Matemática Elementar

Congruências

(Alguns Exemplos e Definições)

Prof. Dr. Sérgio de Albuquerque Souza

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Departamento de Matemática

16 de maio de 2023

Definição

Diremos que os inteiros a e b são **congruentes módulo** n, se $n \mid (a-b)$, ou seja, existe $k \in \mathbb{Z}$ tal que $a - b = k \times n$.

$$a \equiv b \bmod n$$

ou

$$a \equiv b \pmod{n}$$

Exemplos

1. $13 \equiv 5 \bmod 2$, pois: $13 - (5) = 8 = (4) \times 2$
2. $-6 \equiv 15 \bmod 3$, pois: $-6 - (15) = -21 = (-7) \times 3$
3. $28 \equiv -12 \bmod 5$, pois: $28 - (-12) = 40 = (8) \times 5$
4. $-10 \equiv -4 \bmod 6$, pois: $-10 - (-4) = -6 = (-1) \times 6$
5. $2 \equiv 2 \bmod 13$, pois: $2 - (2) = 0 = (0) \times 13$
6. $9 \not\equiv 3 \bmod 4$, pois: $9 - (3) = 6$ não é múltiplo de 4

Teorema

Teorema

Dados os inteiros a e b, temos $a \equiv b \bmod n$ se, e somente se, a e b possuem o mesmo resto quando divididos por n.

Exemplos

1. $-2 \equiv 43 \bmod 9$ pois os restos são iguais a **7**:

$$-2 = -1 \times 9 + \mathbf{7} \qquad \text{e} \qquad 43 = 4 \times 9 + \mathbf{7}$$

2. $28 \equiv -12 \bmod 5$ pois os restos são iguais a **3**:

$$28 = 5 \times 5 + \mathbf{3} \qquad \text{e} \qquad -12 = -3 \times 5 + \mathbf{3}$$

3. $9 \not\equiv 3 \bmod 4$ pois os restos são diferentes:

$$9 = 2 \times 4 + \mathbf{1} \qquad \text{e} \qquad 3 = 0 \times 4 + \mathbf{3}$$

Exemplos de equações

1. Da equivalência $x \equiv 0 \mod 3$, temos que:

$$(x) - (0) = (x) \equiv 0 \mod 3$$

Logo $3 \mid (x)$, ou seja, (x) é múltiplo de 3.

$$x = 3n \Longrightarrow x = 3n \quad \text{(resto 0)}$$

Conjunto solução para $x \in \mathbb{Z}$:

$$Sol = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} = \overline{0}$$

Exemplos de equações

2. Da equivalência $\boxed{x \equiv 1 \mod 3}$, temos que:

$$(x) - (1) = (x-1) \equiv 0 \mod 3$$

Logo $3 \mid (x-1)$, ou seja, $(x-1)$ é múltiplo de 3.

$$x - 1 = 3n \Longrightarrow \boxed{x = 3n+1} \quad \text{(resto 1)}$$

Conjunto solução para $x \in \mathbb{Z}$:

$$\boxed{Sol = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\} = \overline{1}}$$

Exemplos de equações

3. Da equivalência $\boxed{x \equiv 2 \mod 3}$, temos que:

$$(x) - (2) = (x-2) \equiv 0 \mod 3$$

Logo $3 \mid (x-2)$, ou seja, $(x-2)$ é múltiplo de 3.

$$x - 2 = 3n \Longrightarrow \boxed{x = 3n + 2} \quad \text{(resto 2)}$$

Conjunto solução para $x \in \mathbb{Z}$:

$$\boxed{Sol = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\} = \overline{2}}$$

Exemplos de equações

4. Da equivalência $4x \equiv 12 \mod 6$, temos que:

$$(4x) - (12) = (4x - 12) \equiv 0 \mod 6$$

Logo $6 \mid (4x - 12)$, ou seja, $(4x - 12)$ é múltiplo de 6.

$$4x - 12 = 6n \Longrightarrow \boxed{x = \frac{3n+6}{2}}$$

Conjunto solução para $x \in \mathbb{Z}$:

$$\boxed{Sol = \{\ldots, -6, -3, 0, 3, 6, 9, 12, \ldots\}}$$

Exemplos de equações

- Da equivalência $x+3 \equiv 21-x \mod 5$, temos que:

$$(x+3)-(21-x) = (2x-18) \equiv 0 \mod 5$$

Logo $5 \mid (2x-18)$, ou seja, $(2x-18)$ é múltiplo de 5.

