

# Conferencia 2 - Principios de la Teoría de Números

November 18, 2024

**Definición.** Sean  $a, b$ ,  $a \in \mathbb{Z}$ ,  $b \in \mathbb{Z}$ ,  $a \neq 0$  o  $b \neq 0$ , se denota  $\text{mcd}(a, b) = \max\{d \mid d \in \mathbb{Z} \wedge d \mid a \wedge d \mid b\}$  como el máximo común divisor de  $a$  y  $b$ .

El  $\text{mcd}(a, b)$  también suele denotarse  $(a, b)$ .

**Propiedades.**  $\text{mcd}(a, b) = \text{mcd}(-a, b) = \text{mcd}(a, -b) = \text{mcd}(-a, -b)$

**Teorema.** Sean  $a, b$ ,  $a \in \mathbb{Z}$ ,  $b \in \mathbb{Z}$ , si  $a \mid b$  entonces  $\text{mcd}(a, b) = |a|$

El  $\text{mcm}(a, 0) = |a|$  ( $a \neq 0$ ).

**Definición.** Sean  $a, b$ ,  $a \in \mathbb{Z}$ ,  $b \in \mathbb{Z}$ , si el  $\text{mcd}(a, b) = 1$  entonces  $a$  y  $b$  son **primos relativos**

**Definición.** Un entero  $c$  es combinación lineal de los enteros  $a_1, a_2, \dots, a_n$  si existen enteros  $b_1, b_2, \dots, b_n$  tales que  $c = a_1 * b_1 + a_2 * b_2 + \dots + a_n * b_n$ .

**Teorema.** El máximo común divisor de  $a_1, a_2, \dots, a_n$ , números enteros, no todos iguales a 0,  $\text{mcd}(a_1, a_2, \dots, a_n)$  es el menor entero positivo que puede ser expresado como combinación lineal de  $a_1, a_2, \dots, a_n$ .

#### Demostración

Partamos de  $a_1 x_1 + a_2 x_2 + \dots + a_n x_n$ .

Tomando  $x_i = a_i$  se tiene que  $\sum_{i=1}^n a_i x_i = \sum_{i=1}^n a_i^2 \geq 0$

Como existe  $a_k \neq 0$  ( $1 \leq k \leq n$ ) entonces  $\sum_{i=1}^n a_i^2 > 0$

Por tanto existe al menos una combinación lineal positiva.

Sea  $S = \{d \mid d > 0, a_1 x_1 + a_2 x_2 + \dots + a_n x_n, \forall(i) 1 \leq i \leq n, x_i \in \mathbb{Z}\}$

$S \neq \emptyset$

Por el **Principio del Buen Ordenamiento (PBO)** tomemos

$s = a_1 s_1 + a_2 s_2 + \dots + a_n s_n$  como el menor elemento de  $S$ .

Probemos que  $s \mid a_1$

Por el **Algoritmo de la División**

$a_1 = sq + r$   $0 \leq r < s$

Supongamos que  $r > 0$

$r = a_1 - sq$

$r = a_1 - (a_1 s_1 + a_2 s_2 + \dots + a_n s_n)q$

$r = a_1(1 - s_1 q) + a_2(-s_2 q) + \dots + a_n(-s_n q)$

Por tanto  $r$  es una combinación lineal positiva de los  $a_i$  tal que  $r < s$  pero  $s$  es la menor de las combinaciones lineales positivas. Y esto es una contradicción!

