Divisibilidade e Congruência

Giuliano Boava

VII Encontro da Olimpíada Regional de Matemática

Florianópolis, 31 de março de 2012.

Conteúdo

Conteúdo

Definição de divisibilidade

Definição de divisibilidade

Definição

Dados dois números inteiros d e a, dizemos que d **divide** *a se existe $q \in \mathbb{Z}$ tal que $a = qd$. Neste caso, também dizemos que d é um* **divisor** *de a ou que a é um* **múltiplo** *de d. Notação: $d \mid a$ significa que d divide a e $d \nmid a$ significa que d não divide a.*

Exemplos

Exemplos

1. $7 \mid 35$ pois $35 = 5 \cdot 7$.

Exemplos

1. $7 \mid 35$ pois $35 = 5 \cdot 7$.
2. $3 \mid -9$ pois $-9 = (-3) \cdot 3$.

Exemplos

1. $7 \mid 35$ pois $35 = 5 \cdot 7$.
2. $3 \mid -9$ pois $-9 = (-3) \cdot 3$.
3. $-5 \mid 15$, pois $15 = (-3) \cdot (-5)$.

Exemplos

1. $7 \mid 35$ pois $35 = 5 \cdot 7$.
2. $3 \mid -9$ pois $-9 = (-3) \cdot 3$.
3. $-5 \mid 15$, pois $15 = (-3) \cdot (-5)$.
4. $1 \mid a$ para todo $a \in \mathbb{Z}$, pois $a = a \cdot 1$.

Exemplos

1. $7 \mid 35$ pois $35 = 5 \cdot 7$.
2. $3 \mid -9$ pois $-9 = (-3) \cdot 3$.
3. $-5 \mid 15$, pois $15 = (-3) \cdot (-5)$.
4. $1 \mid a$ para todo $a \in \mathbb{Z}$, pois $a = a \cdot 1$.
5. $4 \nmid 7$.

Exemplos

1. $7 \mid 35$ pois $35 = 5 \cdot 7$.
2. $3 \mid -9$ pois $-9 = (-3) \cdot 3$.
3. $-5 \mid 15$, pois $15 = (-3) \cdot (-5)$.
4. $1 \mid a$ para todo $a \in \mathbb{Z}$, pois $a = a \cdot 1$.
5. $4 \nmid 7$.
6. $d \mid 0$ para todo $a \in \mathbb{Z}$, pois $0 = 0 \cdot d$.

Propriedades da divisibilidade

Propriedades da divisibilidade

1. Se $d \mid a$ e $d \mid b$, então $d \mid ax + by$ para quaisquer $x, y \in \mathbb{Z}$.

Propriedades da divisibilidade

1. Se $d \mid a$ e $d \mid b$, então $d \mid ax + by$ para quaisquer $x, y \in \mathbb{Z}$.
2. Se $a \mid b$ e $b \mid c$, então $a \mid c$.

Propriedades da divisibilidade

1. Se $d \mid a$ e $d \mid b$, então $d \mid ax + by$ para quaisquer $x, y \in \mathbb{Z}$.
2. Se $a \mid b$ e $b \mid c$, então $a \mid c$.
3. Se $d \mid a$, então $a = 0$ ou $|d| \leq |a|$.

Propriedades da divisibilidade

1. Se $d \mid a$ e $d \mid b$, então $d \mid ax + by$ para quaisquer $x, y \in \mathbb{Z}$.
2. Se $a \mid b$ e $b \mid c$, então $a \mid c$.
3. Se $d \mid a$, então $a = 0$ ou $|d| \leq |a|$.

Problema

Encontre todos os inteiros n tais que $2n + 1$ divide $3n^2 - n - 1$.

Divisão Euclidiana

Divisão Euclidiana

Teorema

Dados dois números inteiros n e d com $d \neq 0$, então existem $q, r \in \mathbb{Z}$, com $0 \leq r < |d|$, tais que

$$n = dq + r.$$

Além disso, q e r são unicamente determinados a partir de n e d.

