Identidad de Bezout. LCM. Lema de Euclides

Sergio A. Carrillo
sacarrillot@unal.edu.co

Identidad de Bezout

Sean $a, b \in \mathbb{Z}$ no ambos nulos. El máximo común divisor de a y b es el menor entero positivo que puede escribirse como combinación lineal de a y b:

$$\gcd(a, b) = \min\{n \in \mathbb{N}^+ : n = ax + by, x, y \in \mathbb{Z}\}.$$

Ejemplo: $\gcd(7, 11) = 1$ y $7(-3) + 11(2) = 1$.

Ejemplos

- Si $d = ax_0 + by_0$, entonces también

$$d = a(x_0 + kb) + b(y_0 - ka), \qquad k \in \mathbb{Z}.$$

  Por tanto, la solución no es única.

- Tener una combinación lineal de a y b no garantiza que esa combinación sea el máximo común divisor. Por ejemplo $4 = 3(6) + (-7)(2)$, pero $\gcd(6, 2) \neq 4$, este valor es 2.

Proposición

$\gcd(a, b) = 1$ *si y solo si existen* $s, t \in \mathbb{Z}$ *con* $as + bt = 1$.

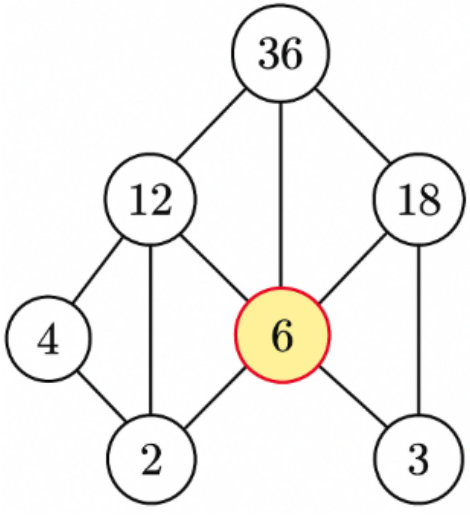
Caracterización del Máximo común divisor

Proposición

$d = \gcd(a, b)$ *si y solo si*

$$(1)\, d > 0, \qquad (2)\, d|a, d|b, \qquad (3)\, f|a, f|b \text{ entonces } f|d.$$

Esto significa que para encontrar el $\gcd(a, b)$ usando el diagrama de Hasse de divisibilidad buscamos la máxima cota inferior de a y b.



gcd(12,18) = 6

Ejemplo

Para expresar el gcd como una combinación lineal basta con deshacer los pasos en el algoritmo de Euclides:

$$\begin{aligned} \mathbf{252} &= \mathbf{198}\cdot 1 + \mathbf{54}, \\ \mathbf{198} &= \mathbf{54}\cdot 3 + \mathbf{36}, \\ \mathbf{54} &= \mathbf{36}\cdot 1 + \mathbf{18}, \\ \mathbf{36} &= \mathbf{18}\cdot 2 + 0. \end{aligned}$$

$$\begin{aligned} \mathbf{18} &= \mathbf{54} + (-1)\cdot \mathbf{36} \\ &= \mathbf{54} + (-1)\cdot(\mathbf{198} + (-3)\cdot \mathbf{54}) \\ &= (-1)\cdot \mathbf{198} + 4\cdot \mathbf{54} \\ &= (-1)\cdot \mathbf{198} + 4\cdot(\mathbf{252} + (-1)\cdot \mathbf{198}) \\ &= 4\cdot \mathbf{252} + (-5)\cdot \mathbf{198}. \end{aligned}$$

Algunas propiedades del gcd

- Si $d = \gcd(a, b)$, entonces $\gcd(a/d, b/d) = 1$.
- (Euclides) Si $a|bc$ y $\gcd(a, b) = 1$, entonces $a|c$.
- Si $a|c, b|c$ y $\gcd(a, b) = 1$, entonces $(ab)|c$.

Algunas propiedades sobre primos

- Si p es primo y $d|p$, entonces $d = 1$ ó p.
- (Lema de Euclides) Si p es primo y $p|ab$, entonces $p|a$ ó $p|b$. Más generalmente, si $p|(a_1 a_2 \cdots a_n)$, entonces $p|a_j$, para algún $j = 1, \ldots, n$.
- Si $p, p_1, \ldots, p_n$ son primos y $p|(p_1 p_2 \cdots p_n)$, entonces $p = p_j$, para algún j.
- Si $\gcd(a, b_1) = 1$ y $\gcd(a, b_2) = 1$, entonces $\gcd(a, b_1 b_2) = 1$. Más generalmente, si $\gcd(a, b_j) = 1$, para $j = 1, \ldots, n$, entonces $\gcd(a, b_1 b_2 \cdots b_n) = 1$.

Mínimo común múltiplo

Definición

Sean $a, b \in \mathbb{Z}$. El menor entero $m \geq 0$ tal que $a|m$ y $b|m$ se conoce como el *mínimo común múltiplo* (least common multiple) entre a y b. Escribiremos

$$\text{lcm}(a, b) \qquad \text{o} \qquad \text{mcm}(a, b).$$

En otras palabras

$$\text{lcm}(a, b) = \min\{k \in \mathbb{N}^+ : a|k \text{ y } b|k\}.$$

Lcm a partir de la factorización

Si $a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ y $b = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$, entonces

$$\text{lcm}(a, b) = p_1^{\max\{a_1,b_1\}} p_2^{\max\{a_2,b_2\}} \cdots p_r^{\max\{a_r,b_r\}}.$$

Ejemplo

$120 = 2^3 \cdot 3 \cdot 5$ y $500 = 2^2 \cdot 5^3$, entonces

$$\text{lcm}(120, 500) = 2^3 \cdot 3^1 \cdot 5^3 = 3000.$$

Mínimo común múltiplo

Proposición

$m = \mathrm{lcm}(a, b)$ *si y solo si*

$$(1)\, m > 0, \qquad (2)\, a|m, b|m, \qquad (3)\, a|n, b|n \text{ entonces } m|n.$$

En términos de congruencias, si $a \equiv b (\mathrm{mod}\ m_1)$ y $a \equiv b (\mathrm{mod}\ m_2)$, entonces $a \equiv b (\mathrm{mod}\ \mathrm{lcm}(m_1, m_2))$.

Si $\gcd(m_1, m_2) = 1$, entonces $a \equiv b (\mathrm{mod}\ m_1 m_2)$.

Ejercicio: Relación entre gcd y lcm

Para todo $a, b \in \mathbb{N}^+$, se satisface que

$$a \cdot b = \gcd(a, b) \cdot \mathsf{lcm}(a, b).$$

Indicación: Comprobar primero la relación

$$\min\{x, y\} + \max\{x, y\} = x + y.$$