Elementos de aritmética (1)
(Teoría de números)

Computación Cuántica: Algorítmica y Software

Joaquín Keller

2026 UCV

Divisibilidad y división euclidiana

$a \in \mathbb{Z} \quad b \in \mathbb{Z}^* \qquad b|a \iff \exists k \in \mathbb{Z} \;\; a = kb$

$b|a$: Se lee "b divide a" – "b es un divisor de a" – "a es divisible por b"

Los divisores de a: $\mathcal{D}(a) = \{x \in \mathbb{Z}^* \mid x|a\}$ [nota: $\mathcal{D}(0) = \mathbb{Z}^*$]

División entera o euclidiana: $a = qb + r \qquad 0 \leq r < b \quad r, b \in \mathbb{N}$

q: cociente r: resto a:dividendo b:divisor

$r = 0 \Leftrightarrow b|a$ Python: `q=a//b` `r=a%b`

Máximo Común Divisor

$a, b \in \mathbb{Z} \quad (a, b) \neq (0, 0) \qquad mcd(a, b) = max\,(\mathcal{D}(a) \cap \mathcal{D}(b))$

$mcd(a, 0) = mcd(a, a) = a$ (ya que $a|0$ y $a|a$)

Ejemplo $mcd(12, 18)$:
$\mathcal{D}(12) = \{1, 2, 3, 4, 6, 12\} \quad \mathcal{D}(18) = \{1, 2, 3, 6, 9, 18\}$
Divisores comunes a 12 y 18: $\mathcal{D}(12) \cap \mathcal{D}(18) = \{1, 2, 3, \mathbf{6}\}$
Resultado: $mcd(12, 18) = 6$

Definición: a y b son *coprimos* (primos entre sí) ssi $mcd(a, b) = 1$

Algoritmo de Euclides par calcular el mcd (1)

$a, b \in \mathbb{N} \quad a > b$ división entera de a por b: $a = qb + r$

$\mathcal{D}(b) \cap \mathcal{D}(r) \subseteq \mathcal{D}(a)$ (ya que $a = qb + r$)

$\mathcal{D}(a) \cap \mathcal{D}(b) \subseteq \mathcal{D}(r)$ (ya que $r = a - qb$)

$$\mathcal{D}(b) \cap \mathcal{D}(r) \cap \mathcal{D}(b) \subseteq \mathcal{D}(a) \cap \mathcal{D}(b) \qquad \mathcal{D}(b) \cap \mathcal{D}(a) \cap \mathcal{D}(b) \subseteq \mathcal{D}(b) \cap \mathcal{D}(r)$$

$$\mathcal{D}(b) \cap \mathcal{D}(r) \subseteq \mathcal{D}(a) \cap \mathcal{D}(b) \qquad \mathcal{D}(a) \cap \mathcal{D}(b) \subseteq \mathcal{D}(b) \cap \mathcal{D}(r)$$

$$\Longrightarrow \mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r)$$

Los divisores comunes de a y b son idénticos a los de b y r

Conclusión: $\boxed{mcd(a, b) = mcd(b, r)}$

Algoritmo de Euclides par calcular el mcd (2)

$a, b \in \mathbb{N} \quad a > b > 0$ $\qquad$ $\boxed{mcd(a,b) = mcd(b,r)}$

Repetir:

dividir a por $b \longrightarrow a = qb + r$

reemplazar (a, b) por (b, r)

Hasta que $b = 0 \longrightarrow mcd(a, 0) = a$

Hemos demostrado también $\mathcal{D}(mcd(a,b)) = \mathcal{D}(a) \cap \mathcal{D}(b)$

Complejidad inferior a $\mathcal{O}(n^3)$ $\qquad$ n: número de dígitos de a y b

Números primos

Un entero $p > 1$ es *primo* ssi sus únicos divisores positivos son 1 y p

Los números primos: $\{p \in \mathbb{N} \mid \mathcal{D}^+(p) = \{1, p\} \wedge p > 1\}$

$\mathcal{D}^+(p) = \mathcal{D}(p) \cap \mathbb{N} = \{k \in \mathbb{N}^* \mid \ k|p\}$ i.e. los divisores positivos de p

Hay una infinidad de números primos (la demostración es de Euclides)

Ejemplos: $2, 3, 5, 7, 11, 13, 17, 23, 29, 31$ (1 no es un número primo)

Descomposición en factores primos

Todo entero $a > 1$ puede escribirse como $a = \prod_{i=1}^{n} p_i^{\alpha_i}$ (Euclides)

Los p_i son primos, los $\alpha_i \in \mathbb{N}^*$ y $p_i < p_{i+1}$

Esa descomposición es única (demostración por Gauss en 1798)

Descomposición alternativa: $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$ $\alpha_i \in \mathbb{N}$

$b = \prod_{i=1}^{\infty} p_i^{\beta_i}$ $ab = \prod_{i=1}^{\infty} p_i^{\alpha_i+\beta_i}$