$$2x-18 = 5n \Longrightarrow \boxed{x = \frac{5n+18}{2}}$$

Conjunto solução para $x \in \mathbb{Z}$:

$$\boxed{Sol = \{\ldots, -6, -1, 4, 9, 14, 19, 24, \ldots\}}$$

Exemplos de equações

6. Da equivalência $x+3 \equiv 21-2x \mod 4$, temos que:

$$(x+3)-(21-2x) = (3x-18) \equiv 0 \mod 4$$

Logo $4 \mid (3x-18)$, ou seja, $(3x-18)$ é múltiplo de 4.

$$3x-18 = 4n \Longrightarrow \boxed{x = \frac{4n+18}{3}}$$

Conjunto solução para $x \in \mathbb{Z}$:

$$\boxed{Sol = \{\ldots, -6, -2, 2, 6, 10, 14, 18, \ldots\}}$$

Definição

Dados os números inteiros a e $n \in \mathbb{Z}$, definiremos o conjunto:

$$\overline{a} = \{x \in \mathbb{Z} / x \equiv a \mod n\}$$

ou seja, a e x possuem o mesmo resto quando divididos por n. Portanto temos o conjunto quociente:

$$\mathbb{Z}/_{\equiv \mod n} = \mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \cdots, \overline{n-1}\}$$

Definição em $\mathbb{Z}_n$

Dados $\overline{a}$ e $\overline{b}$ no conjunto quociente $\mathbb{Z}_n$ definimos:

- A soma $\overline{a}+\overline{b}$ como sendo a classe de equivalência módulo n da soma (usual) $a+b$:

$$\overline{a}+\overline{b}=\overline{a+b}$$

- O produto $\overline{a}\times\overline{b}$ como sendo a classe de equivalência módulo n do produto (usual) $a\times b$:

$$\overline{a}\times\overline{b}=\overline{a\times b}$$

Definição em $\mathbb{Z}_n$

Dado $\overline{a} \in \mathbb{Z}_n$ diremos que $\overline{a} \neq \overline{0}$ possui **inverso multiplicativo** em $\mathbb{Z}_n$ se existir $\overline{b} \neq \overline{0}$ tal que:

$$\overline{a} \times \overline{b} = \overline{1}$$

Dados $\overline{a}$ e $\overline{b}$ em $\mathbb{Z}_n$ diremos que $\overline{a}$ é **divisível** por $\overline{b}$ se existir $\overline{c} \in \mathbb{Z}_n$ tal que $\overline{a} = \overline{b} \times \overline{c}$. Isto é: $\overline{a} \div \overline{b} = \overline{c}$

Exemplo: $\mathbb{Z}_3$

- Em $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ temos as seguintes tabelas de soma e multiplicação:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Exemplo: $\mathbb{Z}_5$

- Em $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ temos as seguintes tabelas de soma e multiplicação:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Exemplo: $\mathbb{Z}_6$

- Em $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ temos as seguintes tabelas de soma e multiplicação:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Exemplos em $\mathbb{Z}_7$

Em $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$, temos que:

- $\overline{12} - \overline{2} + \overline{3} + \overline{4} = \overline{12 - 2 + 3 + 4} = \overline{17} = \overline{3}$
  pois $17 \equiv 3 \mod 7$.

- $\overline{11} \times \overline{3} \times \overline{5} = \overline{11 \times 3 \times 5} = \overline{165} = \overline{4}$
  pois $165 \equiv 4 \mod 7$.

Exemplos em $\mathbb{Z}_7$

- Como $\boxed{(\overline{a})^n = \overline{a^n}}$ teremos os seguintes resultados:
  - $\overline{8^{12}} = (\overline{8})^{12} = (\overline{1})^{12} = \overline{1^{12}} = \overline{1} = \overline{1}$
  - $\overline{9^5} = (\overline{9})^5 = (\overline{2})^5 = \overline{2^5} = \overline{32} = \overline{4}$
  - $\overline{12^5} = (\overline{12})^5 = (\overline{5})^5 = \overline{5^5} = \overline{3125} = \overline{3}$
  - $\overline{-4^3} = (\overline{-4})^3 = (\overline{3})^3 = \overline{3^3} = \overline{27} = \overline{6}$

Exemplos em $\mathbb{Z}_7$

- A Divisão de $\overline{2}$ por $\overline{4}$?
  - Qual é o $\overline{n} \in \mathbb{Z}_7$ tal que $\overline{n} \times \overline{4} = \overline{2}$, isto é, quais os valores de $n \in \mathbb{Z}$ tais que $(4 \times n) \div 7$ tenha resto 2?

