

Relação de Equivalência - Classes de Equivalência nos Inteiros

José Antônio O. Freitas

MAT-UnB

29 de agosto de 2020

Definição

Seja \underline{C} uma classe de equivalência

Definição

Seja C uma classe de equivalência de uma relação de equivalência R .

$$R \subseteq A \times A ; A \neq \emptyset \quad \boxed{C = \{x \in A \mid \exists y \in A, (x, y) \in R\}}$$

b) i) PARA TODOS $\underline{x} \in A$, $\underline{xR} x \quad [\underline{(x, x) \in R}]$

ii) SE \underline{xRy} , ENTÃO \underline{yRx} .

$$(x, y) \in R \quad (y, x) \in R$$

iii) SE xRy E yRz , ENTÃO xRz .

$$(x, y) \in R \quad (y, z) \in R \quad (x, z) \in R$$

Definição

Seja C uma classe de equivalência de uma relação de equivalência R .
Qualquer elemento $y \in C$

Definição

Seja C uma classe de equivalência de uma relação de equivalência R . Qualquer elemento $y \in C$ é chamado representante de C .

$$A = \{1, 2, 3, 4\}; \quad R = A \times A$$

$$\begin{aligned} \bar{1} &= \{ \underline{1}, \underline{2}, \underline{3}, \underline{4} \} = \{ \bar{1}, \bar{2}, \bar{3}, \bar{4} \} \\ \bar{2} &= \{1, 2, 3, 4\} \quad \bar{3} = \bar{4} \end{aligned}$$

Definição

Seja C uma classe de equivalência de uma relação de equivalência R . Qualquer elemento $y \in C$ é chamado **representante** de C .

Proposição

Seja A um conjunto não vazio

Definição

Seja C uma classe de equivalência de uma relação de equivalência R . Qualquer elemento $y \in C$ é chamado **representante** de C .

Proposição

Seja A um conjunto não vazio e R uma relação de equivalência em A .

Definição

Seja C uma classe de equivalência de uma relação de equivalência R . Qualquer elemento $y \in C$ é chamado **representante** de C .

Proposição

Seja A um conjunto não vazio e R uma relação de equivalência em A . Então $\underline{\underline{A}}$ é a união disjunta das classes \bar{b} , $b \in A$, ou seja,

Definição

Seja C uma classe de equivalência de uma relação de equivalência R . Qualquer elemento $y \in C$ é chamado **representante** de C .

Proposição

Seja A um conjunto não vazio e R uma relação de equivalência em A . Então A é a união disjunta das classes \bar{b} , $b \in A$, ou seja,

$$\bar{b} = \{x \in A \mid x R b\} \subseteq A \quad \Rightarrow \quad A = \bigcup_{b \in A} \bar{b}.$$

$\Rightarrow A \subseteq \bigcup_{\substack{b \in A}} \bar{b}$
 $\Rightarrow \bigcup_{\substack{b \in A}} \bar{b} \subseteq A$

$$x \in A \Rightarrow \underline{(x, x)} \in R \Rightarrow x \in \bar{x}$$

Definição

Seja C uma classe de equivalência de uma relação de equivalência R . Qualquer elemento $y \in C$ é chamado **representante** de C .

Proposição

Seja A um conjunto não vazio e R uma relação de equivalência em A . Então A é a união disjunta das classes \bar{b} , $b \in A$, ou seja,

$$A = \bigcup_{b \in A} \bar{b}.$$

Prova: Para todo $b \in A$ temos,

Definição

Seja C uma classe de equivalência de uma relação de equivalência R . Qualquer elemento $y \in C$ é chamado **representante** de C .

Proposição

Seja A um conjunto não vazio e R uma relação de equivalência em A . Então A é a união disjunta das classes \bar{b} , $b \in A$, ou seja,

$$A = \bigcup_{b \in A} \bar{b}.$$

Prova: Para todo $b \in A$ temos, pela definição de classe de equivalência, que $\bar{b} \subseteq A$.

Definição

Seja C uma classe de equivalência de uma relação de equivalência R . Qualquer elemento $y \in C$ é chamado **representante** de C .

Proposição

Seja A um conjunto não vazio e R uma relação de equivalência em A . Então A é a união disjunta das classes \bar{b} , $b \in A$, ou seja,

$$A = \bigcup_{b \in A} \bar{b}.$$

Prova: Para todo $b \in A$ temos, pela definição de classe de equivalência, que $\bar{b} \subseteq A$. Logo $\bigcup_{b \in A} \bar{b} \subseteq A$.

Definição

Seja C uma classe de equivalência de uma relação de equivalência R . Qualquer elemento $y \in C$ é chamado **representante** de C .

Proposição

Seja A um conjunto não vazio e R uma relação de equivalência em A . Então A é a união disjunta das classes \bar{b} , $b \in A$, ou seja,

$$A = \bigcup_{b \in A} \bar{b}.$$

Prova: Para todo $b \in A$ temos, pela definição de classe de equivalência, que $\bar{b} \subseteq A$. Logo $\bigcup_{b \in A} \bar{b} \subseteq A$. Agora seja $x \in A$.

$$(x, x) \in R$$

Definição

Seja C uma classe de equivalência de uma relação de equivalência R . Qualquer elemento $y \in C$ é chamado **representante** de C .

Proposição

Seja A um conjunto não vazio e R uma relação de equivalência em A . Então A é a união disjunta das classes \bar{b} , $b \in A$, ou seja,

$$A = \bigcup_{b \in A} \bar{b}.$$

Prova: Para todo $b \in A$ temos, pela definição de classe de equivalência, que $\bar{b} \subseteq A$. Logo $\bigcup_{b \in A} \bar{b} \subseteq A$. Agora seja $x \in A$. Logo $x \in \bar{x}$

Definição

Seja C uma classe de equivalência de uma relação de equivalência R . Qualquer elemento $y \in C$ é chamado **representante** de C .

Proposição

Seja A um conjunto não vazio e R uma relação de equivalência em A . Então A é a união disjunta das classes \bar{b} , $b \in A$, ou seja,

$$A = \bigcup_{b \in A} \bar{b}.$$

Prova: Para todo $b \in A$ temos, pela definição de classe de equivalência, que $\bar{b} \subseteq A$. Logo $\bigcup_{b \in A} \bar{b} \subseteq A$. Agora seja $x \in A$. Logo $x \in \bar{x}$ e daí $x \in \bigcup_{b \in A} \bar{b}$.

Definição

Seja C uma classe de equivalência de uma relação de equivalência R . Qualquer elemento $y \in C$ é chamado **representante** de C .

Proposição

Seja A um conjunto não vazio e R uma relação de equivalência em A . Então A é a união disjunta das classes \bar{b} , $b \in A$, ou seja,

$$A = \bigcup_{b \in A} \bar{b}.$$

Prova: Para todo $b \in A$ temos, pela definição de classe de equivalência, que $\bar{b} \subseteq A$. Logo $\bigcup_{b \in A} \bar{b} \subseteq A$. Agora seja $x \in A$. Logo $x \in \bar{x}$ e daí $x \in \bigcup_{b \in A} \bar{b}$. Assim $A \subseteq \bigcup_{b \in A} \bar{b}$.

