


# Divisibilidad

Así como la multiplicación puede explicarse como *sumas sucesivas*, el concepto de **división** puede explicarse como *restas sucesivas*.

**Definición.** Decimos que el número entero  $a$  es **divisible entre (o por) el número entero  $b \neq 0$**  si existe un entero  $q$  ( $q$  es por cociente) tal que  $a - q \cdot b = 0 \leftrightarrow a = q \cdot b$ .

 De esta última expresión  $a = q \cdot b$ , también se suele decir que  **$b$  divide a  $a$** , o bien que  **$a$  es un múltiplo de  $b$** .

⚠ Para dos enteros cualesquiera  $a$  y  $b$ , este proceso de *restas sucesivas* (o división) no siempre puede llevarse a cabo un número entero de veces.

Tomemos, por ejemplo,  $a = 17$  y  $b = 3$ . Evidentemente, al restar tantas veces como nos sea posible 3 de 17, el proceso queda *inconcluso*:

$$17 - 5 \cdot 3 \neq 0 \leftrightarrow 17 - 5 \cdot 3 = 2$$

Entonces si tenemos que  $a - q \cdot b = r$ , decimos que  **$a$  no es divisible entre (o por)  $b \neq 0$** . El número entero  $0 \leq r < b$  se conoce como **residuo** de la división y el número entero  $q$  se conoce como **cociente** de la división.

**Teorema** (algoritmo de la división de Euclides)

Para cualesquiera  $a, b \in \mathbb{Z}$  tales que  $b \neq 0$ , existen  $q, r \in \mathbb{Z}$  únicos que satisfacen:

$$a = q \cdot b + r, \text{ con } 0 \leq r < b$$

**Definición.** Se denomina **factor o divisor propio** de un número entero  $a$ , a otro número que es un divisor de  $a$  pero diferente de  $a$ . Los divisores 1 y  $a$  son denominados impropios.

Notación: Usamos la notación  $b \mid a$  para indicar que  $b$  divide a  $a$ ; y  $b \nmid a$  para indicar que  $b$  no divide a  $a$ .

**Definición.** Decimos que un número  $p$  que tiene *exactamente* dos divisores ( $p$  y 1) es un **número primo**. Aquellos números que tienen más de dos divisores son conocidos como **números compuestos**. Y por último, está el número 1, el cual tiene solamente un divisor.

**Definición.** Dados dos enteros  $a$  y  $b$ , decimos que estos tienen un **común divisor**, si existe otro número entero  $c \neq 0$  tal que:

$$c \mid a \text{ y } c \mid b$$

**Propiedad.** Sean  $a, b, c \in \mathbb{Z}$  con  $c \neq 0$ . Si  $c \mid a$  y  $c \mid b$ , entonces  $c \mid (xa + yb)$  con  $x, y \in \mathbb{Z}$ .

*Prueba:*

Supongamos  $c \mid a$  y  $c \mid b$ , entonces  $a = mc$  y  $b = nc$ .

Luego,  $xa + yb = x(mc) + y(nc) = (xm + yn)c = kc$  con  $k \in \mathbb{Z}$ .

$\therefore c \mid (xa + yb)$   $\square$

**Definición.** Dados  $a$  y  $b \in \mathbb{Z}$ , el **máximo común divisor** de  $a$  y  $b$  es el mayor número entero que divide a ambos.

Notación: Usamos la notación  $\text{mcd}(a, b)$  para representar al máximo común divisor de  $a$  y  $b$ .

**Teorema** (fundamental de la aritmética). Todo número entero positivo mayor que 1 es un número primo o bien un único producto de números primos.

⚠ La factorización es única salvo en el orden de los factores.

*Ejemplo 1.* Calcule  $\text{mcd}(60, 48)$ .

Primero factorizamos los números:

60	2
30	2
15	3
5	5
1	

48	2
24	2
12	2
6	2
3	3
1	

El  $\text{mcd}(60, 48)$  es:  $2 \cdot 2 \cdot 3 = 12$

$$60 = 2^2 \cdot 3 \cdot 5 \quad 48 = 2^4 \cdot 3$$

⚠ El inconveniente de este método es que se requiere conocer la factorización prima de cada número y el problema de determinar si un número es primo o no, es un problema de alta complejidad computacional.

🧑 Existe un procedimiento mucho más eficiente para poder calcular el mcd de dos números. Este es conocido como el **algoritmo de Euclides** y su funcionamiento está basado en el resultado del siguiente teorema.

**Teorema.** Sean  $a$  y  $b$  enteros. Si  $a = q \cdot b + r$ ,  $0 \leq r < b$  [algoritmo de la división de Euclides], entonces:  
 $\text{mcd}(a, b) = \text{mcd}(b, r)$

## Ejemplo 2. El algoritmo de Euclides

Calcule el  $\text{mcd}(60,48)$ .

$$\text{Expresamos } 60 = 1 \cdot 48 + 12 \rightarrow \text{mcd}(60,48) = \text{mcd}(48,12)$$

$$\text{Expresamos } 48 = 4 \cdot 12 + 0 \rightarrow \text{mcd}(48,12) = \text{mcd}(12,0)$$

⚠ Como 0 es divisible por cualquier número, entonces  $\text{mcd}(12,0)$  está *limitado* únicamente por 12 y como el número más grande que divide a 12 es 12 mismo, entonces  $\text{mcd}(12,0) = 12$ .

En conclusión,  $\text{mcd}(60,48) = \text{mcd}(48,12) = \text{mcd}(12,0) = 12$ .