Exemplos

Exemplos

1. Para $n = 42$ e $d = 5$, tem-se $q = 8$ e $r = 2$, pois $42 = 5 \cdot 8 + 2$;

Exemplos

1. Para $n = 42$ e $d = 5$, tem-se $q = 8$ e $r = 2$, pois $42 = 5 \cdot 8 + 2$;

2. $-34 = 6 \cdot (-6) + 2$;

Exemplos

1. Para $n = 42$ e $d = 5$, tem-se $q = 8$ e $r = 2$, pois $42 = 5 \cdot 8 + 2$;

2. $-34 = 6 \cdot (-6) + 2$;

3. $38 = (-7) \cdot (-5) + 3$.

Definição de máximo divisor comum

Definição de máximo divisor comum

Definição

Dados dois números inteiros a e b com a e b não nulos, definimos o **máximo divisor comum** *entre a e b como o maior inteiro positivo que divide a e b ao mesmo tempo. Notação:* $\mathrm{mdc}(a, b)$. *Nos casos em que a ou b são iguais a* 0, *definimos* $\mathrm{mdc}(a, 0) = |a|$, $\mathrm{mdc}(0, b) = |b|$ *e* $\mathrm{mdc}(0, 0) = 0$.

Exemplos

Exemplos

1. $\text{mdc}(6, 14) = 2$.

Exemplos

1. $\text{mdc}(6, 14) = 2$.
2. $\text{mdc}(5, 11) = 1$. Neste caso, dizemos que 5 e 11 são primos entre si.

Exemplos

1. $\text{mdc}(6, 14) = 2$.
2. $\text{mdc}(5, 11) = 1$. Neste caso, dizemos que 5 e 11 são primos entre si.
3. $\text{mdc}(-8, 12) = 4$.

Exemplos

1. $\text{mdc}(6, 14) = 2$.
2. $\text{mdc}(5, 11) = 1$. Neste caso, dizemos que 5 e 11 são primos entre si.
3. $\text{mdc}(-8, 12) = 4$.
4. $\text{mdc}(a, 1) = 1$, para qualquer a.

Exemplos

1. $\text{mdc}(6, 14) = 2$.
2. $\text{mdc}(5, 11) = 1$. Neste caso, dizemos que 5 e 11 são primos entre si.
3. $\text{mdc}(-8, 12) = 4$.
4. $\text{mdc}(a, 1) = 1$, para qualquer a.
5. $\text{mdc}(-15, 0) = 15$.

Propriedade do máximo divisor comum

Propriedade do máximo divisor comum

Teorema

Se $a = b \cdot q + r$, *então* $\mathrm{mdc}(a, b) = \mathrm{mdc}(r, b)$.

Propriedade do máximo divisor comum

Teorema

Se $a = b \cdot q + r$, *então* $\mathrm{mdc}(a, b) = \mathrm{mdc}(r, b)$.

Exemplo

Calcule $\mathrm{mdc}(132, 21)$.

Teorema Fundamental da Aritmética

Teorema Fundamental da Aritmética

Teorema

Todo número natural $n \geq 2$ pode ser escrito na forma

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_r^{e_r},$$

em que $p_1, \ldots, p_r$ são números primos. Além disso, se $p_1 \leq p_2 \leq \cdots \leq p_r$ e os expoentes e_i são todos positivos, então tal expressão é unicamente determinada a partir de n.

Exemplos

Exemplos

1. $18 = 2 \cdot 3^2$;

Exemplos

1. $18 = 2 \cdot 3^2$;
2. $60 = 2^2 \cdot 3 \cdot 5$;

Exemplos

1. $18 = 2 \cdot 3^2$;
2. $60 = 2^2 \cdot 3 \cdot 5$;
3. $1000 = 2^3 \cdot 5^3$;

Exemplos

1. $18 = 2 \cdot 3^2$;
2. $60 = 2^2 \cdot 3 \cdot 5$;
3. $1000 = 2^3 \cdot 5^3$;
4. $37 = 37$.

