Teoria dos Números para as Olimpíadas

Aula 2

Prof. Dr. José Carlos de Souza Júnior

VIII Semana da Matemática & IV Workshop PROFMAT

7 de maio de 2025

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

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

Máximo Divisor Comum

Proposição 4

Dados $a, b, c \in \mathbb{Z}^*$, valem:

(i) (Lema de Gauss) Se $a|(b \cdot c)$ e $(a, b) = 1$, então $a|c$.

Máximo Divisor Comum

Proposição 4

Dados $a, b, c \in \mathbb{Z}^*$, valem:

(i) (Lema de Gauss) Se $a|(b \cdot c)$ e $(a, b) = 1$, então $a|c$.

(ii) $(a, b) = (b, a - bq)$.

Máximo Divisor Comum

Proposição 4

Dados $a, b, c \in \mathbb{Z}^*$, valem:

(i) (Lema de Gauss) Se $a|(b \cdot c)$ e $(a, b) = 1$, então $a|c$.

(ii) $(a, b) = (b, a - bq)$.

(iii) Se $(a, b) = 1$, $a|c$ e $b|c$, então $ab|c$.

Máximo Divisor Comum

Proposição 4

Dados $a, b, c \in \mathbb{Z}^*$, valem:

(i) (Lema de Gauss) Se $a|(b \cdot c)$ e $(a, b) = 1$, então $a|c$.

(ii) $(a, b) = (b, a - bq)$.

(iii) Se $(a, b) = 1$, $a|c$ e $b|c$, então $ab|c$.

Observação

Segue da Proposição 4 (ii) que o máximo divisor comum entre a e b é igual ao máximo divisor comum entre b e o resto da divisão de a por b!

Máximo Divisor Comum

Proposição 4

Dados $a, b, c \in \mathbb{Z}^*$, valem:

(i) (Lema de Gauss) Se $a|(b \cdot c)$ e $(a, b) = 1$, então $a|c$.

(ii) $(a, b) = (b, a - bq)$.

(iii) Se $(a, b) = 1$, $a|c$ e $b|c$, então $ab|c$.

Observação

Segue da Proposição 4 (ii) que o máximo divisor comum entre a e b é igual ao máximo divisor comum entre b e o resto da divisão de a por b! Esse resultado nos leva a um método prático para o cálculo do mdc conhecido como Método de Euclides.

Máximo Divisor Comum

Exemplo

Calcule o máximo divisor comum entre 372 e 162.

Máximo Divisor Comum

Exemplo

Calcule o máximo divisor comum entre 372 e 162.

quociente				
372	162			
resto				

Máximo Divisor Comum

Exemplo

Calcule o máximo divisor comum entre 372 e 162.

quociente	2			
372	162			
resto	48			

Máximo Divisor Comum

Exemplo

Calcule o máximo divisor comum entre 372 e 162.

quociente	2			
372	162	48		
resto	48			

Máximo Divisor Comum

Exemplo

Calcule o máximo divisor comum entre 372 e 162.

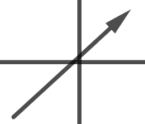
quociente	2	3		
372	162	48		
resto	48	18		

Máximo Divisor Comum

Exemplo

Calcule o máximo divisor comum entre 372 e 162.

quociente	2	3		
372	162	48	18	
resto	48	18		



Máximo Divisor Comum

Exemplo

Calcule o máximo divisor comum entre 372 e 162.

quociente	2	3	2	
372	162	48	18	
resto	48	18	12	

Máximo Divisor Comum

Exemplo

Calcule o máximo divisor comum entre 372 e 162.

quociente	2	3	2		
372	162	48	18	12	
resto	48	18	12		

Máximo Divisor Comum

Exemplo

Calcule o máximo divisor comum entre 372 e 162.

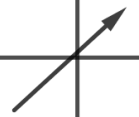
quociente	2	3	2	1	
372	162	48	18	12	
resto	48	18	12	6	

Máximo Divisor Comum

Exemplo

Calcule o máximo divisor comum entre 372 e 162.

quociente	2	3	2	1	
372	162	48	18	12	6
resto	48	18	12	6	



Máximo Divisor Comum

Exemplo

Calcule o máximo divisor comum entre 372 e 162.

quociente	2	3	2	1	2
372	162	48	18	12	$\boxed{6}$
resto	48	18	12	6	0

Máximo Divisor Comum

Exemplo

Calcule o máximo divisor comum entre 372 e 162.

quociente	2	3	2	1	2
372	162	48	18	12	$\boxed{6}$
resto	48	18	12	6	0

Logo, $(372, 162) = 6$.

Máximo Divisor Comum

Problema 3 (IMO 1959)

Se n é um número natural, mostre que $\frac{21n+4}{14n+3}$ é irredutível.

Máximo Divisor Comum

Problema 3 (IMO 1959)

Se n é um número natural, mostre que $\frac{21n+4}{14n+3}$ é irredutível.

Proposição 4

Dados $a, b, c \in \mathbb{Z}^*$, valem:

(i) (Lema de Gauss) Se $a|(b \cdot c)$ e $(a, b) = 1$, então $a|c$.

(ii) $(a, b) = (b, a - bq)$.

(iii) Se $(a, b) = 1$, $a|c$ e $b|c$, então $ab|c$.

Números Primos

Definição

Um número inteiro $p > 1$ é primo se seus únicos divisores positivos forem 1 e p.

Números Primos

Definição

Um número inteiro $p > 1$ é primo se seus únicos divisores positivos forem 1 e p.

Observação

- 1 não é primo.

Números Primos

Definição

Um número inteiro $p > 1$ é primo se seus únicos divisores positivos forem 1 e p.

Observação

- 1 não é primo.
- Os números primos são positivos.

Números Primos

Definição

Um número inteiro $p > 1$ é primo se seus únicos divisores positivos forem 1 e p.

Observação

- 1 não é primo.
- Os números primos são positivos.
- Se p não é primo, então dizemos que ele é composto.

Números Primos

Definição

Um número inteiro $p > 1$ é primo se seus únicos divisores positivos forem 1 e p.

Observação

- 1 não é primo.
- Os números primos são positivos.
- Se p não é primo, então dizemos que ele é composto.
- 2 é o único primo par.

Números Primos

Proposição 5

(i) O conjunto dos números primos é infinito.

Números Primos

Proposição 5

(i) O conjunto dos números primos é infinito.

(ii) Todo inteiro $n > 1$ pode ser expresso como um produto de números primos, não necessariamente distintos.

Números Primos

Proposição 5

(i) O conjunto dos números primos é infinito.

(ii) Todo inteiro $n > 1$ pode ser expresso como um produto de números primos, não necessariamente distintos.

(iii) Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p|ab$, então $p|a$ ou $p|b$.

Números Primos

Proposição 5

(i) O conjunto dos números primos é infinito.

(ii) Todo inteiro $n > 1$ pode ser expresso como um produto de números primos, não necessariamente distintos.

(iii) Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p|ab$, então $p|a$ ou $p|b$.

Exemplos

- $15 = 3 \cdot 5$.

Números Primos

Proposição 5

(i) O conjunto dos números primos é infinito.

(ii) Todo inteiro $n > 1$ pode ser expresso como um produto de números primos, não necessariamente distintos.

(iii) Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p|ab$, então $p|a$ ou $p|b$.

Exemplos

- $15 = 3 \cdot 5$.
- $60 = 2 \cdot 2 \cdot 3 \cdot 5$

Números Primos

Proposição 5

(i) O conjunto dos números primos é infinito.

(ii) Todo inteiro $n > 1$ pode ser expresso como um produto de números primos, não necessariamente distintos.

(iii) Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p|ab$, então $p|a$ ou $p|b$.

Exemplos

- $15 = 3 \cdot 5$.
- $60 = 2 \cdot 2 \cdot 3 \cdot 5 = 2^2 \cdot 3 \cdot 5$.

Problema 4 (OBM)

Se a n-ésima OBM é realizada em um ano múltiplo de n, dizemos que esse ano é super-olímpico. Determine todos os anos super-olímpicos, sabendo que a OBM nunca deixou de ser realizada desde sua primeira edição, em 1979, e supondo que continuará sendo realizada todo ano.