

IIC1253 Matemáticas Discretas

Sasha Kozachinskiy

DCC UC

19.11.2025

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 $\text{MCD}(a, b)$ 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 $\text{MCD}(a, b)$ es el máximo $d \in \mathbb{N}$ tal que $d|a, d|b$.

► $\text{MCD}(0, 0) = +\infty$.

Máximo común divisor

Definición

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

- ▶ $\text{MCD}(0, 0) = +\infty$.
- ▶ si $a \neq 0$, entonces $1 \leq \text{MCD}(a, b) \leq |a|$ 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 $\text{MCD}(a, b)$ es el máximo $d \in \mathbb{N}$ tal que $d|a, d|b$.

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

Máximo común divisor

Definición

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

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

Máximo común divisor

Definición

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

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

Definición

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

Propiedades simples de MCD

Proposición

- a) *Sea $b \in \mathbb{Z}, b \neq 0$. Entonces, $\text{MCD}(a, b) = |b|$ 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 $a/\text{MCD}(a, b), b/\text{MCD}(a, b)$ son coprimos.*

Preguntas MCD

Encuentren todos los posibles valores de

- a) $\text{MCD}(n, 12)$;
- b) $\text{MCD}(n, n + 1)$;
- c) $\text{MCD}(n, n + 6)$.

Identidad de Bezout

Teorema

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

Ejemplo

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

- a) $2u + 7v = \text{MCD}(2, 7)$
- b) $12u + 20v = \text{MCD}(12, 20)$

Aplicaciones: maximalidad de MCD

Proposición

Sean $a, b \in \mathbb{Z}$ tal que $(a, b) \neq (0, 0)$. Entonces, $d \mid \text{MCD}(a, b)$ 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 coprimos. 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, \dots, p_n distintos números primos y $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n$ tal que

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

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

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

Lema

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

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

Entonces, $\text{MCD}(a, b) = \text{MCD}(b, r)$.

El algoritmo de Euclides

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

```
1 while  $b \neq 0$  do
2   Encuentre  $q, r \in \mathbb{Z}$  tal que  $a = bq + r, 0 \leq r < b$  ;
3    $a := b$ ;
4    $b := r$ ;
5 end while
6 return  $a$ ;
```

Ejemplo

$$a = 77, b = 28$$

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.

El algoritmo extendido

- ▶ El algoritmo de Euclides se puede usar para encontrar los coeficientes de la identidad Bezout.

El algoritmo extendido

- ▶ El algoritmo de Euclides se puede usar para encontrar los coeficientes de la identidad Bezout.
- ▶ $(a, b) \mapsto u, v$ tal que $au + bv = \text{MCD}(a, b)$.

El algoritmo extendido

- ▶ El algoritmo de Euclides se puede usar para encontrar los coeficientes de la identidad Bezout.
- ▶ $(a, b) \mapsto u, v$ tal que $au + bv = \text{MCD}(a, b)$.
- ▶ $a_0 = a, a_1 = b,$

$$a_0 = q_0 a_1 + a_2$$

$$a_1 = q_1 a_2 + a_3$$

$$\vdots$$

$$a_{n-1} = q_{n-1} a_n + a_{n+1}$$

$$a_n = q_n a_{n+1} + 0$$

$$\text{MCD}(a, b) = d = a_{n+1}$$

El algoritmo extendido

- ▶ El algoritmo de Euclides se puede usar para encontrar los coeficientes de la identidad Bezout.
- ▶ $(a, b) \mapsto u, v$ tal que $au + bv = \text{MCD}(a, b)$.
- ▶ $a_0 = a, a_1 = b,$

$$a_0 = q_0 a_1 + a_2$$

$$a_1 = q_1 a_2 + a_3$$

$$\vdots$$

$$a_{n-1} = q_{n-1} a_n + a_{n+1}$$

$$a_n = q_n a_{n+1} + 0$$

$$\text{MCD}(a, b) = d = a_{n+1}$$

$$d = a_{n-1} + q_{n-1} a_n$$

$$\vdots$$

$$d = ua_i + va_{i+1}$$

$$\implies$$

$$d = ua_i + v(a_{i-1} - q_{i-1}a_i)$$

Ejercicio

Encuentre los coeficientes de la identidad Bezout para $a = 45, b = 17$.

¡Gracias!