean $a, b \in \mathbb{Z}$ con $a \neq 0$ o $b \neq 0$. Se define el <u>máximo común divisor de a y b</u>, denotado como m.c.d $(a, b)$, como el elemento maximal de $\mathrm{Div}(a, b)$. Es decir, $d = \text{m.c.d}(a, b)$ si

1) $d \mid a$ y $d \mid b$ ($d$ es un divisor común de $a$ y $b$).
2) Si $c \mid a$ y $c \mid b$, entonces $c \leq d$.

En caso contrario, es decir si $a = b = 0$, decimos que

$$\text{m.c.d.}(0, 0) = 0.$$

- $a, b \in \mathbb{Z}$ son <u>primos relativos</u> (o <u>coprimos</u>) si

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

## Observaciones:

1 Si $a$ y $b$ son primos, con $a \neq b$, entonces $a$ y $b$ son primos relativos.

$$\begin{aligned}\mathrm{Div}(a, b) &= \{\text{divisores de } a\} \cap \{\text{divisores de } b\} \\ &= \{\pm 1, \pm a\} \cap \{\pm 1, \pm b\} \\ &= \{\pm 1\},\end{aligned}$$

de donde $\text{m.c.d.}(a, b) = 1$.

② Si $a$ y $b$ son primos relativos, no necesariamente se tiene que $a$ y $b$ son primos. Por ejemplo, 7 y 10 son primos relativos, pero 10 es compuesto.

## Ejemplos:

① $m.c.d.(45, -40) = 5$.

② $m.c.d.(100, 441) = 1$.

100 y 441 son primos relativos.

Existe una manera de hallar el $m.c.d.(a, b)$ sin necesidad de calcular los divisores de $a$ y de $b$. Esto tiene que ver con las propiedades del concepto de máximo común divisor.

## Proposición (propiedades del m.c.d.):

Sean $a, b \in \mathbb{Z}$, con $a \neq 0$ o $b \neq 0$. Entonces, las siguientes afirmaciones se cumplen:

① $m.c.d.(a, b) = m.c.d.(b, a)$

② $m.c.d.(a, b) = m.c.d.(a, -b) = m.c.d.(-a, b)$

$= m.c.d.(-a, -b) = m.c.d.(|a|, |b|)$.

③ $b | a$ si y solamente si $m.c.d.(a, b) = |b|$.

④ Si $a \neq 0$ entonces $m.c.d.(a, 0) = |a|$.

⑤ $m.c.d.(a, b) = m.c.d.(b, a - bx)$ $\forall x \in \mathbb{Z}$, donde $a \neq 0$ y $b \neq 0$.

En particular, si $r$ es el resto de dividir $a$ por $b$, se tiene que

$$m.c.d.(a,b) = m.c.d.(b,r).$$

· Demostración:

① y ② son consecuencia directa de la definición de m.c.d.

③ Supongamos primero que $b|a$. Luego, claramente $|b|$ es el máximo divisor común de $b$ y $a$, es decir, $m.c.d.(a,b) = |b|$.

Ahora, supongamos que $m.c.d.(a,b) = |b|$. Luego, $|b| \mid a$. En particular, $b|a$.

④ Es inmediato de la definición de m.c.d.

⑤ Sean $d = m.c.d.(a,b)$ y $d' = m.c.d.(b, a-xb)$, con $x \in \mathbb{Z}$ fijo.

Como $d|a$ y $d|b$, se tiene que $d|(a-xb)$. Luego, $d$ es un divisor común de $b$ y $a-bx$, de donde $d \leq d'$.

Por otro lado, $d'|b$ y $d'|(a-xb)$, se tiene que $d' \mid [(a-xb)+xb]$, es decir, $d'|a$. Entonces, $d'$ es un divisor común de $a$ y $b$, por lo cual $d' \leq d$.

