

Relação de Equivalência - Classes de Equivalência nos Inteiros

José Antônio O. Freitas

MAT-UnB

29 de agosto de 2020

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 \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,

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

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,

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 $x \in A$.

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, $A = \bigcup_{b \in A} \bar{b}$. ■

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

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 $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.

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 $x, y \in \mathbb{Z}$.

Prova:

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

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 $x, y \in \mathbb{Z}$.

Prova:

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

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 $x, y \in \mathbb{Z}$.

Prova:

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

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 $x, y \in \mathbb{Z}$.

Prova:

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

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 $x, y \in \mathbb{Z}$.

Prova:

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

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 $x, y \in \mathbb{Z}$.

Prova:

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

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 $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a \mid b$ e $b \mid a$, 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) $a \mid a$, 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 $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a \mid b$ e $b \mid a$, 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) $a \mid a$, 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 $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a \mid b$ e $b \mid a$, 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) $a \mid a$, 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 $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a \mid b$ e $b \mid a$, 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) $a \mid a$, 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 $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a \mid b$ e $b \mid a$, 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) $a \mid a$, 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 $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a \mid b$ e $b \mid a$, 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) $a \mid a$, 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 $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a \mid b$ e $b \mid a$, 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) $a \mid a$, 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 $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a \mid b$ e $b \mid a$, 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) $a \mid a$, 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 $x, y \in \mathbb{Z}$.

Prova:

- i) Imediata.
- ii) Como $a \mid b$ e $b \mid a$, 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 $a = b$.

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

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

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

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

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

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, $a \mid c$.

- 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 $a \mid c$

- 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 $c = al$,

- 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 $k, l \in \mathbb{Z}$.

- 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 $bx + cy =$

- 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 $bx + cy = (ka)x + (al)y =$

- 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 $bx + cy = (ka)x + (al)y = a(kx + ly)$

- 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 $kx + ly \in \mathbb{Z}$

- 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 $bx + cy = (ka)x + (al)y = a(kx + ly)$ e como $kx + ly \in \mathbb{Z}$ segue que $a \mid (bx + cy)$. ■

- 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 $kx + ly \in \mathbb{Z}$ segue que $a \mid (bx + cy)$. ■

Definição

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

- 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 $bx + cy = (ka)x + (al)y = a(kx + ly)$ e como $kx + ly \in \mathbb{Z}$ segue que $a \mid (bx + cy)$. ■

Definição

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

- 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 $kx + ly \in \mathbb{Z}$ segue que $a \mid (bx + cy)$. ■

Definição

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

- 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 $kx + ly \in \mathbb{Z}$ segue que $a \mid (bx + cy)$. ■

Definição

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

- 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 $kx + ly \in \mathbb{Z}$ segue que $a \mid (bx + cy)$. ■

Definição

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

- 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 $kx + ly \in \mathbb{Z}$ segue que $a \mid (bx + cy)$. ■

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

- 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 $kx + ly \in \mathbb{Z}$ segue que $a \mid (bx + cy)$. ■

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 $3 \mid (5 - 2)$.

Exemplos

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

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

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 $6 \mid (3 - 9)$.

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} .

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 $m \mid (a - a)$.

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 $m \mid (a - b)$.

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 $(a - b) = km$.

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

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 $m \mid (a - a)$.
- 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 $b \equiv a \pmod{m}$.

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 $a \equiv b \pmod{m}$

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 $b \equiv c \pmod{m}$,

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 $m \mid (a - b)$

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 $m \mid (b - c)$.

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 $m \mid (a - a)$.
- 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, $m \mid [(a - b) + (b - c)]$. Logo, $m \mid (a - c)$,

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 $m \mid (a - a)$.
- 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, $m \mid [(a - b) + (b - c)]$. Logo, $m \mid (a - c)$, 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 $m \mid (a - a)$.
- 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, $m \mid [(a - b) + (b - c)]$. Logo, $m \mid (a - c)$, 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 $m \mid (a - a)$.
- 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, $m \mid [(a - b) + (b - c)]$. Logo, $m \mid (a - c)$, isto é, $a \equiv c \pmod{m}$.

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

Teorema

A relação de congruência módulo m 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 $\text{mdc}(d, m) = 1$ 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 $a_1 \equiv b_1 \pmod{m}$ 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 $a \equiv b \pmod{m}$.

Prova: Provemos o item iii).

Prova: Provemos o item iii).

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

Prova: Provemos o item iii).

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

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

$$a_1 - b_1 = km$$

$$a_2 - b_2 = lm,$$

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

$$a_1 - b_1 = km$$

$$a_2 - b_2 = lm,$$

isto é,

$$a_1 = b_1 + km$$

$$a_2 = b_2 + lm,$$

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

$$a_1 - b_1 = km$$

$$a_2 - b_2 = lm,$$

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

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

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

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

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

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

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

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

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

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

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 $c = lb_1 + kb_2 + klm \in \mathbb{Z}$.

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, $a_1 a_2 - b_1 b_2 = cm$, 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, $a_1 a_2 \equiv b_1 b_2 \pmod{m}$. ■