Congruência módulo m e relações de equivalência em $\mathbb{Z}$

José Antônio O. Freitas

MAT-UnB

Definição

Seja C uma classe de equivalência

Definição

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

$R = \{(x,y) \in A \times A\}$; $A \neq \emptyset$

$y \in R$

$C(y) = \bar{y} = \{x \in A \mid xRy\} \subseteq A$

$(x,y) \in R$

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.*

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

$\overline{1} = \{x \in A \mid x R 1\} = \{1, 2, 3, 4\} = \overline{2}$

$= \overline{3}$

$= \overline{4}$

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 A é a união disjunta das classes $\overline{b}$, $b \in A$, 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 $\overline{b}$, $b \in A$, ou seja,

$$\subseteq$$

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

$$\supseteq$$

$$\overline{a}, \overline{b}$$

$$\overline{a} \cap \overline{b} = \emptyset \quad \text{ou}$$

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

PROVA: PRECISAMOS MOSTRAR QUE

i) $\bigcup_{b\in A} \bar{b} \subseteq A$

ii) $A \subseteq \boxed{\bigcup_{b\in A} \bar{b}}$

PARA MOSTRAR (i) BASTA OBSERVAR QUE DA DEFINIÇÃO DE CLASSE DE EQUIVALÊNCIA, SEGUE QUE $\overline{b} \subseteq A$, PARA TODO $b \in A$. LOGO

PARA TODO $x \in A$

$x R x \Rightarrow x \in \overline{x}$

$\bigcup_{b \in A} \overline{b} \subseteq A$.

AGORA PARA MOSTRAR (iii) SEJA

$x \in A$. DA DEFINIÇÃO DE

RELAÇÃO DE EQUIVALÊNCIA TEMOS

$x \in \overline{x}$, OU SEJA, $x \in \bigcup_{b \in A} \overline{b}$.

LOGO $A \subseteq \bigcup_{b \in A} \overline{b}$.

PORTANTO DE (i) E (ii) TEMOS

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

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 $\overline{b}$, $b \in A$, ou seja,

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

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 $\overline{b}$, $b \in A$, ou seja,

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

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 $b \mid a$.*

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 $b \mid a$. 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 $b \mid a$. 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 $b \mid a$. 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 $a = (-1)(-a)$.*

$1 \mid a$ e $-1 \mid a$

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 $b \mid a$. 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 $b = 0a$.*

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 $b \mid a$. 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 $\pm b$.*

$-b = -1\,b \Rightarrow b \mid -b$

$b = 1\,b \Rightarrow b \mid b$

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 $b \mid a$. 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 $0 = b0$.*

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 $b \mid a$. 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) $3 \nmid 8$. $8 = 3k,\ k \in \mathbb{Z}$

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 $b \mid a$. 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) $17 \mid 51$. $51 = 17 \cdot 3$

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 $b \mid a$. 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) $17 \mid 51$.

$a = a \cdot 1$

Proposição

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

Proposição

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

ii) *Se* $a \mid b$ *e* $b \mid a$, $\boxed{a,\ b > 0}$ *então* $a = b$.

Proposição

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

ii) Se $a \mid b$ *e* $b \mid a$, $a, b > 0$ *então* $a = b$.

iii) Se $a \mid b$ *e* $b \mid c$, *então* $a \mid c$.

Proposição

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

ii) *Se* $a \mid b$ *e* $b \mid a$, $a, b > 0$ *então* $a = b$.

iii) *Se* $a \mid b$ *e* $b \mid c$, *então* $a \mid c$.

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

Proposição

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

ii) Se $a \mid b$ e $b \mid a$, $a, b \geq 0$ então $a = b$.

iii) Se $a \mid b$ e $b \mid c$, então $a \mid c$.

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

PROVA: i) IMEDIATA POIS $a = a \cdot 1$.

ii) COMO $a \mid b$ E $b \mid a$, EXISTEM

$k, l \in \mathbb{Z}$ TAIS QUE

$$b = a \boxed{k} \quad \text{E} \quad \boxed{a = b \cdot \boxed{l}}$$

SUBSTITUINDO A EXPRESSÃO DE a

EM b OBTEMOS

$$b = (b(\ell)n)$$

$$b = b(\ell n)$$

$$b - b(\ln) = 0$$

$$b(1 - \ln) = 0$$

COMO $b > 0$, SEGUE

$$1 - \ln = 0$$

OU SEJA, $kl = 1$. ASSIM $k = l = 1$

OU $k = \cancel{l =} -1$. MAS $a, b > 0$ DAÍ

$k = l = 1$ E COM ISSO $a = b$.

$a \mid c \Leftrightarrow c = a \cdot (k)$

$\in \mathbb{Z}$

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

$k, l \in \mathbb{Z}$ TAIS QUE

$$b = a k \quad \text{e} \quad c = b l$$

ASSIM

$$\boxed{c} = (ak)l = a\underbrace{(kl)}_{\mathbb{Z}}$$

OU SEJA, $a \mid c$.

iv) SUPONHA QUE $a \mid b$ E $a \mid c$.

ASSIM EXISTEM $k, l \in \mathbb{Z}$ TAIS QUE

$$a \mid (bx + cy) \quad ; \quad x, y \in \mathbb{Z}$$

$b = ka$ e $c = la$

Assim dados $x, y \in \mathbb{Z}$ temos

$$bx + cy = (ka)x + (la)y = (a(k))x + (a(l))y$$

$$= a(kx) + a(ly) = a(\underbrace{\underbrace{kx}_{\in \mathbb{Z}} + \underbrace{ly}_{\in \mathbb{Z}}}_{\in \mathbb{Z}})$$

Como $kx + ly \in \mathbb{Z}$, então $a \mid (bx + cy)$.

#

Definição

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

Definição

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

Definição

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

Definição

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

Definição

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

Definição

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

Definição

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

Exemplos

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

Definição

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

Exemplos

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

2) $3 \equiv -5 \pmod 2$, *pois* $2 \mid (3-(-5))$.

$\overset{\shortparallel}{8}$

$8 = 2 \cdot 4$

Definição

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

Exemplos

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

2) $3 \equiv -5 \pmod 2$, *pois* $2 \mid (3-(-5))$.

3) $21 \equiv 3 \pmod 6$, *pois* $6 \mid (\underbrace{21-3}_{18})$.

Definição

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

Exemplos

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

2) $3 \equiv -5 \pmod 2$, *pois* $2 \mid (3 - (-5))$.

3) $21 \equiv 3 \pmod 6$, *pois* $6 \mid (21 - 3)$.

Proposição

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

Proposição

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

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

↳ RELAÇÃO DE EQUIVALÊNCIA.

PROVA: SEJA

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

PROVEMOS QUE R É UMA

RELAÇÃO DE EQUIVALÊNCIA.

$x R x \iff x \equiv x \pmod{m}$

$m \mid (\underbrace{x - x}_{0})$

PRIMEIRO, SEJA $x \in \mathbb{Z}$. COMO

$x - x = 0 = 0 \cdot m$

ENTÃO $x \equiv x \pmod{m}$, OU SEJA,

$x R x$.

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

$m \mid (x-y)$

AGORA, SUPONHA QUE $x R y$. ASSIM

$x \equiv y \pmod{m}$, OU SEJA, $m \mid (x-y)$.

LOGO, EXISTE $k \in \mathbb{Z}$ TAL QUE

$x - y = km$

MAS

$$y - x = -(x - y) = -(mk) = m(\underbrace{-k}_{\in \mathbb{Z}})$$

DAÍ $m \mid (y - x)$, OU SEJA,

$y \equiv x \pmod{m}$. COM ISSO, $y R x$.

POR ÚLTIMO, SUPONHA QUE xRy

E yRz. ASSIM $x \equiv y \pmod{m}$

E $y \equiv z \pmod{m}$. LOGO, $m \mid (x-y)$

E $m \mid (y-z)$. DAÍ

$m \mid [(x-\cancel{y}) + (\cancel{y}-z)]$, ISTO É,

$m \mid (x-z)$. COMO ISSO $x \equiv z \pmod{m}$

E ENTÃO $x R z$.

PORTANTO A CONGRUÊNCIA

MÓDULO m É UMA RELAÇÃO DE

EQUIVALÊNCIA EM $\mathbb{Z}$. #

Teorema

A relação de congruência módulo m satisfaz as seguintes propriedades:

Teorema

A relação de congruência módulo m satisfaz as seguintes propriedades:

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

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* $a_1 \equiv b_1 \pmod{m}$ *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* $a_1 \equiv b_1 \pmod{m}$ *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* $\boxed{x \in \mathbb{Z}}$.

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* $mdc(d, m) = 1$ *então* $ad \equiv bd \pmod{m}$ *implica* $a \equiv b \pmod{m}$.

PROVA: iii) SUPONHA QUE

$a_1 \equiv b_1 \pmod{m}$ E $a_2 \equiv b_2 \pmod{m}$.

ASSIM EXISTEM $k, l \in \mathbb{Z}$ TAIS

QUE

$m \mid (a_1 - b_1)$ e $m \mid (a_2 - b_2)$

$a_1 - b_1 = km$ $\qquad a_2 - b_2 = lm$

$a_1 = b_1 + km$ $\qquad a_2 = b_2 + lm$

Assim

$$a_1 a_2 = (b_1 + km)(b_2 + lm)$$

$$= b_1 b_2 + b_1 l \underline{m} + k \underline{m} b_2 + kl \underline{m}^2$$

$$= b_1 b_2 + m(b_1 l + k b_2 + klm)$$

ou SEJA,

$$\underline{a_1 a_2 - b_1 b_2} = m(\underbrace{b_1 l + k b_2 + k l m}_{\in \mathbb{Z}})$$

ASSIM $m \mid (a_1 a_2 - b_1 b_2)$, LOGO

$$a_1 a_2 \equiv b_1 b_2 \pmod{m}. \qquad \#$$

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* $mdc(d, m) = 1$ *então* $ad \equiv bd \pmod{m}$ *implica* $a \equiv b \pmod{m}$.