Definição

Seja C uma classe de equivalência de uma relação de equivalência R . Qualquer elemento $y \in C$ é chamado **representante** de C .

Proposição

Seja A um conjunto não vazio e R uma relação de equivalência em A . Então A é a união disjunta das classes \bar{b} , $b \in A$, ou seja,

$$A = \bigcup_{b \in A} \bar{b}.$$

Prova: Para todo $b \in A$ temos, pela definição de classe de equivalência, que $\bar{b} \subseteq A$. Logo $\bigcup_{b \in A} \bar{b} \subseteq A$. Agora seja $x \in A$. Logo $x \in \bar{x}$ e daí $x \in \bigcup_{b \in A} \bar{b}$. Assim $A \subseteq \bigcup_{b \in A} \bar{b}$. Portanto, $A = \bigcup_{b \in A} \bar{b}$. ■

Definição

Seja C uma classe de equivalência de uma relação de equivalência R . Qualquer elemento $y \in C$ é chamado **representante** de C .

Proposição

Seja A um conjunto não vazio e R uma relação de equivalência em A . Então A é a união disjunta das classes \bar{b} , $b \in A$, ou seja,

$$A = \bigcup_{b \in A} \bar{b}.$$

Prova: Para todo $b \in A$ temos, pela definição de classe de equivalência, que $\bar{b} \subseteq A$. Logo $\bigcup_{b \in A} \bar{b} \subseteq A$. Agora seja $x \in A$. Logo $x \in \bar{x}$ e daí $x \in \bigcup_{b \in A} \bar{b}$. Assim $A \subseteq \bigcup_{b \in A} \bar{b}$. Portanto, $A = \bigcup_{b \in A} \bar{b}$. ■

$$A = \{1, 2, 3, 4\}$$

$$\text{--- } R_1 = A \times A ; \quad \overline{I} = \{1, 2, 3, 4\}$$

$$A = \overline{I}$$

$$\text{--- } R_3 = \{(1,1), (2,2), (3,3), (4,4), (1,2), (2,1)\}$$

$$\overline{I} = \{1, 2\}; \quad \overline{3} = \{3\}, \quad \overline{4} = \{4\}; \quad A = \overline{I} \cup \overline{3} \cup \overline{4}$$

$$\Rightarrow R_4 = \{(1,1), (2,2), (3,3), (4,4)\}$$

$$\overline{I} = \{1\}, \quad \overline{2} = \{2\}, \quad \overline{3} = \{3\}, \quad \overline{4} = \{4\}$$

$$\Rightarrow A = \overline{I} \cup \overline{2} \cup \overline{3} \cup \overline{4}$$

Definição

Sejam $a, b \in \mathbb{Z}$,

Definição

Sejam $a, b \in \mathbb{Z}$, $b \neq 0$.

Definição

Sejam $a, b \in \mathbb{Z}$, $b \neq 0$. Dizemos que b divide a

Definição

Sejam $a, b \in \mathbb{Z}$, $b \neq 0$. Dizemos que b **divide** a quando existe um inteiro k tal que $a = bk$.

Definição

Sejam $a, b \in \mathbb{Z}$, $b \neq 0$. Dizemos que b **divide** a quando existe um inteiro k tal que $a = bk$. Nesse caso escrevemos $\underline{b \mid a}$. $\textcolor{red}{a = b \cdot k}$

Definição

Sejam $a, b \in \mathbb{Z}$, $b \neq 0$. Dizemos que b **divide** a quando existe um inteiro k tal que $a = bk$. Nesse caso escrevemos $b | a$. Quando b **não divide** a ,

Definição

Sejam $a, b \in \mathbb{Z}$, $b \neq 0$. Dizemos que b **divide** a quando existe um inteiro k tal que $a = bk$. Nesse caso escrevemos $b | a$. Quando b **não divide** a , escrevemos $b \nmid a$.

Definição

Sejam $a, b \in \mathbb{Z}$, $b \neq 0$. Dizemos que b **divide** a quando existe um inteiro k tal que $a = bk$. Nesse caso escrevemos $b | a$. Quando b **não divide** a , escrevemos $b \nmid a$.

$\cancel{K} b$

Exemplos

- 1) Os inteiros 1 e -1 dividem qualquer número inteiro a , pois $a = 1a$ e $a = (-1)(-a)$.

$$a = a \cdot 1$$

$$a = (-1) \cdot (-a)$$

Definição

Sejam $a, b \in \mathbb{Z}$, $b \neq 0$. Dizemos que b **divide** a quando existe um inteiro k tal que $a = bk$. Nesse caso escrevemos $b | a$. Quando b **não divide** a , escrevemos $b \nmid a$.

Exemplos

- 1) Os inteiros 1 e -1 dividem qualquer número inteiro a , pois $a = 1a$ e $a = (-1)(-a)$.
- 2) O número 0 não divide nenhum inteiro b , pois não existe $a \in \mathbb{Z}$ tal que $b = 0a$.

~~0~~

0

Definição

Sejam $a, b \in \mathbb{Z}$, $b \neq 0$. Dizemos que b **divide** a quando existe um inteiro k tal que $a = bk$. Nesse caso escrevemos $b | a$. Quando b **não divide** a , escrevemos $b \nmid a$.

Exemplos

- 1) Os inteiros 1 e -1 dividem qualquer número inteiro a , pois $a = 1a$ e $a = (-1)(-a)$.
- 2) O número 0 não divide nenhum inteiro b , pois não existe $a \in \mathbb{Z}$ tal que $b = 0a$.
- 3) Para todo $b \neq 0$, b divide $\pm b$.

$$\begin{array}{ll} b = 1 \cdot b & b | b \\ -b = (-1)b & b | (-1) \end{array}$$

Definição

Sejam $a, b \in \mathbb{Z}$, $b \neq 0$. Dizemos que b **divide** a quando existe um inteiro k tal que $a = bk$. Nesse caso escrevemos $b | a$. Quando b **não divide** a , escrevemos $b \nmid a$.

Exemplos

- 1) Os inteiros 1 e -1 dividem qualquer número inteiro a , pois $a = 1a$ e $a = (-1)(-a)$.
- 2) O número 0 não divide nenhum inteiro b , pois não existe $a \in \mathbb{Z}$ tal que $b = 0a$.
- 3) Para todo $b \neq 0$, b divide $\pm b$.
- 4) Para todo inteiro $b \neq 0$, b divide 0, pois $0 = b0$.

$$b | 0$$

Definição

Sejam $a, b \in \mathbb{Z}$, $b \neq 0$. Dizemos que b **divide** a quando existe um inteiro k tal que $a = bk$. Nesse caso escrevemos $b | a$. Quando b **não divide** a , escrevemos $b \nmid a$.