Por lo tanto, $d = d'$. ∎

Ejemplos: Sin hallar todos los divisores de los números involucrados, hallar el máximo común divisor de:

① $a = 45$ y $b = -40$:

- $45 = (-1)(-40) + 5$, $m.c.d.(45, -40) = m.c.d.(-40, 5)$

Como $5 \mid (-40)$, se tiene por las propiedades vistas que $m.c.d.(-40, 5) = 5$.

Por lo tanto, $m.c.d.(45, -40) = 5.$ //

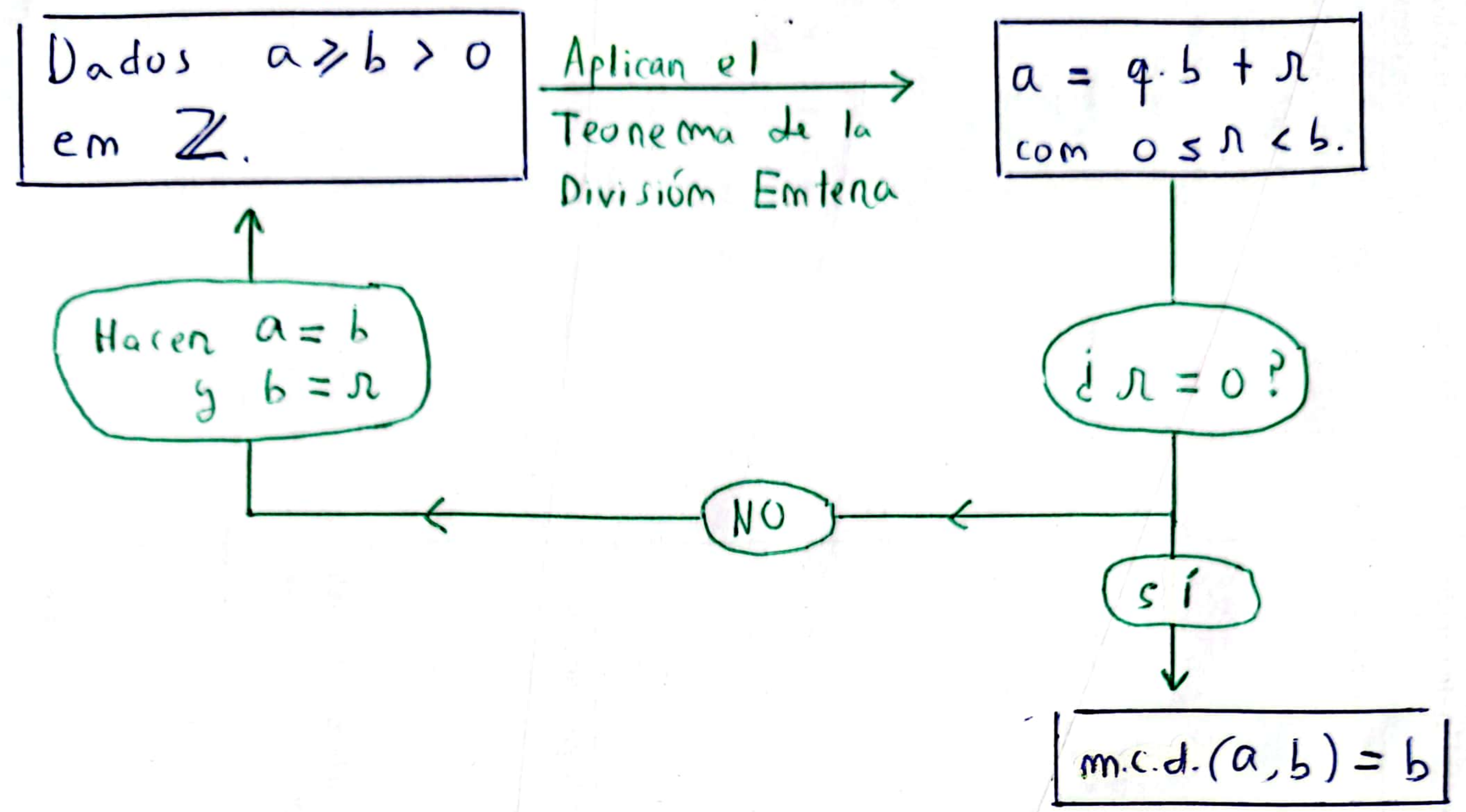
② $a = 441$ y $b = 100$:

- $441 = 4 \cdot 100 + 41$, $m.c.d(441, 100) = m.c.d.(100, 41)$.
- $100 = 2 \cdot 41 + 18$, $m.c.d.(100, 41) = m.c.d.(41, 18)$.
- $41 = 2 \cdot 18 + 5$, $m.c.d.(41, 18) = m.c.d.(18, 5)$.
- $18 = 3 \cdot 5 + 3$, $m.c.d.(18, 5) = m.c.d.(5, 3)$.
- $5 = 1 \cdot 3 + 2$, $m.c.d.(5, 3) = m.c.d.(3, 2)$.
- $3 = 1 \cdot 2 + 1$, $m.c.d.(3, 2) = m.c.d.(2, 1) = 1$.

$\Longrightarrow m.c.d.(441, 100) = \cdots = m.c.d.(2, 1) = 1.$

El procedimiento para hallar el máximo común divisor mostrado en los ejemplos anteriores se conoce como <u>Algoritmo de Euclides</u>.

# Descripción general del algoritmo de Euclides:




Volvamos al ejemplo anterior, donde tenemos las siguientes igualdades:

$$\left.\begin{aligned} 441 &= 4 \cdot 100 + 41 \\ 100 &= 2 \cdot 41 + 18 \\ 41 &= 2 \cdot 18 + 5 \\ 18 &= 3 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \end{aligned}\right] \xrightarrow[\text{consecutivas "hacia atrás"}]{\text{sustituciones}}$$

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (5 - 1 \cdot 3) \\ &= -1 \cdot 5 + 2 \cdot 3 \\ &= -1 \cdot 5 + 2 \cdot (18 - 3 \cdot 5) \\ &= 2 \cdot 18 + (-7) \cdot 5 \\ &= 2 \cdot 18 + (-7) \cdot (41 - 2 \cdot 18) \\ &= (-7) \cdot 41 + 16 \cdot 18 \\ &= (-7) \cdot 41 + 16\,(100 - 2 \cdot 41) \\ &= 16 \cdot 100 + (-39) \cdot 41 \\ &= 16 \cdot 100 + (-39)(441 - 4 \cdot 100) \\ &= (-39) \cdot 441 + 172 \cdot 100 \end{aligned}$$

Por lo tanto, vemos que $1 = \text{m.c.d.}(441, 100)$ se puede escribir como combinación lineal entera de 441 y 100.

El procedimiento empleado en el ejemplo anterior para hallar dicha combinación se conoce como <u>algoritmo de Euclides extendido</u> o <u>por sustitución</u>.

Se puede aplicar para cualquier par de enteros $a \geq b > 0$. Este hecho está basado en el siguiente Resultado.

<u>Teorema de Bézout</u>: Sean $a, b \in \mathbb{Z}$ con $a \geq b > 0$. Entonces,

$$m.c.d.(a,b) = \min\{xa + yb \in \mathbb{Z}^+ / x, y \in \mathbb{Z}\}$$

En particular, existen $x_0, y_0 \in \mathbb{Z}$ tales que

$$\boxed{m.c.d.(a,b) = x_0 a + y_0 b.}$$

Igualdad de Bézout

· <u>Demostración</u>: Consideramos el conjunto

$$S = \{xa + yb \in \mathbb{Z}^+ / x, y \in \mathbb{Z}\}.$$

Es decir, $S$ es el conjunto de las combinaciones lineales enteras positivas de $a$ y $b$.