Luego  $r = 0$  y, por tanto,  $s \mid a_1$

Análogamente, se puede demostrar que  $s \mid a_i$ ,  $1 \leq i \leq n$

Entonces  $s$  es divisor común de  $a_i$ ,  $1 \leq i \leq n$

Ahora, sea  $d$  el mayor de los divisores comunes de  $a_i$ , entonces  $s \leq d$

Por otra parte,  $d$  divide a cualquier combinación lineal de  $a_i$ , entonces  $d \mid s$  y, por tanto,  $d \leq s$

Entonces, como  $d \leq s \leq d$  se tiene que  $s = d$

**Teorema.** Sean  $a, b$ ,  $a \in \mathbb{Z}$ ,  $b \in \mathbb{Z}$ , el conjunto de los divisores comunes de  $a$  y  $b$  coincide con el conjunto de los divisores del  $\text{mcd}(a, b)$

**Corolario.** Si  $a_1, a_2, \dots, a_n$  son números enteros no todos iguales a 0 entonces  $\text{mcd}(a_1, a_2, \dots, a_n) = \text{mcd}(a_1, \text{mcd}(a_2, a_3, \dots, a_n))$

**Corolario.** Sean  $a, b$ ,  $a \in \mathbb{Z}$ ,  $b \in \mathbb{Z}$ , no simultáneamente nulos, entonces  $\frac{a}{\text{mcd}(a,b)}$  y  $\frac{b}{\text{mcd}(a,b)}$  son **primos relativos**. O sea,  $\text{mcd}(\frac{a}{\text{mcd}(a,b)}, \frac{b}{\text{mcd}(a,b)}) = 1$

**Teorema.** Sea  $a$ ,  $a \in \mathbb{Z}$ ,  $a \neq 0$ ,  $b_i \in \mathbb{Z}$ ,  $1 \leq i \leq n$ , si  $a|b_1 * b_2 * \dots * b_n$  y para todo  $j$ ,  $1 \leq j \leq n-1$ , se cumple que  $\text{mcd}(a, b_j) = 1$  entonces  $a|b_n$

**Corolario.** Sean  $a, b, q, r$  tales que  $a \in \mathbb{Z}$ ,  $b \in \mathbb{Z}$ ,  $q \in \mathbb{Z}$ ,  $r \in \mathbb{Z}$ ,  $b \neq 0$ , y  $a = q * b + r$  entonces  $\text{mcd}(a, b) = \text{mcd}(b, r)$

#### **Demostración**

Si  $x|a$  y  $x|b$  entonces se tiene que  $a = xy_1$  y  $b = xy_2$ , luego

$$a = qb + r$$

$$xy_1 = qxy_2 + r$$

$$r = xy_1 - qxy_2$$

$$r = x(y_1 - qy_2)$$

Por lo que  $x|r$

De igual modo, si  $x|b$  y  $x|r$  entonces se tiene que  $b = xy_2$  y  $r = xy_3$ , luego

$$a = qb + r$$

$$a = qxy_2 + xy_3$$

$$a = x(qy_2 + y_3)$$

Por lo que  $x|a$

Como los divisores comunes de  $a$  y  $b$  coinciden con los de  $b$  y  $r$ , entonces tendrán el mismo máximo común divisor.

**Definición.** Sean  $a, b, c$ ,  $a \in \mathbb{Z}$ ,  $b \in \mathbb{Z}$ ,  $c \in \mathbb{Z}$ ,  $a \neq 0$ ,  $b \neq 0$  se dice que  $ax + by = c$  es una ecuación lineal diofantina si esta es resuelta con  $x \in \mathbb{Z}$  y  $y \in \mathbb{Z}$

**Teorema.** La ecuación lineal diofantina  $ax + by = c$  tiene solución si y solo si  $\text{mcd}(a, b)|c$

#### **Demostración**

Se debe demostrar en ambos sentidos.

Demostremos que si  $ax + by = c$  tiene solución entonces  $\text{mcd}(a, b)|c$ .

Como  $ax + by = c$  tiene solución tomemos  $d = \text{mcd}(a, b)$ , luego se sabe que  $d|ax + by$  y, por tanto,  $d|c$ .

Demostremos ahora que si  $\text{mcd}(a, b)|c$  entonces  $ax + by = c$  tiene solución.

