

# Relação de Equivalência - Classes de Equivalência nos Inteiros - Continuação

José Antônio O. Freitas

MAT-UnB

29 de agosto de 2020

Dado  $n \in \mathbb{Z}$ , temos

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

$$\mathcal{B}_b = \{ x \in \mathbb{Z} \mid x \equiv b \pmod{m} \}$$

$$\begin{aligned} \mathcal{O} &= \{ x \in \mathbb{Z} \mid \underbrace{x \equiv 0 \pmod{m}}_{m \mid (x - 0)} \} = m\mathbb{Z} \\ &\quad (\Rightarrow x = km, k \in \mathbb{Z}) \end{aligned}$$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} =$$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) =$$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid$$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid \underbrace{x \equiv n \pmod{m}}\}.$$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}.$$

Vamos dentoar  $C(n)$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}.$$

Vamos dentoar  $C(n)$  por  $R_m(n)$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}.$$

Vamos denotar  $C(n)$  por  $R_m(n)$  ou  $\underline{\bar{n}}$ ,

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}.$$

Vamos dentoar  $C(n)$  por  $R_m(n)$  ou  $\bar{n}$ , quando não houver possibilidade de confusão.

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}.$$

Vamos dentoar  $C(n)$  por  $R_m(n)$  ou  $\bar{n}$ , quando não houver possibilidade de confusão. Assim fixando  $m > 1$  vamos escrever

$\bar{n}$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}.$$

Vamos dentoar  $C(n)$  por  $R_m(n)$  ou  $\bar{n}$ , quando não houver possibilidade de confusão. Assim fixando  $m > 1$  vamos escrever

$$R_{\underline{m}}(0) =$$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}.$$

Vamos dentoar  $C(n)$  por  $R_m(n)$  ou  $\bar{n}$ , quando não houver possibilidade de confusão. Assim fixando  $m > 1$  vamos escrever

$$R_m(0) = \{x \in \mathbb{Z} \mid$$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}.$$

Vamos dentoar  $C(n)$  por  $R_m(n)$  ou  $\bar{n}$ , quando não houver possibilidade de confusão. Assim fixando  $m > 1$  vamos escrever

$$R_m(0) = \{x \in \mathbb{Z} \mid \underline{x \equiv 0 \pmod{m}}\}$$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}.$$

Vamos dentoar  $C(n)$  por  $R_m(n)$  ou  $\bar{n}$ , quando não houver possibilidade de confusão. Assim fixando  $m > 1$  vamos escrever

$$R_m(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{m}\} = \{x \in \mathbb{Z} \mid$$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}.$$

Vamos dentoar  $C(n)$  por  $R_m(n)$  ou  $\bar{n}$ , quando não houver possibilidade de confusão. Assim fixando  $m > 1$  vamos escrever

$$R_m(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{m}\} = \{x \in \mathbb{Z} \mid \underline{x = mk}, k \in \mathbb{Z}\}$$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}.$$

Vamos dentoar  $C(n)$  por  $R_m(n)$  ou  $\bar{n}$ , quando não houver possibilidade de confusão. Assim fixando  $m > 1$  vamos escrever

$$R_m(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{m}\} = \{x \in \mathbb{Z} \mid x = mk, k \in \mathbb{Z}\} = \underline{m\mathbb{Z}}$$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}.$$

Vamos dentoar  $C(n)$  por  $R_m(n)$  ou  $\bar{n}$ , quando não houver possibilidade de confusão. Assim fixando  $m > 1$  vamos escrever

$$R_m(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{m}\} = \{x \in \mathbb{Z} \mid x = mk, k \in \mathbb{Z}\} = m\mathbb{Z}$$

$$R_m(1) =$$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}.$$

Vamos dentoar  $C(n)$  por  $R_m(n)$  ou  $\bar{n}$ , quando não houver possibilidade de confusão. Assim fixando  $m > 1$  vamos escrever

$$R_m(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{m}\} = \{x \in \mathbb{Z} \mid x = mk, k \in \mathbb{Z}\} = m\mathbb{Z}$$

$$R_m(1) = \{x \in \mathbb{Z} \mid$$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}.$$

Vamos dentoar  $C(n)$  por  $R_m(n)$  ou  $\bar{n}$ , quando não houver possibilidade de confusão. Assim fixando  $m > 1$  vamos escrever

$$R_m(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{m}\} = \{x \in \mathbb{Z} \mid x = mk, k \in \mathbb{Z}\} = m\mathbb{Z}$$

$$R_m(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{m}\}$$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}.$$

Vamos dentoar  $C(n)$  por  $R_m(n)$  ou  $\bar{n}$ , quando não houver possibilidade de confusão. Assim fixando  $m > 1$  vamos escrever

$$R_m(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{m}\} = \{x \in \mathbb{Z} \mid x = mk, k \in \mathbb{Z}\} = m\mathbb{Z}$$

$$R_m(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{m}\} = \{x \in \mathbb{Z} \mid$$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}.$$

Vamos dentoar  $C(n)$  por  $R_m(n)$  ou  $\bar{n}$ , quando não houver possibilidade de confusão. Assim fixando  $m > 1$  vamos escrever

$$R_m(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{m}\} = \{x \in \mathbb{Z} \mid x = mk, k \in \mathbb{Z}\} = m\mathbb{Z}$$

$$R_m(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{m}\} = \{x \in \mathbb{Z} \mid x = \underline{1} + \underline{km}, k \in \mathbb{Z}\}$$

*|km + 1*

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}.$$

Vamos dentoar  $C(n)$  por  $R_m(n)$  ou  $\bar{n}$ , quando não houver possibilidade de confusão. Assim fixando  $m > 1$  vamos escrever

$$R_m(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{m}\} = \{x \in \mathbb{Z} \mid x = mk, k \in \mathbb{Z}\} = m\mathbb{Z}$$

$$R_m(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{m}\} = \{x \in \mathbb{Z} \mid x = 1 + km, k \in \mathbb{Z}\}$$

⋮

$$R_m(\underline{n}) =$$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}.$$

Vamos dentoar  $C(n)$  por  $R_m(n)$  ou  $\bar{n}$ , quando não houver possibilidade de confusão. Assim fixando  $m > 1$  vamos escrever

$$R_m(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{m}\} = \{x \in \mathbb{Z} \mid x = mk, k \in \mathbb{Z}\} = m\mathbb{Z}$$

$$R_m(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{m}\} = \{x \in \mathbb{Z} \mid x = 1 + km, k \in \mathbb{Z}\}$$

⋮

$$R_m(n) = \{x \in \mathbb{Z} \mid$$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}.$$

Vamos dentoar  $C(n)$  por  $R_m(n)$  ou  $\bar{n}$ , quando não houver possibilidade de confusão. Assim fixando  $m > 1$  vamos escrever

$$R_m(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{m}\} = \{x \in \mathbb{Z} \mid x = mk, k \in \mathbb{Z}\} = m\mathbb{Z}$$

$$R_m(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{m}\} = \{x \in \mathbb{Z} \mid x = 1 + km, k \in \mathbb{Z}\}$$

⋮

$$R_m(n) = \{x \in \mathbb{Z} \mid x = \underline{n} + \underline{km}, k \in \mathbb{Z}\}$$

Dado  $n \in \mathbb{Z}$ , temos

$$\bar{n} = C(n) = \{x \in \mathbb{Z} \mid \underline{x \equiv n \pmod{m}}\}.$$

Vamos dentoar  $C(n)$  por  $R_m(n)$  ou  $\bar{n}$ , quando não houver possibilidade de confusão. Assim fixando  $m > 1$  vamos escrever

$$R_m(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{m}\} = \{x \in \mathbb{Z} \mid x = mk, k \in \mathbb{Z}\} = m\mathbb{Z}$$

$$R_m(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{m}\} = \{x \in \mathbb{Z} \mid x = 1 + km, k \in \mathbb{Z}\}$$

⋮

$$R_m(n) = \{x \in \mathbb{Z} \mid x = n + km, k \in \mathbb{Z}\}$$

## Proposição

*As classes de equivalência definidas pela congruência módulo  $m$*

## Proposição

As classes de equivalência definidas pela congruência módulo  $m$  são determinadas pelos restos da divisão inteira por  $m$ .

$\exists m \in \mathbb{Z}, m > 1$ , EXISTEM ÚNICOS  
 $q, r \in \mathbb{Z}$  com  $0 \leq r < m$  TAIIS QUE

$$n = mq + \boxed{r}.$$

## Proposição

*As classes de equivalência definidas pela congruência módulo  $m$  são determinadas pelos restos da divisão inteira por  $m$ . Em outras palavras,  $R_m(n)$*

## Proposição

As classes de equivalência definidas pela congruência módulo  $m$  são determinadas pelos restos da divisão inteira por  $m$ . Em outras palavras,  $\underline{R_m(n)}$  é o conjunto dos números inteiros

## Proposição

As classes de equivalência definidas pela congruência módulo  $m$  são determinadas pelos restos da divisão inteira por  $m$ . Em outras palavras,  $R_m(n)$  é o conjunto dos números inteiros cujo resto na divisão inteira por  $m$  é  $n$ .

## Proposição

As classes de equivalência definidas pela congruência módulo  $m$  são determinadas pelos restos da divisão inteira por  $m$ . Em outras palavras,  $R_m(n)$  é o conjunto dos números inteiros cujo resto na divisão inteira por  $m$  é  $n$ .

## Corolário

$$R_m(\underline{k}) = R_m(\underline{l})$$

$$\bar{a} \cap \bar{b} \neq \emptyset \Leftrightarrow \underline{\underline{a \sim b}} \Rightarrow \underline{\underline{\bar{a} = \bar{b}}}$$

## Proposição

As classes de equivalência definidas pela congruência módulo  $m$  são determinadas pelos restos da divisão inteira por  $m$ . Em outras palavras,  $R_m(n)$  é o conjunto dos números inteiros cujo resto na divisão inteira por  $m$  é  $n$ .

## Corolário

→  $R_m(k) = R_m(l)$  se, e somente se,  $k \equiv l \pmod{m}$ .

## Proposição

As classes de equivalência definidas pela congruência módulo  $m$  são determinadas pelos restos da divisão inteira por  $m$ . Em outras palavras,  $R_m(n)$  é o conjunto dos números inteiros cujo resto na divisão inteira por  $m$  é  $n$ .

## Corolário

$R_m(k) = R_m(l)$  se, e somente se,  $k \equiv l \pmod{m}$ .

## Exemplos

i) Se  $m = 2$ ,

$$\mathcal{R} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \equiv y \pmod{2}\}$$

EXISTEM 2 CLASSES DE EQUIVALENCIA POIS OS POSSÍVEIS NESTA DIVISÃO PELA 2 SÃO 0 E 1

## Exemplos

i) Se  $m = 2$ , então os possíveis restos na divisão inteira por 2 são 0 e 1.

## Exemplos

i) Se  $m = 2$ , então os possíveis restos na divisão inteira por 2 são 0 e 1.  
Logo, existem duas classes de equivalência, a saber

## Exemplos

i) Se  $m = 2$ , então os possíveis restos na divisão inteira por 2 são 0 e 1.  
Logo, existem duas classes de equivalência, a saber

$$R_2(0) = \{ x \in \mathbb{Z} \mid \underbrace{x \equiv 0 \pmod{2}}_{2 \mid (x - 0)} (\Rightarrow 2 \mid x \Rightarrow x = 2k) \}$$

## Exemplos

i) Se  $m = 2$ , então os possíveis restos na divisão inteira por 2 são 0 e 1.  
Logo, existem duas classes de equivalência, a saber

$$R_2(0) = \{x \in \mathbb{Z} \mid$$

## Exemplos

i) Se  $m = 2$ , então os possíveis restos na divisão inteira por 2 são 0 e 1.  
Logo, existem duas classes de equivalência, a saber

$$R_2(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{2}\} =$$

## Exemplos

i) Se  $m = 2$ , então os possíveis restos na divisão inteira por 2 são 0 e 1.  
Logo, existem duas classes de equivalência, a saber

$$R_2(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{2}\} = \{x \in \mathbb{Z} \mid$$

## Exemplos

i) Se  $m = 2$ , então os possíveis restos na divisão inteira por 2 são 0 e 1.  
Logo, existem duas classes de equivalência, a saber

$$R_2(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{2}\} = \{x \in \mathbb{Z} \mid x = 2k, k \in \mathbb{Z}\}$$

$$R_2(0) = \{0, \pm 2, \pm 4, \dots\}$$

## Exemplos

i) Se  $m = 2$ , então os possíveis restos na divisão inteira por 2 são 0 e 1.  
 Logo, existem duas classes de equivalência, a saber

$$R_2(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{2}\} = \{x \in \mathbb{Z} \mid x = 2k, k \in \mathbb{Z}\}$$

$$R_2(1) = \left\{ x \in \mathbb{Z} \mid \underbrace{x \equiv 1 \pmod{2}}_{2|(x-1)} \right\}$$

$$2|(x-1) \Leftrightarrow x-1 = 2l$$

$$\Rightarrow x = 2l+1, l \in \mathbb{Z}$$

## Exemplos

i) Se  $m = 2$ , então os possíveis restos na divisão inteira por 2 são 0 e 1.  
Logo, existem duas classes de equivalência, a saber

$$R_2(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{2}\} = \{x \in \mathbb{Z} \mid x = 2k, k \in \mathbb{Z}\}$$

$$R_2(1) = \{x \in \mathbb{Z} \mid$$

## Exemplos

i) Se  $m = 2$ , então os possíveis restos na divisão inteira por 2 são 0 e 1.  
Logo, existem duas classes de equivalência, a saber

$$R_2(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{2}\} = \{x \in \mathbb{Z} \mid x = 2k, k \in \mathbb{Z}\}$$

$$R_2(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{2}\} =$$

## Exemplos

i) Se  $m = 2$ , então os possíveis restos na divisão inteira por 2 são 0 e 1.  
Logo, existem duas classes de equivalência, a saber

$$R_2(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{2}\} = \{x \in \mathbb{Z} \mid x = 2k, k \in \mathbb{Z}\}$$

$$R_2(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{2}\} = \{x \in \mathbb{Z} \mid$$

## Exemplos

i) Se  $m = 2$ , então os possíveis restos na divisão inteira por 2 são 0 e 1.  
Logo, existem duas classes de equivalência, a saber

$$R_2(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{2}\} = \{x \in \mathbb{Z} \mid x = 2k, k \in \mathbb{Z}\}$$

$$R_2(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{2}\} = \{x \in \mathbb{Z} \mid x = 1 + 2k, k \in \mathbb{Z}\}.$$

## Exemplos

i) Se  $m = 2$ , então os possíveis restos na divisão inteira por 2 são 0 e 1.  
 Logo, existem duas classes de equivalência, a saber

$$R_2(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{2}\} = \{x \in \mathbb{Z} \mid x = 2k, k \in \mathbb{Z}\}$$

$$R_2(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{2}\} = \{x \in \mathbb{Z} \mid x = 1 + 2k, k \in \mathbb{Z}\}.$$

$$\begin{aligned} \mathcal{I} &= \{\pm 1, \pm 3, \dots\} \\ \mathcal{S} &= \{(x, y) \in \mathbb{Z}^2 \mid \underline{x - y} = 2k, k \in \mathbb{Z}\} \end{aligned}$$

## Exemplos

ii) Se  $m = 3$ ,

$$\mathbb{R} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \equiv y \pmod{3}\}$$

$$0 \leq n < 3 \Rightarrow 0 \leq n \leq 2$$

0, 1, 2

## Exemplos

ii) Se  $m = 3$ , então os possíveis restos da divisão inteira são 0, 1 e 2.

## Exemplos

ii) Se  $m = 3$ , então os possíveis restos da divisão inteira são 0, 1 e 2. Daí

## Exemplos

ii) Se  $m = 3$ , então os possíveis restos da divisão inteira são 0, 1 e 2. Daí

$$R_3(0) = \{ x \in \mathbb{Z} \mid x \equiv 0 \pmod{3} \}$$

## Exemplos

ii) Se  $m = 3$ , então os possíveis restos da divisão inteira são 0, 1 e 2. Daí

$$R_3(0) = \{x \in \mathbb{Z} \mid$$

## Exemplos

ii) Se  $m = 3$ , então os possíveis restos da divisão inteira são 0, 1 e 2. Daí

$$R_3(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{3}\} =$$

## Exemplos

ii) Se  $m = 3$ , então os possíveis restos da divisão inteira são 0, 1 e 2. Daí

$$R_3(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{3}\} = \{x \in \mathbb{Z} \mid$$

## Exemplos

ii) Se  $m = 3$ , então os possíveis restos da divisão inteira são 0, 1 e 2. Daí

$$R_3(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{3}\} = \{x \in \mathbb{Z} \mid \underline{x = 3k}, k \in \mathbb{Z}\}$$

$$R_3(0) = \{0, \pm 3, \pm 6, \pm 9, \dots\}$$

## Exemplos

ii) Se  $m = 3$ , então os possíveis restos da divisão inteira são 0, 1 e 2. Daí

$$R_3(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k, k \in \mathbb{Z}\}$$

$$R_3(1) =$$

## Exemplos

ii) Se  $m = 3$ , então os possíveis restos da divisão inteira são 0, 1 e 2. Daí

$$R_3(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k, k \in \mathbb{Z}\}$$

$$R_3(1) = \{x \in \mathbb{Z} \mid$$

## Exemplos

ii) Se  $m = 3$ , então os possíveis restos da divisão inteira são 0, 1 e 2. Daí

$$R_3(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k, k \in \mathbb{Z}\}$$

$$R_3(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{3}\} =$$

$x \equiv 1 \pmod{3}$

## Exemplos

ii) Se  $m = 3$ , então os possíveis restos da divisão inteira são 0, 1 e 2. Daí

$$R_3(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k, k \in \mathbb{Z}\}$$

$$R_3(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{3}\} = \{x \in \mathbb{Z} \mid$$

$$3 \mid (x-1) \quad (\Rightarrow x-1 = 3K)$$

$$x = 3K + 1$$

## Exemplos

ii) Se  $m = 3$ , então os possíveis restos da divisão inteira são 0, 1 e 2. Daí

$$R_3(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k, k \in \mathbb{Z}\}$$

$$R_3(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = \underline{3k+1}, k \in \mathbb{Z}\}$$

$$R_3(1) = \{-5, -2, 0, 1, 4, 7, \dots\}$$

## Exemplos

ii) Se  $m = 3$ , então os possíveis restos da divisão inteira são 0, 1 e 2. Daí

$$R_3(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k, k \in \mathbb{Z}\}$$

$$R_3(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k + 1, k \in \mathbb{Z}\}$$

$$R_3(2) =$$

## Exemplos

ii) Se  $m = 3$ , então os possíveis restos da divisão inteira são 0, 1 e 2. Daí

$$R_3(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k, k \in \mathbb{Z}\}$$

$$R_3(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k + 1, k \in \mathbb{Z}\}$$

$$R_3(2) = \{x \in \mathbb{Z} \mid$$

## Exemplos

ii) Se  $m = 3$ , então os possíveis restos da divisão inteira são 0, 1 e 2. Daí

$$R_3(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k, k \in \mathbb{Z}\}$$

$$R_3(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k + 1, k \in \mathbb{Z}\}$$

$$R_3(2) = \{x \in \mathbb{Z} \mid \underline{x \equiv 2 \pmod{3}}\} =$$

$$3 \mid (x - 2) \quad (\Rightarrow x - 2 = 3k)$$

$$x = 3k + 2$$

## Exemplos

ii) Se  $m = 3$ , então os possíveis restos da divisão inteira são 0, 1 e 2. Daí

$$R_3(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k, k \in \mathbb{Z}\}$$

$$R_3(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k + 1, k \in \mathbb{Z}\}$$

$$R_3(2) = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod{3}\} = \{x \in \mathbb{Z} \mid$$

## Exemplos

ii) Se  $m = 3$ , então os possíveis restos da divisão inteira são 0, 1 e 2. Daí

$$R_3(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k, k \in \mathbb{Z}\}$$

$$R_3(0) = \{0, \pm 3, \pm 6, \pm 9, \dots\}$$

$$R_3(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k + 1, k \in \mathbb{Z}\}$$

$$R_3(1) = \{\dots, -5, -2, 1, 4, 7, \dots\}$$

$$R_3(2) = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k + 2, k \in \mathbb{Z}\}$$

$$R_3(2) = \{\dots, -4, -1, 2, 5, 8, \dots\}$$

## Exemplos

ii) Se  $m = 3$ , então os possíveis restos da divisão inteira são 0, 1 e 2. Daí

$$R_3(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k, k \in \mathbb{Z}\}$$

$$R_3(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k + 1, k \in \mathbb{Z}\}$$

$$R_3(2) = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k + 2, k \in \mathbb{Z}\}$$

## Proposição

*Na relação de equivalência módulo  $m$  existem  $m$  classes de equivalência.*

$$0 \leq r < m$$

$$\begin{array}{c} 0 \leq r \leq m-1 \\ a, b \xrightarrow{r} a \equiv b \pmod{m} \end{array}$$

$$|a - b| < m$$

## Proposição

*Na relação de equivalência módulo  $m$  existem  $m$  classes de equivalência.*

**Prova:** Os possíveis restos na divisão inteira por  $m$

## Proposição

*Na relação de equivalência módulo  $m$  existem  $m$  classes de equivalência.*

**Prova:** Os possíveis restos na divisão inteira por  $m$  são  $0, 1, \dots, (m - 1)$ .

## Proposição

*Na relação de equivalência módulo  $m$  existem  $m$  classes de equivalência.*

**Prova:** Os possíveis restos na divisão inteira por  $m$  são  $0, 1, \dots, (m - 1)$ . Como cada possível resto define uma classe de equivalência diferente,

## Proposição

*Na relação de equivalência módulo  $m$  existem  $m$  classes de equivalência.*

**Prova:** Os possíveis restos na divisão inteira por  $m$  são  $0, 1, \dots, (m - 1)$ . Como cada possível resto define uma classe de equivalência diferente, existem exatamente  $m$  classes de equivalência. ■

## Proposição

*Na relação de equivalência módulo  $m$  existem  $m$  classes de equivalência.*

**Prova:** Os possíveis restos na divisão inteira por  $m$  são  $0, 1, \dots, (m - 1)$ . Como cada possível resto define uma classe de equivalência diferente, existem exatamente  $m$  classes de equivalência. ■

$$\text{Def} \quad R_m(m) = \bar{m}$$

## Observação:

*Fixado  $m$  inteiro positivo,*

## Observação:

*Fixado  $m$  inteiro positivo, denotaremos*

## Observação:

Fixado  $m$  inteiro positivo, denotaremos

$$\underline{R_m(0)} = \overline{0}$$

## Observação:

Fixado  $m$  inteiro positivo, denotaremos

$$R_m(0) = \bar{0}$$

$$R_m(1) = \bar{1}$$

## Observação:

Fixado  $m$  inteiro positivo, denotaremos

$$R_m(0) = \bar{0}$$

$$R_m(1) = \bar{1}$$

⋮

$$R_m(m-1) = \underline{\overline{m-1}}$$

## Observação:

Fixado  $m$  inteiro positivo, denotaremos

$$R_m(0) = \bar{0}$$

$$R_m(1) = \bar{1}$$

⋮

$$R_m(m-1) = \overline{m-1}$$

O conjunto quociente

## Observação:

Fixado  $m$  inteiro positivo, denotaremos

$$R_m(0) = \overline{0}$$

$$R_m(1) = \overline{1}$$

:

$$R_m(m-1) = \overline{m-1}$$

O conjunto quociente desta relação será denotado por  $\frac{\mathbb{Z}}{m\mathbb{Z}}$

## Observação:

Fixado  $m$  inteiro positivo, denotaremos

$$R_m(0) = \bar{0}$$

$$R_m(1) = \bar{1}$$

⋮

$$R_m(m-1) = \overline{m-1}$$

O conjunto quociente desta relação será denotado por  $\frac{\mathbb{Z}}{m\mathbb{Z}}$  ou  $\mathbb{Z}_m$ .

## Observação:

Fixado  $m$  inteiro positivo, denotaremos

$$R_m(0) = \bar{0}$$

$$R_m(1) = \bar{1}$$

⋮

$$R_m(m-1) = \overline{m-1}$$

O conjunto quociente desta relação será denotado por  $\frac{\mathbb{Z}}{m\mathbb{Z}}$  ou  $\mathbb{Z}_m$ . Assim

## Observação:

Fixado  $m$  inteiro positivo, denotaremos

$$R_m(0) = \bar{0}$$

$$R_m(1) = \bar{1}$$

⋮

$$R_m(m-1) = \overline{m-1}$$

O conjunto quociente desta relação será denotado por  $\frac{\mathbb{Z}}{m\mathbb{Z}}$  ou  $\mathbb{Z}_m$ . Assim

$$\underline{\mathbb{Z}_m} =$$

## Observação:

Fixado  $m$  inteiro positivo, denotaremos

$$R_m(0) = \bar{0}$$

$$R_m(1) = \bar{1}$$

⋮

$$R_m(m-1) = \overline{m-1}$$

O conjunto quociente desta relação será denotado por  $\frac{\mathbb{Z}}{m\mathbb{Z}}$  ou  $\mathbb{Z}_m$ . Assim

$$\mathbb{Z}_m = \frac{\mathbb{Z}}{m\mathbb{Z}} =$$

## Observação:

Fixado  $m$  inteiro positivo, denotaremos

$$R_m(0) = \bar{0}$$

$$R_m(1) = \bar{1}$$

⋮

$$R_m(m-1) = \overline{m-1}$$

O conjunto quociente desta relação será denotado por  $\frac{\mathbb{Z}}{m\mathbb{Z}}$  ou  $\mathbb{Z}_m$ . Assim

$$\mathbb{Z}_m = \frac{\mathbb{Z}}{m\mathbb{Z}} = \{\bar{0}, \bar{1}, \dots, \overbrace{\bar{m-1}}^{\text{magenta}}\}.$$

$$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\} \quad ; \quad \mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$$

## Observação:

Fixado  $m$  inteiro positivo, denotaremos

$$R_m(0) = \bar{0}$$

$$R_m(1) = \bar{1}$$

⋮

$$R_m(m-1) = \overline{m-1}$$



O conjunto quociente desta relação será denotado por  $\frac{\mathbb{Z}}{m\mathbb{Z}}$  ou  $\mathbb{Z}_m$ . Assim

$$\mathbb{Z}_m = \frac{\mathbb{Z}}{m\mathbb{Z}} = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}.$$

Vamos definir um meio de somar

Vamos definir um meio de somar e multiplicar os elementos de  $\mathbb{Z}_m$ .

Vamos definir um meio de somar e multiplicar os elementos de  $\mathbb{Z}_m$ . Por exemplo, em  $\mathbb{Z}_2 =$

Vamos definir um meio de somar e multiplicar os elementos de  $\mathbb{Z}_m$ . Por exemplo, em  $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$

Vamos definir um meio de somar e multiplicar os elementos de  $\mathbb{Z}_m$ . Por exemplo, em  $\underline{\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}}$  temos:

$\oplus$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$$\begin{aligned} \bar{0} &= \{\underline{2k}, k \in \mathbb{Z}\} \\ \bar{1} &= \{2l+1, l \in \mathbb{Z}\} \end{aligned}$$

$$\begin{aligned} \bar{0} + \bar{0} &= 2(n+l) \in \bar{0} \\ \underbrace{2n}_{\in \bar{0}} + \underbrace{2l}_{\in \bar{1}} &= \cancel{2(k+l)} + \cancel{2} \end{aligned}$$

$$\underbrace{(2n+1)}_{\in \bar{0}} + \underbrace{(2l+1)}_{\in \bar{1}} = 2(n+l) + 2 = \cancel{2} \underbrace{(n+l+1)}_{\in \bar{0}}$$

$$\bar{0} = \{2k, k \in \mathbb{Z}\}$$

$$\bar{1} = \{2l+1, l \in \mathbb{Z}\}$$

Para multiplicação, temos

$\otimes$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

$$\underbrace{2k}_\in \bar{0} \cdot \underbrace{2k}_\in \bar{0} = \cancel{4k^2} = \cancel{2(2k)} \underbrace{2k}_\in \bar{0}$$

$$\begin{aligned} & (\underbrace{2n}_\in \bar{1})(\underbrace{2l+1}_\in \bar{1}) = \cancel{4nl} + \cancel{2k} \\ & = \cancel{2}(\cancel{2kl} + \cancel{n+l}) \end{aligned}$$

$$\begin{aligned} & (\underbrace{2n+1}_\in \bar{1})(\underbrace{2l+1}_\in \bar{1}) = \cancel{4nl} + \cancel{2k} + \cancel{2l} + \cancel{l} \\ & = \cancel{2}(\cancel{2kl} + \cancel{n+l}) + \cancel{l} \end{aligned}$$

## Definição

Dados  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  definimos

## Definição

Dados  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  definimos

$$\bar{a} \oplus \bar{b} = \overline{\underline{a+b}}$$

## Definição

Dados  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  definimos

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

## Definição

Dados  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  definimos

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

$$\bar{a} \otimes \bar{b} = \overline{\underline{a \cdot b}}$$

## Definição

Dados  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  definimos

$$\left\{ \begin{array}{l} \bar{a} \oplus \bar{b} = \overbrace{\bar{a} + b} \\ \bar{a} \otimes \bar{b} = \overbrace{ab} \end{array} \right.$$

$$\boxed{\bar{0}} = \{ 0, \pm 9, \pm 4, \dots \} = \boxed{\overline{100}} = -\overline{50}$$

$$\boxed{\bar{1}} = \{ \pm 1, \pm 3, \pm 5, \dots \} = \boxed{\overline{1001}} = -\overline{113}$$

## Definição

Dados  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  definimos

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

$$\bar{a} \otimes \bar{b} = \overline{ab}.$$

## Proposição

As operações de soma

## Definição

Dados  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  definimos

$$\left. \begin{array}{l} \bar{a} \oplus \bar{b} = \overline{a + b} \\ \bar{a} \otimes \bar{b} = \overline{ab}. \end{array} \right\}$$

## Proposição

As operações de soma e a multiplicação

## Definição

Dados  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  definimos

$$\textcircled{1} \quad \bar{a} \oplus \bar{b} = \overline{a + b}$$

$$\bar{a} \otimes \textcircled{2} \bar{b} = \overline{ab}.$$

## Proposição

As operações de soma e a multiplicação definidas acima são independentes dos representantes das classes.

## Definição

Dados  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  definimos

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

$$\bar{a} \otimes \bar{b} = \overline{ab}.$$

## Proposição

As operações de soma e a multiplicação definidas acima são independentes dos representantes das classes.

## Prova:

## Definição

Dados  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  definimos

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

$$\bar{a} \otimes \bar{b} = \overline{ab}.$$

## Proposição

As operações de soma e a multiplicação definidas acima são independentes dos representantes das classes.

**Prova:** Dadas duas classes em  $\mathbb{Z}_m$  com representantes diferentes,

## Definição

Dados  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  definimos

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

$$\bar{a} \otimes \bar{b} = \overline{ab}.$$

## Proposição

As operações de soma e a multiplicação definidas acima são independentes dos representantes das classes.

**Prova:** Dadas duas classes em  $\mathbb{Z}_m$  com representantes diferentes,  $\bar{a}_1 = \underline{\bar{a}_2}$  e

## Definição

Dados  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  definimos

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

$$\bar{a} \otimes \bar{b} = \overline{ab}.$$

## Proposição

As operações de soma e a multiplicação definidas acima são independentes dos representantes das classes.

**Prova:** Dadas duas classes em  $\mathbb{Z}_m$  com representantes diferentes,  $\bar{a}_1 = \bar{a}_2$  e  $\bar{b}_1 = \bar{b}_2$ ,

## Definição

Dados  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  definimos

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

$$\bar{a} \otimes \bar{b} = \overline{ab}.$$

## Proposição

As operações de soma e a multiplicação definidas acima são independentes dos representantes das classes.

**Prova:** Dadas duas classes em  $\mathbb{Z}_m$  com representantes diferentes,  $\bar{a}_1 = \bar{a}_2$  e  $\bar{b}_1 = \bar{b}_2$ , com  $a_1 \neq a_2$

## Definição

Dados  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  definimos

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

$$\bar{a} \otimes \bar{b} = \overline{ab}.$$

## Proposição

As operações de soma e a multiplicação definidas acima são independentes dos representantes das classes.

**Prova:** Dadas duas classes em  $\mathbb{Z}_m$  com representantes diferentes,  $\bar{a}_1 = \bar{a}_2$  e  $\bar{b}_1 = \bar{b}_2$ , com  $a_1 \neq a_2$  e  $b_1 \neq b_2$ ,

$$\begin{aligned}\bar{a}_1 \oplus \bar{b}_1 &\stackrel{?}{=} \bar{a}_2 \oplus \bar{b}_2 \\ \bar{a}_1 \otimes \bar{b}_1 &\stackrel{??}{=} \bar{a}_2 \otimes \bar{b}_2\end{aligned}$$

## Definição

Dados  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  definimos

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

$$\bar{a} \otimes \bar{b} = \overline{ab}.$$

## Proposição

As operações de soma e a multiplicação definidas acima são independentes dos representantes das classes.

**Prova:** Dadas duas classes em  $\mathbb{Z}_m$  com representantes diferentes,  $\bar{a}_1 = \bar{a}_2$  e  $\bar{b}_1 = \bar{b}_2$ , com  $a_1 \neq a_2$  e  $b_1 \neq b_2$ , temos:

## Definição

Dados  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  definimos

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

$$\bar{a} \otimes \bar{b} = \overline{ab}.$$

## Proposição

As operações de soma e a multiplicação definidas acima são independentes dos representantes das classes.

**Prova:** Dadas duas classes em  $\mathbb{Z}_m$  com representantes diferentes,  $\bar{a}_1 = \bar{a}_2$  e  $\bar{b}_1 = \bar{b}_2$ , com  $a_1 \neq a_2$  e  $b_1 \neq b_2$ , temos:

$$\underbrace{a_1 \equiv a_2 \pmod{m}}$$

## Definição

Dados  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  definimos

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

$$\bar{a} \otimes \bar{b} = \overline{ab}.$$

## Proposição

As operações de soma e a multiplicação definidas acima são independentes dos representantes das classes.

**Prova:** Dadas duas classes em  $\mathbb{Z}_m$  com representantes diferentes,  $\bar{a}_1 = \bar{a}_2$  e  $\bar{b}_1 = \bar{b}_2$ , com  $a_1 \neq a_2$  e  $b_1 \neq b_2$ , temos:

$$\begin{aligned}\bar{a}_1 \oplus \bar{b}_1 &= \bar{a}_2 \oplus \bar{b}_2 \\ a_1 b_1 &\equiv a_2 b_2 \pmod{m}\end{aligned}$$

$$\begin{aligned}\bar{a}_1 \oplus \bar{b}_1 &= \bar{a}_1 \oplus \bar{b}_2 \\ a_1 + b_1 &\equiv a_2 + b_2 \pmod{m}\end{aligned}$$



Daí,

$$\underline{a_1 + b_1} \equiv \underline{a_2 + b_2} \pmod{m}$$

Daí,

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \pmod{m} \\ \underline{a_1 b_1} &\equiv \underline{a_2 b_2} \pmod{m}. \end{aligned}$$

Daí,

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \pmod{m} \\ a_1 b_1 &\equiv a_2 b_2 \pmod{m}. \end{aligned}$$

Mas de  $\underline{a_1 + b_1} \equiv \underline{a_2 + b_2} \pmod{m}$

$$\overline{\overline{a_1} \oplus \overline{b_1}} = \overline{\overline{a_1 + b_1}} = \overline{a_2 + b_2} = \overline{\overline{a_2} \oplus \overline{b_2}}$$

Daí,

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \pmod{m} \\ a_1 b_1 &\equiv a_2 b_2 \pmod{m}. \end{aligned}$$

Mas de  $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$  segue que  $\overline{a_1 + b_1} =$

Daí,

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \pmod{m} \\ a_1 b_1 &\equiv a_2 b_2 \pmod{m}. \end{aligned}$$

Mas de  $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$  segue que  $\overline{a_1 + b_1} = \overline{\underline{a_2 + b_2}}$ .

Daí,

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \pmod{m} \\ a_1 b_1 &\equiv a_2 b_2 \pmod{m}. \end{aligned}$$

Mas de  $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$  segue que  $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ . Assim

$$\overline{a_1} \oplus \overline{b_1} =$$

Daí,

$$\begin{aligned}a_1 + b_1 &\equiv a_2 + b_2 \pmod{m} \\a_1 b_1 &\equiv a_2 b_2 \pmod{m}.\end{aligned}$$

Mas de  $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$  segue que  $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ . Assim

$$\overline{a_1} \oplus \overline{b_1} = \overline{\underline{a_1 + b_1}} =$$

Daí,

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \pmod{m} \\ a_1 b_1 &\equiv a_2 b_2 \pmod{m}. \end{aligned}$$

Mas de  $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$  segue que  $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ . Assim

$$\overline{a_1} \oplus \overline{b_1} = \overline{a_1 + b_1} = \overline{a_2 + b_2} =$$

Daí,

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \pmod{m} \\ a_1 b_1 &\equiv a_2 b_2 \pmod{m}. \end{aligned}$$

Mas de  $\underline{a}_1 + b_1 \equiv \underline{a}_2 + b_2 \pmod{m}$  segue que  $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ . Assim

$$\overline{\bar{a}_1 \oplus \bar{b}_1} = \overline{\overline{a_1 + b_1}} = \overline{\overline{a_2 + b_2}} = \overline{\bar{a}_2 \oplus \bar{b}_2}.$$

Daí,

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \pmod{m} \\ a_1 b_1 &\equiv a_2 b_2 \pmod{m}. \end{aligned}$$

Mas de  $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$  segue que  $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ . Assim

$$\overline{a_1} \oplus \overline{b_1} = \overline{a_1 + b_1} = \overline{a_2 + b_2} = \overline{a_2} \oplus \overline{b_2}.$$

Agora de  $\underline{a_1} \underline{b_1} \equiv \underline{a_2} \underline{b_2} \pmod{m}$

$$\underline{\overline{a}_1 \otimes \overline{b}_1} = \overline{\underline{a}_1} \underline{b_1} = \overline{\underline{a}_2} \underline{b_2} = \underline{\overline{a}_2 \otimes \overline{b}_2}$$

Daí,

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \pmod{m} \\ a_1 b_1 &\equiv a_2 b_2 \pmod{m}. \end{aligned}$$

Mas de  $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$  segue que  $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ . Assim

$$\overline{a_1} \oplus \overline{b_1} = \overline{a_1 + b_1} = \overline{a_2 + b_2} = \overline{a_2} \oplus \overline{b_2}.$$

Agora de  $a_1 b_1 \equiv a_2 b_2 \pmod{m}$  segue que  $\overline{a_1 b_2} =$

Daí,

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \pmod{m} \\ a_1 b_1 &\equiv a_2 b_2 \pmod{m}. \end{aligned}$$

Mas de  $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$  segue que  $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ . Assim

$$\overline{a_1} \oplus \overline{b_1} = \overline{a_1 + b_1} = \overline{a_2 + b_2} = \overline{a_2} \oplus \overline{b_2}.$$

Agora de  $a_1 b_1 \equiv a_2 b_2 \pmod{m}$  segue que  $\overline{a_1 b_1} = \overline{a_2 b_2}$ .

Daí,

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \pmod{m} \\ a_1 b_1 &\equiv a_2 b_2 \pmod{m}. \end{aligned}$$

Mas de  $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$  segue que  $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ . Assim

$$\overline{a_1} \oplus \overline{b_1} = \overline{a_1 + b_1} = \overline{a_2 + b_2} = \overline{a_2} \oplus \overline{b_2}.$$

Agora de  $a_1 b_1 \equiv a_2 b_2 \pmod{m}$  segue que  $\overline{a_1 b_1} = \overline{a_2 b_2}$ . Assim

$$\underline{\overline{a_1}} \otimes \underline{\overline{b_1}} =$$

Daí,

$$\begin{aligned}a_1 + b_1 &\equiv a_2 + b_2 \pmod{m} \\a_1 b_1 &\equiv a_2 b_2 \pmod{m}.\end{aligned}$$

Mas de  $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$  segue que  $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ . Assim

$$\overline{a_1} \oplus \overline{b_1} = \overline{a_1 + b_1} = \overline{a_2 + b_2} = \overline{a_2} \oplus \overline{b_2}.$$

Agora de  $a_1 b_1 \equiv a_2 b_2 \pmod{m}$  segue que  $\overline{a_1 b_1} = \overline{a_2 b_2}$ . Assim

$$\overline{a_1} \otimes \overline{b_1} = \overline{\underline{a_1 b_1}} =$$

Daí,

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \pmod{m} \\ a_1 b_1 &\equiv a_2 b_2 \pmod{m}. \end{aligned}$$

Mas de  $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$  segue que  $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ . Assim

$$\overline{a_1} \oplus \overline{b_1} = \overline{a_1 + b_1} = \overline{a_2 + b_2} = \overline{a_2} \oplus \overline{b_2}.$$

Agora de  $a_1 b_1 \equiv a_2 b_2 \pmod{m}$  segue que  $\overline{a_1 b_1} = \overline{a_2 b_2}$ . Assim

$$\overline{a_1} \otimes \overline{b_1} = \overline{a_1 b_1} = \underline{\overline{a_2 b_2}} =$$

Daí,

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \pmod{m} \\ a_1 b_1 &\equiv a_2 b_2 \pmod{m}. \end{aligned}$$

Mas de  $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$  segue que  $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ . Assim

$$\overline{a_1} \oplus \overline{b_1} = \overline{a_1 + b_1} = \overline{a_2 + b_2} = \overline{a_2} \oplus \overline{b_2}.$$

Agora de  $a_1 b_1 \equiv a_2 b_2 \pmod{m}$  segue que  $\overline{a_1 b_1} = \overline{a_2 b_2}$ . Assim

$$\overline{a_1} \otimes \overline{b_1} = \overline{a_1 b_1} = \overline{a_2 b_2} = \overline{\cancel{a_2}} \otimes \overline{\cancel{b_2}}.$$

Daí,

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \pmod{m} \\ a_1 b_1 &\equiv a_2 b_2 \pmod{m}. \end{aligned}$$

•

Mas de  $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$  segue que  $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ . Assim

$$\overline{a_1} \oplus \overline{b_1} = \overline{a_1 + b_1} = \overline{a_2 + b_2} = \overline{a_2} \oplus \overline{b_2}.$$

Agora de  $a_1 b_1 \equiv a_2 b_2 \pmod{m}$  segue que  $\overline{a_1 b_1} = \overline{a_2 b_2}$ . Assim

$$\overline{a_1} \otimes \overline{b_1} = \overline{a_1 b_1} = \overline{a_2 b_2} = \overline{a_2} \otimes \overline{b_2}.$$

Portanto a soma e a multiplicação

Daí,

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \pmod{m} \\ a_1 b_1 &\equiv a_2 b_2 \pmod{m}. \end{aligned}$$

Mas de  $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$  segue que  $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ . Assim

$$\overline{a_1} \oplus \overline{b_1} = \overline{a_1 + b_1} = \overline{a_2 + b_2} = \overline{a_2} \oplus \overline{b_2}.$$

Agora de  $a_1 b_1 \equiv a_2 b_2 \pmod{m}$  segue que  $\overline{a_1 b_1} = \overline{a_2 b_2}$ . Assim

$$\overline{a_1} \otimes \overline{b_1} = \overline{a_1 b_1} = \overline{a_2 b_2} = \overline{a_2} \otimes \overline{b_2}.$$

Portanto a soma e a multiplicação não dependem dos representantes que escolhemos para as classes de equivalência,

Daí,

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \pmod{m} \\ a_1 b_1 &\equiv a_2 b_2 \pmod{m}. \end{aligned}$$

Mas de  $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$  segue que  $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ . Assim

$$\overline{a_1} \oplus \overline{b_1} = \overline{a_1 + b_1} = \overline{a_2 + b_2} = \overline{a_2} \oplus \overline{b_2}.$$

Agora de  $a_1 b_1 \equiv a_2 b_2 \pmod{m}$  segue que  $\overline{a_1 b_1} = \overline{a_2 b_2}$ . Assim

$$\overline{a_1} \otimes \overline{b_1} = \overline{a_1 b_1} = \overline{a_2 b_2} = \overline{a_2} \otimes \overline{b_2}.$$

Portanto a soma e a multiplicação não dependem dos representantes que escolhemos para as classes de equivalência, como queríamos. ■

## Exemplo

A soma e a multiplicação em  $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

## Exemplo

A soma e a multiplicação em  $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$  são dadas nas tabelas abaixo:

## Exemplo

A soma e a multiplicação em  $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$  são dadas nas tabelas abaixo:

Tabela: Soma em  $\mathbb{Z}_4$

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$$\bar{0} \oplus \bar{0} = \bar{0} + \bar{0} = \bar{0}$$

$$\bar{1} \oplus \bar{1} = \bar{1} + \bar{1} = \bar{2}$$

$$\bar{1} \oplus \bar{2} = \bar{1} + \bar{2} = \bar{3}$$

$$\bar{1} \oplus \bar{3} = \bar{1} + \bar{3} = \bar{4} = \bar{0}$$

$$\bar{2} \oplus \bar{2} = \bar{2} + \bar{2} = \bar{4} = \bar{0}$$

$$\bar{2} \oplus \bar{3} = \bar{2} + \bar{3} = \bar{5} = \bar{1}$$

$$\bar{3} \oplus \bar{3} = \bar{3} + \bar{3} = \bar{6} = \bar{2}$$

## Exemplo

Tabela: Multiplicação em  $\mathbb{Z}_4$

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{1}$

$$\bar{0} \otimes \bar{b} = \bar{0} \cdot \bar{b} = \bar{0}$$

$$\bar{1} \otimes \bar{b} = \bar{1} \cdot \bar{b} = \bar{b}$$

$$\bar{2} \otimes \bar{2} = \bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$$

$$\bar{2} \otimes \bar{3} = \bar{2} \cdot \bar{3} = \bar{6} = \bar{2}$$

$$\bar{3} \otimes \bar{3} = \bar{3} \cdot \bar{3} = \bar{9} = \bar{1}$$

$\mathbb{Z}_m$ ,  $\bar{a} + \bar{b}$   $a+b > m$

# Proposição

*As operações de soma  $\oplus$*

# Proposição

*As operações de soma  $\oplus$  e multiplicação  $\otimes$*

## Proposição

As operações de soma  $\oplus$  e multiplicação  $\otimes$  em  $\mathbb{Z}_m$  satisfazem as seguintes propriedades:

## Proposição

As operações de soma  $\oplus$  e multiplicação  $\otimes$  em  $\mathbb{Z}_m$  satisfazem as seguintes propriedades:

- i) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :

## Proposição

As operações de soma  $\oplus$  e multiplicação  $\otimes$  em  $\mathbb{Z}_m$  satisfazem as seguintes propriedades:

- i) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\underline{\bar{x}} \oplus \underline{\bar{y}} = \underline{\bar{y}} \oplus \underline{\bar{x}}$ .

## Proposição

As operações de soma  $\oplus$  e multiplicação  $\otimes$  em  $\mathbb{Z}_m$  satisfazem as seguintes propriedades:

i) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \oplus \bar{y} = \bar{y} \oplus \bar{x}$ .

ii) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :

## Proposição

As operações de soma  $\oplus$  e multiplicação  $\otimes$  em  $\mathbb{Z}_m$  satisfazem as seguintes propriedades:

- i) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \oplus \bar{y} = \bar{y} \oplus \bar{x}$ .
- ii) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} =$

## Proposição

As operações de soma  $\oplus$  e multiplicação  $\otimes$  em  $\mathbb{Z}_m$  satisfazem as seguintes propriedades:

i) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \oplus \bar{y} = \bar{y} \oplus \bar{x}$ .

ii) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .

## Proposição

As operações de soma  $\oplus$  e multiplicação  $\otimes$  em  $\mathbb{Z}_m$  satisfazem as seguintes propriedades:

- i) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \oplus \bar{y} = \bar{y} \oplus \bar{x}$ .
- ii) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .
- iii) Para todo  $\underline{\bar{x}} \in \mathbb{Z}_m$ ,

## Proposição

As operações de soma  $\oplus$  e multiplicação  $\otimes$  em  $\mathbb{Z}_m$  satisfazem as seguintes propriedades:

- i) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \oplus \bar{y} = \bar{y} \oplus \bar{x}$ .
- ii) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .
- iii) Para todo  $\bar{x} \in \mathbb{Z}_m$ ,  $\bar{x} \oplus \textcircled{0} = \underline{\bar{x}}$ .

## Proposição

As operações de soma  $\oplus$  e multiplicação  $\otimes$  em  $\mathbb{Z}_m$  satisfazem as seguintes propriedades:

- i) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \oplus \bar{y} = \bar{y} \oplus \bar{x}$ .
- ii) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .
- iii) Para todo  $\bar{x} \in \mathbb{Z}_m$ ,  $\bar{x} \oplus \bar{0} = \bar{x}$ .
- iv) Para todo  $\bar{x} \in \mathbb{Z}_m$ ,

## Proposição

As operações de soma  $\oplus$  e multiplicação  $\otimes$  em  $\mathbb{Z}_m$  satisfazem as seguintes propriedades:

- i) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \oplus \bar{y} = \bar{y} \oplus \bar{x}$ .
- ii) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .
- iii) Para todo  $\bar{x} \in \mathbb{Z}_m$ ,  $\bar{x} \oplus \bar{0} = \bar{x}$ .
- iv) Para todo  $\bar{x} \in \mathbb{Z}_m$ , existe  $\bar{y} \in \mathbb{Z}_m$

## Proposição

As operações de soma  $\oplus$  e multiplicação  $\otimes$  em  $\mathbb{Z}_m$  satisfazem as seguintes propriedades:

- i) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \oplus \bar{y} = \bar{y} \oplus \bar{x}$ .
- ii) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .
- iii) Para todo  $\bar{x} \in \mathbb{Z}_m$ ,  $\bar{x} \oplus \bar{0} = \bar{x}$ .
- iv) Para todo  $\bar{x} \in \mathbb{Z}_m$ , existe  $\bar{y} \in \mathbb{Z}_m$  tal que  $\underline{\bar{x} \oplus \bar{y}} = \bar{0}$ . ←

$$\begin{aligned} x \in \mathbb{Z}, \text{ existe } y \text{ com} \\ x+y=0 \end{aligned}$$

## Proposição

As operações de soma  $\oplus$  e multiplicação  $\otimes$  em  $\mathbb{Z}_m$  satisfazem as seguintes propriedades:

- i) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \oplus \bar{y} = \bar{y} \oplus \bar{x}$ .
- ii) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .
- iii) Para todo  $\bar{x} \in \mathbb{Z}_m$ ,  $\bar{x} \oplus \bar{0} = \bar{x}$ .
- iv) Para todo  $\bar{x} \in \mathbb{Z}_m$ , existe  $\bar{y} \in \mathbb{Z}_m$  tal que  $\bar{x} \oplus \bar{y} = \bar{0}$ .
- v) Para todos  $\bar{x}$ ,  $\bar{y} \in \mathbb{Z}_m$ :

## Proposição

As operações de soma  $\oplus$  e multiplicação  $\otimes$  em  $\mathbb{Z}_m$  satisfazem as seguintes propriedades:

- i) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \oplus \bar{y} = \bar{y} \oplus \bar{x}$ .
- ii) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .
- iii) Para todo  $\bar{x} \in \mathbb{Z}_m$ ,  $\bar{x} \oplus \bar{0} = \bar{x}$ .
- iv) Para todo  $\bar{x} \in \mathbb{Z}_m$ , existe  $\bar{y} \in \mathbb{Z}_m$  tal que  $\bar{x} \oplus \bar{y} = \bar{0}$ .
- v) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\underline{\bar{x}} \otimes \underline{\bar{y}} = \underline{\bar{y}} \otimes \underline{\bar{x}}$ .

## Proposição

As operações de soma  $\oplus$  e multiplicação  $\otimes$  em  $\mathbb{Z}_m$  satisfazem as seguintes propriedades:

- i) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \oplus \bar{y} = \bar{y} \oplus \bar{x}$ .
- ii) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .
- iii) Para todo  $\bar{x} \in \mathbb{Z}_m$ ,  $\bar{x} \oplus \bar{0} = \bar{x}$ .
- iv) Para todo  $\bar{x} \in \mathbb{Z}_m$ , existe  $\bar{y} \in \mathbb{Z}_m$  tal que  $\bar{x} \oplus \bar{y} = \bar{0}$ .
- v) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \otimes \bar{y} = \bar{y} \otimes \bar{x}$ .
- vi) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :

## Proposição

As operações de soma  $\oplus$  e multiplicação  $\otimes$  em  $\mathbb{Z}_m$  satisfazem as seguintes propriedades:

- i) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \oplus \bar{y} = \bar{y} \oplus \bar{x}$ .
- ii) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .
- iii) Para todo  $\bar{x} \in \mathbb{Z}_m$ ,  $\bar{x} \oplus \bar{0} = \bar{x}$ .
- iv) Para todo  $\bar{x} \in \mathbb{Z}_m$ , existe  $\bar{y} \in \mathbb{Z}_m$  tal que  $\bar{x} \oplus \bar{y} = \bar{0}$ .
- v) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \otimes \bar{y} = \bar{y} \otimes \bar{x}$ .
- vi) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \otimes \bar{y}) \otimes \bar{z} =$

## Proposição

As operações de soma  $\oplus$  e multiplicação  $\otimes$  em  $\mathbb{Z}_m$  satisfazem as seguintes propriedades:

- i) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \oplus \bar{y} = \bar{y} \oplus \bar{x}$ .
- ii) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .
- iii) Para todo  $\bar{x} \in \mathbb{Z}_m$ ,  $\bar{x} \oplus \bar{0} = \bar{x}$ .
- iv) Para todo  $\bar{x} \in \mathbb{Z}_m$ , existe  $\bar{y} \in \mathbb{Z}_m$  tal que  $\bar{x} \oplus \bar{y} = \bar{0}$ .
- v) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \otimes \bar{y} = \bar{y} \otimes \bar{x}$ .
- vi) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \otimes \bar{y}) \otimes \bar{z} = \bar{x} \otimes (\bar{y} \otimes \bar{z})$ .

## Proposição

As operações de soma  $\oplus$  e multiplicação  $\otimes$  em  $\mathbb{Z}_m$  satisfazem as seguintes propriedades:

- i) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \oplus \bar{y} = \bar{y} \oplus \bar{x}$ .
- ii) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .
- iii) Para todo  $\bar{x} \in \mathbb{Z}_m$ ,  $\bar{x} \oplus \bar{0} = \bar{x}$ .
- iv) Para todo  $\bar{x} \in \mathbb{Z}_m$ , existe  $\bar{y} \in \mathbb{Z}_m$  tal que  $\bar{x} \oplus \bar{y} = \bar{0}$ .
- v) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \otimes \bar{y} = \bar{y} \otimes \bar{x}$ .
- vi) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \otimes \bar{y}) \otimes \bar{z} = \bar{x} \otimes (\bar{y} \otimes \bar{z})$ .
- vii) Para todo  $\underline{\bar{x}} \in \mathbb{Z}_m$ :

## Proposição

As operações de soma  $\oplus$  e multiplicação  $\otimes$  em  $\mathbb{Z}_m$  satisfazem as seguintes propriedades:

- i) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \oplus \bar{y} = \bar{y} \oplus \bar{x}$ .
- ii) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .
- iii) Para todo  $\bar{x} \in \mathbb{Z}_m$ ,  $\bar{x} \oplus \bar{0} = \bar{x}$ .
- iv) Para todo  $\bar{x} \in \mathbb{Z}_m$ , existe  $\bar{y} \in \mathbb{Z}_m$  tal que  $\bar{x} \oplus \bar{y} = \bar{0}$ .
- v) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \otimes \bar{y} = \bar{y} \otimes \bar{x}$ .
- vi) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \otimes \bar{y}) \otimes \bar{z} = \bar{x} \otimes (\bar{y} \otimes \bar{z})$ .
- vii) Para todo  $\bar{x} \in \mathbb{Z}_m$ :  $\bar{x} \otimes \bar{1} = \bar{x}$ .

## Proposição

As operações de soma  $\oplus$  e multiplicação  $\otimes$  em  $\mathbb{Z}_m$  satisfazem as seguintes propriedades:

- i) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\underline{\bar{x}} \oplus \underline{\bar{y}} = \underline{\bar{y}} \oplus \underline{\bar{x}}$ .
- ii) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .
- iii) Para todo  $\bar{x} \in \mathbb{Z}_m$ ,  $\bar{x} \oplus \bar{0} = \bar{x}$ .
- iv) Para todo  $\bar{x} \in \mathbb{Z}_m$ , existe  $\bar{y} \in \mathbb{Z}_m$  tal que  $\bar{x} \oplus \bar{y} = \bar{0}$ .
- v) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \otimes \bar{y} = \bar{y} \otimes \bar{x}$ .
- vi) Para todos  $\bar{x}, \bar{y}$  e  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \otimes \bar{y}) \otimes \bar{z} = \bar{x} \otimes (\bar{y} \otimes \bar{z})$ .
- vii) Para todo  $\bar{x} \in \mathbb{Z}_m$ :  $\bar{x} \otimes \bar{1} = \bar{x}$ .

Prova:

$$\overline{x \oplus y} = \overline{\boxed{x+y}} = \overline{y+x} = \overline{y} \oplus \overline{x}$$

**Prova:**

i)  $\underline{\bar{x}} \oplus \underline{\bar{y}} =$

**Prova:**

i)  $\bar{x} \oplus \bar{y} = \underline{\underline{\bar{x} + y}} =$

**Prova:**

i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \underline{\overline{y+x}} =$

**Prova:**

i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \underline{\bar{y} \oplus \bar{x}}$ .

ii)  $\underline{\bar{x} \oplus \bar{y}} \oplus z = \overline{\bar{x}+y} + \bar{z} = \overline{(x+y)+z}$

$$= \overline{x+(\bar{y}+z)} = \bar{x} \oplus \overline{\bar{y}+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$$

**Prova:**

i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}$ .

**Prova:**

i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}$ .

ii)  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} =$

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \underline{\overline{x+y}}$$

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \underline{\bar{z}} =$$

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \underline{\underline{(\overline{x+y}) + z}} =$$

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y) + z} = \overline{x + \underline{(y+z)}}$$

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y) + z} = \overline{x + (y+z)} = \bar{x} \oplus$$

**Prova:**

$$\text{i}) \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii}) (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y) + z} = \overline{x + (y+z)} = \underline{\bar{x}} \oplus \underline{\overline{y+z}}$$

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y) + z} = \overline{x + (y+z)} = \bar{x} \oplus \overline{y+z} = \\ \bar{x} \oplus$$

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y) + z} = \overline{x + (y+z)} = \bar{x} \oplus \overline{y+z} = \\ \bar{x} \oplus (\bar{y} \oplus \bar{z}).$$

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y) + z} = \overline{x + (y+z)} = \bar{x} \oplus \overline{y+z} = \\ \bar{x} \oplus (\bar{y} \oplus \bar{z}).$$

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y) + z} = \overline{x + (y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z}).$$

$$\text{iii) } \bar{x} \oplus \bar{0} = \cancel{\bar{x} + 0} = \bar{x}$$

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y) + z} = \overline{x + (y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z}).$$

$$\text{iii) } \bar{x} \oplus \bar{0} = \overline{x+0} =$$

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y) + z} = \overline{x + (y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z}).$$

$$\text{iii) } \bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}.$$

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y) + z} = \overline{x + (y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z}).$$

$$\text{iii) } \bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}.$$

**Prova:**

- i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}$ .
- ii)  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .
- iii)  $\bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}$ .
- iv) Dado  $\bar{x} \in \mathbb{Z}_m$

$$\begin{aligned} \bar{y} &\in \mathbb{Z}_m & x+y &= m \\ -y &= \overline{m-x} && \in \mathbb{Z} \\ && \nwarrow & \\ && \mathbb{Z}_m & \end{aligned}$$

**Prova:**

i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}$ .

ii)  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .

iii)  $\bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}$ .

iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\underline{\bar{y}} =$

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z}).$$

$$\text{iii) } \bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}.$$

iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\bar{y} = \underline{\underline{m-x}} \in \mathbb{Z}_m$ .

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{\bar{x} + \bar{y}} = \overline{\bar{y} + \bar{x}} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{\bar{x} + \bar{y}} \oplus \bar{z} = \overline{(\bar{x} + \bar{y}) + \bar{z}} = \overline{\bar{x} + (\bar{y} + \bar{z})} = \bar{x} \oplus \overline{\bar{y} + \bar{z}} = \bar{x} \oplus (\bar{y} \oplus \bar{z}).$$

$$\text{iii) } \bar{x} \oplus \bar{0} = \overline{\bar{x} + \bar{0}} = \bar{x}.$$

iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\bar{y} = \overline{m - x} \in \mathbb{Z}_m$ . Assim  
 $\bar{x} \oplus \bar{y} =$

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z}).$$

$$\text{iii) } \bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}.$$

iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\bar{y} = \overline{m-x} \in \mathbb{Z}_m$ . Assim

$$\bar{x} \oplus \bar{y} = \cancel{\bar{x}} \oplus$$

**Prova:**

i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}$ .

ii)  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .

iii)  $\bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}$ .

iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\bar{y} = \overline{m-x} \in \mathbb{Z}_m$ . Assim  
 $\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \cancel{\bar{x} + (m-x)} = \cancel{m} = \bar{0}$

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y) + z} = \overline{x + (y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z}).$$

$$\text{iii) } \bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}.$$

$$\text{iv) Dado } \bar{x} \in \mathbb{Z}_m \text{ escolha } \bar{y} = \overline{m-x} \in \mathbb{Z}_m. \text{ Assim}$$
$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \underline{\bar{x} + (m-x)} =$$

**Prova:**

- i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}$ .
- ii)  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .
- iii)  $\bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}$ .
- iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\bar{y} = \overline{m-x} \in \mathbb{Z}_m$ . Assim  
 $\bar{x} \oplus \bar{y} = \bar{x} \oplus m-x = x + (m-x) = \underline{\bar{m}} = \underline{\bar{0}}$ .

**Prova:**

- i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}$ .
- ii)  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .
- iii)  $\bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}$ .
- iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\bar{y} = \overline{m-x} \in \mathbb{Z}_m$ . Assim  
 $\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x+(m-x)} = \overline{m} = \bar{0}$ .

**Prova:**

i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}$ .

ii)  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .

iii)  $\bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}$ .

iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\bar{y} = \overline{m-x} \in \mathbb{Z}_m$ . Assim  
 $\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x+(m-x)} = \overline{m} = \bar{0}$ .

v)  $\bar{x} \otimes \bar{y} = \overline{\cancel{x} \cdot \cancel{y}} = \overline{y \cdot x} = \bar{y} \otimes \bar{x}$

**Prova:**

i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}$ .

ii)  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .

iii)  $\bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}$ .

iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\bar{y} = \overline{m-x} \in \mathbb{Z}_m$ . Assim  
 $\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x+(m-x)} = \overline{m} = \bar{0}$ .

v)  $\bar{x} \otimes \bar{y} = \overline{x \cdot y} =$

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z}).$$

$$\text{iii) } \bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}.$$

$$\text{iv) Dado } \bar{x} \in \mathbb{Z}_m \text{ escolha } \bar{y} = \overline{m-x} \in \mathbb{Z}_m. \text{ Assim}$$
$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x+(m-x)} = \overline{m} = \bar{0}.$$

$$\text{v) } \bar{x} \otimes \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} =$$

**Prova:**

- i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$
- ii)  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z}).$
- iii)  $\bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}.$
- iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\bar{y} = \overline{m-x} \in \mathbb{Z}_m$ . Assim  
 $\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x+(m-x)} = \overline{m} = \bar{0}.$
- v)  $\bar{x} \otimes \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \otimes \bar{x}.$

**Prova:**

- i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$
- ii)  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z}).$
- iii)  $\bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}.$
- iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\bar{y} = \overline{m-x} \in \mathbb{Z}_m$ . Assim  
 $\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x+(m-x)} = \overline{m} = \bar{0}.$
- v)  $\bar{x} \otimes \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \otimes \bar{x}.$

**Prova:**

- i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}$ .
- ii)  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .
- iii)  $\bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}$ .
- iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\bar{y} = \overline{m-x} \in \mathbb{Z}_m$ . Assim  
 $\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x+(m-x)} = \overline{m} = \bar{0}$ .
- v)  $\bar{x} \otimes \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \otimes \bar{x}$ .
- vi)  $(\bar{x} \otimes \bar{y}) \otimes \bar{z} = \overline{\bar{x} \cdot \bar{y}} \otimes \bar{z} = \overline{(\bar{x} \cdot \bar{y}) \cdot \bar{z}} = \overline{\bar{x} \cdot (\bar{y} \bar{z})} =$   
 $= \bar{x} \otimes \overline{\bar{y} \cdot \bar{z}} = \bar{x} \otimes (\bar{y} \otimes \bar{z})$

**Prova:**

- i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$
- ii)  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z}).$
- iii)  $\bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}.$
- iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\bar{y} = \overline{m-x} \in \mathbb{Z}_m$ . Assim  
 $\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x+(m-x)} = \overline{m} = \bar{0}.$
- v)  $\bar{x} \otimes \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \otimes \bar{x}.$
- vi)  $(\bar{x} \otimes \bar{y}) \otimes \bar{z} = \underline{\bar{x} \cdot y} \otimes$

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z}).$$

$$\text{iii) } \bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}.$$

$$\text{iv) Dado } \bar{x} \in \mathbb{Z}_m \text{ escolha } \bar{y} = \overline{m-x} \in \mathbb{Z}_m. \text{ Assim}$$
$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x+(m-x)} = \overline{m} = \bar{0}.$$

$$\text{v) } \bar{x} \otimes \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \otimes \bar{x}.$$

$$\text{vi) } (\bar{x} \otimes \bar{y}) \otimes \bar{z} = \overline{x \cdot y} \otimes \bar{z} =$$

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y) + z} = \overline{x + (y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z}).$$

$$\text{iii) } \bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}.$$

$$\text{iv) Dado } \bar{x} \in \mathbb{Z}_m \text{ escolha } \bar{y} = \overline{m-x} \in \mathbb{Z}_m. \text{ Assim}$$
$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x + (m-x)} = \overline{m} = \bar{0}.$$

$$\text{v) } \bar{x} \otimes \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \otimes \bar{x}.$$

$$\text{vi) } (\bar{x} \otimes \bar{y}) \otimes \bar{z} = \overline{x \cdot y} \otimes \bar{z} = \overline{\underline{(x \cdot y) \cdot z}}$$

**Prova:**

i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}$ .

ii)  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .

iii)  $\bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}$ .

iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\bar{y} = \overline{m-x} \in \mathbb{Z}_m$ . Assim  
 $\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x+(m-x)} = \overline{m} = \bar{0}$ .

v)  $\bar{x} \otimes \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \otimes \bar{x}$ .

vi)  $(\bar{x} \otimes \bar{y}) \otimes \bar{z} = \overline{x \cdot y} \otimes \bar{z} = \overline{(x \cdot y) \cdot z} = \overline{x \cdot (\cancel{y \cdot z})} =$

**Prova:**

- i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}$ .
- ii)  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .
- iii)  $\bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}$ .
- iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\bar{y} = \overline{m-x} \in \mathbb{Z}_m$ . Assim  
 $\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x+(m-x)} = \overline{m} = \bar{0}$ .
- v)  $\bar{x} \otimes \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \otimes \bar{x}$ .
- vi)  $(\bar{x} \otimes \bar{y}) \otimes \bar{z} = \overline{x \cdot y} \otimes \bar{z} = \overline{(x \cdot y) \cdot z} = \overline{x \cdot (y \cdot z)} = \textcircled{\bar{x}} \otimes$

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z}).$$

$$\text{iii) } \bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}.$$

$$\text{iv) Dado } \bar{x} \in \mathbb{Z}_m \text{ escolha } \bar{y} = \overline{m-x} \in \mathbb{Z}_m. \text{ Assim}$$
$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x+(m-x)} = \overline{m} = \bar{0}.$$

$$\text{v) } \bar{x} \otimes \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \otimes \bar{x}.$$

$$\text{vi) } (\bar{x} \otimes \bar{y}) \otimes \bar{z} = \overline{x \cdot y} \otimes \bar{z} = \overline{(x \cdot y) \cdot z} = \overline{x \cdot (y \cdot z)} = \bar{x} \otimes \underline{\overline{y \cdot z}} =$$

**Prova:**

$$\text{i) } \bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}.$$

$$\text{ii) } (\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y) + z} = \overline{x + (y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z}).$$

$$\text{iii) } \bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}.$$

$$\text{iv) Dado } \bar{x} \in \mathbb{Z}_m \text{ escolha } \bar{y} = \overline{m-x} \in \mathbb{Z}_m. \text{ Assim}$$
$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x + (m-x)} = \overline{m} = \bar{0}.$$

$$\text{v) } \bar{x} \otimes \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \otimes \bar{x}.$$

$$\text{vi) } (\bar{x} \otimes \bar{y}) \otimes \bar{z} = \overline{x \cdot y} \otimes \bar{z} = \overline{(x \cdot y) \cdot z} = \overline{x \cdot (y \cdot z)} = \bar{x} \otimes \overline{y \cdot z} = \bar{x} \otimes$$

**Prova:**

i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}$ .

ii)  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .

iii)  $\bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}$ .

iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\bar{y} = \overline{m-x} \in \mathbb{Z}_m$ . Assim  
 $\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x+(m-x)} = \overline{m} = \bar{0}$ .

v)  $\bar{x} \otimes \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \otimes \bar{x}$ .

vi)  $(\bar{x} \otimes \bar{y}) \otimes \bar{z} = \overline{x \cdot y} \otimes \bar{z} = \overline{(x \cdot y) \cdot z} = \overline{x \cdot (y \cdot z)} = \bar{x} \otimes \overline{y \cdot z} = \bar{x} \otimes (\bar{y} \otimes \bar{z})$ .

**Prova:**

i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}$ .

ii)  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .

iii)  $\bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}$ .

iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\bar{y} = \overline{m-x} \in \mathbb{Z}_m$ . Assim  
 $\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x+(m-x)} = \overline{m} = \bar{0}$ .

v)  $\bar{x} \otimes \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \otimes \bar{x}$ .

vi)  $(\bar{x} \otimes \bar{y}) \otimes \bar{z} = \overline{x \cdot y} \otimes \bar{z} = \overline{(x \cdot y) \cdot z} = \overline{x \cdot (y \cdot z)} = \bar{x} \otimes \overline{y \cdot z} = \bar{x} \otimes (\bar{y} \otimes \bar{z})$ .

**Prova:**

i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}$ .

ii)  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .

iii)  $\bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}$ .

iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\bar{y} = \overline{m-x} \in \mathbb{Z}_m$ . Assim  
 $\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x+(m-x)} = \overline{m} = \bar{0}$ .

v)  $\bar{x} \otimes \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \otimes \bar{x}$ .

vi)  $(\bar{x} \otimes \bar{y}) \otimes \bar{z} = \overline{x \cdot y} \otimes \bar{z} = \overline{(x \cdot y) \cdot z} = \overline{x \cdot (y \cdot z)} = \bar{x} \otimes \overline{y \cdot z} = \bar{x} \otimes (\bar{y} \otimes \bar{z})$ .

vii)  $\bar{x} \otimes \bar{1} = \overline{\cancel{x} \cdot 1} = \overline{\cancel{x}} = \bar{x}$

**Prova:**

- i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}$ .
- ii)  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .
- iii)  $\bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}$ .
- iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\bar{y} = \overline{m-x} \in \mathbb{Z}_m$ . Assim  
 $\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x+(m-x)} = \overline{m} = \bar{0}$ .
- v)  $\bar{x} \otimes \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \otimes \bar{x}$ .
- vi)  $(\bar{x} \otimes \bar{y}) \otimes \bar{z} = \overline{x \cdot y} \otimes \bar{z} = \overline{(x \cdot y) \cdot z} = \overline{x \cdot (y \cdot z)} = \bar{x} \otimes \overline{y \cdot z} = \bar{x} \otimes (\bar{y} \otimes \bar{z})$ .
- vii)  $\bar{x} \otimes \bar{1} = \overline{x \cdot 1} =$

**Prova:**

i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}$ .

ii)  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .

iii)  $\bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}$ .

iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\bar{y} = \overline{m-x} \in \mathbb{Z}_m$ . Assim  
 $\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x+(m-x)} = \overline{m} = \bar{0}$ .

v)  $\bar{x} \otimes \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \otimes \bar{x}$ .

vi)  $(\bar{x} \otimes \bar{y}) \otimes \bar{z} = \overline{x \cdot y} \otimes \bar{z} = \overline{(x \cdot y) \cdot z} = \overline{x \cdot (y \cdot z)} = \bar{x} \otimes \overline{y \cdot z} = \bar{x} \otimes (\bar{y} \otimes \bar{z})$ .

vii)  $\underline{\bar{x} \otimes \bar{1}} = \overline{x \cdot 1} = \underline{\bar{x}}$ .



**Prova:**

- i)  $\bar{x} \oplus \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} \oplus \bar{x}$ .
- ii)  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \overline{x+y} \oplus \bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x} \oplus \overline{y+z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .
- iii)  $\bar{x} \oplus \bar{0} = \overline{x+0} = \bar{x}$ .
- iv) Dado  $\bar{x} \in \mathbb{Z}_m$  escolha  $\bar{y} = \overline{m-x} \in \mathbb{Z}_m$ . Assim  
 $\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x+(m-x)} = \overline{m} = \bar{0}$ .
- v)  $\bar{x} \otimes \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \otimes \bar{x}$ .
- vi)  $(\bar{x} \otimes \bar{y}) \otimes \bar{z} = \overline{x \cdot y} \otimes \bar{z} = \overline{(x \cdot y) \cdot z} = \overline{x \cdot (y \cdot z)} = \bar{x} \otimes \overline{y \cdot z} = \bar{x} \otimes (\bar{y} \otimes \bar{z})$ .
- vii)  $\bar{x} \otimes \bar{1} = \overline{x \cdot 1} = \bar{x}$ .

■

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível**

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  
 $\bar{a} \otimes \bar{b} =$

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ .

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

$$(\bar{a})^{-1} + \frac{1}{\bar{a}}$$

$$\bar{3} \otimes \bar{3} = \bar{9} = \bar{1} \text{ em } \mathbb{Z}_4$$

$$(\bar{3})^{-1} = \bar{3}$$

$$\bar{2}$$

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe,

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe, então ele é único.

$$\begin{aligned}
 & a \in \mathbb{Z}_m \Rightarrow \text{EXISTEM } \bar{b}, \bar{d} \in \mathbb{Z}_m \text{ s.t. } \bar{a} \otimes \bar{b} = \bar{1} \\
 & \bar{a} \otimes \bar{d} = \bar{1} \\
 & \textcircled{1} \quad \bar{b} = \bar{b} \otimes \bar{1} = (\bar{b} \otimes (\bar{a} \otimes \bar{d})) = (\bar{b} \otimes \bar{a}) \otimes \bar{d} = \bar{1} \otimes \bar{d} = \bar{d}
 \end{aligned}$$

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe, então ele é único.

## Prova:

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe, então ele é único.

**Prova:** De fato,

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe, então ele é único.

**Prova:** De fato, dado  $\bar{a} \in \mathbb{Z}_m$ ,

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe, então ele é único.

**Prova:** De fato, dado  $\bar{a} \in \mathbb{Z}_m$ , suponha que existem  $\bar{b}$ ,

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe, então ele é único.

**Prova:** De fato, dado  $\bar{a} \in \mathbb{Z}_m$ , suponha que existem  $\bar{b}, \bar{d} \in \mathbb{Z}_m$

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe, então ele é único.

**Prova:** De fato, dado  $\bar{a} \in \mathbb{Z}_m$ , suponha que existem  $\bar{b}, \bar{d} \in \mathbb{Z}_m$  tais que  $\bar{a} \otimes \bar{b} = \bar{1}$

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe, então ele é único.

**Prova:** De fato, dado  $\bar{a} \in \mathbb{Z}_m$ , suponha que existem  $\bar{b}, \bar{d} \in \mathbb{Z}_m$  tais que  $\bar{a} \otimes \bar{b} = \bar{1} = \bar{a} \otimes \bar{d}$ ,

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe, então ele é único.

**Prova:** De fato, dado  $\bar{a} \in \mathbb{Z}_m$ , suponha que existem  $\bar{b}, \bar{d} \in \mathbb{Z}_m$  tais que  $\bar{a} \otimes \bar{b} = \bar{1} = \bar{a} \otimes \bar{d}$ , então

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe, então ele é único.

**Prova:** De fato, dado  $\bar{a} \in \mathbb{Z}_m$ , suponha que existem  $\bar{b}, \bar{d} \in \mathbb{Z}_m$  tais que  $\bar{a} \otimes \bar{b} = \bar{1} = \bar{a} \otimes \bar{d}$ , então

$$\underline{\bar{b}} =$$

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe, então ele é único.

**Prova:** De fato, dado  $\bar{a} \in \mathbb{Z}_m$ , suponha que existem  $\bar{b}, \bar{d} \in \mathbb{Z}_m$  tais que  $\bar{a} \otimes \bar{b} = \bar{1} = \bar{a} \otimes \bar{d}$ , então

$$\bar{b} = \underline{\bar{b}} \otimes \underline{\bar{1}} =$$

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe, então ele é único.

**Prova:** De fato, dado  $\bar{a} \in \mathbb{Z}_m$ , suponha que existem  $\bar{b}, \bar{d} \in \mathbb{Z}_m$  tais que  $\bar{a} \otimes \bar{b} = \bar{1} = \bar{a} \otimes \bar{d}$ , então

$$\bar{b} = \bar{b} \otimes \bar{1} = \bar{b} \otimes$$

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe, então ele é único.

**Prova:** De fato, dado  $\bar{a} \in \mathbb{Z}_m$ , suponha que existem  $\bar{b}, \bar{d} \in \mathbb{Z}_m$  tais que  $\bar{a} \otimes \bar{b} = \bar{1} = \bar{a} \otimes \bar{d}$ , então

$$\bar{b} = \bar{b} \otimes \bar{1} = (\bar{b} \otimes (\bar{a} \otimes \bar{d})) =$$

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe, então ele é único.

**Prova:** De fato, dado  $\bar{a} \in \mathbb{Z}_m$ , suponha que existem  $\bar{b}, \bar{d} \in \mathbb{Z}_m$  tais que  $\bar{a} \otimes \bar{b} = \bar{1} = \bar{a} \otimes \bar{d}$ , então

$$\bar{b} = \bar{b} \otimes \bar{1} = \bar{b} \otimes (\bar{a} \otimes \bar{d}) = (\bar{b} \otimes \bar{a})$$

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe, então ele é único.

**Prova:** De fato, dado  $\bar{a} \in \mathbb{Z}_m$ , suponha que existem  $\bar{b}, \bar{d} \in \mathbb{Z}_m$  tais que  $\bar{a} \otimes \bar{b} = \bar{1} = \bar{a} \otimes \bar{d}$ , então

$$\bar{b} = \bar{b} \otimes \bar{1} = \bar{b} \otimes (\bar{a} \otimes \bar{d}) = (\bar{b} \otimes \bar{a}) \otimes \bar{d} =$$

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe, então ele é único.

**Prova:** De fato, dado  $\bar{a} \in \mathbb{Z}_m$ , suponha que existem  $\bar{b}, \bar{d} \in \mathbb{Z}_m$  tais que  $\bar{a} \otimes \bar{b} = \bar{1} = \bar{a} \otimes \bar{d}$ , então

$$\bar{b} = \bar{b} \otimes \bar{1} = \bar{b} \otimes (\bar{a} \otimes \bar{d}) = (\bar{b} \otimes \bar{a}) \otimes \bar{d} = \bar{1} \otimes \bar{d} =$$

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe, então ele é único.

**Prova:** De fato, dado  $\bar{a} \in \mathbb{Z}_m$ , suponha que existem  $\bar{b}, \bar{d} \in \mathbb{Z}_m$  tais que  $\bar{a} \otimes \bar{b} = \bar{1} = \bar{a} \otimes \bar{d}$ , então

$$\textcircled{\bar{b}} = \bar{b} \otimes \bar{1} = \bar{b} \otimes (\bar{a} \otimes \bar{d}) = (\bar{b} \otimes \bar{a}) \otimes \bar{d} = \bar{1} \otimes \bar{d} = \textcircled{\bar{d}}$$

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe, então ele é único.

**Prova:** De fato, dado  $\bar{a} \in \mathbb{Z}_m$ , suponha que existem  $\bar{b}, \bar{d} \in \mathbb{Z}_m$  tais que  $\bar{a} \otimes \bar{b} = \bar{1} = \bar{a} \otimes \bar{d}$ , então

$$\bar{b} = \bar{b} \otimes \bar{1} = \bar{b} \otimes (\bar{a} \otimes \bar{d}) = (\bar{b} \otimes \bar{a}) \otimes \bar{d} = \bar{1} \otimes \bar{d} = \bar{d}$$

Portanto o inverso de  $\bar{a}$  é único,

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe, então ele é único.

**Prova:** De fato, dado  $\bar{a} \in \mathbb{Z}_m$ , suponha que existem  $\bar{b}, \bar{d} \in \mathbb{Z}_m$  tais que  $\bar{a} \otimes \bar{b} = \bar{1} = \bar{a} \otimes \bar{d}$ , então

$$\bar{b} = \bar{b} \otimes \bar{1} = \bar{b} \otimes (\bar{a} \otimes \bar{d}) = (\bar{b} \otimes \bar{a}) \otimes \bar{d} = \bar{1} \otimes \bar{d} = \bar{d}$$

Portanto o inverso de  $\bar{a}$  é único, como queríamos. ■

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **inversível** se, e somente se, existe  $\bar{b} \in \mathbb{Z}_m$  tal que  $\bar{a} \otimes \bar{b} = \bar{1}$ . Neste caso,  $\bar{b}$  é chamado **inverso** de  $\bar{a}$  e denotaremos  $\bar{b} = (\bar{a})^{-1}$ .

## Proposição

Se o inverso existe, então ele é único.

**Prova:** De fato, dado  $\bar{a} \in \mathbb{Z}_m$ , suponha que existem  $\bar{b}, \bar{d} \in \mathbb{Z}_m$  tais que  $\bar{a} \otimes \bar{b} = \bar{1} = \bar{a} \otimes \bar{d}$ , então

$$\bar{b} = \bar{b} \otimes \bar{1} = \bar{b} \otimes (\bar{a} \otimes \bar{d}) = (\bar{b} \otimes \bar{a}) \otimes \bar{d} = \bar{1} \otimes \bar{d} = \bar{d}$$

Portanto o inverso de  $\bar{a}$  é único, como queríamos. ■

## Proposição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é

## Proposição

*Um elemento  $\bar{a} \in \mathbb{Z}_m$  é inversível*

## Proposição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é inversível se, e somente se,  $\text{mdc}(\underline{a}, m) = 1$ .

$$\mathbb{Z}_4, \quad \text{mdc}(2, 4) = 2$$

$$\text{mdc}(1, 4) = \text{mdc}(3, 4) = 1$$

## Proposição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é inversível se, e somente se,  $\text{mdc}(a, m) = 1$ .

## Corolário

Se  $m$  é um número primo,

## Proposição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é inversível se, e somente se,  $\text{mdc}(a, m) = 1$ .

## Corolário

Se  $m$  é um número primo, então para todo  $\bar{x} \in \mathbb{Z}_m$ ,

## Proposição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é inversível se, e somente se,  $\text{mdc}(a, m) = 1$ .

## Corolário

Se  $m$  é um número primo, então para todo  $\bar{x} \in \mathbb{Z}_m$ ,  $\bar{x} \neq \bar{0}$ ,

## Proposição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é inversível se, e somente se,  $\text{mdc}(a, m) = 1$ .

## Corolário

Se  $m$  é um número primo, então para todo  $\bar{x} \in \mathbb{Z}_{(m)}$ ,  $\bar{x} \neq \bar{0}$ , existe inverso.

## Proposição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é inversível se, e somente se,  $\text{mdc}(a, m) = 1$ .

## Corolário

Se  $m$  é um número primo, então para todo  $\bar{x} \in \mathbb{Z}_m$ ,  $\bar{x} \neq \bar{0}$ , existe inverso.

## Exemplos

- i) Em  $\mathbb{Z}_4$  existem dois elementos inversíveis

## Proposição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é inversível se, e somente se,  $\text{mdc}(a, m) = 1$ .

## Corolário

Se  $m$  é um número primo, então para todo  $\bar{x} \in \mathbb{Z}_m$ ,  $\bar{x} \neq \bar{0}$ , existe inverso.

## Exemplos

i) Em  $\mathbb{Z}_4$  existem dois elementos inversíveis que são  $\bar{1}$ ,

## Proposição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é inversível se, e somente se,  $\text{mdc}(a, m) = 1$ .

## Corolário

Se  $m$  é um número primo, então para todo  $\bar{x} \in \mathbb{Z}_m$ ,  $\bar{x} \neq \bar{0}$ , existe inverso.

## Exemplos

i) Em  $\mathbb{Z}_4$  existem dois elementos inversíveis que são  $\bar{1}$ , cujo inverso é  $\bar{1}$ ,

## Proposição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é inversível se, e somente se,  $\text{mdc}(a, m) = 1$ .

## Corolário

Se  $m$  é um número primo, então para todo  $\bar{x} \in \mathbb{Z}_m$ ,  $\bar{x} \neq \bar{0}$ , existe inverso.

## Exemplos

- i) Em  $\mathbb{Z}_4$  existem dois elementos inversíveis que são  $\bar{1}$ , cujo inverso é  $\bar{1}$ , e o  $\bar{3}$ ,

## Proposição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é inversível se, e somente se,  $\text{mdc}(a, m) = 1$ .

## Corolário

Se  $m$  é um número primo, então para todo  $\bar{x} \in \mathbb{Z}_m$ ,  $\bar{x} \neq \bar{0}$ , existe inverso.

## Exemplos

- i) Em  $\mathbb{Z}_4$  existem dois elementos inversíveis que são  $\bar{1}$ , cujo inverso é  $\bar{1}$ , e o  $\bar{3}$ , cujo inverso é  $\bar{3}$ .

## Proposição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é inversível se, e somente se,  $\text{mdc}(a, m) = 1$ .

## Corolário

Se  $m$  é um número primo, então para todo  $\bar{x} \in \mathbb{Z}_m$ ,  $\bar{x} \neq \bar{0}$ , existe inverso.

## Exemplos

- i) Em  $\mathbb{Z}_4$  existem dois elementos inversíveis que são  $\bar{1}$ , cujo inverso é  $\bar{1}$ , e o  $\bar{3}$ , cujo inverso é  $\bar{3}$ .

## Exemplos

ii) Em  $\mathbb{Z}_{11}$ ,

## Exemplos

ii) Em  $\mathbb{Z}_{11}$ , todos elementos, exceto  $\underline{\bar{0}}$ ,

# Exemplos

ii) Em  $\mathbb{Z}_{11}$ , todos elementos, exceto  $\bar{0}$ , possuem inverso:

Tabela: Inversos em  $\mathbb{Z}_{11}$

Elemento	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\bar{10}$
Inverso	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{3}$	$\bar{9}$	$\bar{2}$	$\bar{8}$	$\bar{7}$	$\bar{5}$	$\bar{10}$

$$\bar{1} \otimes \bar{6} = \bar{1} \cdot \bar{6} = \bar{1} = \bar{6} \otimes \bar{1} \quad \left| \begin{array}{l} \bar{1} \otimes \bar{1} = \bar{1} \\ \bar{6} \otimes \bar{6} = \bar{1} \end{array} \right.$$

$$\bar{3} \otimes \bar{4} = \bar{3} \cdot \bar{4} = \bar{1} = \bar{4} \otimes \bar{3} \quad \left| \begin{array}{l} \bar{1} \otimes \bar{1} = \bar{1} \\ \bar{9} \otimes \bar{9} = \bar{1} \end{array} \right.$$

$$\bar{5} \otimes \bar{5} = \bar{5} \cdot \bar{5} = \bar{44+1} = \bar{1}$$

$$\bar{7} \otimes \bar{7} = \bar{7} \cdot \bar{7} = \bar{55+1} = \bar{1}$$