

Teoria dos Números para as Olimpíadas

Aula 3

Prof. Dr. José Carlos de Souza Júnior

VIII Semana da Matemática & IV Workshop PROFMAT

8 de maio de 2025

Congruência Linear

Problema 5

Qual é o resto que o número 2^{2k+1} , $k \in \mathbb{N}$, deixa quando dividido por 3?

Congruência Linear

Problema 5

Qual é o resto que o número 2^{2k+1} , $k \in \mathbb{N}$, deixa quando dividido por 3?

Observação

Essa questão ilustra a importância de se trabalhar olhando os restos!

Proposição 6

Dados $a, b, n \in \mathbb{Z}$, com $n \neq 0$ e r_a, r_b os restos da divisão por a e b por n , respectivamente, então as seguintes afirmações são verdadeiras:

- (a) O resto de $a + b$ na divisão por n é igual ao resto de $r_a + r_b$ na divisão por n .

Proposição 6

Dados $a, b, n \in \mathbb{Z}$, com $n \neq 0$ e r_a, r_b os restos da divisão por a e b por n , respectivamente, então as seguintes afirmações são verdadeiras:

- (a) O resto de $a + b$ na divisão por n é igual ao resto de $r_a + r_b$ na divisão por n .
- (b) O resto de $a - b$ na divisão por n é igual ao resto de $r_a - r_b$ na divisão por n .

Proposição 6

Dados $a, b, n \in \mathbb{Z}$, com $n \neq 0$ e r_a, r_b os restos da divisão por a e b por n , respectivamente, então as seguintes afirmações são verdadeiras:

- (a) O resto de $a + b$ na divisão por n é igual ao resto de $r_a + r_b$ na divisão por n .
- (b) O resto de $a - b$ na divisão por n é igual ao resto de $r_a - r_b$ na divisão por n .
- (c) O resto de $a \cdot b$ na divisão por n é igual ao resto de $r_a \cdot r_b$ na divisão por n .

Proposição 6

Dados $a, b, n \in \mathbb{Z}$, com $n \neq 0$ e r_a, r_b os restos da divisão por a e b por n , respectivamente, então as seguintes afirmações são verdadeiras:

- (a) O resto de $a + b$ na divisão por n é igual ao resto de $r_a + r_b$ na divisão por n .
- (b) O resto de $a - b$ na divisão por n é igual ao resto de $r_a - r_b$ na divisão por n .
- (c) O resto de $a \cdot b$ na divisão por n é igual ao resto de $r_a \cdot r_b$ na divisão por n .

Lema 7

$n|(a - b) \Leftrightarrow a$ e b deixam o mesmo resto na divisão por n .

Definição (Congruência)

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b).$$

Definição (Congruência)

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b).$$

Observação

Dois números são “iguais” sob a ótica da divisão por n , quando deixam o mesmo resto na divisão por n .

Definição (Congruência)

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b).$$

Observação

Dois números são “iguais” sob a ótica da divisão por n , quando deixam o mesmo resto na divisão por n .

Exemplos

- $5 \equiv 3 \pmod{2}$,

Definição (Congruência)

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b).$$

Observação

Dois números são “iguais” sob a ótica da divisão por n , quando deixam o mesmo resto na divisão por n .

Exemplos

- $5 \equiv 3 \pmod{2}$, pois $2 \mid (5 - 3)$.

Definição (Congruência)

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b).$$

Observação

Dois números são “iguais” sob a ótica da divisão por n , quando deixam o mesmo resto na divisão por n .

Exemplos

- $5 \equiv 3 \pmod{2}$, pois $2 \mid (5 - 3)$.
- $17 \equiv 2 \pmod{3}$,

Definição (Congruência)

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b).$$

Observação

Dois números são “iguais” sob a ótica da divisão por n , quando deixam o mesmo resto na divisão por n .

Exemplos

- $5 \equiv 3 \pmod{2}$, pois $2 \mid (5 - 3)$.
- $17 \equiv 2 \pmod{3}$, pois $3 \mid (17 - 2)$.

