

IIC1253 Matemáticas Discretas

Sasha Kozachinskiy

DCC UC

01.09.2025

Hoy...

Teoría de números: divisibilidad, división euclídea

Divisibilidad

Definición

Sean $a, b \in \mathbb{Z}$. Entonces, $a|b$ si existe $k \in \mathbb{Z}$ tal que $ak = b$.

Divisibilidad

Definición

Sean $a, b \in \mathbb{Z}$. Entonces, $a|b$ si existe $k \in \mathbb{Z}$ tal que $ak = b$.

Nota: $1|a$, $(-1)|a$ para todo $a \in \mathbb{Z}$;

Divisibilidad

Definición

Sean $a, b \in \mathbb{Z}$. Entonces, $a|b$ si existe $k \in \mathbb{Z}$ tal que $ak = b$.

Nota: $1|a$, $(-1)|a$ para todo $a \in \mathbb{Z}$;

Nota: $a|0$ para todo $a \in \mathbb{Z}$.

¿Verdadero o falso?

Ejercicio

- a) si $a|b, b|c$, entonces $a|c$;
- b) si $a|b, a|c$, entonces $a|(b + c)$;
- c) si $ac|bc$, entonces $a|b$;
- d) si $a|b$, entonces $ac|bc$.

el teorema de división euclídea

Teorema

Para todo $a, b \in \mathbb{Z}$, $b \neq 0$ existen los únicos $q \in \mathbb{Z}$ (el cociente de división) y r (el resto de división) tales que:

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

Ejercicios de división euclídea

Ejercicio

Encontrar el cociente y el resto cuando el dividiente a y el divisor b son:

- a) $a = -24, b = -10$
- b) $a = 1996, b = -17$
- c) $a = n^2 + n + 1, b = n + 1$ para $n \in \mathbb{N}$.

Ejercicios de división euclídea

Ejercicio

- a) $2|n^2 - n$ para todo n ;
- b) si $2 \nmid k, 3 \nmid k, 5 \nmid k$, entonces $240|k^4 - 1$ para todo $k \in \mathbb{Z}$.

Aritmética modular

Definición

Sean $a, b, k \in \mathbb{Z}$, $k \neq 0$. Entonces, a, b son congruentes módulo k si $k|(a - b)$.

Aritmética modular

Definición

Sean $a, b, k \in \mathbb{Z}$, $k \neq 0$. Entonces, a, b son congruentes módulo k si $k|(a - b)$.

Notación: $a \equiv_k b$, $a \equiv b \pmod{k}$.

Aritmética modular

Definición

Sean $a, b, k \in \mathbb{Z}$, $k \neq 0$. Entonces, a, b son congruentes módulo k si $k|(a - b)$.

Notación: $a \equiv_k b$, $a \equiv b \pmod{k}$.

Proposición

Sean $a, b, k \in \mathbb{Z}$, $k \neq 0$. Entonces, $a \equiv_k b$ si i sólo si a, b tienen el mismo resto de la división sobre k .

Aritmética modular y operaciones aritméticas

Proposición

Sean $a_1, a_2, b_1, b_2, k \in \mathbb{Z}$, $k \neq 0$. Si $a_1 \equiv_k a_2$, $b_1 \equiv_k b_2$, entonces:

- a) $a_1 + a_2 \equiv_k b_1 + b_2$;
- b) $a_1 a_2 \equiv_k b_1 b_2$;

Aritmética modular y operaciones aritméticas

Proposición

Sean $a_1, a_2, b_1, b_2, k \in \mathbb{Z}$, $k \neq 0$. Si $a_1 \equiv_k a_2, b_1 \equiv_k b_2$, entonces:

- a) $a_1 + a_2 \equiv_k b_1 + b_2$;
- b) $a_1 a_2 \equiv_k b_1 b_2$;

Ejercicio

- ▶ un número natural n es divisible por 3 si i sólo si la suma de su dígitos es divisible por 3;
- ▶ $37 \mid \underbrace{11 \dots 1}_{2025}$
- ▶ encontrar el último dígito de $2026^{2026^{2026}}$.

¡Gracias!