Teoria dos Números para as Olimpíadas

Aula 1

Prof. Dr. José Carlos de Souza Júnior

VIII Semana da Matemática & IV Workshop PROFMAT

6 de maio de 2025

O que você encontrará nesse curso

Procurando aprimorar seu domínio em Teoria dos Números para as Olimpíadas?

O que você encontrará nesse curso

Procurando aprimorar seu domínio em Teoria dos Números para as Olimpíadas?

Espero que este breve curso te ajude!

O que você encontrará nesse curso

Procurando aprimorar seu domínio em Teoria dos Números para as Olimpíadas?

Espero que este breve curso te ajude!

Iremos abordar alguns conceitos da Teoria dos Números e veremos alguns padrões de ideias usados na resolução de problemas olímpicos.

O que você encontrará nesse curso

Procurando aprimorar seu domínio em Teoria dos Números para as Olimpíadas?

Espero que este breve curso te ajude!

Iremos abordar alguns conceitos da Teoria dos Números e veremos alguns padrões de ideias usados na resolução de problemas olímpicos.

O que você irá aprender/revisar:

O que você encontrará nesse curso

Procurando aprimorar seu domínio em Teoria dos Números para as Olimpíadas?

Espero que este breve curso te ajude!

Iremos abordar alguns conceitos da Teoria dos Números e veremos alguns padrões de ideias usados na resolução de problemas olímpicos.

O que você irá aprender/revisar:

- Divisibilidade e suas propriedades fundamentais.

O que você encontrará nesse curso

Procurando aprimorar seu domínio em Teoria dos Números para as Olimpíadas?

Espero que este breve curso te ajude!

Iremos abordar alguns conceitos da Teoria dos Números e veremos alguns padrões de ideias usados na resolução de problemas olímpicos.

O que você irá aprender/revisar:

- Divisibilidade e suas propriedades fundamentais.
- Relações de Congruência e principais resultados.

O que você encontrará nesse curso

Procurando aprimorar seu domínio em Teoria dos Números para as Olimpíadas?

Espero que este breve curso te ajude!

Iremos abordar alguns conceitos da Teoria dos Números e veremos alguns padrões de ideias usados na resolução de problemas olímpicos.

O que você irá aprender/revisar:

- Divisibilidade e suas propriedades fundamentais.
- Relações de Congruência e principais resultados.
- Teorema Chinês dos Restos e Equações Diofantinas.

Livros recomendados

Livros recomendados em português:

- HEFEZ, A. Aritmética. Coleção PROFMAT. Rio de Janeiro: SBM, 2013.
- MUNIZ NETO, A.C. Tópicos de Matemática Elementar - Volume 5. Coleção Professor de Matemática. Rio de Janeiro: SBM, 2012.

Livros recomendados em inglês:

- ANDREESCU, T.; VENTULLO, A. Number Theory Problems for Mathematics Competitions. Editora: XYZ Press, 2024.
- ANDREESCU, T.; VENTULLO, A. Introduction to Number Theory in Mathematics Contests - Book 1. Editora: XYZ Press, 2023.
- ANDREESCU, T.; VENTULLO, A. Introduction to Number Theory in Mathematics Contests - Book 2. Editora: XYZ Press, 2024.

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Nosso foco é estudar o conjunto dos inteiros sob a ótica da divisão.

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Nosso foco é estudar o conjunto dos inteiros sob a ótica da divisão.

Definição

Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, dizemos que b divide a quando existir $c \in \mathbb{Z}$, tal que

$$a = b \cdot c.$$

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Nosso foco é estudar o conjunto dos inteiros sob a ótica da divisão.

Definição

Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, dizemos que b divide a quando existir $c \in \mathbb{Z}$, tal que

$$a = b \cdot c.$$

- b é um divisor de a;

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Nosso foco é estudar o conjunto dos inteiros sob a ótica da divisão.

Definição

Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, dizemos que b divide a quando existir $c \in \mathbb{Z}$, tal que

$$a = b \cdot c.$$

- b é um divisor de a;
- a é um múltiplo de b;

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Nosso foco é estudar o conjunto dos inteiros sob a ótica da divisão.

Definição

Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, dizemos que b divide a quando existir $c \in \mathbb{Z}$, tal que

$$a = b \cdot c.$$

- b é um divisor de a;
- a é um múltiplo de b;
- Notação: $b|a$ *(b divide a)* ou $b \nmid a$ *(b não divide a)*.

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Nosso foco é estudar o conjunto dos inteiros sob a ótica da divisão.

Definição

Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, dizemos que b divide a quando existir $c \in \mathbb{Z}$, tal que

$$a = b \cdot c.$$

- b é um divisor de a;
- a é um múltiplo de b;
- Notação: $b|a$ *(b divide a)* ou $b \nmid a$ *(b não divide a)*.

Exemplos

- $2|10$,

$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

Nosso foco é estudar o conjunto dos inteiros sob a ótica da divisão.

Definição

Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, dizemos que b divide a quando existir $c \in \mathbb{Z}$, tal que

$$a = b \cdot c.$$

- b é um divisor de a;
- a é um múltiplo de b;
- Notação: $b|a$ *(b divide a)* ou $b \nmid a$ *(b não divide a)*.

