Teoria dos Números para as Olimpíadas

Aula 4

Prof. Dr. José Carlos de Souza Júnior

VIII Semana da Matemática & IV Workshop PROFMAT

9 de maio de 2025

Proposição 10

Para todo $a \in \mathbb{Z}$, temos:

(a) $a^2 \equiv 0, 1, 4, 5, 6$ ou 9 $(mod\ 10)$.

Proposição 10

Para todo $a \in \mathbb{Z}$, temos:

(a) $a^2 \equiv 0, 1, 4, 5, 6$ ou 9 $(mod\ 10)$.

(b) $a^2 \equiv 0$ ou 1 $(mod\ 3)$.

Proposição 10

Para todo $a \in \mathbb{Z}$, temos:

(a) $a^2 \equiv 0, 1, 4, 5, 6$ ou 9 $(mod\ 10)$.

(b) $a^2 \equiv 0$ ou 1 $(mod\ 3)$.

(c) $a^2 \equiv 0$ ou 1 $(mod\ 4)$.

Proposição 10

Para todo $a \in \mathbb{Z}$, temos:

(a) $a^2 \equiv 0, 1, 4, 5, 6$ ou 9 $(mod\ 10)$.

(b) $a^2 \equiv 0$ ou 1 $(mod\ 3)$.

(c) $a^2 \equiv 0$ ou 1 $(mod\ 4)$.

(d) $a^2 \equiv 0, 1$ ou 4 $(mod\ 8)$.

Proposição 10

Para todo $a \in \mathbb{Z}$, temos:

(a) $a^2 \equiv 0, 1, 4, 5, 6$ ou 9 $(mod\ 10)$.

(b) $a^2 \equiv 0$ ou 1 $(mod\ 3)$.

(c) $a^2 \equiv 0$ ou 1 $(mod\ 4)$.

(d) $a^2 \equiv 0, 1$ ou 4 $(mod\ 8)$.

(e) $a^4 \equiv 0$ ou 1 $(mod\ 16)$.

Proposição 10

Para todo $a \in \mathbb{Z}$, temos:

(a) $a^2 \equiv 0, 1, 4, 5, 6$ ou 9 $(mod\ 10)$.

(b) $a^2 \equiv 0$ ou 1 $(mod\ 3)$.

(c) $a^2 \equiv 0$ ou 1 $(mod\ 4)$.

(d) $a^2 \equiv 0, 1$ ou 4 $(mod\ 8)$.

(e) $a^4 \equiv 0$ ou 1 $(mod\ 16)$.

Problema 13

Mostre que a equação $x^2 - 7 = 10y$ não tem soluções inteiras.

Proposição 10

Para todo $a \in \mathbb{Z}$, temos:

(a) $a^2 \equiv 0, 1, 4, 5, 6$ ou 9 $(mod\ 10)$.

(b) $a^2 \equiv 0$ ou 1 $(mod\ 3)$.

(c) $a^2 \equiv 0$ ou 1 $(mod\ 4)$.

(d) $a^2 \equiv 0, 1$ ou 4 $(mod\ 8)$.

(e) $a^4 \equiv 0$ ou 1 $(mod\ 16)$.

Problema 14

Mostre que a equação $15x^2 - 7y^2 = 9$ não tem soluções inteiras.

Problema 15

Mostre que $36^{36} + 41^{41}$ é divisível por 77.

Problema 16 (OCM 2001)

Ache o menor natural n tal que 2001 é a soma dos quadrados de n inteiros.

Problema 16 (OCM 2001)

Ache o menor natural n tal que 2001 é a soma dos quadrados de n inteiros.

Proposição 10

Para todo $a \in \mathbb{Z}$, temos:

(a) $a^2 \equiv 0, 1, 4, 5, 6$ ou 9 $(mod\ 10)$.

(b) $a^2 \equiv 0$ ou 1 $(mod\ 3)$.

(c) $a^2 \equiv 0$ ou 1 $(mod\ 4)$.

(d) $a^2 \equiv 0, 1$ ou 4 $(mod\ 8)$.

(e) $a^4 \equiv 0$ ou 1 $(mod\ 16)$.

Proposição 11

Se um número natural $n > 1$ não tem um fator primo p tal que

$$2 \leq p \leq \sqrt{n},$$

então n é um número primo.

Proposição 11

Se um número natural $n > 1$ não tem um fator primo p tal que

$$2 \leq p \leq \sqrt{n},$$

então n é um número primo.

Exemplo

2027 é um número primo?

Proposição 11

Se um número natural $n > 1$ não tem um fator primo p tal que

$$2 \leq p \leq \sqrt{n},$$

então n é um número primo.

Exemplo

2027 é um número primo?

Temos que $\sqrt{2027} \approx 45,02$.

Proposição 11

Se um número natural $n > 1$ não tem um fator primo p tal que

$$2 \leq p \leq \sqrt{n},$$

então n é um número primo.

Exemplo

2027 é um número primo?

Temos que $\sqrt{2027} \approx 45,02$.

Os primos satisfazendo $2 \leq p \leq \sqrt{2027}$ são:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41 \text{ e } 43.$$

Proposição 11

Se um número natural $n > 1$ não tem um fator primo p tal que

$$2 \leq p \leq \sqrt{n},$$

então n é um número primo.

Exemplo

2027 é um número primo?

Temos que $\sqrt{2027} \approx 45,02$.

Os primos satisfazendo $2 \leq p \leq \sqrt{2027}$ são:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41 \text{ e } 43.$$

Com o uso de uma calculadora, verificamos que nenhum desses fatores divide 2027.

Proposição 11

Se um número natural $n > 1$ não tem um fator primo p tal que

$$2 \leq p \leq \sqrt{n},$$

então n é um número primo.

Exemplo

2027 é um número primo?

Temos que $\sqrt{2027} \approx 45,02$.

Os primos satisfazendo $2 \leq p \leq \sqrt{2027}$ são:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41 \text{ e } 43.$$

Com o uso de uma calculadora, verificamos que nenhum desses fatores divide 2027. Portanto, 2027 é primo!

Teorema 12 (Pequeno Teorema de Fermat)

Para $a, p \in \mathbb{Z}$, com p primo, temos

$$a^p \equiv a \pmod{p}.$$

Teorema 12 (Pequeno Teorema de Fermat)

Para $a, p \in \mathbb{Z}$, com p primo, temos

$$a^{\,p} \equiv a \,(mod\ p).$$

Em particular, se $(a, p) = 1$, então

$$a^{\,p-1} \equiv 1 \,(mod\ p).$$

Teorema 12 (Pequeno Teorema de Fermat)

Para $a, p \in \mathbb{Z}$, com p primo, temos

$$a^{p} \equiv a \ (mod\ p).$$

Em particular, se $(a, p) = 1$, então

$$a^{p-1} \equiv 1 \ (mod\ p).$$

Problema 17

Mostre que $2027 | (2026^{2026} - 1)$.

Problema 18

Se p e q são primos distintos, mostre que pq divide $p^{q-1} + q^{p-1} - 1$.

Problema 18

Se p e q são primos distintos, mostre que pq divide $p^{q-1} + q^{p-1} - 1$.

Teorema 12 (Pequeno Teorema de Fermat)

Para $a, p \in \mathbb{Z}$, com p primo, temos

$$a^{p} \equiv a \ (mod\ p).$$

Em particular, se $(a, p) = 1$, então

$$a^{p-1} \equiv 1 \ (mod\ p).$$

Definição

A função φ de Euler é a função $\varphi : \mathbb{N} \to \mathbb{N}$ dada por

$$\varphi(n) = \#\{x,\ \text{com } 1 \leq x \leq n,\ \text{tal que } (x, n) = 1\}.$$

Definição

A função φ de Euler é a função $\varphi : \mathbb{N} \to \mathbb{N}$ dada por

$$\varphi(n) = \#\{x,\ \text{com } 1 \leq x \leq n,\ \text{tal que } (x, n) = 1\}.$$

Em outras palavras, $\varphi(n)$ conta quantos inteiros de 1 até n são primos com n.

Definição

A função φ de Euler é a função $\varphi : \mathbb{N} \to \mathbb{N}$ dada por

$$\varphi(n) = \#\{x, \text{ com } 1 \leq x \leq n, \text{ tal que } (x, n) = 1\}.$$

Em outras palavras, $\varphi(n)$ conta quantos inteiros de 1 até n são primos com n.

Exemplo

Calcule $\varphi(2)$.

Definição

A função φ de Euler é a função $\varphi : \mathbb{N} \to \mathbb{N}$ dada por

$$\varphi(n) = \#\{x, \text{ com } 1 \leq x \leq n, \text{ tal que } (x, n) = 1\}.$$

Em outras palavras, $\varphi(n)$ conta quantos inteiros de 1 até n são primos com n.

Exemplo

Calcule $\varphi(2)$.
Na lista $\{1, 2\}$, temos:

Definição

A função φ de Euler é a função $\varphi : \mathbb{N} \to \mathbb{N}$ dada por

$$\varphi(n) = \#\{x,\ \text{com } 1 \leq x \leq n,\ \text{tal que } (x, n) = 1\}.$$

Em outras palavras, $\varphi(n)$ conta quantos inteiros de 1 até n são primos com n.

Exemplo

Calcule $\varphi(2)$.
Na lista $\{1, 2\}$, temos:

- $(1, 2) = 1$.

Definição

A função φ de Euler é a função $\varphi : \mathbb{N} \to \mathbb{N}$ dada por

$$\varphi(n) = \#\{x, \text{ com } 1 \leq x \leq n, \text{ tal que } (x, n) = 1\}.$$

Em outras palavras, $\varphi(n)$ conta quantos inteiros de 1 até n são primos com n.

Exemplo

Calcule $\varphi(2)$.
Na lista $\{1, 2\}$, temos:

- $(1, 2) = 1$.
- $(2, 2) = 2$.

Definição

A função φ de Euler é a função $\varphi : \mathbb{N} \to \mathbb{N}$ dada por

$$\varphi(n) = \#\{x,\ \text{com } 1 \leq x \leq n,\ \text{tal que } (x, n) = 1\}.$$

Em outras palavras, $\varphi(n)$ conta quantos inteiros de 1 até n são primos com n.

Exemplo

Calcule $\varphi(2)$.
Na lista $\{1, 2\}$, temos:

- $(1, 2) = 1$.
- $(2, 2) = 2$.

Logo, $\varphi(2) = 1$.

Exemplo

Calcule $\varphi(3)$.

Exemplo

Calcule $\varphi(3)$.
Na lista $\{1, 2, 3\}$, temos:

Exemplo

Calcule $\varphi(3)$.
Na lista $\{1, 2, 3\}$, temos:

- $(1, 3) = 1$.

Exemplo

Calcule $\varphi(3)$.
Na lista $\{1, 2, 3\}$, temos:

- $(1, 3) = 1$.
- $(2, 3) = 1$.

Exemplo

Calcule $\varphi(3)$.
Na lista $\{1, 2, 3\}$, temos:

- $(1, 3) = 1$.
- $(2, 3) = 1$.
- $(3, 3) = 3$.

Exemplo

Calcule $\varphi(3)$.
Na lista $\{1, 2, 3\}$, temos:

- $(1, 3) = 1$.
- $(2, 3) = 1$.
- $(3, 3) = 3$.

Logo, $\varphi(3) = 2$.

Exemplo

Calcule $\varphi(10)$.

Exemplo

Calcule $\varphi(10)$.
Analisando a lista $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, temos

Exemplo

Calcule $\varphi(10)$.
Analisando a lista $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, temos

Exemplo

Calcule $\varphi(10)$.
Analisando a lista $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, temos $\varphi(10) = 4$.

Teorema 13 (Euler)

Se a e n são inteiros primos entre si, com $n > 1$, então

$$a^{\varphi(n)} \equiv 1 \ (mod \ n).$$

Teorema 13 (Euler)

Se a e n são inteiros primos entre si, com $n > 1$, então

$$a^{\varphi(n)} \equiv 1 \ (mod \ n).$$

Problema 19 (OBM)

Mostre que existe um inteiro $k > 2$, tal que o número $1\underbrace{99\ldots9}_{k}1$ é múltiplo de 1991.