Exemplos

- 1) Os inteiros 1 e -1 dividem qualquer número inteiro a , pois $a = 1a$ e $a = (-1)(-a)$.
- 2) O número 0 não divide nenhum inteiro b , pois não existe $a \in \mathbb{Z}$ tal que $b = 0a$.
- 3) Para todo $b \neq 0$, b divide $\pm b$.
- 4) Para todo inteiro $b \neq 0$, b divide 0, pois $0 = b0$.

5) $3 \nmid 8$. $8 = 3 \cdot \underline{k}$; $2 | 8 \Rightarrow 8 = 2 \cdot \underline{k}$
 $8 \nmid 2$; $2 = 8 \cdot \underline{l}$

Definição

Sejam $a, b \in \mathbb{Z}$, $b \neq 0$. Dizemos que b **divide** a quando existe um inteiro k tal que $a = bk$. Nesse caso escrevemos $b | a$. Quando b **não divide** a , escrevemos $b \nmid a$.

Exemplos

- 1) Os inteiros 1 e -1 dividem qualquer número inteiro a , pois $a = 1a$ e $a = (-1)(-a)$.
- 2) O número 0 não divide nenhum inteiro b , pois não existe $a \in \mathbb{Z}$ tal que $b = 0a$.
- 3) Para todo $b \neq 0$, b divide $\pm b$.
- 4) Para todo inteiro $b \neq 0$, b divide 0, pois $0 = b0$.
- 5) $3 \nmid 8$.
- 6) $17 | 51$. $51 = 17 \cdot 3$

Definição

Sejam $a, b \in \mathbb{Z}$, $b \neq 0$. Dizemos que b **divide** a quando existe um inteiro k tal que $a = bk$. Nesse caso escrevemos $b | a$. Quando b **não divide** a , escrevemos $b \nmid a$.

Exemplos

- 1) Os inteiros 1 e -1 dividem qualquer número inteiro a , pois $a = 1a$ e $a = (-1)(-a)$.
- 2) O número 0 não divide nenhum inteiro b , pois não existe $a \in \mathbb{Z}$ tal que $b = 0a$.
- 3) Para todo $b \neq 0$, b divide $\pm b$.
- 4) Para todo inteiro $b \neq 0$, b divide 0, pois $0 = b0$.
- 5) $3 \nmid 8$.
- 6) $17 | 51$.

Proposição

i) $\underline{a} \mid a$, para todo $a \in \mathbb{Z}$.

Proposição

i) $a | a$, para todo $a \in \mathbb{Z}$.

ii) Se $\underline{a} | b$ e $\underline{b} | a$, $\underline{a}, \underline{b} > 0$ então $\underline{a} = \underline{b}$.

Proposição

- i) $a | a$, para todo $a \in \mathbb{Z}$.
- ii) Se $a | b$ e $b | a$, $a, b > 0$ então $a = b$.
- iii) Se $a | b$ e $b | c$, então $a | c$.

Proposição

- i) $a | a$, para todo $a \in \mathbb{Z}$.
- ii) Se $a | b$ e $b | a$, $a, b > 0$ então $a = b$.
- iii) Se $a | b$ e $b | c$, então $a | c$.
- iv) Se $a | b$ e $a | c$, então $a | (\underline{bx} + \underline{cy})$, para todos $x, y \in \mathbb{Z}$.

i) $a = 1 \cdot a$

Proposição

i) $a | a$, para todo $a \in \mathbb{Z}$.

$$lK = 1$$

ii) Se $a | b$ e $b | a$, $a, b > 0$ então $a = b$.

$$l = k = 1 \Leftrightarrow$$

iii) Se $a | b$ e $b | c$, então $a | c$.

iv) Se $a | b$ e $a | c$, então $a | (bx + cy)$, para todos $x, y \in \mathbb{Z}$.

~~$$l = k = 1 \Leftrightarrow$$~~

Prova:

i) Imediata.

$$(i) a | b \rightarrow \underbrace{b \mid a}_{\substack{\downarrow \\ a}} ; a, b > 0$$

$$\begin{cases} b = blk \\ blk - b = 0 \\ (lk - 1)b = 0 \\ lk - 1 = 0 \end{cases}$$

$\frac{a = b}{l \in \mathbb{Z}}$

Proposição

- i) $a | a$, para todo $a \in \mathbb{Z}$.
- ii) Se $a | b$ e $b | a$, $a, b > 0$ então $a = b$.
- iii) Se $a | b$ e $b | c$, então $a | c$.
- iv) Se $a | b$ e $a | c$, então $a | (bx + cy)$, para todos $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a | b$ e $b | a$,

Proposição

- i) $a | a$, para todo $a \in \mathbb{Z}$.
- ii) Se $a | b$ e $b | a$, $a, b > 0$ então $a = b$.
- iii) Se $a | b$ e $b | c$, então $a | c$.
- iv) Se $a | b$ e $a | c$, então $a | (bx + cy)$, para todos $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a | b$ e $b | a$, existem $k, l \in \mathbb{Z}$

Proposição

- i) $a | a$, para todo $a \in \mathbb{Z}$.
- ii) Se $a | b$ e $b | a$, $a, b > 0$ então $a = b$.
- iii) Se $a | b$ e $b | c$, então $a | c$.
- iv) Se $a | b$ e $a | c$, então $a | (bx + cy)$, para todos $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a | b$ e $b | a$, existem $k, l \in \mathbb{Z}$ tais que $b = \underline{ka}$

Proposição

- i) $a | a$, para todo $a \in \mathbb{Z}$.
- ii) Se $a | b$ e $b | a$, $a, b > 0$ então $a = b$.
- iii) Se $a | b$ e $b | c$, então $a | c$.
- iv) Se $a | b$ e $a | c$, então $a | (bx + cy)$, para todos $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a | b$ e $b | a$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $a = lb$.

Proposição

- i) $a | a$, para todo $a \in \mathbb{Z}$.
- ii) Se $a | b$ e $b | a$, $a, b > 0$ então $a = b$.
- iii) Se $a | b$ e $b | c$, então $a | c$.
- iv) Se $a | b$ e $a | c$, então $a | (bx + cy)$, para todos $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a | b$ e $b | a$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $a = lb$. Assim $b = \underline{kl}b$,

Proposição

- i) $a | a$, para todo $a \in \mathbb{Z}$.
- ii) Se $a | b$ e $b | a$, $a, b > 0$ então $a = b$.
- iii) Se $a | b$ e $b | c$, então $a | c$.
- iv) Se $a | b$ e $a | c$, então $a | (bx + cy)$, para todos $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a | b$ e $b | a$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $a = lb$. Assim $b = klb$, isto é, $\cancel{b(1 - kl)} = 0$.

