

# 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

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

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

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

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

Vamos denotar  $C(n)$

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  $R_m(n)$



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  $\bar{n}$ ,

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

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  $\bar{n}$ , quando não houver possibilidade de confusão. Assim fixando  $m > 1$  vamos escrever

$$R_m(0) =$$

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

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

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

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



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  $\bar{n}$ , quando não houver possibilidade de confusão. Assim fixando  $m > 1$  vamos escrever

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

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

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

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

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  $\bar{n}$ , quando não houver possibilidade de confusão. Assim fixando  $m > 1$  vamos escrever

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

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

$\vdots$

$$R_m(n) =$$

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  $\bar{n}$ , quando não houver possibilidade de confusão. Assim fixando  $m > 1$  vamos escrever

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

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

$\vdots$

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



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

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

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

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

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

$\vdots$

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

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

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

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

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

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

$\vdots$

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

## 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  $m$ .*

## 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,  $R_m(n)$  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

$$R_m(k) = R_m(l)$$



## 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

1) Se  $m = 2$ ,

## Exemplos

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

## Exemplos

- 1) *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

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

$$R_2(0) =$$

## Exemplos

- 1) *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

- 1) *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

- 1) *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

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

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

## Exemplos

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

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

$$R_2(1) =$$

## Exemplos

- 1) *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

- 1) *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

- 1) *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

- 1) *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

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

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

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

- 2) *Se  $m = 3$ ,*



## Exemplos

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

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

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

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

## Exemplos

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

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

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

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

## Exemplos

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

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

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

- 2) *Se  $m = 3$ , então os possíveis restos da divisão inteira são 0, 1 e 2. Daí*  
 $R_3(0) =$

## Exemplos

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

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

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

- 2) *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

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

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

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

- 2) *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

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

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

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

- 2) *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

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

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

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

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

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

## Exemplos

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

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

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

- 2) 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

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

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

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

- 2) *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

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

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

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

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

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

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

## Exemplos

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

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

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

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

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

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

## Exemplos

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

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

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

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

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

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

## Exemplos

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

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

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

- 2) 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

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

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

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

- 2) 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

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

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

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

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

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

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

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

## Exemplos

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

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

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

- 2) 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

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

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

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

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

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

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

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

## Exemplos

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

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

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

- 2) 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.*

## 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. ■



## Observação:

*Fixado  $m$  inteiro positivo,*

## Observação:

*Fixado  $m$  inteiro positivo, denotaremos*

## Observação:

*Fixado  $m$  inteiro positivo, denotaremos*

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

## Observação:

*Fixado  $m$  inteiro positivo, denotaremos*

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

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

## Observação:

*Fixado  $m$  inteiro positivo, denotaremos*

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

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

$$\vdots$$

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

## Observação:

*Fixado  $m$  inteiro positivo, denotaremos*

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

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

$$\vdots$$

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

*O conjunto quociente*

## Observação:

*Fixado  $m$  inteiro positivo, denotaremos*

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

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

$$\vdots$$

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

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

## Observação:

*Fixado  $m$  inteiro positivo, denotaremos*

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

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

$$\vdots$$

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

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



## Observação:

*Fixado  $m$  inteiro positivo, denotaremos*

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

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

$$\vdots$$

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

*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*

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

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

$$\vdots$$

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

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

$$\mathbb{Z}_m =$$

## Observação:

*Fixado  $m$  inteiro positivo, denotaremos*

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

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

$$\vdots$$

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

*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*

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

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

$$\vdots$$

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

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

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

## Observação:

*Fixado  $m$  inteiro positivo, denotaremos*

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

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

$$\vdots$$

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

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

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

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  $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$  temos que a soma de pares é par,

Vamos definir um meio de somar e multiplicar os elementos de  $\mathbb{Z}_m$ . Por exemplo, em  $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$  temos que a soma de pares é par, soma de par com ímpar

Vamos definir um meio de somar e multiplicar os elementos de  $\mathbb{Z}_m$ . Por exemplo, em  $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$  temos que a soma de pares é par, soma de par com ímpar é ímpar

Vamos definir um meio de somar e multiplicar os elementos de  $\mathbb{Z}_m$ . Por exemplo, em  $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$  temos que a soma de pares é par, soma de par com ímpar é ímpar e a soma de ímpares é par.

Vamos definir um meio de somar e multiplicar os elementos de  $\mathbb{Z}_m$ . Por exemplo, em  $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$  temos que a soma de pares é par, soma de par com ímpar é ímpar e a soma de ímpares é par. Assim podemos escrever

Vamos definir um meio de somar e multiplicar os elementos de  $\mathbb{Z}_m$ . Por exemplo, em  $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$  temos que a soma de pares é par, soma de par com ímpar é ímpar e a soma de ímpares é par. Assim podemos escrever

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

Para multiplicação, temos

Vamos definir um meio de somar e multiplicar os elementos de  $\mathbb{Z}_m$ . Por exemplo, em  $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$  temos que a soma de pares é par, soma de par com ímpar é ímpar e a soma de ímpares é par. Assim podemos escrever

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

Para multiplicação, temos

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



## Definição

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

## Definição

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

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

## 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

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

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

## Definição

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

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

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

## 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

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

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

## Proposição

*As operações de soma e produto*

## 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 produto 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 produto 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 produto 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

## 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 produto 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 produto 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 produto 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  $b_1 \neq b_2$ ,

## 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 produto 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 produto 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:

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

## 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 produto 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:

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

$$b_1 \equiv b_2 \pmod{m}.$$



## 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 produto 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:

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

$$b_1 \equiv b_2 \pmod{m}.$$

Daí,

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

## 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 produto 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:

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

$$b_1 \equiv b_2 \pmod{m}.$$

Daí,

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

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

## 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 produto 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:

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

$$b_1 \equiv b_2 \pmod{m}.$$

Daí,

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

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

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

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

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

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

$$\bar{a}_1 \oplus \bar{b}_1 =$$

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

$$\bar{a}_1 \oplus \bar{b}_1 = \overline{a_1 + b_1} =$$



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$\bar{a}_1 \otimes \bar{b}_1 =$$

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

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

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

$$\bar{a}_1 \otimes \bar{b}_1 = \overline{a_1 b_1} =$$

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

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

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

$$\bar{a}_1 \otimes \bar{b}_1 = \overline{a_1 b_1} = \overline{a_2 b_2} =$$



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

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

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

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

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

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

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

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

Portanto a soma e a multiplicação

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

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

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

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

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

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

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

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

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

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  $\mathbb{Z}_4$

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

## Exemplo

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

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



## 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  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \oplus \bar{y} = \bar{y} \oplus \bar{x}$ .*

## 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  $\bar{z} \in \mathbb{Z}_m$ :  $(\bar{x} \oplus \bar{y}) \oplus \bar{z} = \bar{x} \oplus (\bar{y} \oplus \bar{z})$ .

## 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  $\bar{x} \in \mathbb{Z}_m$ ,  $\bar{x} \oplus \bar{0} = \bar{x}$ .

## 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  $\bar{x} \oplus \bar{y} = \bar{0}$ .

## 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  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \otimes \bar{y} = \bar{y} \otimes \bar{x}$ .



## 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  $\bar{x} \in \mathbb{Z}_m$ :  $\bar{x} \otimes \bar{1} = \bar{x}$ .

## Proposição

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

- i) Para todos  $\bar{x}, \bar{y} \in \mathbb{Z}_m$ :  $\bar{x} \oplus \bar{y} = \bar{y} \oplus \bar{x}$ .
- 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  $\bar{x} \in \mathbb{Z}_m$ :  $\bar{x} \otimes \bar{1} = \bar{x}$ .

**Prova:**

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

**Prova:**

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

**Prova:**

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

**Prova:**

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

## Prova:

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

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



**Prova:**

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

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

## Prova:

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

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

## Prova:

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

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

## Prova:

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

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

## 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:

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

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

## 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:

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

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

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

## Prova:

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

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

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

## 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:

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

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

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

$$\text{iv) Dado } \bar{x} \in \mathbb{Z}_m$$

## Prova:

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

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

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

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

## 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  $\bar{y} = \overline{m - x} \in \mathbb{Z}_m.$

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

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



## Prova:

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

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

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

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

$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m - x} =$$

## 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  
 $\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m - x} = \overline{x + (m - x)} =$

## 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  
 $\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m - x} = \overline{x + (m - x)} = \bar{m} = \bar{0}.$

## Prova:

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

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

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

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

$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m - x} = \overline{x + (m - x)} = \bar{m} = \bar{0}.$$

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

## Prova:

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

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

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

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

$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m - x} = \overline{x + (m - x)} = \bar{m} = \bar{0}.$$

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

## Prova:

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

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

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

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

$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m - x} = \overline{x + (m - x)} = \bar{m} = \bar{0}.$$

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

## Prova:

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

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

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

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

$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m-x} = \overline{x + (m-x)} = \bar{m} = \bar{0}.$$

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

## Prova:

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

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

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

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

$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m - x} = \overline{x + (m - x)} = \bar{m} = \bar{0}.$$

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

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



## Prova:

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

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

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

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

$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m - x} = \overline{x + (m - x)} = \bar{m} = \bar{0}.$$

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

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

## Prova:

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

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

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

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

$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m - x} = \overline{x + (m - x)} = \bar{m} = \bar{0}.$$

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

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

## Prova:

- 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  
 $\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m - x} = \overline{x + (m - x)} = \bar{m} = \bar{0}.$
- v)  $\bar{x} \otimes \bar{y} = \overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \otimes \bar{x}.$
- vi)  $(\bar{x} \otimes \bar{y}) \otimes \bar{z} = \overline{x \cdot y} \otimes \bar{z} = \overline{(x \cdot y) \cdot z}$

## Prova:

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

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

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

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

$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m - x} = \overline{x + (m - x)} = \bar{m} = \bar{0}.$$

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

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

## Prova:

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

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

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

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

$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m - x} = \overline{x + (m - x)} = \bar{m} = \bar{0}.$$

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

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

## Prova:

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

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

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

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

$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m - x} = \overline{x + (m - x)} = \bar{m} = \bar{0}.$$

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

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

## Prova:

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

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

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

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

$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m - x} = \overline{x + (m - x)} = \bar{m} = \bar{0}.$$

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

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

## Prova:

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

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

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

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

$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m - x} = \overline{x + (m - x)} = \bar{m} = \bar{0}.$$

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

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



## Prova:

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

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

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

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

$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m - x} = \overline{x + (m - x)} = \bar{m} = \bar{0}.$$

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

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

$$\text{vii)} \quad \bar{x} \otimes \bar{1} =$$

## Prova:

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

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

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

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

$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m - x} = \overline{x + (m - x)} = \bar{m} = \bar{0}.$$

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

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

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

## Prova:

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

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

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

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

$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m - x} = \overline{x + (m - x)} = \bar{m} = \bar{0}.$$

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

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

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

## Prova:

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

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

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

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

$$\bar{x} \oplus \bar{y} = \bar{x} \oplus \overline{m - x} = \overline{x + (m - x)} = \bar{m} = \bar{0}.$$

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

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

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



## Definição

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

## Definição

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

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **invertível** 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 **invertível** 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 **invertível** 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 **invertível** 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 **invertível** 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  $\bar{b} = (\bar{a})^{-1}$ .

## Definição

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

## Definição

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

$$\bar{b} =$$

## Definição

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

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

## Definição

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

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

## Definição

Um elemento  $\bar{a} \in \mathbb{Z}_m$  é **invertível** 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 **invertível** 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,  $\text{mdc}(a, m) = 1$ .*

## 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

1) 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

1) 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

1) 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

- 1) 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

- 1) *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

- 1) *Em  $\mathbb{Z}_4$  existem dois elementos inversíveis que são  $\bar{1}$ , cujo inverso é  $\bar{1}$ , e o  $\bar{3}$ , cujo inverso é  $\bar{3}$ .*
- 2) *Em  $\mathbb{Z}_{11}$ ,*

## 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

- 1) *Em  $\mathbb{Z}_4$  existem dois elementos inversíveis que são  $\bar{1}$ , cujo inverso é  $\bar{1}$ , e o  $\bar{3}$ , cujo inverso é  $\bar{3}$ .*
- 2) *Em  $\mathbb{Z}_{11}$ , todos elementos, exceto  $\bar{0}$ ,*

## 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.

## Exemplos

- 1) Em  $\mathbb{Z}_4$  existem dois elementos inversíveis que são  $\bar{1}$ , cujo inverso é  $\bar{1}$ , e o  $\bar{3}$ , cujo inverso é  $\bar{3}$ .
- 2) 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										