Definição (Congruência)

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b).$$

Observação

Dois números são “iguais” sob a ótica da divisão por n , quando deixam o mesmo resto na divisão por n .

Exemplos

- $5 \equiv 3 \pmod{2}$, pois $2 \mid (5 - 3)$.
- $17 \equiv 2 \pmod{3}$, pois $3 \mid (17 - 2)$.
- $20 \not\equiv 3 \pmod{3}$,

Definição (Congruência)

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b).$$

Observação

Dois números são “iguais” sob a ótica da divisão por n , quando deixam o mesmo resto na divisão por n .

Exemplos

- $5 \equiv 3 \pmod{2}$, pois $2 \mid (5 - 3)$.
- $17 \equiv 2 \pmod{3}$, pois $3 \mid (17 - 2)$.
- $20 \not\equiv 3 \pmod{3}$, pois $3 \nmid (20 - 3)$.

Proposição 8 (Classe de Equivalência)

Dados $a, b, c, n \in \mathbb{Z}$, com $n > 1$, então:

(a) $a \equiv a \pmod{n}$, para todo $a \in \mathbb{Z}$.

(Reflexiva)

Proposição 8 (Classe de Equivalência)

Dados $a, b, c, n \in \mathbb{Z}$, com $n > 1$, então:

(a) $a \equiv a \pmod{n}$, para todo $a \in \mathbb{Z}$.

(Reflexiva)

(b) Se $a \equiv b \pmod{n}$, então $b \equiv a \pmod{n}$.

(Simétrica)

Proposição 8 (Classe de Equivalência)

Dados $a, b, c, n \in \mathbb{Z}$, com $n > 1$, então:

- (a) $a \equiv a \pmod{n}$, para todo $a \in \mathbb{Z}$. (Reflexiva)
- (b) Se $a \equiv b \pmod{n}$, então $b \equiv a \pmod{n}$. (Simétrica)
- (c) Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então $a \equiv c \pmod{n}$. (Transitiva)

Proposição 9 (Propriedades)

Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então:

(i) $a + c \equiv b + d \pmod{n}$.

Proposição 9 (Propriedades)

Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então:

- (i) $a + c \equiv b + d \pmod{n}$.
- (ii) $a - c \equiv b - d \pmod{n}$.

Proposição 9 (Propriedades)

Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então:

- (i) $a + c \equiv b + d \pmod{n}$.
- (ii) $a - c \equiv b - d \pmod{n}$.
- (iii) $a + k \equiv b + k \pmod{n}$, para todo $k \in \mathbb{Z}$.

Proposição 9 (Propriedades)

Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então:

- (i) $a + c \equiv b + d \pmod{n}$.
- (ii) $a - c \equiv b - d \pmod{n}$.
- (iii) $a + k \equiv b + k \pmod{n}$, para todo $k \in \mathbb{Z}$.
- (iv) $k \cdot a \equiv k \cdot b \pmod{n}$, para todo $k \in \mathbb{Z}$.

Proposição 9 (Propriedades)

Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então:

- (i) $a + c \equiv b + d \pmod{n}$.
- (ii) $a - c \equiv b - d \pmod{n}$.
- (iii) $a + k \equiv b + k \pmod{n}$, para todo $k \in \mathbb{Z}$.
- (iv) $k \cdot a \equiv k \cdot b \pmod{n}$, para todo $k \in \mathbb{Z}$.
- (v) $a \cdot c \equiv b \cdot d \pmod{n}$.

Proposição 9 (Propriedades)

Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então:

- (i) $a + c \equiv b + d \pmod{n}$.
- (ii) $a - c \equiv b - d \pmod{n}$.
- (iii) $a + k \equiv b + k \pmod{n}$, para todo $k \in \mathbb{Z}$.
- (iv) $k \cdot a \equiv k \cdot b \pmod{n}$, para todo $k \in \mathbb{Z}$.
- (v) $a \cdot c \equiv b \cdot d \pmod{n}$.
- (vi) $a^k \equiv b^k \pmod{n}$, para todo $k \in \mathbb{N}$.