Proposição

- i) $a | a$, para todo $a \in \mathbb{Z}$.
- ii) Se $a | b$ e $b | a$, $a, b > 0$ então $a = b$.
- iii) Se $a | b$ e $b | c$, então $a | c$.
- iv) Se $a | b$ e $a | c$, então $a | (bx + cy)$, para todos $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a | b$ e $b | a$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $a = lb$. Assim $b = klb$, isto é, $b(1 - kl) = 0$. Como $b \neq 0$

Proposição

- i) $a | a$, para todo $a \in \mathbb{Z}$.
- ii) Se $a | b$ e $b | a$, $a, b > 0$ então $a = b$.
- iii) Se $a | b$ e $b | c$, então $a | c$.
- iv) Se $a | b$ e $a | c$, então $a | (bx + cy)$, para todos $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a | b$ e $b | a$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $a = lb$. Assim $b = klb$, isto é, $b(1 - kl) = 0$. Como $b \neq 0$ então $1 - kl = 0$.

Proposição

- i) $a | a$, para todo $a \in \mathbb{Z}$.
- ii) Se $a | b$ e $b | a$, $a, b > 0$ então $a = b$.
- iii) Se $a | b$ e $b | c$, então $a | c$.
- iv) Se $a | b$ e $a | c$, então $a | (bx + cy)$, para todos $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a | b$ e $b | a$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $a = lb$. Assim $b = klb$, isto é, $b(1 - kl) = 0$. Como $b \neq 0$ então $1 - kl = 0$. Daí $kl = 1$

Proposição

- i) $a | a$, para todo $a \in \mathbb{Z}$.
- ii) Se $a | b$ e $b | a$, $a, b > 0$ então $a = b$.
- iii) Se $a | b$ e $b | c$, então $a | c$.
- iv) Se $a | b$ e $a | c$, então $a | (bx + cy)$, para todos $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a | b$ e $b | a$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $a = lb$. Assim $b = klb$, isto é, $b(1 - kl) = 0$. Como $b \neq 0$ então $1 - kl = 0$. Daí $kl = 1$ e então $k = \pm 1$

Proposição

- i) $a | a$, para todo $a \in \mathbb{Z}$.
- ii) Se $a | b$ e $b | a$, $a, b > 0$ então $a = b$.
- iii) Se $a | b$ e $b | c$, então $a | c$.
- iv) Se $a | b$ e $a | c$, então $a | (bx + cy)$, para todos $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a | b$ e $b | a$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $a = lb$. Assim $b = klb$, isto é, $b(1 - kl) = 0$. Como $b \neq 0$ então $1 - kl = 0$. Daí $kl = 1$ e então $k = \pm 1$ e $l = \pm 1$.

Proposição

- i) $a | a$, para todo $a \in \mathbb{Z}$.
- ii) Se $a | b$ e $b | a$, $a, b > 0$ então $a = b$.
- iii) Se $a | b$ e $b | c$, então $a | c$.
- iv) Se $a | b$ e $a | c$, então $a | (bx + cy)$, para todos $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a | b$ e $b | a$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $a = lb$. Assim $b = klb$, isto é, $b(1 - kl) = 0$. Como $b \neq 0$ então $1 - kl = 0$. Daí $kl = 1$ e então $k = \pm 1$ e $l = \pm 1$. Mas $a > 0$ e $b > 0$,

Proposição

- i) $a | a$, para todo $a \in \mathbb{Z}$.
- ii) Se $a | b$ e $b | a$, $a, b > 0$ então $a = b$. a = b
- iii) Se $a | b$ e $b | c$, então $a | c$.
- iv) Se $a | b$ e $a | c$, então $a | (bx + cy)$, para todos $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a | b$ e $b | a$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $a = lb$. Assim $b = klb$, isto é, $b(1 - kl) = 0$. Como $b \neq 0$ então $1 - kl = 0$. Daí $kl = 1$ e então $k = \pm 1$ e $l = \pm 1$. Mas $a > 0$ e $b > 0$, logo $k = l = 1$.

Proposição

- i) $a | a$, para todo $a \in \mathbb{Z}$.
- ii) Se $a | b$ e $b | a$, $a, b > 0$ então $a = b$.
- iii) Se $a | b$ e $b | c$, então $a | c$.
- iv) Se $a | b$ e $a | c$, então $a | (bx + cy)$, para todos $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a | b$ e $b | a$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $a = lb$. Assim $b = klb$, isto é, $b(1 - kl) = 0$. Como $b \neq 0$ então $1 - kl = 0$. Daí $kl = 1$ e então $k = \pm 1$ e $l = \pm 1$. Mas $a > 0$ e $b > 0$, logo $k = l = 1$. Logo $a = b$.

Proposição

- i) $a | a$, para todo $a \in \mathbb{Z}$.
- ii) Se $a | b$ e $b | a$, $a, b > 0$ então $a = b$.
- iii) Se $a | b$ e $b | c$, então $a | c$.
- iv) Se $a | b$ e $a | c$, então $a | (bx + cy)$, para todos $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a | b$ e $b | a$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $a = lb$. Assim $b = klb$, isto é, $b(1 - kl) = 0$. Como $b \neq 0$ então $1 - kl = 0$. Daí $kl = 1$ e então $k = \pm 1$ e $l = \pm 1$. Mas $a > 0$ e $b > 0$, logo $k = l = 1$. Logo $a = b$.

$$a \mid c \Leftrightarrow c = a \cdot k \quad (\text{F})$$

iii) Como $a \mid b$ e $b \mid c$,

$$\begin{aligned} b &= ak ; \quad c = bl \Rightarrow c = a \underbrace{k \cdot l}_{\in \mathbb{Z}} \\ n, l &\in \mathbb{Z} \end{aligned}$$

iii) Como $\underline{a \mid b}$ e $\underline{b \mid c}$, existem $\underline{k}, \underline{l} \in \mathbb{Z}$

iii) Como $a | b$ e $b | c$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$

iii) Como $a | b$ e $b | c$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $c = bl$.

iii) Como $a | b$ e $b | c$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $c = bl$. Assim
 $c = \underline{\underline{kal}} = \underline{(kl)}a,$

iii) Como $a | b$ e $b | c$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $c = bl$. Assim $c = kal = (kl)a$, ou seja, $a | c$.

iii) Como $a | b$ e $b | c$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $c = bl$. Assim $c = kbl = (kl)a$, ou seja, $a | c$.

iv) Como $\underline{a | b}$ e $\underline{a | c}$

$$a | (bx + cy)$$

$$b = \underline{ka} ; c = \underline{a \cdot l} \\ n, l \in \mathbb{Z}$$

$$\begin{aligned} bx + cy &= \underline{ka \cdot x + a \cdot ly} \\ &= \underline{a} \left(\underline{kx + ly} \right) \\ &\quad \Downarrow \\ &a | (bx + cy) \end{aligned}$$

- iii) Como $a | b$ e $b | c$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $c = bl$. Assim $c = kal = (kl)a$, ou seja, $a | c$.
- iv) Como $a | b$ e $a | c$ temos $b = ka$ e $c = al$,