    Note que os elementos do conjunto abaixo, satisfazem a condição:

    $$\{\ldots, -10, -3, 4, 11, 18, \ldots\} = \overline{4}$$

    Logo a divisão de $\overline{2}$ por $\overline{4}$ é $\overline{4}$

Exemplos em $\mathbb{Z}_7$

- A Divisão de $\overline{4}$ por $\overline{6}$?
  - Qual é o $\overline{n} \in \mathbb{Z}_7$ tal que $\overline{n} \times \overline{6} = \overline{4}$, isto é, quais os valores de $n \in \mathbb{Z}$ tais que $(6 \times n) \div 7$ tenha resto 4?

    Note que os elementos do conjunto abaixo, satisfazem a condição:

    $$\{\ldots, -11, -4, 3, 10, 17, \ldots\} = \overline{3}$$

    Logo a divisão de $\overline{4}$ por $\overline{6}$ é $\overline{3}$

Exemplos em $\mathbb{Z}_7$

- O inverso multiplicativo de $\overline{3}$?
  - Qual é o $\overline{n} \in \mathbb{Z}_7$ tal que $\overline{n} \times \overline{3} = \overline{3} \times \overline{n} = \overline{1}$, isto é, quais os valores de $n \in \mathbb{Z}$ tais que $(3 \times n) \div 7$ tenha resto 1?

    Note que os elementos do conjunto abaixo, satisfazem a condição:

    $$\{\ldots, -9, -2, 5, 12, 19, \ldots\} = \overline{5}$$

    Logo o inverso multiplicativo de $\overline{3}$ é $\overline{5}$

Exemplos em $\mathbb{Z}_7$

- O inverso multiplicativo de $\overline{6}$?
  - Qual é o $\overline{n} \in \mathbb{Z}_7$ tal que $\overline{n} \times \overline{6} = \overline{6} \times \overline{n} = \overline{1}$, isto é, quais os valores de $n \in \mathbb{Z}$ tais que $(6 \times n) \div 7$ tenha resto 1?

    Note que os elementos do conjunto abaixo, satisfazem a condição:

    $$\{\ldots, -8, -1, 6, 13, 20, \ldots\} = \overline{6}$$

    Logo o inverso multiplicativo de $\overline{6}$ é $\overline{6}$.

Exemplos em $\mathbb{Z}_7$

- Soluções para a equação $\overline{x}^2 - \overline{1} = \overline{3}$?
  - Simplificando a equação temos: $\overline{x}^2 = \overline{4}$
  - Quais os valores de $n \in \mathbb{Z}$ tais que $(n^2) \div 7$ tenha resto 4?

    Note que os conjuntos abaixo, satisfazem a condição:

    $$\{\ldots, -5, 2, 9, \ldots\} = \overline{2} \text{ e } \{\ldots, -2, 5, 12, \ldots\} = \overline{5}$$

    Logo temos duas soluções para a equação: $\overline{2}$ e $\overline{5}$.

Algumas Propriedades

- Se $a \equiv b \bmod n$, então

$$a^n \equiv b^n \bmod n \quad \text{e} \quad (a+d) \equiv (b+d) \bmod n$$

- Se a e b são inteiros, temos que

a é divisível por b se, e somente se, $a \equiv 0 \bmod b$

Ex.: 6 é divisível por 3, pois $6 \equiv 0 \bmod 3$.

Exemplo

- Observe que $2^{222}+2$ é divisível por 3.
  - Como $2 \equiv -1 \bmod 3$, então: $2^{222} \equiv 1 \bmod 3$
  - Agora basta somar 2 e obtemos

$$(2^{222}+2) \equiv (1+2) \bmod 3 \equiv 0 \bmod 3$$

  - Logo $2^{222}+2$ é divisível por 3.

Dúvidas!!!

Prof. Sérgio

e-mails:

sergio.souza@academico.ufpb.br

sergio@mat.ufpb.br

Página do Professor:

mat.ufpb.br/sergio

Apresentação utilizando o Beamer/LaTeX