

# Matemática Discreta I

## Clase 12 - Máximo común divisor (2)

FAMAF / UNC

2 de mayo de 2023

## Algoritmo de Euclides

Para calcular el mcd de enteros  $a$  y  $b$ , con  $b > 0$ , definimos  $q_i$  y  $r_i$  recursivamente de la siguiente manera:  $r_0 = a$ ,  $r_1 = b$ , y

$$(e_1) \quad r_0 = r_1 q_1 + r_2 \quad (0 < r_2 < r_1)$$

$$(e_2) \quad r_1 = r_2 q_2 + r_3 \quad (0 < r_3 < r_2)$$

$$(e_3) \quad r_2 = r_3 q_3 + r_4 \quad (0 < r_4 < r_3)$$

...

$$(e_i) \quad r_{i-1} = r_i q_i + r_{i+1} \quad (0 < r_{i+1} < r_i)$$

...

$$(e_{k-1}) \quad r_{k-2} = r_{k-1} q_{k-1} + r_k \quad (0 < r_k < r_{k-1})$$

$$(e_k) \quad r_{k-1} = r_k q_k + 0,$$

Entonces  $r_k = \text{mcd}(a, b)$  (Se usa en filmina 5)

Ejemplifiquemos el algoritmo de Euclides.

### Ejemplo

Encuentre el mcd de 2406 y 654.

### Solución

Tenemos

$$2406 = 654 \cdot 3 + 444, \quad \text{entonces} \quad (2406, 654) = (654, 444)$$

$$654 = 444 \cdot 1 + 210, \quad \text{entonces} \quad (654, 444) = (444, 210)$$

$$444 = 210 \cdot 2 + 24, \quad \text{entonces} \quad (444, 210) = (210, 24)$$

$$210 = 24 \cdot 8 + 18, \quad \text{entonces} \quad (210, 24) = (24, 18)$$

$$24 = 18 \cdot 1 + 6, \quad \text{entonces} \quad (24, 18) = (18, 6)$$

$$18 = 6 \cdot 3 + 0 \quad \text{entonces} \quad (18, 6) = (6, 0) = 6$$

Por lo tanto  $(2406, 654) = 6$ .

- El algoritmo de Euclides es fácilmente implementable en un lenguaje de programación.
- A continuación una versión del mismo en pseudocódigo (estilo Python).

## Algoritmo de Euclides

```
# pre: a y b son números positivos
# post: obtenemos d = mcd(a,b)
i, j = a, b
while j != 0:
    # invariante: mcd(a, b) = mcd(i, j)
    resto = i % j # i = q * j + resto
    i, j = j, resto
d = i
```

## Teorema

Sean  $a, b \in \mathbb{Z}$ , alguno de ellos no nulo. Entonces, existen  $s, t \in \mathbb{Z}$  tal que

$$\text{mcd}(a, b) = sa + tb.$$

## Demostración.

Supongamos que  $b > 0$  y sea  $d = \text{mcd}(a, b)$ . Entonces,  $d$  es el último resto no nulo del algoritmo (ver p. 2).

Cada resto puede ser calculado en base a los dos anteriores:

$$(e_{i-1}) \quad r_{i-2} = r_{i-1}q_{i-1} + r_i \quad \Rightarrow \quad r_i = r_{i-2} - r_{i-1}q_{i-1}. \quad (1)$$

Aplicando repetidamente (1) a los restos correspondientes,  $\Rightarrow$  cada resto puede ser escrito como combinación lineal entera de  $r_0 = a$  y  $r_1 = b$ .

En particular,  $d = r_k$  puede ser escrito como combinación lineal entera de  $r_0 = a$  y  $r_1 = b$ .

Más precisamente, de la filmina 2 :

$$(e_{i-1}) \quad r_{i-2} = r_{i-1}q_{i-1} + r_i.$$

Esto implica que

$$(i) \quad r_i = r_{i-2} - r_{i-1}q_{i-1}.$$

Lo cual nos dice que  $r_i$  puede ser calculado usando  $r_{i-1}$  y  $r_{i-2}$ .

$$\begin{aligned} d &= r_k \stackrel{(k)}{=} r_{k-2} - r_{k-1}q_k = s_k r_{k-2} + t_k r_{k-1} \\ &\stackrel{(k-1)}{=} s_k r_{k-2} + t_k (r_{k-3} - r_{k-2}q_{k-2}) = s_{k-1} r_{k-3} + t_{k-1} r_{k-2} \\ &\dots \dots \\ &\stackrel{(3)}{=} s_4 r_2 + t_k (r_1 - r_2 q_2) = s_3 r_1 + t_3 r_2 \\ &\stackrel{(2)}{=} s_3 r_1 + t_3 (r_0 - r_1 q_1) = s_2 r_0 + t_2 r_1 = s_2 a + t_2 b. \end{aligned}$$



## Corolario

Sean  $a$  y  $b$  enteros,  $b$  no nulo, entonces

$$(a, b) = 1 \Leftrightarrow \text{existen } s, t \in \mathbb{Z} \text{ tales que } 1 = sa + tb.$$

## Definición

Si  $(a, b) = 1$  entonces decimos que  $a$  y  $b$  son *coprimos*.

## Observación

NO es cierto que si existen  $s, t \in \mathbb{Z}$  tales que  $d = sa + tb \Rightarrow d = (a, b)$ .

