# ALGORITMO DE LA DIVISION: NUMEROS PRIMOS

Si $a, b \in \mathbb{Z}$ y $b \neq 0$, decimos que $b$ divide a $a$, y lo denotamos $b|a$, si existe un entero $n$ tal que $a = bn$. Cuando esto ocurre, decimos que $b$ es un divisor de $a$, o que $a$ es múltiplo de $b$.

Con esta definición podemos hablar de la división dentro de $\mathbb{Z}$ sin pasar a $\mathbb{Q}$. Dicha propiedad cumple diferentes propiedades:

Para cualquiera $a, b, c, x, y, z \in \mathbb{Z}$ (recuerde que el divisor no puede ser 0)

1. $1|a$ y $a|0$
2. $[(a|b) \wedge (b|a)] \Rightarrow a = \pm b$
3. $[(a|b) \wedge (b|c)] \Rightarrow a|c$
4. $a|b \Rightarrow a|bx$
5. Si $x = y + z$ y $a$ divide a dos de los enteros $x, y, z$, entonces $a$ divide al entero restante.
6. $[(a|b) \wedge (a|c)] \Rightarrow a|(bx + cy)$. ($bx + cy$ es combinación lineal entera de $b$ y $c$)
7. Si $\forall 1 \leq i \leq n$, $c_i \in \mathbb{Z}$ y $a|c_i$ entonces $a|(c_1x_1 + c_2x_2 + ... + c_nx_n)$

Lema: Si $n \in \mathbb{Z}^+$ y $n$ es compuesto, entonces existe un primo $p$ tal que $p|n$.

Teorema: Existen infinitos primos

Ejemplos:

- ¿Existen enteros $x, y, z$ tales que $6x + 9y + 15z = 107$?
- Si $2a + 3b$ es múltiplo de 17, demuestre que $17|(9a + 5b)$. $\forall a, b \in \mathbb{Z}$.

## ALGORITMO DE LA DIVISION

Si $a, b \in \mathbb{Z}$, $b > 0$, entonces existen único $q, r \in \mathbb{Z}$ tales que $a = qb + r$, con $0 \leq r < b$.

Al entero $b$ se lo llama *divisor* y $a$ *es el dividendo*

Ejemplos: Indicar cociente y resto en la división entre $a$ por $b$

- $a = 170$ y $b = 11$
- $a = 98$ y $b = 7$
- $a = -45$ y $b = 8$

Si $n \in \mathbb{Z}^+$ y $n$ es compuesto, entonces existe un primo $p$ tal que $p|n$ y $p \leq \sqrt{n}$.

Esto constituye un criterio básico para evaluar si un número $n$ es primo o no, ya que si $n$ no es divisible por algunos de los primos menores o iguales a su raíz cuadrada, entonces $n$ es compuesto.

Ejemplos: Evaluar la primalidad de 3553 y de 7919.

# MAXIMO COMUN DIVISOR: ALGORITMO DE EUCLIDES

Sean $a, b \in \mathbb{Z}$, donde $a \neq 0$ o $b \neq 0$. Entonces $c \in \mathbb{Z}^+$ es el *máximo común divisor* de $a, b$ si:

- $c|a$, $c|b$ ($c$ es divisor común de $a, b$)
- para cualquier divisor $d$ de $a, b$, tenemos que $d|c$.

Para cualquiera $a, b \in \mathbb{Z}^+$, existe un único $c \in \mathbb{Z}^+$ que es *el* máximo común divisor de $a, b$.

Ahora sabemos que para cualquier $a, b \in \mathbb{Z}^+$, el máximo común divisor de $a, b$ existe y es único. Se denota con $mcd(a, b)$. Se puede verificar que:

- $mcd(a, b) = mcd(b, a)$
- Para $a \neq 0$, $mcd(a, 0) = |a|$
- $mcd(-a, b) = mcd(a, -b) = mcd(-a, -b) = mcd(a, b)$
- $mcd(0, 0)$ no está definido

Se dice que $a, b$ son *primos relativos (o coprimos)* si $mcd(a, b) = 1$. El $mcd(a, b)$ es el entero positivo más pequeño que podemos escribir como combinación lineal de $a$ y $b$.

