# Classes de Equivalência na Congruência módulo $m$

José Antônio O. Freitas

MAT-UnB

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

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

$$\overline{b} = \{x \in \mathbb{Z} \mid x \equiv b \pmod{m}\}$$

$$\overline{0} = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{m}\} = m\mathbb{Z}$$

$$m \mid (x - 0) \Leftrightarrow m \mid x$$

$$\Leftrightarrow x = km, \; k \in \mathbb{Z}$$

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

$$\overline{n} =$$

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

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

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

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

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

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

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

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

Vamos dentoar $C(n)$

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

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

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

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

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

Vamos dentoar $C(n)$ por $R_m(n)$ ou $\overline{n}$,

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

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

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

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

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

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

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

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

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

$$R_m(0) =$$

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

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

Vamos dentoar $C(n)$ por $R_m(n)$ ou $\overline{n}$, 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

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

Vamos dentoar $C(n)$ por $R_m(n)$ ou $\overline{n}$, 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

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

Vamos dentoar $C(n)$ por $R_m(n)$ ou $\overline{n}$, 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

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

Vamos dentoar $C(n)$ por $R_m(n)$ ou $\overline{n}$, 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

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

Vamos dentoar $C(n)$ por $R_m(n)$ ou $\overline{n}$, 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

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

Vamos dentoar $C(n)$ por $R_m(n)$ ou $\overline{n}$, 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

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

Vamos dentoar $C(n)$ por $R_m(n)$ ou $\overline{n}$, 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

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

Vamos dentoar $C(n)$ por $R_m(n)$ ou $\overline{n}$, 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

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

Vamos dentoar $C(n)$ por $R_m(n)$ ou $\overline{n}$, 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

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

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

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

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

$km + 1$

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

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

Vamos dentoar $C(n)$ por $R_m(n)$ ou $\overline{n}$, 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

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

Vamos dentoar $C(n)$ por $R_m(n)$ ou $\overline{n}$, 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

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

Vamos dentoar $C(n)$ por $R_m(n)$ ou $\overline{n}$, 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

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

Vamos dentoar $C(n)$ por $R_m(n)$ ou $\overline{n}$, 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.*

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

$$a = mq + r.$$

## 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,* $R_m(n)$ *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

$R_m(k) = R_m(l)$

$\bar{a} \cap \bar{b} \neq \emptyset \Leftrightarrow a \mathcal{R} b \Rightarrow \bar{a} = \bar{b}$

## 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 EQUIVALÊNCIA POIS OS POSSÍVEIS RESTOS NA DIVISÃO POR 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*

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

$2 \mid (x - 0) \Leftrightarrow 2 \mid x \Leftrightarrow x = 2k$

## 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*

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

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

## 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*

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

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

$$2 \mid (x-1) \Leftrightarrow x - 1 = 2\ell$$

$$\Leftrightarrow x = 2\ell + 1, \ \ell \in \mathbb{Z}$$

## 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*

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

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

$I = \{\pm 1, \pm 3, \pm 5, \cdots\}$

$S = \{(x, y) \in \mathbb{Z} \mid x - y = 2k, k \in \mathbb{Z}\}$

## Exemplos

*ii) Se $m = 3$,*

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

$$0 \leq r < 3 \iff 0 \leq r \leq 2$$

$$0, 1, 2$$

## 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*

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

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

## 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*

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

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

## Exemplos

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

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

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

$3 \mid (x-1) \Leftrightarrow x - 1 = 3k$

$x = 3k + 1$

## Exemplos

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

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

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

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

## 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*

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

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

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

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

$x = 3k + 2$

## 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*

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

$$R_3(0) = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$

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

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

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

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

## 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.*

$0 \leq r < m$

$0 \leq r \leq m-1$

$a \cdot b \qquad a \equiv b \pmod{m}$

$m \nmid a - b < m$

**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 $0, 1, ..., (m-1)$.

**Proposição**

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

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

$m > 1$

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

## Observação:

*Fixado m inteiro positivo,*

## Observação:

*Fixado m inteiro positivo, denotaremos*

## Observação:

*Fixado m inteiro positivo, denotaremos*

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

## 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*

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

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

## 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*

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

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 $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$