① $S \neq \emptyset$ ya que $b = 0 \cdot a + 1 \cdot b \in \mathbb{Z}^+$.

② $S$ está acotado inferiormente (por 0). 

① y ② $\Rightarrow$ $S$ posee un elemento minimal
(usamos el dual del Principio
del Elemento Maximal).

Sea $d := \min S$. Veamos que $d = m.c.d.(a,b)$.

- $d$ es un divisor común de $a$ y $b$:

Sean $x_0, y_0 \in \mathbb{Z}$ tales que $d = x_0 a + y_0 b$.

Por otro lado, por el teorema de la división entera, existen $q, r \in \mathbb{Z}$ tales que

$$a = q \cdot d + r \quad \text{con} \quad 0 \leq r < d.$$

Luego,

$$a = q \cdot (x_0 a + y_0 b) + r$$

$$r = (1 - q \cdot x_0) a + (-y_0) b.$$

Como $r < d$, se tiene que $r \notin S$, de donde $r \leq 0$. Por otro lado, $r \geq 0$, por lo cual nos queda $r = 0$.

Se sigue entonces que $d \mid a$.

De manera análoga se puede probar que $d \mid b$.

Por lo tanto, $d \in Div(a,b)$.

- Como $d$ es un divisor común de $a$ y $b$, tenemos que $m.c.d.(a,b) \geq d$.

- $m.c.d.(a,b) \mid a$, $m.c.d.(a,b) \mid b$ $\Rightarrow m.c.d(a,b) \mid d$.
  y $d = x_0 a + y_0 b$

  Luego, $m.c.d.(a,b) \leq d$.

  Por lo tanto, $m.c.d.(a,b) = d$. ■

## Aplicaciones de la igualdad de Bézout:

Sean $a, b \in \mathbb{Z}$ con $a \neq 0$ y $b \neq 0$.
Las siguientes propiedades se cumplen:

(1) $e \mid a$ y $e \mid b \iff e \mid m.c.d.(a,b)$

(2) $a$ y $b$ son coprimos si y solamente si existen $x_0, y_0 \in \mathbb{Z}$ tales que $x_0 a + y_0 b = 1$.

(3) $m.c.d.(a,b) = m.c.d.(a,c) = 1 \Rightarrow m.c.d.(a, bc) = 1$.

(4) $n \in \mathbb{Z} \Rightarrow m.c.d.(na, nb) = |n|\, m.c.d.(a,b)$.

(5) Sea $d \in \mathbb{Z}^+$ tal que $d \mid a$ y $d \mid b$ (por lo cual $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$). Entonces,

$d = m.c.d.(a,b)$ si y solamente si $m.c.d.\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

(6) Lema de Euclides: Si $a$ y $b$ son coprimos y $c \in \mathbb{Z}$ es tal que $a \mid bc$, entonces $a \mid c$.

- Demostración:

① Por la igualdad de Bézout, existen $x_0, y_0 \in \mathbb{Z}$ tales que

$$\text{m.c.d.}(a,b) = x_0 a + y_0 b.$$

Como $e \mid a$ y $e \mid b$, se tiene que $e$ divide a cualquier combinación lineal entera de $a$ y $b$, de donde

$$e \mid (x_0 a + y_0 b).$$

Es decir, $e \mid \text{m.c.d.}(a,b)$.

② Supongamos primero que $a$ y $b$ son coprimos, es decir, $\text{m.c.d.}(a,b) = 1$. Por la igualdad de Bézout, existen $x_0$ e $y_0$ en $\mathbb{Z}$ tales que

$$1 = x_0 a + y_0 b.$$

Ahora supongamos que $1 = x_0 a + y_0 b$ para algunos $x_0, y_0 \in \mathbb{Z}$. Sea $c$ un divisor común de $a$ y $b$. Entonces $c$ divide a cualquier combinación lineal entera de $a$ y $b$. En particular, $c \mid (x_0 a + y_0 b)$. Es decir, $c \mid 1$, por lo cual $c = \pm 1$. Se tiene entonces que $\text{m.c.d.}(a,b) = 1$.