## Algorítmo de Euclides

Si $a, b \in \mathbb{Z}^+$, aplicamos el algorítmo de la división como sigue:

$$
\begin{array}{ll}
a = q_1 b + r_1 & 0 < r_1 < b \\
b = q_2 r_1 + r_2 & 0 < r_2 < r_1 \\
r_1 = q_3 r_2 + r_3 & 0 < r_3 < r_2 \\
\ldots & \ldots \\
r_i = q_{i+2} r_{i+1} + r_{i+2} & 0 < r_{i+2} < r_{i+1} \\
\ldots & \ldots \\
r_{k-3} = q_{k-1} r_{k-2} + r_{k-1} & 0 < r_{k-1} < r_{k-2} \\
r_{k-2} = q_k r_{k-1} + r_k & 0 < r_k < r_{k-1} \\
r_{k-1} = q_{k+1} r_k & .
\end{array}
$$

entonces, $r_k$, el último resto no nulo, es igual al $mcd(a, b)$.

De esta manera, y mediante una sustitución de los restos *hacia atrás* se puede expresar al $mcd(a, b) = r_k$ como combinación lineal de $a$ y $b$.

Ejemplos:

- Determinar el $mcd(259, 111)$ y expresarlo como una combinación lineal de estos enteros.
- Hallar una expresión general que permita encontrar todos los enteros $x$ e $y$ tales que $mcd(259, 111) = 259x + 111y$

- Para cualquier $n \in \mathbb{Z}^+$, demostrar que los enteros $8n + 3$ y $5n + 2$ son primos relativos.
- Juan depura un programa en Pascal en 6 minutos, pero en Python tarda 10 minutos. Si trabaja en forma continua durante 104 minutos y no le sobró tiempo, ¿cuántos programas depuró en cada lenguaje?

Las ecuaciones que requieren soluciones enteras reciben el nombre de *ecuaciones diofánticas*.

Si $a, b \in \mathbb{Z}^+$, la ecuación diofántica $ax + by = c$ tiene una solución entera $x = x_0$, $y = y_0$ si y sólo si $mcd(a, b)$ divide a $c$.

## Mínimo común múltiplo

Si $a, b, c \in \mathbb{Z}^+$, $c$ es un múltiplo común de $a, b$ si $c$ es un múltiplo de $a$ y de $b$. Además, $c$ es el mínimo común múltiplo de $a, b$ si es el más pequeño del los enteros positivos que son múltiplos comunes de $a, b$. Denotamos a $c$ como $mcm(a, b)$.

Sean $a, b, c \in \mathbb{Z}^+$ con $c = mcm(a, b)$. Si $d$ es un múltiplo común de $a$ y $b$, entonces $c|d$.

Para $a, b \in \mathbb{Z}^+$, $ab = mcm(a, b).mcd(a, b)$

Ejemplos:

- Hallar el $mcm(456, 624)$ sabiendo que $mcd(456, 624) = 24$.
- Verificar que $mcm(250, 111) = 27750$.
- Generalizar la idea del ejemplo anterior.

# Teorema fundamental de la aritmética

Si $a, b \in \mathbb{Z}^+$, $p$ es un primo y $p|ab$, entonces $p|a$ o $p|b$.

Y generalizando esta idea:

Sea $a_i \in \mathbb{Z}^+$ para todo $1 \leq i \leq n$. Si $p$ es primo y $p|a_1 a_2 ... a_n$, entonces $p|a_i$ para algún $1 \leq i \leq n$.

Cada entero $n > 1$ puede escribirse como un producto de primos de forma **única**, excepto por el orden de éstos. (Si $n$ es primo se considera un producto de un factor).

- Determinar la factorización como producto de primos de 980220.
- Justificar por qué $17|n$ si $10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot n = 21 \cdot 20 \cdot 19 \cdot 18 \cdot 17 \cdot 16 \cdot 15 \cdot 14$

Para $m, n \in \mathbb{Z}^+$, $n > 1$, sus expresiones como producto de primos son:

$$n = {p_1}^{e_1} {p_2}^{e_2} ... p_k^{e_k} \qquad m = {p_1}^{f_1} {p_2}^{f_2} ... p_k^{f_k}$$

Si $m|n$, entonces $0 \leq f_i \leq e_i$, para todo $1 \leq i \leq k$, por la regla del producto, el número de divisores positivos de $n$ es

$$(e_1 + 1)(e_2 + 1)...(e_k + 1)$$

Para el número $29338848000 = 2^8 3^5 5^3 7^3 11$, determinar la cantidad de divisores positivos que tiene, y cuántos son cuadrados perfectos.