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:

| $\oplus$ | $\overline{0}$ | $\overline{1}$ |
|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{0}$ |

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

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

$\overline{0} \quad \overline{0}$

$2k + 2l = 2(k+l) \in \overline{0}$

$2k + (2l+1) = 2(k+l) + 1$

$2k \in \overline{0}$, $(2l+1) \in \overline{1}$, $2(k+l)+1 \in \overline{1}$

$(2k+1) + (2l+1) = 2(k+l) + 2 = 2(k+l+1)$

$(2k+1) \in \overline{1}$, $(2l+1) \in \overline{1}$, $2(k+l+1) \in \overline{0}$

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

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

Para multiplicação, temos

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

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

$\underbrace{(2k)}_{\in \bar{0}}\underbrace{(2l+1)}_{\in \bar{1}} = 4kl + 2k$

$= \underbrace{2(2kl+k)}_{\in \bar{0}}$

$\underbrace{(2k+1)}_{\in \bar{1}}\underbrace{(2l+1)}_{\in \bar{1}} = 4kl + 2k + 2l + 1$

$= \underbrace{2(2kl+k+l)+1}_{\in \bar{1}}$

## Definição

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

## Definição

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

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

## Definição

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

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

## Definição

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

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

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

## Definição

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

$$\begin{cases} \overline{a} \oplus \overline{b} = \overline{a+b} \\ \overline{a} \otimes \overline{b} = \overline{ab}. \end{cases}$$

$\overline{0} = \{\ldots, 0, \pm 2, \pm 4, \ldots\}$ $\quad y = \overline{100} = -50$

$\overline{1} = \{\ldots, \pm 1, \pm 3, \pm 5, \ldots\}$ $\quad y = \overline{1001} = -113$

## Definição

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

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

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

## Proposição

*As operações de soma*

## Definição

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

$$\begin{cases} \overline{a} \oplus \overline{b} = \overline{a+b} \\ \\ \overline{a} \otimes \overline{b} = \overline{ab}. \end{cases}$$

## Proposição

*As operações de soma e a multiplicação*

## Definição

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

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

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

## Proposição

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

## Definição

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

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

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

## Proposição

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

**Prova:**

## Definição

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

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

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

## 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* $\overline{a}$, $\overline{b} \in \mathbb{Z}_m$ *definimos*

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

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

## 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, $\overline{a}_1 = \overline{a}_2$ e

## Definição

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

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

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

## 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, $\overline{a}_1 = \overline{a}_2$ e $\overline{b}_1 = \overline{b}_2$,

## Definição

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

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

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

## 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, $\overline{a}_1 = \overline{a}_2$ e $\overline{b}_1 = \overline{b}_2$, com $a_1 \neq a_2$

## Definição

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

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

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

## 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, $\overline{a}_1 = \overline{a}_2$ e $\overline{b}_1 = \overline{b}_2$, com $a_1 \neq a_2$ e $b_1 \neq b_2$,

$$\overline{a}_1 \oplus \overline{b}_1 \stackrel{?}{=} \overline{a}_2 \oplus \overline{b}_2$$

$$\overline{a}_1 \otimes \overline{b}_1 \stackrel{??}{=} \overline{a}_2 \otimes \overline{b}_2$$

## Definição

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

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

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

## 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, $\overline{a}_1 = \overline{a}_2$ e $\overline{b}_1 = \overline{b}_2$, com $a_1 \neq a_2$ e $b_1 \neq b_2$, temos:

## Definição

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

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

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

## 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, $\overline{a}_1 = \overline{a}_2$ e $\overline{b}_1 = \overline{b}_2$, com $a_1 \neq a_2$ e $b_1 \neq b_2$, temos:

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

## Definição

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

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

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

## 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, $\overline{a}_1 = \overline{a}_2$ e $\overline{b}_1 = \overline{b}_2$, com $a_1 \neq a_2$ e $b_1 \neq b_2$, temos:

$$\begin{array}{l} a_1 \equiv a_2 \pmod{m} \\ b_1 \equiv b_2 \pmod{m}. \end{array} \times$$

$\overline{a}_1 \otimes \overline{b}_1 = \overline{a}_2 \otimes \overline{b}_2$

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

$\overline{a}_1 \oplus \overline{b}_1 = \overline{a}_2 \oplus \overline{b}_2$

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

Daí,

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

Daí,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$ 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 $\overline{a_1 b_2} = \overline{a_2 b_2}$. 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,

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

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

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

Mas de $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$ 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 $\overline{a_1 b_2} = \overline{a_2 b_2}$. 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* $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$

## Exemplo

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

# Exemplo

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

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

| $\oplus$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{0}$ |
| $\overline{2}$ | $\overline{2}$ | $\overline{3}$ | $\overline{0}$ | $\overline{1}$ |
| $\overline{3}$ | $\overline{3}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |

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

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

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

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

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

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

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

# Exemplo

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

| $\otimes$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
| $\overline{2}$ | $\overline{0}$ | $\overline{2}$ | $\overline{0}$ | $\overline{2}$ |
| $\overline{3}$ | $\overline{0}$ | $\overline{3}$ | $\overline{2}$ | $\overline{1}$ |

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

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

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

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

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

$\mathbb{Z}_m$, $\overline{a} \oplus \overline{b}$ $\boxed{a+b} > m$

## 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 $\overline{x}, \overline{y} \in \mathbb{Z}_m$:*

## Proposição

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

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

## Proposição

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

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

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

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

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

## Proposição

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

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

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

*iii) Para todo $\overline{x} \in \mathbb{Z}_m$,*

## Proposição

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

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

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

*iii) Para todo $\overline{x} \in \mathbb{Z}_m$, $\overline{x} \oplus \overline{0} = \overline{x}$.*

## Proposição

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

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

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

*iii) Para todo $\overline{x} \in \mathbb{Z}_m$, $\overline{x} \oplus \overline{0} = \overline{x}$.*

*iv) Para todo $\overline{x} \in \mathbb{Z}_m$,*

## Proposição

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

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

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

*iii) Para todo $\overline{x} \in \mathbb{Z}_m$, $\overline{x} \oplus \overline{0} = \overline{x}$.*

*iv) Para todo $\overline{x} \in \mathbb{Z}_m$, existe $\overline{y} \in \mathbb{Z}_m$*

## Proposição

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

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

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

*iii)* Para todo $\overline{x} \in \mathbb{Z}_m$, $\overline{x} \oplus \overline{0} = \overline{x}$.

*iv)* Para todo $\overline{x} \in \mathbb{Z}_m$, existe $\overline{y} \in \mathbb{Z}_m$ tal que $\overline{x} \oplus \overline{y} = \overline{0}$.

$x \in \mathbb{Z}$, existe $y$ com $x + y = 0$

## Proposição

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

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

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

*iii)* Para todo $\overline{x} \in \mathbb{Z}_m$, $\overline{x} \oplus \overline{0} = \overline{x}$.

*iv)* Para todo $\overline{x} \in \mathbb{Z}_m$, existe $\overline{y} \in \mathbb{Z}_m$ tal que $\overline{x} \oplus \overline{y} = \overline{0}$.

*v)* Para todos $\overline{x}, \overline{y} \in \mathbb{Z}_m$:

## Proposição

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

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

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

*iii)* Para todo $\overline{x} \in \mathbb{Z}_m$, $\overline{x} \oplus \overline{0} = \overline{x}$.

*iv)* Para todo $\overline{x} \in \mathbb{Z}_m$, existe $\overline{y} \in \mathbb{Z}_m$ tal que $\overline{x} \oplus \overline{y} = \overline{0}$.

*v)* