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.

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.*

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,

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

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 $b \mid a$.*

MAT-UnB

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 $a = (-1)(-a)$.*

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 $\pm b$.*

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) $3 \nmid 8$.

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) $17 \mid 51$.

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) $17 \mid 51$.

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* $b \mid a$, $a, b > 0$ *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* $b \mid a$, $a, b > 0$ *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* $x, y \in \mathbb{Z}$.

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* $3 \mid (5-2)$.

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* $2 \mid (3-(-5))$.

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* $6 \mid (21 - 3)$.

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 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* $x \in \mathbb{Z}$.

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* $a \equiv b \pmod{m}$.

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* $a \equiv b \pmod{m}$.