- iii) Como $a | b$ e $b | c$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $c = bl$. Assim $c = kal = (kl)a$, ou seja, $a | c$.
- iv) Como $a | b$ e $a | c$ temos $b = ka$ e $c = al$, com $k, l \in \mathbb{Z}$.

iii) Como $a \mid b$ e $b \mid c$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $c = bl$. Assim $c = kal = (kl)a$, ou seja, $a \mid c$.

iv) Como $a \mid b$ e $a \mid c$ temos $b = ka$ e $c = al$, com $k, l \in \mathbb{Z}$. Daí

$$\cancel{bx} + \cancel{cy} =$$

- iii) Como $a | b$ e $b | c$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $c = bl$. Assim $c = kal = (kl)a$, ou seja, $a | c$.
- iv) Como $a | b$ e $a | c$ temos $b = ka$ e $c = al$, com $k, l \in \mathbb{Z}$. Daí
$$bx + cy = (\cancel{ka})x + (\cancel{al})y =$$

- iii) Como $a | b$ e $b | c$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $c = bl$. Assim $c = kal = (kl)a$, ou seja, $a | c$.
- iv) Como $a | b$ e $a | c$ temos $b = ka$ e $c = al$, com $k, l \in \mathbb{Z}$. Daí $bx + cy = (ka)x + (al)y = \underline{\underline{a(kx + ly)}}$

- iii) Como $a \mid b$ e $b \mid c$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $c = bl$. Assim $c = kal = (kl)a$, ou seja, $a \mid c$.
- iv) Como $a \mid b$ e $a \mid c$ temos $b = ka$ e $c = al$, com $k, l \in \mathbb{Z}$. Daí $bx + cy = (ka)x + (al)y = a(kx + ly)$ e como $\underline{kx + ly \in \mathbb{Z}}$

- iii) Como $a | b$ e $b | c$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $c = bl$. Assim $c = kal = (kl)a$, ou seja, $a | c$.
- iv) Como $a | b$ e $a | c$ temos $b = ka$ e $c = al$, com $k, l \in \mathbb{Z}$. Daí $bx + cy = (ka)x + (al)y = a(kx + ly)$ e como $kx + ly \in \mathbb{Z}$ segue que $a | (bx + cy)$. ■

- iii) Como $a | b$ e $b | c$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $c = bl$. Assim $c = kal = (kl)a$, ou seja, $a | c$.
- iv) Como $a | b$ e $a | c$ temos $b = ka$ e $c = al$, com $k, l \in \mathbb{Z}$. Daí $bx + cy = (ka)x + (al)y = a(kx + ly)$ e como $kx + ly \in \mathbb{Z}$ segue que $a | (bx + cy)$. ■

Definição

Sejam $a, b \in \mathbb{Z}$,

- iii) Como $a | b$ e $b | c$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $c = bl$. Assim $c = kal = (kl)a$, ou seja, $a | c$.
- iv) Como $a | b$ e $a | c$ temos $b = ka$ e $c = al$, com $k, l \in \mathbb{Z}$. Daí $bx + cy = (ka)x + (al)y = a(kx + ly)$ e como $kx + ly \in \mathbb{Z}$ segue que $a | (bx + cy)$. ■

Definição

Sejam $a, b \in \mathbb{Z}$, dizemos que a é congruente à b

- iii) Como $a | b$ e $b | c$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $c = bl$. Assim $c = kal = (kl)a$, ou seja, $a | c$.
- iv) Como $a | b$ e $a | c$ temos $b = ka$ e $c = al$, com $k, l \in \mathbb{Z}$. Daí $bx + cy = (ka)x + (al)y = a(kx + ly)$ e como $kx + ly \in \mathbb{Z}$ segue que $a | (bx + cy)$. ■

Definição

Sejam $a, b \in \mathbb{Z}$, dizemos que a é **congruente à b módulo m**

- iii) Como $a | b$ e $b | c$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $c = bl$. Assim $c = kal = (kl)a$, ou seja, $a | c$.
- iv) Como $a | b$ e $a | c$ temos $b = ka$ e $c = al$, com $k, l \in \mathbb{Z}$. Daí $bx + cy = (ka)x + (al)y = a(kx + ly)$ e como $kx + ly \in \mathbb{Z}$ segue que $a | (bx + cy)$. ■

Definição

Sejam $a, b \in \mathbb{Z}$, dizemos que a é congruente à b módulo m se $\boxed{m} | \boxed{(a - b)}$.

- iii) Como $a | b$ e $b | c$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $c = bl$. Assim $c = kal = (kl)a$, ou seja, $a | c$.
- iv) Como $a | b$ e $a | c$ temos $b = ka$ e $c = al$, com $k, l \in \mathbb{Z}$. Daí $bx + cy = (ka)x + (al)y = a(kx + ly)$ e como $kx + ly \in \mathbb{Z}$ segue que $a | (bx + cy)$. ■

Definição

Sejam $a, b \in \mathbb{Z}$, dizemos que a é **congruente à b módulo m** se $m | (a - b)$. Neste caso, escrevemos $a \equiv_m b$

- iii) Como $a | b$ e $b | c$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $c = bl$. Assim $c = kal = (kl)a$, ou seja, $a | c$.
- iv) Como $a | b$ e $a | c$ temos $b = ka$ e $c = al$, com $k, l \in \mathbb{Z}$. Daí $bx + cy = (ka)x + (al)y = a(kx + ly)$ e como $kx + ly \in \mathbb{Z}$ segue que $a | (bx + cy)$. ■

Definição

Sejam $a, b \in \mathbb{Z}$, dizemos que a é **congruente à b módulo m** se $m | (a - b)$. Neste caso, escrevemos $a \equiv_m b$ ou $a \equiv b \pmod{m}$.

- iii) Como $a | b$ e $b | c$, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $c = bl$. Assim $c = kal = (kl)a$, ou seja, $a | c$.
- iv) Como $a | b$ e $a | c$ temos $b = ka$ e $c = al$, com $k, l \in \mathbb{Z}$. Daí $bx + cy = (ka)x + (al)y = a(kx + ly)$ e como $kx + ly \in \mathbb{Z}$ segue que $a | (bx + cy)$. ■

Definição

Sejam $a, b \in \mathbb{Z}$, dizemos que a é **congruente à b módulo m** se $\underline{m} | (a - b)$. Neste caso, escrevemos $a \equiv_m b$ ou $a \underline{\equiv} b \ (\text{mod } m)$.

Exemplos

1) $\underline{5} \equiv \underline{2} \pmod{3}$, pois $3 \mid \underline{(5 - 2)}$.

$$5 - 2 = 3$$

Exemplos

1) $5 \equiv 2 \pmod{3}$, pois $3 \mid (5 - 2)$.

2) $\underline{3} \equiv \underline{1} \pmod{\underline{2}}$, pois $\underline{2} \mid (\underline{3} - \underline{1})$.

$$\underline{3} - \underline{1} \simeq \underline{2}$$

Exemplos

1) $5 \equiv 2 \pmod{3}$, pois $3 \mid (5 - 2)$.