Si  $\text{mcd}(a, b)|c$  entonces existe  $k$ ,  $k \in \mathbb{Z}$  tal que  $c = k(a, b)$ .

Ahora, sabemos que existe  $x_0, y_0 \in \mathbb{Z}$  tal que

$$ax_0 + by_0 = (a, b)$$

por lo que

$$akx_0 + bky_0 = k(a, b)$$

Entonces, si se toma  $x = kx_0$  y  $y = ky_0$  se cumple que existe  $x, y \in \mathbb{Z}$  tal que

$$ax + by = c$$

**Teorema. Algoritmo de Euclides.** Sean  $a, b$ ,  $a \in \mathbb{Z}$ ,  $b \in \mathbb{Z}$ ,  $a > b$ , si se realizan los siguientes cálculos:

$$a = q_1 * b + r_1 \quad 0 \leq r_1 < b$$

$$b = q_2 * r_1 + r_2 \quad 0 \leq r_2 < r_1$$

$$r_1 = q_3 * r_2 + r_3 \quad 0 \leq r_3 < r_2$$

$$r_2 = q_4 * r_3 + r_4 \quad 0 \leq r_4 < r_3$$

...

...

...

$$r_{k-2} = q_k * r_{k-1} + r_k \quad 0 \leq r_k < r_{k-1}$$

$$r_{k-1} = q_{k+1} * r_k \quad 0 = r_{k+1}$$

donde  $r_k$  es el último resto diferente de 0, entonces  $r_k = \text{mcd}(a, b)$

**Ejemplo** Para calcular el máximo común divisor de 3088 y 456:

$$3088 = 6 * 456 + 352$$

$$456 = 1 * 352 + 104$$

$$352 = 3 * 104 + 40$$

$$104 = 2 * 40 + 24$$

$$40 = 1 * 24 + 16$$

$$24 = 1 * 16 + 8$$

$$16 = 2 * 8 + 0$$

Entonces 8 es el último resto distinto de 0. Por tanto  $\text{mcd}(3088, 456) = 8$

A partir del **Algoritmo de Euclides** también se puede calcular la combinación lineal de la siguiente forma:

$$A_1 = 1 \quad B_1 = -q_k$$

$$A_2 = B_1 \quad B_2 = A_1 - q_{k-1} * B_1$$

...

$$A_{i+1} = B_i \quad B_{i+1} = A_i - q_{k-i} * B_i$$

...

$$A_{k-1} = B_{k-2} \quad B_{k-1} = A_{k-2} - q_2 * B_{k-2}$$

$$A_k = B_{k-1} \quad B_k = A_{k-1} - q_1 * B_{k-1}$$

Luego  $r_k = a * A_k + b * B_k$  y, por lo tanto,  $r_k = a * A_k + b * B_k = \text{mcd}(a, b)$

**Ejemplo** Para calcular la combinación lineal de 3088 y 456 con la que se obtiene su  $\text{mcd}$  se tiene:

$$3088 = 6 * 456 + 352 \quad A_1 = 1 \quad B_1 = -1$$

$$456 = 1 * 352 + 104 \quad A_2 = -1 \quad B_2 = 1 - 1 * (-1) = 2$$

$$352 = 3 * 104 + 40 \quad A_3 = 2 \quad B_3 = -1 - 2 * 2 = -5$$

$$104 = 2 * 40 + 24 \quad A_4 = -5 \quad B_4 = 2 - 3 * (-5) = 17$$

$$40 = 1 * 24 + 16 \quad A_5 = 17 \quad B_5 = -5 - 1 * 17 = -22$$

$$24 = 1 * 16 + 8 \quad A_6 = -22 \quad B_6 = 17 - 6 * (-22) = 149$$

$$16 = 2 * 8 + 0$$

$$\text{Por tanto } 8 = \text{mcd}(3088, 456) = 3088 * (-22) + 456 * 149$$

**Teorema.** Si  $x_0, y_0$  son una solución de la ecuación diofantina  $ax + by = c$  entonces  $x = x_0 + k \frac{b}{(a,b)}$  y  $y = y_0 - k \frac{a}{(a,b)}$  con  $k \in \mathbb{Z}$  es la solución general de la ecuación diofantina.