Exemplos

- $2|10$, pois $10 = 2 \cdot 5$.

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Nosso foco é estudar o conjunto dos inteiros sob a ótica da divisão.

Definição

Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, dizemos que b divide a quando existir $c \in \mathbb{Z}$, tal que

$$a = b \cdot c.$$

- b é um divisor de a;
- a é um múltiplo de b;
- Notação: $b|a$ *(b divide a)* ou $b \nmid a$ *(b não divide a)*.

Exemplos

- $2|10$, pois $10 = 2 \cdot 5$.
- $3|27$,

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Nosso foco é estudar o conjunto dos inteiros sob a ótica da divisão.

Definição

Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, dizemos que b divide a quando existir $c \in \mathbb{Z}$, tal que

$$a = b \cdot c.$$

- b é um divisor de a;
- a é um múltiplo de b;
- Notação: $b|a$ *(b divide a)* ou $b \nmid a$ *(b não divide a)*.

Exemplos

- $2|10$, pois $10 = 2 \cdot 5$.
- $3|27$, pois $27 = 3 \cdot 9$.

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Nosso foco é estudar o conjunto dos inteiros sob a ótica da divisão.

Definição

Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, dizemos que b divide a quando existir $c \in \mathbb{Z}$, tal que

$$a = b \cdot c.$$

- b é um divisor de a;
- a é um múltiplo de b;
- Notação: $b|a$ *(b divide a)* ou $b \nmid a$ *(b não divide a)*.

Exemplos

- $2|10$, pois $10 = 2 \cdot 5$.
- $3|27$, pois $27 = 3 \cdot 9$.
- $5 \nmid 17$,

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Nosso foco é estudar o conjunto dos inteiros sob a ótica da divisão.

Definição

Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, dizemos que b divide a quando existir $c \in \mathbb{Z}$, tal que

$$a = b \cdot c.$$

- b é um divisor de a;
- a é um múltiplo de b;
- Notação: $b|a$ *(b divide a)* ou $b \nmid a$ *(b não divide a)*.

Exemplos

- $2|10$, pois $10 = 2 \cdot 5$.
- $3|27$, pois $27 = 3 \cdot 9$.
- $5 \nmid 17$, pois não existe $n \in \mathbb{Z}$ tal que $17 = 5 \cdot n$.

Proposição 1

Dados $a, b \in \mathbb{Z}^*, x, y \in \mathbb{Z}$, então valem:

(i) Se $a|b$, então $|a| \leq |b|$.

(ii) Se $a|b$ e $b|a$, então $a = \pm b$.

(iii) Se $c|a$ e $c|b$, então $c|(ax + by)$.

Proposição 1

Dados $a, b \in \mathbb{Z}^*, x, y \in \mathbb{Z}$, então valem:

(i) Se $a|b$, então $|a| \leq |b|$.

(ii) Se $a|b$ e $b|a$, então $a = \pm b$.

(iii) Se $c|a$ e $c|b$, então $c|(ax + by)$.

Problema 1

Se o número $\overline{abc}$ é divisível por 37, mostre que a somas dos números $\overline{bca}$ e $\overline{cab}$ também é divisível por 37.

Algoritmo da Divisão

Teorema 2 (Divisão Euclidiana)

Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, existem únicos q e r inteiros tais que

$$a = b \cdot q + r, \text{ com } 0 \leq r < |b|.$$

Algoritmo da Divisão

Teorema 2 (Divisão Euclidiana)

Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, existem únicos q e r inteiros tais que

$$a = b \cdot q + r, \text{ com } 0 \leq r < |b|.$$

q recebe o nome de quociente e r é chamado de resto da divisão de a por b.

Algoritmo da Divisão

Teorema 2 (Divisão Euclidiana)

Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, existem únicos q e r inteiros tais que

$$a = b \cdot q + r, \text{ com } 0 \leq r < |b|.$$

q recebe o nome de quociente e r é chamado de resto da divisão de a por b.

Exemplos

- O quociente e o resto da divisão de 19 por 5 são

Algoritmo da Divisão

Teorema 2 (Divisão Euclidiana)

Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, existem únicos q e r inteiros tais que

$$a = b \cdot q + r, \text{ com } 0 \leq r < |b|.$$

q recebe o nome de quociente e r é chamado de resto da divisão de a por b.

Exemplos

- O quociente e o resto da divisão de 19 por 5 são $q = 3$ e $r = 4$, pois $19 = 5 \cdot \underbrace{(3)}_{q} + \underbrace{4}_{r}$, sendo $0 \leq 4 < |5|$.

Algoritmo da Divisão

Teorema 2 (Divisão Euclidiana)

Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, existem únicos q e r inteiros tais que

$$a = b \cdot q + r, \text{ com } 0 \leq r < |b|.$$

q recebe o nome de quociente e r é chamado de resto da divisão de a por b.