2) $3 \equiv 1 \pmod{2}$, pois $2 \mid (3 - 1)$.

3) $\underline{3} \equiv \underline{9} \pmod{6}$, pois $6 \mid (3 - 9)$.

$$3 - 9 = -6$$

$$1 \not\equiv 3 \pmod{4}$$

$$1 - 3 = -2$$

$$4 \nmid (-2)$$

Exemplos

1) $5 \equiv 2 \pmod{3}$, pois $3 \mid (5 - 2)$.

2) $3 \equiv 1 \pmod{2}$, pois $2 \mid (3 - 1)$.

3) $3 \equiv 9 \pmod{6}$, pois $6 \mid (3 - 9)$.

Proposição

A congruência módulo m é uma relação de equivalência em \mathbb{Z} .

$$R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \equiv y \pmod{m}\}$$

i) $x \in \mathbb{Z} \Rightarrow x R x$

$$x \equiv x \pmod{m} \Leftrightarrow m \mid (x - x) \Leftrightarrow 0 = 0 \cdot m$$

ii) SE $x R y$, ENTÃO $x \equiv y \pmod{m} \Rightarrow$

$$m \mid (x - y) \qquad y R x \Rightarrow y \equiv x \pmod{m}$$

$$m \mid (y - x)$$

$$\underline{y - x} = -(x - y) = -1m = (-1)\underline{m}$$

Proposição

A congruência módulo m é uma relação de equivalência em \mathbb{Z} .

Prova

- i) Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$

Proposição

A congruência módulo m é uma relação de equivalência em \mathbb{Z} .

Prova

- i) Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$ pois $\underline{m} \mid \underline{(a - a)}$.

Proposição

A congruência módulo m é uma relação de equivalência em \mathbb{Z} .

Prova

- i) Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$ pois $m \mid (a - a)$.
- ii) Se $a \equiv b \pmod{m}$,

Proposição

A congruência módulo m é uma relação de equivalência em \mathbb{Z} .

Prova

- i) Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$ pois $m \mid (a - a)$.
- ii) Se $a \equiv b \pmod{m}$, então $m \mid \underline{(a - b)}$.

Proposição

A congruência módulo m é uma relação de equivalência em \mathbb{Z} .

Prova

- i) Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$ pois $m \mid (a - a)$.
- ii) Se $a \equiv b \pmod{m}$, então $m \mid (a - b)$. Daí existe $k \in \mathbb{Z}$,

Proposição

A congruência módulo m é uma relação de equivalência em \mathbb{Z} .

Prova

- i) Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$ pois $m \mid (a - a)$.
- ii) Se $a \equiv b \pmod{m}$, então $m \mid (a - b)$. Daí existe $k \in \mathbb{Z}$, tal que $(a - b) = \underline{km}$.

Proposição

A congruência módulo m é uma relação de equivalência em \mathbb{Z} .

Prova

- i) Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$ pois $m \mid (a - a)$.
- ii) Se $a \equiv b \pmod{m}$, então $m \mid (a - b)$. Daí existe $k \in \mathbb{Z}$, tal que $(a - b) = km$. Agora, $(b - a) = -(a - b)$

Proposição

A congruência módulo m é uma relação de equivalência em \mathbb{Z} .

Prova

- i) Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$ pois $m | (a - a)$.
- ii) Se $a \equiv b \pmod{m}$, então $m | (a - b)$. Daí existe $k \in \mathbb{Z}$, tal que $(a - b) = km$. Agora, $(b - a) = -(a - b) = -(km) = \cancel{(-k)m}$,

Proposição

A congruência módulo m é uma relação de equivalência em \mathbb{Z} .

Prova

- i) Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$ pois $m \mid (a - a)$.
- ii) Se $a \equiv b \pmod{m}$, então $m \mid (a - b)$. Daí existe $k \in \mathbb{Z}$, tal que $(a - b) = km$. Agora, $(b - a) = -(a - b) = -(km) = (-k)m$, ou seja, $m \mid (b - a)$.

Proposição

A congruência módulo m é uma relação de equivalência em \mathbb{Z} .

Prova

- i) Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$ pois $m | (a - a)$.
- ii) Se $a \equiv b \pmod{m}$, então $m | (a - b)$. Daí existe $k \in \mathbb{Z}$, tal que $(a - b) = km$. Agora, $(b - a) = -(a - b) = -(km) = (-k)m$, ou seja, $m | (b - a)$. Daí $b \equiv a \pmod{m}$.

$$\begin{aligned} x &\equiv y \pmod{m} & \Rightarrow y &\equiv z \pmod{m} \\ m &\mid (x - y) & m &\mid (y - z) \\ x &\equiv z \pmod{m} & m &\mid (x - z) \end{aligned}$$

Proposição

A congruência módulo m é uma relação de equivalência em \mathbb{Z} .

Prova

- i) Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$ pois $m | (a - a)$.
- ii) Se $a \equiv b \pmod{m}$, então $m | (a - b)$. Daí existe $k \in \mathbb{Z}$, tal que $(a - b) = km$. Agora, $(b - a) = -(a - b) = -(km) = (-k)m$, ou seja, $m | (b - a)$. Daí $b \equiv a \pmod{m}$.
- iii) Se $a \equiv b \pmod{m}$

Proposição

A congruência módulo m é uma relação de equivalência em \mathbb{Z} .

Prova

- i) Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$ pois $m | (a - a)$.
- ii) Se $a \equiv b \pmod{m}$, então $m | (a - b)$. Daí existe $k \in \mathbb{Z}$, tal que $(a - b) = km$. Agora, $(b - a) = -(a - b) = -(km) = (-k)m$, ou seja, $m | (b - a)$. Daí $b \equiv a \pmod{m}$.
- iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$,

Proposição

A congruência módulo m é uma relação de equivalência em \mathbb{Z} .

Prova

- i) Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$ pois $m | (a - a)$.
- ii) Se $a \equiv b \pmod{m}$, então $m | (a - b)$. Daí existe $k \in \mathbb{Z}$, tal que $(a - b) = km$. Agora, $(b - a) = -(a - b) = -(km) = (-k)m$, ou seja, $m | (b - a)$. Daí $b \equiv a \pmod{m}$.
- iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $m | (a - b)$ e $m | (b - c)$. Daí $m | ((a - b) + (b - c)) = m | (a - c)$.

Proposição

A congruência módulo m é uma relação de equivalência em \mathbb{Z} .

Prova

- i) Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$ pois $m | (a - a)$.
- ii) Se $a \equiv b \pmod{m}$, então $m | (a - b)$. Daí existe $k \in \mathbb{Z}$, tal que $(a - b) = km$. Agora, $(b - a) = -(a - b) = -(km) = (-k)m$, ou seja, $m | (b - a)$. Daí $b \equiv a \pmod{m}$.
- iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $m | (a - b)$ e $m | (b - c)$.

