

$$a, b \in \mathbb{Z} \quad b \neq 0$$

existen números α, β :

$$a = \alpha \cdot b + \boxed{\beta}$$

$$\boxed{0 \leq \beta < |b|}$$

además son únicos

$$a \bmod b = \beta$$

$$13 = 1 \cdot 5 + \cancel{8}$$

$$13 \bmod 5 = 3$$

$$13 = 2 \cdot 5 + \boxed{3}$$

$$-10 \bmod -3 = 2$$

$$-10 = 4(-3) + \boxed{2}$$

Def: $\boxed{a \equiv b \bmod n}$ si
 $n \mid (b - a)$

Prop: $a \equiv b \bmod n$ si
 $a \bmod n = b \bmod n$

mod 5

$$3 \equiv 8 \pmod{5}$$

$$5 \mid 8 - 3$$

$$3 \pmod{5} = 3 = 8 \pmod{5}$$

4, 5

$$0 \leq B < 5$$

$$\{0, 1, 2, 3, 4\}$$

Prop:

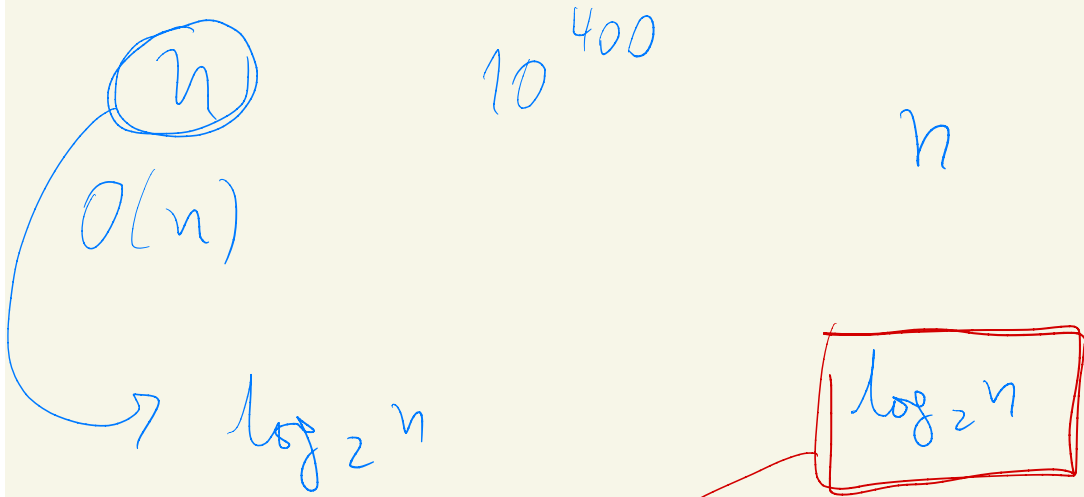
$$a \equiv b \pmod{n}$$

$$c \equiv d \pmod{n}$$

$$\Rightarrow \left. \begin{array}{l} (a+c) \equiv (b+d) \pmod{n} \\ (a \cdot c) \equiv (b \cdot d) \pmod{n} \end{array} \right\}$$

Algoritmos básicos

MCD: máximo común divisor



$$a \geq b$$

$$\text{MCD}(a, b)$$

A diagram showing the relationship between $\log_2 n$ and its powers. A red box contains the expression $\log_2 n$. A curved red arrow points from this box down to the expression $O((\log_2 n)^k)$. Below this is the expression $O((\log_2 a)^2)$.

$$O((\log_2 n)^k)$$
$$O((\log_2 a)^2)$$

MCD

$$\boxed{MCD(a, b)}$$

$$a \geq b$$

$$a > 0$$

$$\boxed{\begin{array}{l} a = p_1^{s_1} \dots p_l^{s_l} \\ b = p_1^{t_1} \dots p_l^{t_l} \end{array}}$$

$$12 = 2^2 \cdot 3$$

$$14 = 2 \cdot 7$$

$$\boxed{\begin{array}{l} 12 = 2^2 \cdot 3^1 \cdot 7^0 \\ 14 = 2^1 \cdot 3^0 \cdot 7^1 \end{array}}$$

$$MCD(a, b) = p_1^{\min(s_1, t_1)} \dots p_l^{\min(s_l, t_l)}$$

$$MCM(a, b) = p_1^{\max(s_1, t_1)} \dots p_l^{\max(s_l, t_l)}$$

$$N \rightsquigarrow \textcircled{P}$$

$$\frac{N}{P}$$

$$12 \xrightarrow{4} 12 \quad \begin{array}{c} \downarrow \\ 2 \cdot 2 \end{array} \quad \frac{12}{4}$$

$$\text{MCD}(a, b) =$$

$$a \geq b \geq 0$$

$$a \neq 0$$

$$\boxed{\begin{array}{l} \text{MCD}(b, \\ a \bmod b) \end{array}}$$

$$b > 0$$

$$a$$

$$b = 0$$

$$\text{MCD}(5, 0) = 5$$

$$\text{MCD}(14, 12) = \text{MCD}(12, 2)$$

$$= \text{MCD}(2, 0)$$

$$= 2$$

Prop: $a \geq b \geq 0 \quad a \neq 0$
 $a \bmod b < \frac{a}{2}$