Conteúdo

Definição de congruência

Definição de congruência

Definição

Dados três números inteiros a, b e n, dizemos que a **é congruente a** *b* **módulo** *n se* $n \mid a - b$*, isto é, se* $a - b$ *é múltiplo de n. Notação:* $a \equiv b \bmod(n)$.

Exemplos

Exemplos

1. $5 \equiv 2 \mod(3)$;

Exemplos

1. $5 \equiv 2 \mod(3)$;
2. $5 \equiv 7 \mod(2)$;

Exemplos

1. $5 \equiv 2 \mod(3)$;
2. $5 \equiv 7 \mod(2)$;
3. $15 \equiv 0 \mod(-5)$;

Exemplos

1. $5 \equiv 2 \mod(3)$;
2. $5 \equiv 7 \mod(2)$;
3. $15 \equiv 0 \mod(-5)$;
4. $-3 \equiv 12 \mod(5)$;

Exemplos

1. $5 \equiv 2 \mod(3)$;
2. $5 \equiv 7 \mod(2)$;
3. $15 \equiv 0 \mod(-5)$;
4. $-3 \equiv 12 \mod(5)$;
5. $5 \equiv 5 \mod(46)$;

Exemplos

1. $5 \equiv 2 \mod(3)$;
2. $5 \equiv 7 \mod(2)$;
3. $15 \equiv 0 \mod(-5)$;
4. $-3 \equiv 12 \mod(5)$;
5. $5 \equiv 5 \mod(46)$;
6. Se a e b deixam o mesmo resto na divisão por n, então $a \equiv b \mod(n)$.

Propriedades da congruência

Propriedades da congruência

1. $a \equiv a \bmod(n)$;

Propriedades da congruência

1. $a \equiv a \bmod(n)$;
2. $a \equiv b \bmod(n) \implies b \equiv a \bmod(n)$;

Propriedades da congruência

1. $a \equiv a \bmod(n)$;
2. $a \equiv b \bmod(n) \implies b \equiv a \bmod(n)$;
3. $a \equiv b \bmod(n)$ e $b \equiv c \bmod(n) \implies a \equiv c \bmod(n)$;

Propriedades da congruência

1. $a \equiv a \bmod(n)$;
2. $a \equiv b \bmod(n) \implies b \equiv a \bmod(n)$;
3. $a \equiv b \bmod(n)$ e $b \equiv c \bmod(n) \implies a \equiv c \bmod(n)$;
4. $a \equiv b \bmod(n) \implies a + c \equiv b + c \bmod(n)$, $a - c \equiv b - c \bmod(n)$ e $ac \equiv bc \bmod(n)$;

Propriedades da congruência

1. $a \equiv a \bmod(n)$;
2. $a \equiv b \bmod(n) \implies b \equiv a \bmod(n)$;
3. $a \equiv b \bmod(n)$ e $b \equiv c \bmod(n) \implies a \equiv c \bmod(n)$;
4. $a \equiv b \bmod(n) \implies a + c \equiv b + c \bmod(n)$, $a - c \equiv b - c \bmod(n)$ e $ac \equiv bc \bmod(n)$;
5. $a \equiv b \bmod(n)$ e $c \equiv d \bmod(n) \implies a + c \equiv b + d \bmod(n)$, $a - c \equiv b - d \bmod(n)$ e $ac \equiv bd \bmod(n)$;

Propriedades da congruência

1. $a \equiv a \bmod(n)$;
2. $a \equiv b \bmod(n) \implies b \equiv a \bmod(n)$;
3. $a \equiv b \bmod(n)$ e $b \equiv c \bmod(n) \implies a \equiv c \bmod(n)$;
4. $a \equiv b \bmod(n) \implies a + c \equiv b + c \bmod(n)$, $a - c \equiv b - c \bmod(n)$ e $ac \equiv bc \bmod(n)$;
5. $a \equiv b \bmod(n)$ e $c \equiv d \bmod(n) \implies a + c \equiv b + d \bmod(n)$, $a - c \equiv b - d \bmod(n)$ e $ac \equiv bd \bmod(n)$;
6. $a \equiv b \bmod(n) \implies a^k \equiv b^k \bmod(n)$;