Proposição

A congruência módulo m é uma relação de equivalência em \mathbb{Z} .

Prova

- i) Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$ pois $m \mid (a - a)$.
- ii) Se $a \equiv b \pmod{m}$, então $m \mid (a - b)$. Daí existe $k \in \mathbb{Z}$, tal que $(a - b) = km$. Agora, $(b - a) = -(a - b) = -(km) = (-k)m$, ou seja, $m \mid (b - a)$. Daí $b \equiv a \pmod{m}$.
- iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $m \mid (a - b)$ e $m \mid (b - c)$. Assim, $m \mid [(a - b) + (b - c)]$.

Proposição

A congruência módulo m é uma relação de equivalência em \mathbb{Z} .

Prova

- i) Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$ pois $m | (a - a)$.
- ii) Se $a \equiv b \pmod{m}$, então $m | (a - b)$. Daí existe $k \in \mathbb{Z}$, tal que $(a - b) = km$. Agora, $(b - a) = -(a - b) = -(km) = (-k)m$, ou seja, $m | (b - a)$. Daí $b \equiv a \pmod{m}$.
- iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $m | (a - b)$ e $m | (b - c)$. Assim, $m | [(a - b) + (b - c)]$. Logo, $m | \underline{(a - c)}$,

Proposição

A congruência módulo m é uma relação de equivalência em \mathbb{Z} .

Prova

- i) Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$ pois $m | (a - a)$.
- ii) Se $a \equiv b \pmod{m}$, então $m | (a - b)$. Daí existe $k \in \mathbb{Z}$, tal que $(a - b) = km$. Agora, $(b - a) = -(a - b) = -(km) = (-k)m$, ou seja, $m | (b - a)$. Daí $b \equiv a \pmod{m}$.
- iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $m | (a - b)$ e $m | (b - c)$. Assim, $m | [(a - b) + (b - c)]$. Logo, $m | (a - c)$, isto é, $a \equiv c \pmod{m}$.

Proposição

A congruência módulo m é uma relação de equivalência em \mathbb{Z} .

Prova

- i) Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$ pois $m | (a - a)$.
- ii) Se $a \equiv b \pmod{m}$, então $m | (a - b)$. Daí existe $k \in \mathbb{Z}$, tal que $(a - b) = km$. Agora, $(b - a) = -(a - b) = -(km) = (-k)m$, ou seja, $m | (b - a)$. Daí $b \equiv a \pmod{m}$.
- iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $m | (a - b)$ e $m | (b - c)$. Assim, $m | [(a - b) + (b - c)]$. Logo, $m | (a - c)$, isto é, $a \equiv c \pmod{m}$.

Portanto a congruência módulo m é uma relação de equivalência. ■

Proposição

A congruência módulo m é uma relação de equivalência em \mathbb{Z} .

Prova

- i) Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$ pois $m | (a - a)$.
- ii) Se $a \equiv b \pmod{m}$, então $m | (a - b)$. Daí existe $k \in \mathbb{Z}$, tal que $(a - b) = km$. Agora, $(b - a) = -(a - b) = -(km) = (-k)m$, ou seja, $m | (b - a)$. Daí $b \equiv a \pmod{m}$.
- iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $m | (a - b)$ e $m | (b - c)$. Assim, $m | [(a - b) + (b - c)]$. Logo, $m | (a - c)$, isto é, $a \equiv c \pmod{m}$.

Portanto a congruência módulo m é uma relação de equivalência. ■

Teorema

A relação de congruência módulo m satisfaaz as seguintes propriedades:

Teorema

A relação de congruência módulo m satisfaz as seguintes propriedades:

- i) $\underline{a_1 \equiv b_1 \pmod{m}}$ se, e somente se, $\underline{a_1 - b_1 \equiv 0 \pmod{m}}$.

Teorema

A relação de congruência módulo m satisfaz as seguintes propriedades:

- i) $a_1 \equiv b_1 \pmod{m}$ se, e somente se, $a_1 - b_1 \equiv 0 \pmod{m}$.
- ii) Se $a_1 \equiv b_1 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, então $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$.

Teorema

A relação de congruência módulo m satisfaz as seguintes propriedades:

- i) $a_1 \equiv b_1 \pmod{m}$ se, e somente se, $a_1 - b_1 \equiv 0 \pmod{m}$.
- ii) Se $a_1 \equiv b_1 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, então $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$.
- iii) Se $\cancel{a_1} \equiv \cancel{b_1} \pmod{m}$ e $\cancel{a_2} \equiv \cancel{b_2} \pmod{m}$, então $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

Teorema

A relação de congruência módulo m satisfaz as seguintes propriedades:

- i) $a_1 \equiv b_1 \pmod{m}$ se, e somente se, $a_1 - b_1 \equiv 0 \pmod{m}$.
- ii) Se $a_1 \equiv b_1 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, então $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$.
- iii) Se $a_1 \equiv b_1 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, então $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.
- iv) Se $a \equiv b \pmod{m}$, então $ax \equiv bx \pmod{m}$, para todo $x \in \mathbb{Z}$.

Teorema

A relação de congruência módulo m satisfaz as seguintes propriedades:

- i) $a_1 \equiv b_1 \pmod{m}$ se, e somente se, $a_1 - b_1 \equiv 0 \pmod{m}$.
- ii) Se $a_1 \equiv b_1 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, então $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$.
- iii) Se $a_1 \equiv b_1 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, então $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.
- iv) Se $a \equiv b \pmod{m}$, então $ax \equiv bx \pmod{m}$, para todo $x \in \mathbb{Z}$.
- v) Vale a lei do cancelamento: se $d \in \mathbb{Z}$ e $\text{mdc}(d, m) = 1$ então $ad \equiv bd \pmod{m}$ implica $a \equiv b \pmod{m}$.

Teorema

A relação de congruência módulo m satisfaz as seguintes propriedades:

- i) $a_1 \equiv b_1 \pmod{m}$ se, e somente se, $a_1 - b_1 \equiv 0 \pmod{m}$.
- ii) Se $a_1 \equiv b_1 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, então $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$.
- iii) Se $\underline{a_1 \equiv b_1 \pmod{m}}$ e $\underline{a_2 \equiv b_2 \pmod{m}}$, então $\underline{a_1 a_2 \equiv b_1 b_2 \pmod{m}}$.
- iv) Se $a \equiv b \pmod{m}$, então $ax \equiv bx \pmod{m}$, para todo $x \in \mathbb{Z}$.
- v) Vale a lei do cancelamento: se $d \in \mathbb{Z}$ e $\text{mdc}(d, m) = 1$ então $ad \equiv bd \pmod{m}$ implica $a \equiv b \pmod{m}$.

Prova: Provemos o item iii).

$$a_1 \equiv b_1 \pmod{m}$$

Prova: Provemos o item iii).

Como $a_1 \equiv b_1 \pmod{m}$

Prova: Provemos o item iii).