③ m.c.d. $(a, b) = 1 \Rightarrow$ existen $x_0, y_0 \in \mathbb{Z}$ tales que

$$1 = x_0 a + y_0 b$$

m.c.d. $(a, c) = 1 \Rightarrow$ existen $x_0', y_0' \in \mathbb{Z}$ tales que

$$1 = x_0' a + y_0' c$$

Luego,

$$1 = 1 \cdot 1 = (x_0 a + y_0 b)(x_0' a + y_0' c)$$
$$= x_0 x_0' a^2 + x_0 y_0' ac + x_0' y_0 ab + y_0 y_0' bc$$
$$= (x_0 x_0' a + x_0 y_0' c + x_0' y_0 b) a + (y_0 y_0')(bc)$$

Por la parte ②, tenemos que m.c.d. $(a, bc) = 1$..

④ Sea $d =$ m.c.d. $(a, b)$. Tenemos que $d | a$ y $d | b$. Luego, $|m| d \,|\, ma$ y $|m| d \,|\, mb$, es decir, $|m| d$ es un divisor común de $ma$ y $mb$. Entonces,

$$|m| d \leq \text{m.c.d. } (ma, mb) \qquad (*)$$

Por otro lado, por la igualdad de Bézout existen $x_0, y_0 \in \mathbb{Z}$ tales que

$$d = x_0 a + y_0 b.$$

Así, $|m| d = x_0 |m| a + y_0 |m| b = (\pm x_0)(ma) + (\pm y_0)(mb)$.
Vemos entonces que

$$|m| d \in S = \{ x(ma) + y(mb) \in \mathbb{Z}^+ \,/\, x, y \in \mathbb{Z} \}.$$

Como m.c.d.$(ma, mb) = \min S$, se tiene que

$$\text{m.c.d.}(ma, mb) \leq |m| d \quad (**)$$

Combinando las desigualdades $(*)$ y $(**)$, obtenemos finalmente que

$$|m| d = \text{mcd}(ma, mb).$$

5) Supongamos primero que $d = \text{m.c.d.}(a, b)$.
Por la parte 4), se tiene que

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

$$d\left(\text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) - 1\right) = 0.$$

Como $d \neq 0$, obtenemos $\text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Ahora supongamos que $\text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Multiplicando esta igualdad por $d$, obtenemos que

$$d = d \cdot 1 = d \cdot \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) \underset{\substack{\uparrow \\ \text{parte } 4}}{=} \text{m.c.d.}\left(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}\right) = \text{m.c.d.}(a, b)$$

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

(6) $a \mid bc \Rightarrow bc = qa$ para algún $q \in \mathbb{Z}$.

Por otro lado, m.c.d. $(a, b) = 1 \Rightarrow$ existen $x_0, y_0 \in \mathbb{Z}$ tales que

$$1 = x_0 a + y_0 b.$$

Tenemos lo siguiente:

$$1 = x_0 a + y_0 b \Rightarrow c = x_0 ac + y_0 bc$$

$$c = x_0 ac + y_0 q a$$

$$c = (x_0 c + y_0 q) a$$

Por lo tanto, $a \mid c$.

## Algunas aplicaciones a primalidad (pruebas de irracionalidad):

Comencemos con algunas aplicaciones del resultado anterior para el caso en el que se tienen números primos involucrados.

**Corolario**: Las siguientes condiciones son equivalentes para todo $p \in \mathbb{N}$ con $p \geq 2$.

(a) $p$ es primo.

(b) $\forall a, b \in \mathbb{Z}$, $p \mid ab \Rightarrow p \mid a$ o $p \mid b$.