Propriedades da congruência

1. $a \equiv a \bmod(n)$;
2. $a \equiv b \bmod(n) \implies b \equiv a \bmod(n)$;
3. $a \equiv b \bmod(n)$ e $b \equiv c \bmod(n) \implies a \equiv c \bmod(n)$;
4. $a \equiv b \bmod(n) \implies a + c \equiv b + c \bmod(n)$, $a - c \equiv b - c \bmod(n)$ e $ac \equiv bc \bmod(n)$;
5. $a \equiv b \bmod(n)$ e $c \equiv d \bmod(n) \implies a + c \equiv b + d \bmod(n)$, $a - c \equiv b - d \bmod(n)$ e $ac \equiv bd \bmod(n)$;
6. $a \equiv b \bmod(n) \implies a^k \equiv b^k \bmod(n)$;
7. Se $\mathrm{mdc}(c, n) = 1$ e $ac \equiv bc \bmod(n)$, então $a \equiv b \bmod(n)$.

Exemplos

Exemplos

1. Como $3 \equiv 7 \mod(4)$ e $7 \equiv 31 \mod(4)$, então $3 \equiv 31 \mod(4)$.

Exemplos

1. Como $3 \equiv 7 \mod(4)$ e $7 \equiv 31 \mod(4)$, então $3 \equiv 31 \mod(4)$.

2. $5 \equiv 12 \mod(7) \implies 8 \cdot 5 \equiv 8 \cdot 12 \mod(7)$.

Exemplos

1. Como $3 \equiv 7 \mod(4)$ e $7 \equiv 31 \mod(4)$, então $3 \equiv 31 \mod(4)$.

2. $5 \equiv 12 \mod(7) \implies 8 \cdot 5 \equiv 8 \cdot 12 \mod(7)$.

3. Como $7 \equiv 37 \mod(6)$ e $8 \equiv 14 \mod(6)$, então $7 + 8 \equiv 37 + 14 \mod(6)$ e $7 \cdot 8 \equiv 37 \cdot 14 \mod(6)$.

Exemplos

1. Como $3 \equiv 7 \mod(4)$ e $7 \equiv 31 \mod(4)$, então $3 \equiv 31 \mod(4)$.

2. $5 \equiv 12 \mod(7) \implies 8 \cdot 5 \equiv 8 \cdot 12 \mod(7)$.

3. Como $7 \equiv 37 \mod(6)$ e $8 \equiv 14 \mod(6)$, então $7 + 8 \equiv 37 + 14 \mod(6)$ e $7 \cdot 8 \equiv 37 \cdot 14 \mod(6)$.

4. $21 \equiv 33 \mod(4) \implies 7 \equiv 11 \mod(4)$, pois $\mathrm{mdc}(3, 4) = 1$.

Problemas

Problemas

Problema

Calcule o resto da divisão de 2^{1000} *por* 31.

Problemas

Problema

Calcule o resto da divisão de 2^{1000} *por* 31.

Problema

Calcule o resto da divisão de 3^{50} *por* 28.

Problemas

Problema

Calcule o resto da divisão de 2^{1000} *por* 31.

Problema

Calcule o resto da divisão de 3^{50} *por* 28.

Problema

Calcule o resto da divisão de 7^{10} *por* 47.

Função φ de Euler

Função φ de Euler

Definição

Dado um inteiro $n \geq 2$ definimos $\varphi(n)$ como o número de inteiros de 1 até n que são primos com n. A função φ é denominada **função de Euler**.

