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 $\text{MCD}(a, b)$ al **máximo común divisor** de $a$ y $b$.

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

Ejemplos:

$$\begin{aligned} \text{MCD}(10, 18) &= 2 \\ \text{MCD}(18, 24) &= 6 \\ \text{MCD}(15, 17) &= 1 \\ \text{MCD}(0, 17) &= 17 \\ \text{MCD}(-10, 18) &= 2 \\ \text{MCD}(-10, -18) &= 2 \end{aligned}$$

¿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 $c \in \mathbb{Z}$:

$$c \mid a \quad \text{y} \quad c \mid b \quad \Longleftrightarrow \quad c \mid b \quad \text{y} \quad c \mid a \bmod b$$

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

¿Cómo calculamos MCD$(a, b)$?

**Proposición:**

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

**Demostración:**

$$c \mid a \quad \text{y} \quad c \mid b \quad \Longleftrightarrow \quad c \mid b \quad \text{y} \quad c \mid a \bmod b$$

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 $c \mid a$.

De lo anterior, concluimos la siguiente identidad:

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

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

- ¿Cómo se ve este algoritmo?

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:

$$\begin{aligned} r_0 &= a \\ r_1 &= b \\ r_i &= r_{i-2} \bmod r_{i-1} \qquad (i \geq 2) \end{aligned}$$

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

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

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:

$$s_0 = 1 \qquad t_0 = 0$$
$$s_1 = 0 \qquad t_1 = 1$$

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:

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

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

**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:

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

**Ejemplo:**

Por lo tanto:

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

Y el proceso continua:

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

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

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:

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

**Lema:**

Sea $p$ un número primo. Si $p \mid (a \cdot b)$, entonces $p \mid a$ o $p \mid b$.

Notar que el lema anterior no es cierto si $p$ no es un primo:

$$4 \mid (6 \cdot 10), \text{ pero } 4 \nmid 6 \text{ y } 4 \nmid 10.$$

Demostración (Propuesta):

Razone por contradicción y aplique la identidad de Bézout. (ayudantía)

**Teorema (fundamental de la aritmética):**

Cada número natural $n \geq 2$ se puede expresar de una única manera como producto de potencias de números primos.

**Ejemplos:**

$$\begin{aligned} 7 &= 7 \\ 10 &= 2 \cdot 5 \\ 18 &= 2 \cdot 3^2 \\ 8466612 &= 2^2 \cdot 3 \cdot 7^3 \cdot 11^2 \cdot 17 \end{aligned}$$

Ya demostramos que cada número natural se puede expresar como producto de potencias de números primos.

- Faltaba demostrar la unicidad.

**Demostración (Propuesta):**

Aplique el lema anterior. (ayudantía)