

Unidad VII: Teoría de números

# Teoría de números: MCD y algoritmos de Euclides

Clase 20 - Matemáticas Discretas (IIC1253)

Prof. Miguel Romero

## Máximo común divisor

Sean  $a, b \in \mathbb{Z}$ .

Denotamos por **MCD( $a, b$ )** al **máximo común divisor** de  $a$  y  $b$ .

- El máximo número  $k \in \mathbb{Z}$  tal que  $k | a$  y  $k | b$ .

Ejemplos:

$$\text{MCD}(10, 18) = 2$$

$$\text{MCD}(18, 24) = 6$$

$$\text{MCD}(15, 17) = 1$$

$$\text{MCD}(0, 17) = 17$$

$$\text{MCD}(-10, 18) = 2$$

$$\text{MCD}(-10, -18) = 2$$

## Máximo común divisor

¿Cómo calculamos  $\text{MCD}(a, b)$ ?

Proposición:

Si  $b \neq 0$ , entonces  $\text{MCD}(a, b) = \text{MCD}(b, a \bmod b)$

Demostración:

Demostraremos que para todo  $c \in \mathbb{Z}$ :

$$c | a \quad y \quad c | b \iff c | b \quad y \quad c | a \bmod b$$

De esto se concluye que  $\text{MCD}(a, b) = \text{MCD}(b, a \bmod b)$ . (¿por qué?)

# Máximo común divisor

¿Cómo calculamos  $\text{MCD}(a, b)$ ?

**Proposición:**

Si  $b \neq 0$ , entonces  $\text{MCD}(a, b) = \text{MCD}(b, a \bmod b)$

**Demostración:**

$$c \mid a \quad y \quad c \mid b \quad \iff \quad c \mid b \quad y \quad c \mid a \bmod b$$

Tenemos que  $a = \alpha \cdot b + (a \bmod b)$ .

( $\Rightarrow$ ) Suponga que  $c \mid a$  y  $c \mid b$ .

Dado que  $(a \bmod b) = a - \alpha \cdot b$ , obtenemos que  $c \mid (a \bmod b)$ .

( $\Leftarrow$ ) Suponga que  $c \mid b$  y  $c \mid (a \bmod b)$ .

Dado que  $a = \alpha \cdot b + (a \bmod b)$ , obtenemos que  $c \mid a$ .

## Cálculo de máximo común divisor

De lo anterior, concluimos la siguiente identidad:

$$\text{MCD}(a, b) = \begin{cases} a & b = 0 \\ \text{MCD}(b, a \bmod b) & b \neq 0 \end{cases}$$

Podemos usar esta identidad para generar un algoritmo recursivo para calcular el máximo común divisor.

- ¿Cómo se ve este algoritmo?

## Algoritmo extendido de Euclides

El algoritmo anterior puede ser extendido para calcular números  $s, t \in \mathbb{Z}$  tales que:

$$\text{MCD}(a, b) = s \cdot a + t \cdot b$$

Vamos a mostrar cómo funciona el algoritmo suponiendo que  $a$  y  $b$  son números naturales tales que  $b \neq 0$ .

- Bajo este supuesto tenemos que  $a = \left\lfloor \frac{a}{b} \right\rfloor \cdot b + a \bmod b$ .

### Ejercicio:

Suponiendo que tiene el algoritmo para el caso anterior, indique cómo se ve el algoritmo en el caso general en que  $a, b \in \mathbb{Z}$  y  $b \neq 0$ .

## Algoritmo extendido de Euclides

Suponga que  $a \geq b > 0$ , y defina la siguiente sucesión:

$$r_0 = a$$

$$r_1 = b$$

$$r_i = r_{i-2} \bmod r_{i-1} \quad (i \geq 2)$$

Calculamos esta sucesión hasta un número  $k$  tal que  $r_k = 0$ .

- Tenemos que  $\text{MCD}(a, b) = r_{k-1}$ .

## Algoritmo extendido de Euclides

Al mismo tiempo calculamos sucesiones  $s_i, t_i$  tales que:

$$r_i = s_i \cdot a + t_i \cdot b$$

Tenemos que:  $\text{MCD}(a, b) = r_{k-1} = s_{k-1} \cdot a + t_{k-1} \cdot b$

Sean:

$$s_0 = 1 \quad t_0 = 0$$

$$s_1 = 0 \quad t_1 = 1$$

Se tiene que:

$$r_0 = s_0 \cdot a + t_0 \cdot b$$

$$r_1 = s_1 \cdot a + t_1 \cdot b$$

## Algoritmo extendido de Euclides

Dado que  $r_{i-2} = \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor \cdot r_{i-1} + r_{i-2} \bmod r_{i-1}$ , tenemos que:

$$r_{i-2} = \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor \cdot r_{i-1} + r_i$$

Por lo tanto:

$$s_{i-2} \cdot a + t_{i-2} \cdot b = \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor \cdot (s_{i-1} \cdot a + t_{i-1} \cdot b) + r_i$$

Concluimos que:

$$r_i = (s_{i-2} - \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor \cdot s_{i-1}) \cdot a + (t_{i-2} - \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor \cdot t_{i-1}) \cdot b$$

Definimos entonces:

$$s_i = s_{i-2} - \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor \cdot s_{i-1}$$

$$t_i = t_{i-2} - \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor \cdot t_{i-1}$$

## Algoritmo extendido de Euclides

### Ejemplo:

Vamos a usar el algoritmo para  $a = 60$  y  $b = 13$ .

Inicialmente:

$$\begin{array}{lll} r_0 = 60 & s_0 = 1 & t_0 = 0 \\ r_1 = 13 & s_1 = 0 & t_1 = 1 \end{array}$$

Entonces tenemos que:

$$\begin{aligned} r_2 &= r_0 \bmod r_1 \\ s_2 &= s_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor \cdot s_1 \\ t_2 &= t_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor \cdot t_1 \end{aligned}$$

## Algoritmo extendido para calcular el máximo común divisor

Ejemplo:

Por lo tanto:

$$r_2 = 8 \quad s_2 = 1 \quad t_2 = -4$$

Y el proceso continua:

$$\begin{array}{lll} r_3 = 5 & s_3 = -1 & t_3 = 5 \\ r_4 = 3 & s_4 = 2 & t_4 = -9 \\ r_5 = 2 & s_5 = -3 & t_5 = 14 \\ \textcolor{red}{r_6 = 1} & \textcolor{blue}{s_6 = 5} & \textcolor{teal}{t_6 = -23} \\ r_7 = 0 & s_7 = -13 & t_7 = 60 \end{array}$$

Tenemos que:  $\text{MCD}(60, 13) = 1 = 5 \cdot 60 + (-23) \cdot 13$

## La identidad de Bézout

Del algoritmo extendido de Euclides obtenemos la siguiente identidad:

**Teorema (Identidad de Bézout):**

Para cada  $a, b \in \mathbb{Z}$  tal que  $a \neq 0$  o  $b \neq 0$ , existen  $s, t \in \mathbb{Z}$  tal que:

$$\text{MCD}(a, b) = s \cdot a + t \cdot b.$$