Exemplos

Exemplos

1. $\varphi(4) = 2$;

Exemplos

1. $\varphi(4) = 2$;
2. $\varphi(7) = 6$;

Exemplos

1. $\varphi(4) = 2$;
2. $\varphi(7) = 6$;
3. $\varphi(12) = 4$;

Exemplos

1. $\varphi(4) = 2$;
2. $\varphi(7) = 6$;
3. $\varphi(12) = 4$;
4. $\varphi(16) = 8$.

Fórmula para calcular $\varphi(n)$

Fórmula para calcular $\varphi(n)$

Teorema

Fórmula para calcular $\varphi(n)$

Teorema

- *Se p é primo, então* $\varphi(p) = p - 1$.

Fórmula para calcular $\varphi(n)$

Teorema

- *Se p é primo, então $\varphi(p) = p - 1$.*
- *Se $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_r^{e_r}$ é a fatoração em primos de n, então*

$$\varphi(n) = n \cdot \left(\frac{p_1 - 1}{p_1}\right) \cdot \left(\frac{p_2 - 1}{p_2}\right) \cdots \cdot \left(\frac{p_r - 1}{p_r}\right).$$

Exemplos

Exemplos

1. $\varphi(73) = 72$, pois 73 é primo.

Exemplos

1. $\varphi(73) = 72$, pois 73 é primo.

2. $\varphi(12) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$.

Exemplos

1. $\varphi(73) = 72$, pois 73 é primo.
2. $\varphi(12) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$.
3. $\varphi(60) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 16$.

Exemplos

1. $\varphi(73) = 72$, pois 73 é primo.
2. $\varphi(12) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$.
3. $\varphi(60) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 16$.
4. $\varphi(100) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$.

Teorema de Euler-Fermat

Teorema de Euler-Fermat

Teorema

Se $\mathrm{mdc}(a, n) = 1$, *então*

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

Em particular, se p é primo e a não é múltiplo de p, então

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

Exemplos

Exemplos

1. $7^4 \equiv 1 \mod(12)$ pois $\mathrm{mdc}(7, 12) = 1$ e $\varphi(12) = 4$.

Exemplos

1. $7^4 \equiv 1 \mod(12)$ pois $\mathrm{mdc}(7, 12) = 1$ e $\varphi(12) = 4$.

2. $28^{10} \equiv 1 \mod(11)$.

Exemplos

1. $7^4 \equiv 1 \mod(12)$ pois $\mathrm{mdc}(7, 12) = 1$ e $\varphi(12) = 4$.
2. $28^{10} \equiv 1 \mod(11)$.
3. $3^{42} \equiv 9 \mod(100)$.

Problemas

Problemas

Problema

Mostre que $2^{70} + 3^{70}$ *é múltiplo de* 13.

Problemas

Problema

Mostre que $2^{70} + 3^{70}$ *é múltiplo de* 13.

Problema

Encontre os dois últimos dígitos de 3^{1005} *na notação decimal.*

Problemas

Problema

Mostre que $2^{70} + 3^{70}$ *é múltiplo de* 13.

Problema

Encontre os dois últimos dígitos de 3^{1005} *na notação decimal.*

Problema

Mostre que não existe um inteiro x *tal que* $x^5 - 2$ *é múltiplo de* 41.

Problemas

Problemas

Problema

Mostre que existem infinitos números da forma $2000\cdots009$ *que são múltiplos de 2009.*

Problemas

Problema

Mostre que existem infinitos números da forma $2000\cdots009$ *que são múltiplos de 2009.*

Problema

Mostre que não existem inteiros x, y *e* z *tais que* $x^2 + y^2 + z^2 = 8007$.

Conteúdo

Bibliografia

Bibliografia

- F. B. MARTINEZ, C. G. T. A. MOREIRA, N. SALDANHA, E. TENGAN - *Teoria dos Números*, IMPA, 2010.

Bibliografia

- F. B. MARTINEZ, C. G. T. A. MOREIRA, N. SALDANHA, E. TENGAN - *Teoria dos Números*, IMPA, 2010.

- J. P. de O. SANTOS - *Introdução à Teoria dos Números*, IMPA, 2000.

FIM