### **Demostración**

Se debe demostrar, primero que es solución y luego que toda solución es de esa forma.

La demostración de lo primero es trivial, basta sustituir en la ecuación original.

Para demostrar lo segundo, asumamos que  $x_1, y_1$  son otra solución de la ecuación, luego

$$ax_0 + by_0 = ax_1 + by_1$$

$$a(x_0 - x_1) = b(y_1 - y_0)$$

$$\frac{a}{(a,b)}(x_0 - x_1) = \frac{b}{(a,b)}(y_1 - y_0)$$

Esto implica que

$$\frac{b}{(a,b)} \mid \frac{a}{(a,b)}(x_0 - x_1)$$

pero como se sabe que  $(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1$  entonces  $\frac{b}{(a,b)} \mid x_0 - x_1$

por tanto existe  $k \in \mathbb{Z}$  tal que  $x_1 = x_0 + k \frac{b}{(a,b)}$  luego

$$\frac{a}{(a,b)}(x_0 - x_1) = \frac{b}{(a,b)}(y_1 - y_0)$$

$$\frac{a}{(a,b)}(x_0 - x_0 - k \frac{b}{(a,b)}) = \frac{b}{(a,b)}(y_1 - y_0)$$

$$\frac{a}{(a,b)}(-k \frac{b}{(a,b)}) = \frac{b}{(a,b)}(y_1 - y_0)$$

$$-k \frac{a}{(a,b)} = y_1 - y_0$$

$$y_1 = y_0 - k \frac{a}{(a,b)}$$

Entonces  $x = x_0 + k \frac{b}{(a,b)}$  y  $y = y_0 - k \frac{a}{(a,b)}$  son solución general de la ecuación.

**Definición.** Sean  $a, b, c$ ,  $a \in \mathbb{Z}$ ,  $b \in \mathbb{Z}$ ,  $c \in \mathbb{Z}$ , los tres distintos de 0, se dice que  $c$  es múltiplo común de  $a$  y  $b$  si  $c$  es múltiplo de  $a$  y  $c$  es múltiplo de  $b$ . Se dice que  $c$  es el mínimo común múltiplo de  $a$  y  $b$ , si es el menor entero positivo múltiplo común de  $a$  y  $b$ , lo que se denota  $mcm(a, b)$ .

El  $mcm(a, b)$  también suele denotarse  $[a, b]$ .

**Teorema.** Sean  $a, b$ ,  $a \in \mathbb{Z}_+$ ,  $b \in \mathbb{Z}_+$ , todo múltiplo común de  $a$  y  $b$  se expresa como  $k \frac{a*b}{(a,b)}$  donde  $k \in \mathbb{Z}$

### **Demostración**

Sea  $m$  múltiplo común de  $a$  y  $b$ , entonces

$$m = k_1 a = k_2 b$$

$$k_1 \frac{a}{(a,b)} = k_2 \frac{b}{(a,b)}$$

Por tanto

$$\frac{b}{(a,b)} \mid k_1 \frac{a}{(a,b)} \text{ pero como } (\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1$$

$$\frac{b}{(a,b)} \mid k_1 \text{ luego existe } k \in \mathbb{Z} \text{ tal que } k_1 = k \frac{b}{(a,b)}$$

$$\text{y por tanto } m = k_1 a = k \frac{a*b}{(a,b)}$$

**Corolario.** El  $mcm(a, b) = \frac{|a*b|}{mcd(a,b)}$ , lo que es lo mismo  $(a, b) = \frac{|a*b|}{[a,b]}$

**Corolario.** Todo múltiplo común de  $a$  y  $b$  es múltiplo común de  $[a, b]$