Por ejemplo,  $4 = 2 \cdot 6 + (-2) \cdot 4$  y  $(6, 4) = 2$ .

## Ejemplo

Encuentre  $d$ , el mcd de 174 y 72 y escribir  $d = s \cdot 174 + t \cdot 72$ .

## Solución

$$174 = 72 \cdot 2 + 30, \quad \Rightarrow \quad 30 = 174 - 72 \cdot 2 \quad (1)$$

$$72 = 30 \cdot 2 + 12, \quad \Rightarrow \quad 12 = 72 - 30 \cdot 2 \quad (2)$$

$$30 = 12 \cdot 2 + 6, \quad \Rightarrow \quad 6 = 30 - 12 \cdot 2 \quad (3)$$

$$12 = 6 \cdot 2 + 0.$$

Por lo tanto,  $(174, 72) = 6$  y,



$$6 \stackrel{(3)}{=} 30 - 12 \cdot 2$$

$$\stackrel{(2)}{=} 30 - (72 - 30 \cdot 2) \cdot 2$$

$$= 5 \cdot 30 + (-2) \cdot 72$$

$$\stackrel{(1)}{=} 5 \cdot (174 - 72 \cdot 2) + (-2) \cdot 72$$

$$= 5 \cdot 174 + (-12) \cdot 72$$

Concluyendo:

- $(174, 72) = 6$  y,
- $6 = 5 \cdot 174 + (-12) \cdot 72$ .



## Ejemplo

Encuentre  $d$ , el mcd de 470 y 55 y escribir  $d = s \cdot 470 + t \cdot 55$ .

## Solución

Por el algoritmo de Euclides obtenemos

$$470 = 55 \cdot 8 + 30 \Rightarrow 30 = 470 + (-8) \cdot 55 \quad (1)$$

$$55 = 30 \cdot 1 + 25 \Rightarrow 25 = 55 + (-1) \cdot 30 \quad (2)$$

$$30 = 25 \cdot 1 + 5 \Rightarrow 5 = 30 + (-1) \cdot 25 \quad (3)$$

$$25 = 5 \cdot 5 + 0.$$

Luego

$$5 \stackrel{(3)}{=} 30 + (-1) \cdot 25$$

$$\stackrel{(2)}{=} 30 + (-1) \cdot (55 + (-1) \cdot 30) = 2 \cdot 30 + (-1) \cdot 55$$

$$\stackrel{(1)}{=} 2 \cdot (470 + (-8) \cdot 55) + (-1) \cdot 55 = 2 \cdot 470 + (-17) \cdot 55 \quad \square$$

# Mínimo común múltiplo

## Definición

Si  $a$  y  $b$  son enteros decimos que un entero no negativo  $m$  es el *mínimo común múltiplo*, o *mcm*, de  $a$  y  $b$  si

- a)  $a|m$  y  $b|m$ ;
- b) si  $a|n$  y  $b|n$  entonces  $m|n$ .

- La condición (a) nos dice que  $m$  es múltiplo común de  $a$  y  $b$ .
- La condición (b) nos dice que cualquier otro múltiplo de  $a$  y  $b$  también debe ser múltiplo de  $m$ .

## Ejemplo

Halleemos el mínimo común múltiplo entre 8 y 14.

## Solución

Escribamos los múltiplos de ambos números y busquemos el menor común a ambos.

Los primeros múltiplos de 8 son: 8, 16, 24, 32, 40, 48, 56, ...

Los primeros múltiplos de 14 son: 14, 28, 42, 56, 72, ...

Luego se tiene  $\text{mcm}(8, 14) = 56$ . Nos faltaría comprobar que cualquier múltiplo de 8 y 14 es múltiplo de 56, pero eso se deduce fácilmente de los resultados que veremos a continuación.

## Teorema

*Sean  $a$  y  $b$  enteros no nulos, entonces*

$$\text{mcm}(a, b) = \frac{|ab|}{\text{mcd}(a, b)}.$$

En particular este resultado implica que si  $a$  y  $b$  son naturales coprimos, entonces  $\text{mcm}(a, b) = ab$ .

## Ejemplo

Encontrar el mcm de 8 y 14.

## Solución

Es claro que  $2 = \text{mcd}(8, 14)$ , luego  $\text{mcm}(8, 14) = 8 \cdot 14 / 2 = 56$ .

## Ejercicio

Demostrar que si  $a$ ,  $b$  y  $n$  son enteros no nulos, entonces  $\text{mcd}(na, nb) = n \text{mcd}(a, b)$ .

## Solución

Sea  $d = (a, b)$ , debemos probar que  $nd = (na, nb)$ . Es decir,

- a)  $d|a$  y  $d|b$ ;
- b) si  $c|a$  y  $c|b$  entonces  $c|d$ .



- a')  $nd|na$  y  $nd|nb$ ;
- b') si  $c|na$  y  $c|nb$  entonces  $c|nd$ .

a')

Por a),  $a = d \cdot q_1$ ,  $b = d \cdot q_2$ , luego

$$na = d \cdot nq_1, \quad nb = d \cdot nq_2,$$

es decir

$$nd|na, \quad nd|nb.$$

b')

Sea  $c$  tal que  $c|na$  y  $c|nb$ .

Ahora bien

$$d = ra + sb \Rightarrow nd = s(na) + t(nb),$$

Luego,

$$c|na, c|nb \Rightarrow c|s(na) + t(nb) = nd.$$

Esto prueba b').

