IIC1253 Matemáticas Discretas

Sasha Kozachinskiy

DCC UC

10.11.2025

Hoy...

Teoría de números: divisibilidad, división euclídea, aritmética modular

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 $a \in \mathbb{Z}$.

$a|0$

¿Verdadero o falso?

Ejercicio

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

a) $a|b \quad b = k_1 \cdot a$ para $k_1 \in \mathbb{Z}$

$b|c \Rightarrow c = k_2 \cdot b \quad k_2 \in \mathbb{Z}$

$c = k_2 \cdot b = \underbrace{k_2 \cdot k_1}\, a$

$\Rightarrow a|c$

b) $a|b \Rightarrow b = k_1 \cdot a$
$c = k_2 a$

para algunos $k_1, k_2 \in \mathbb{N}$

$b + c = k_1 \cdot a + k_2 a = \underbrace{(k_1 + k_2)}_{k_3} a \Rightarrow a | b+c$

c) $ac \mid bc \Rightarrow a \mid b$

$a=3$, $\cancel{c=2}$, $b=2$, $c=0$ ~ es un contraejemplo

$0 \mid 0$, $3 \nmid 2$.

d) $a \mid b \Rightarrow ac \mid bc$

$a \mid b \Rightarrow \exists k \in \mathbb{Z}$ $b = ka \Rightarrow$ $\cancel{a}$ $b \cdot c =$

$= k \cdot a \cdot c$

$\Rightarrow$ $\cancel{a}$ $ac \mid bc$

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) y* r *(el resto) tales que:*

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

Ejercicios de división euclídea

$24, 10 \quad 0 \le 4 < 10$

$24 = 2 \cdot 10 + 4$

Ejercicio

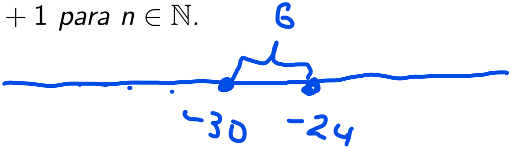
Encontrar el cociente y el resto cuando el dividendo a y el divisor b son:

$-24 = 2 \cdot (-10) - 4$

a) $a = -24, b = -10$

b) $a = 1996, b = -17$

c) $a = n^2 + n + 1, b = n + 1$ *para* $n \in \mathbb{N}$.



$a = -24, \; b = -10$

$-24 = 3 \cdot (-10) + 6 \qquad 0 \le 6 < |-10|$

b) $1996 \qquad (-17)$

$r = 7.$

$1996 =$ ~~[illegible]~~

$1700 + 340 = 2040$

$\underline{2040} - 3 \cdot 17 = \underline{1989} =$

Ejercicios de división euclídea

Ejercicio

a) $2 | n^2 - n$ *para todo* n;

b) *si* n *es impar,* $16 | n^4 - 1$;

c) *encontrar todos los posibles restos para el dividendo* $a = 57$.

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

Nota: $k|a \iff a \equiv_k 0$ para todo $a, k \in \mathbb{Z}$, $k \neq 0$.

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: $a \equiv_k b$, $a \equiv b \pmod{k}$.
Nota: $k|a \iff a \equiv_k 0$ para todo $a, k \in \mathbb{Z}$, $k \neq 0$.

Proposición

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

Aritmética modular respete 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) $a_1 a_2 \equiv_k b_1 b_2$;

Aplicaciones – reglas de divisibilidad

Teorema

Sea $n = \overline{d_{m-1} \ldots d_0} \in \mathbb{N}$ *(donde* $d_{m-1}, \ldots, d_0 \in \{0, 1 \ldots, 9\}$ *son dígitos de* n*). Entonces,*

a) $3 | n$ *si y sólo si* $3 | (d_0 + \ldots + d_{m-1})$*;*

b) $9 | n$ *si y sólo si* $9 | (d_0 + \ldots + d_{m-1})$

c) $11 | n$ *si y sólo si* $11 | (d_0 - d_1 + d_2 - \ldots + (-1)^{m-1} d_{m-1})$

Más ejercicios

Ejercicio

- $37 | \underbrace{11\ldots1}_{2025}$
- *encontrar el último dígito de* $1993^{1993^{1993}}$.

¡Gracias!