Exemplos

- O quociente e o resto da divisão de 19 por 5 são $q = 3$ e $r = 4$, pois $19 = 5 \cdot \underbrace{(3)}_{q} + \underbrace{4}_{r}$, sendo $0 \leq 4 < |5|$.
- O quociente e o resto da divisão de -26 por -8 são

Algoritmo da Divisão

Teorema 2 (Divisão Euclidiana)

Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, existem únicos q e r inteiros tais que

$$a = b \cdot q + r, \text{ com } 0 \leq r < |b|.$$

q recebe o nome de quociente e r é chamado de resto da divisão de a por b.

Exemplos

- O quociente e o resto da divisão de 19 por 5 são $q = 3$ e $r = 4$, pois $19 = 5 \cdot \underbrace{(3)}_{q} + \underbrace{4}_{r}$, sendo $0 \leq 4 < |5|$.
- O quociente e o resto da divisão de -26 por -8 são $q = 4$ e $r = 6$, pois $-26 = (-8) \cdot \underbrace{(4)}_{q} + \underbrace{6}_{r}$, sendo $0 \leq 6 < |-8|$.

Problema 2 (OBM 97)

No edifício mais alto de *Terra Brasilis* moram Eduardo e Augusto. O número do andar do apartamento de Eduardo coincide com o número do apartamento de Augusto. A soma dos números dos dois apartamentos é 2164. Calcule o número do apartamento de Eduardo, sabendo que há 12 apartamentos por andar. (por exemplo, no primeiro andar estão os apartamentos de 1 a 12, no segundo de 13 a 24, e assim por diante.)

Máximo Divisor Comum

Definição

Dados $a, b \in \mathbb{Z}^*$, o máximo divisor comum de a e b é o maior dentre os divisores de a e b.

Máximo Divisor Comum

Definição

Dados $a, b \in \mathbb{Z}^*$, o máximo divisor comum de a e b é o maior dentre os divisores de a e b.

Notação: $mdc(a, b)$ ou (a, b).

Máximo Divisor Comum

Definição

Dados $a, b \in \mathbb{Z}^*$, o máximo divisor comum de a e b é o maior dentre os divisores de a e b.

Notação: $mdc(a, b)$ ou (a, b).

Exemplo

Divisores de 12: $\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$.

Máximo Divisor Comum

Definição

Dados $a, b \in \mathbb{Z}^*$, o máximo divisor comum de a e b é o maior dentre os divisores de a e b.

Notação: $mdc(a, b)$ ou (a, b).

Exemplo

Divisores de 12: $\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$.

Divisores de 18: $\{\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18\}$.

Máximo Divisor Comum

Definição

Dados $a, b \in \mathbb{Z}^*$, o máximo divisor comum de a e b é o maior dentre os divisores de a e b.

Notação: $mdc(a, b)$ ou (a, b).

Exemplo

Divisores de 12: $\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$.

Divisores de 18: $\{\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18\}$.

Assim, $(12, 18) = 6$.

Máximo Divisor Comum

Observação

- $(a, b) \geq 1$.

Máximo Divisor Comum

Observação

- $(a, b) \geq 1$. Pois se $d|a$, então $-d|a$.

Máximo Divisor Comum

Observação

- $(a, b) \geq 1$. Pois se $d|a$, então $-d|a$. Estamos interessados no maior. Portanto, positivo!

Máximo Divisor Comum

Observação

- $(a, b) \geq 1$. Pois se $d|a$, então $-d|a$. Estamos interessados no maior. Portanto, positivo!
- Se $d = (a, b)$, então $d|a$ e $d|b$.

Máximo Divisor Comum

Observação

- $(a, b) \geq 1$. Pois se $d|a$, então $-d|a$. Estamos interessados no maior. Portanto, positivo!
- Se $d = (a, b)$, então $d|a$ e $d|b$. Segue da Proposição 1 que $d|(ax + by)$, para todo $x, y \in \mathbb{Z}$.

Máximo Divisor Comum

Observação

- $(a, b) \geq 1$. Pois se $d|a$, então $-d|a$. Estamos interessados no maior. Portanto, positivo!
- Se $d = (a, b)$, então $d|a$ e $d|b$. Segue da Proposição 1 que $d|(ax + by)$, para todo $x, y \in \mathbb{Z}$.
- Se $(a, b) = 1$, dizemos que a e b são primos entre si.

Máximo Divisor Comum

Teorema 3 (Bézout)

Dados $a, b \in \mathbb{Z}^*$, existem $x_0, y_0 \in \mathbb{Z}$, tais que

$$(a, b) = ax_0 + by_0.$$

Máximo Divisor Comum

Teorema 3 (Bézout)

Dados $a, b \in \mathbb{Z}^*$, existem $x_0, y_0 \in \mathbb{Z}$, tais que

$$(a, b) = ax_0 + by_0.$$

Exemplo

Vimos que $(12, 18) = 6$.

Máximo Divisor Comum

Teorema 3 (Bézout)

Dados $a, b \in \mathbb{Z}^*$, existem $x_0, y_0 \in \mathbb{Z}$, tais que

$$(a, b) = ax_0 + by_0.$$

Exemplo

Vimos que $(12, 18) = 6$. Temos que

$$6 = 12 \cdot (-1) + 18 \cdot (1).$$