Como $\underline{a_1 \equiv b_1 \pmod m}$ e $\underline{a_2 \equiv b_2 \pmod m}$,

Prova: Provemos o item iii).

Como $a_1 \equiv b_1 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, existem $k, l \in \mathbb{Z}$ tais que

Prova: Provemos o item iii).

Como $a_1 \equiv b_1 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, existem $k, l \in \mathbb{Z}$ tais que

$$\underline{a_1 - b_1 = km}$$

$$\underline{a_2 - b_2 = lm},$$

Prova: Provemos o item iii).

Como $a_1 \equiv b_1 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, existem $k, l \in \mathbb{Z}$ tais que

$$\begin{aligned} a_1 - b_1 &= km \\ a_2 - b_2 &= lm, \end{aligned}$$

isto é,

$$\begin{aligned} a_1 &= b_1 + km \\ a_2 &= b_2 + lm, \end{aligned}$$

$$\underline{a_1 a_2} \equiv \underline{b_1 b_2} \pmod{\sim}$$

Prova: Provemos o item iii).

Como $a_1 \equiv b_1 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, existem $k, l \in \mathbb{Z}$ tais que

$$a_1 - b_1 = km$$

$$a_2 - b_2 = lm,$$

isto é,

$$a_1 = b_1 + km$$

$$a_2 = b_2 + lm,$$

Assim

$$a_1 a_2 =$$

Prova: Provemos o item iii).

Como $a_1 \equiv b_1 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, existem $k, l \in \mathbb{Z}$ tais que

$$a_1 - b_1 = km$$

$$a_2 - b_2 = lm,$$

isto é,

$$a_1 = b_1 + km$$

$$a_2 = b_2 + lm,$$

Assim

$$a_1 a_2 = (\underline{b_1} + km)(\underline{b_2} + lm)$$

Prova: Provemos o item iii).

Como $a_1 \equiv b_1 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, existem $k, l \in \mathbb{Z}$ tais que

$$a_1 - b_1 = km$$

$$a_2 - b_2 = lm,$$

isto é,

$$a_1 = b_1 + km$$

$$a_2 = b_2 + lm,$$

Assim

$$\begin{aligned} a_1 a_2 &= (b_1 + km)(b_2 + lm) \\ &= \underline{b_1 b_2} + \underline{b_1 lm} + \underline{b_2 km} + \underline{klm^2} \end{aligned}$$

Prova: Provemos o item iii).

Como $a_1 \equiv b_1 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, existem $k, l \in \mathbb{Z}$ tais que

$$a_1 - b_1 = km$$

$$a_2 - b_2 = lm,$$

isto é,

$$a_1 = b_1 + km$$

$$a_2 = b_2 + lm,$$

Assim

$$\begin{aligned} a_1 a_2 &= (b_1 + km)(b_2 + lm) \\ &= b_1 b_2 + \cancel{b_1 lm} + b_2 km + klm^2 = \cancel{b_1 b_2} + \underbrace{(lb_1 + kb_2 + klm)}_{\in \mathbb{Z}} m \end{aligned}$$

Prova: Provemos o item iii).

Como $a_1 \equiv b_1 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, existem $k, l \in \mathbb{Z}$ tais que

$$a_1 - b_1 = km$$

$$a_2 - b_2 = lm,$$

isto é,

$$a_1 = b_1 + km$$

$$a_2 = b_2 + lm,$$

Assim

$$\begin{aligned} a_1 a_2 &= (b_1 + km)(b_2 + lm) \\ &= b_1 b_2 + b_1 lm + b_2 km + klm^2 = b_1 b_2 + \underbrace{(lb_1 + kb_2 + klm)}_{\in \mathbb{Z}} m \end{aligned}$$

Prova: Provemos o item iii).

Como $a_1 \equiv b_1 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, existem $k, l \in \mathbb{Z}$ tais que

$$a_1 - b_1 = km$$

$$a_2 - b_2 = lm,$$

isto é,

$$a_1 = b_1 + km$$

$$a_2 = b_2 + lm,$$

Assim

$$\begin{aligned} a_1 a_2 &= (b_1 + km)(b_2 + lm) \\ &= b_1 b_2 + b_1 lm + b_2 km + klm^2 = \cancel{b_1 b_2} + \underbrace{(lb_1 + kb_2 + klm)}_{\in \mathbb{Z}} m \end{aligned}$$

Ou seja, $a_1 a_2 - b_1 b_2 = cm$,

Prova: Provemos o item iii).

Como $a_1 \equiv b_1 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, existem $k, l \in \mathbb{Z}$ tais que

$$a_1 - b_1 = km$$

$$a_2 - b_2 = lm,$$

isto é,

$$a_1 = b_1 + km$$

$$a_2 = b_2 + lm,$$

Assim

$$\begin{aligned} a_1 a_2 &= (b_1 + km)(b_2 + lm) \\ &= b_1 b_2 + b_1 lm + b_2 km + klm^2 = b_1 b_2 + \underbrace{(lb_1 + kb_2 + klm)}_{\in \mathbb{Z}} m \end{aligned}$$

Ou seja, $a_1 a_2 - b_1 b_2 = cm$, onde $c = \underline{lb_1 + kb_2 + klm} \in \mathbb{Z}$.

Prova: Provemos o item iii).

Como $a_1 \equiv b_1 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, existem $k, l \in \mathbb{Z}$ tais que

$$a_1 - b_1 = km$$

$$a_2 - b_2 = lm,$$

isto é,

$$a_1 = b_1 + km$$

$$a_2 = b_2 + lm,$$

Assim

$$\begin{aligned} a_1 a_2 &= (b_1 + km)(b_2 + lm) \\ &= b_1 b_2 + b_1 lm + b_2 km + klm^2 = b_1 b_2 + \underbrace{(lb_1 + kb_2 + klm)}_{\in \mathbb{Z}} m \end{aligned}$$

Ou seja, $\underline{a_1 a_2 - b_1 b_2 = cm}$, onde $c = lb_1 + kb_2 + klm \in \mathbb{Z}$. Portanto,
 $a_1 a_2 \equiv b_1 b_2 \pmod{m}$. ■

Prova: Provemos o item iii).

Como $a_1 \equiv b_1 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, existem $k, l \in \mathbb{Z}$ tais que

$$a_1 - b_1 = km$$

$$a_2 - b_2 = lm,$$

isto é,

$$a_1 = b_1 + km$$

$$a_2 = b_2 + lm,$$

Assim

$$\begin{aligned} a_1 a_2 &= (b_1 + km)(b_2 + lm) \\ &= b_1 b_2 + b_1 lm + b_2 km + klm^2 = b_1 b_2 + \underbrace{(lb_1 + kb_2 + klm)}_{\in \mathbb{Z}} m \end{aligned}$$

Ou seja, $a_1 a_2 - b_1 b_2 = cm$, onde $c = lb_1 + kb_2 + klm \in \mathbb{Z}$. Portanto,
 $a_1 a_2 \equiv b_1 b_2 \pmod{m}$. ■