IIC1253 Matemáticas Discretas

Sasha Kozachinskiy

DCC UC

10.11.2025

Hoy...

Teoría de números: MCD, identidad de Bezout,algoritmo extendido de Euclides

Máximo común divisor

Definición

Sean $a, b \in \mathbb{Z}$*. El* **máximo común divisor** *de* a, b*, denotado como* $\mathrm{MCD}(a, b)$ *es el máximo* $d \in \mathbb{N}$ *tal que* $d|a, d|b$*.*

Máximo común divisor

Definición

Sean $a, b \in \mathbb{Z}$. *El* **máximo común divisor** *de* a, b, *denotado como* $\mathrm{MCD}(a, b)$ *es el máximo* $d \in \mathbb{N}$ *tal que* $d|a, d|b$.

- $\mathrm{MCD}(0, 0) = +\infty$.

Máximo común divisor

Definición

Sean $a, b \in \mathbb{Z}$*. El* **máximo común divisor** *de* a, b*, denotado como* $\mathrm{MCD}(a, b)$ *es el máximo* $d \in \mathbb{N}$ *tal que* $d|a, d|b$*.*

- $\mathrm{MCD}(0, 0) = +\infty$.
- si $a \neq 0$, entonces $1 \leq \mathrm{MCD}(a, b) \leq |a|$ para todo $b \in \mathbb{Z}$.

Máximo común divisor

Definición

Sean $a, b \in \mathbb{Z}$. El **máximo común divisor** *de a, b, denotado como $\mathrm{MCD}(a, b)$ es el máximo $d \in \mathbb{N}$ tal que $d|a, d|b$.*

- $\mathrm{MCD}(0, 0) = +\infty$.
- si $a \neq 0$, entonces $1 \leq \mathrm{MCD}(a, b) \leq |a|$ para todo $b \in \mathbb{Z}$.
- $\mathrm{MCD}(10, 0) =$

Máximo común divisor

Definición

Sean $a, b \in \mathbb{Z}$*. El* **máximo común divisor** *de* a, b*, denotado como* $\mathrm{MCD}(a, b)$ *es el máximo* $d \in \mathbb{N}$ *tal que* $d|a, d|b$*.*

- $\mathrm{MCD}(0,0) = +\infty$.
- si $a \neq 0$, entonces $1 \leq \mathrm{MCD}(a, b) \leq |a|$ para todo $b \in \mathbb{Z}$.
- $\mathrm{MCD}(10,0) =$
- $\mathrm{MCD}(-4,-6) =$

Máximo común divisor

Definición

Sean $a, b \in \mathbb{Z}$. El **máximo común divisor** *de a, b, denotado como $\mathrm{MCD}(a, b)$ es el máximo $d \in \mathbb{N}$ tal que $d|a, d|b$.*

- $\mathrm{MCD}(0, 0) = +\infty$.
- si $a \neq 0$, entonces $1 \leq \mathrm{MCD}(a, b) \leq |a|$ para todo $b \in \mathbb{Z}$.
- $\mathrm{MCD}(10, 0) =$
- $\mathrm{MCD}(-4, -6) =$

Definición

Los números $a, b \in \mathbb{Z}$ se llaman **coprimos** *si $\mathrm{MCD}(a, b) = 1$.*

Propiedades simples de MCD

Proposición

a) *Sea* $b \in \mathbb{Z}, b \neq 0$. *Entonces,* $\mathrm{MCD}(a, b) = |b|$ *si y sólo si* $b|a$ *para todo* $a \in \mathbb{Z}$.

b) *para todo* $a, b \in \mathbb{Z}$ *tal que* $(a, b) \neq (0, 0)$, *tenemos que* $a/\mathrm{MCD}(a, b)$, $b/\mathrm{MCD}(a, b)$ *son coprimos.*

Preguntas MCD

Encuentren todos los posibles valores de

a) $\mathrm{MCD}(n, 12)$;

b) $\mathrm{MCD}(n, n+1)$;

c) $\mathrm{MCD}(n, n+6)$.

Identidad de Bezout

Teorema

Para todo $a, b \in \mathbb{Z}, (a, b) \neq (0, 0)$ *existen* $u, v \in \mathbb{Z}$ *tal que* $au + bv = \mathrm{MCD}(a, b)$.

Ejemplo

Encuentre $u, v \in \mathbb{Z}$ *tales que:*

a) $2u + 7v = \mathrm{MCD}(2, 7)$

b) $12u + 20v = \mathrm{MCD}(12, 20)$

Aplicaciones: maximalidad de MCD

Proposición

Sean $a, b \in \mathbb{Z}$ *tal que* $(a, b) \neq (0, 0)$. *Entonces,* $d | \mathrm{MCD}(a, b)$ *para todo divisor común* d *de* a *y* b.

Aplicaciones: inverso modular

Proposición

Sean $a, m \in \mathbb{Z}, m > 0$*. Entonces, existe* $x \in \mathbb{Z}$ *tal que* $ax \equiv_m 1$ *si y sólo si* a, m *son coprimos.*

Aplicaciones: inverso modular

Proposición

Sean $a, m \in \mathbb{Z}, m > 0$. *Entonces, existe* $x \in \mathbb{Z}$ *tal que* $ax \equiv_m 1$ *si y sólo si* a, m *son coprimos.*

Ejemplo

Encuentre el inverso de 3 *módulo* 7.

Divisibilidad y coprimos

Proposición

Sean $a, b, c \in \mathbb{Z}$ *tal que* a, b *son comprimos. Si* $a | bc$, *entonces* $a | c$.

Teorema fundamental de aritmética

Definición

Un número natural $p \geq 2$ *se llama primo si no posee divisores en* $(1, p)$.

Teorema fundamental de aritmética

Definición

Un número natural $p \geq 2$ se llama primo si no posee divisores en $(1, p)$.

Teorema

Sean $p_1, \ldots, p_n$ distintos números primos y $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ tal que

$$p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n} = p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n}.$$

Entonces, $\alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n$.

¿Como encontrar $\mathrm{MCD}(a, b)$ rápido?

Lema

Sean $a > b > 0$ enteros y $q, r \in \mathbb{Z}$ tal que

$$a = qb + r, \qquad 0 \leq r < b.$$

Entonces, $\mathrm{MCD}(a, b) = \mathrm{MCD}(b, q)$.

El algoritmo de Euclides

Algorithm 1: Input: $a > b > 0$, output: $\mathrm{MCD}(a, b)$

```
while b ≠ 0 do
    Encuentre q, r ∈ ℤ tal que a = bq + r, 0 ≤ r < b ;
    a : = b;
    b : = r;
end while
return a;
```

Ejemplo

$a = 2025, b = 1233$

El análisis del algoritmo

Lema

Sean a_i, a_{i+1}, a_{i+2} *tres valores de a consecutivos en una ejecución del algoritmo de Euclides. Entonces,* $a_{i+2} < a_i/2$.

Corolario

El algoritmo de Euclides demora no más que $O(\log a)$ *pasos.*

¡Gracias!