Proposição 9 (Propriedades)

Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então:

- (i) $a + c \equiv b + d \pmod{n}$.
- (ii) $a - c \equiv b - d \pmod{n}$.
- (iii) $a + k \equiv b + k \pmod{n}$, para todo $k \in \mathbb{Z}$.
- (iv) $k \cdot a \equiv k \cdot b \pmod{n}$, para todo $k \in \mathbb{Z}$.
- (v) $a \cdot c \equiv b \cdot d \pmod{n}$.
- (vi) $a^k \equiv b^k \pmod{n}$, para todo $k \in \mathbb{N}$.
- (vii) Se $(k, n) = d$, então

$$k \cdot a \equiv k \cdot b \pmod{n} \Leftrightarrow a \equiv b \pmod{\frac{n}{d}}.$$

Proposição 9 (Propriedades)

Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então:

- (i) $a + c \equiv b + d \pmod{n}$.
- (ii) $a - c \equiv b - d \pmod{n}$.
- (iii) $a + k \equiv b + k \pmod{n}$, para todo $k \in \mathbb{Z}$.
- (iv) $k \cdot a \equiv k \cdot b \pmod{n}$, para todo $k \in \mathbb{Z}$.
- (v) $a \cdot c \equiv b \cdot d \pmod{n}$.
- (vi) $a^k \equiv b^k \pmod{n}$, para todo $k \in \mathbb{N}$.
- (vii) Se $(k, n) = d$, então

$$k \cdot a \equiv k \cdot b \pmod{n} \Leftrightarrow a \equiv b \pmod{\frac{n}{d}}.$$

Em particular, se $(k, n) = 1$, então

$$k \cdot a \equiv k \cdot b \pmod{n} \Leftrightarrow a \equiv b \pmod{n}.$$

Com as propriedades vistas na Proposição 9, o Problema 5 passa a ter uma solução mais simples:

Problema 5

Qual é o resto que o número 2^{2k+1} , $k \in \mathbb{N}$, deixa quando dividido por 3?

Problema 6

Qual é o resto da divisão de 7^{10} por 51?

Problema 6

Qual é o resto da divisão de 7^{10} por 51?

Problema 7

Qual é o resto da divisão de 5^{21} por 127?

Problema 6

Qual é o resto da divisão de 7^{10} por 51?

Problema 7

Qual é o resto da divisão de 5^{21} por 127?

Problema 8

Qual é o resto da divisão de 2^{100} por 11?

Problema 6

Qual é o resto da divisão de 7^{10} por 51?

Problema 7

Qual é o resto da divisão de 5^{21} por 127?

Problema 8

Qual é o resto da divisão de 2^{100} por 11?

Problema 9

Qual é o resto da divisão de $116 + 17^{17}$ por 8?

Problema 10

Qual é o resto da divisão de $13^{16} - 2^{25} \cdot 5^{15}$ por 3?

$$13 \equiv 1 \pmod{3} \Rightarrow 13^{16} \equiv 1 \pmod{3}.$$

$$5 \equiv 2 \pmod{3} \Rightarrow 5^{15} \equiv 2^{15} \pmod{3}.$$

Assim,

$$13^{16} - 2^{25} \cdot 5^{15} \equiv 1 - 2^{25} \cdot 2^{15} \equiv 1 - 40^{20} \pmod{3}.$$

Como $4 \equiv 1 \pmod{3} \Rightarrow 4^{20} \equiv 1 \pmod{3}$. Portanto,

$$13^{16} - 2^{25} \cdot 5^{15} \equiv 1 - 40^{20} \equiv 1 - 1 = 0 \pmod{3}.$$

Consequentemente, o resto é zero!

Problema 11

Qual é o resto da divisão de $1! + 2! + \dots + (10^{10})!$ por 40?

Problema 11

Qual é o resto da divisão de $1! + 2! + \dots + (10^{10})!$ por 40?

Problema 12

Determine o algarismo da unidade de 9^{9^9} .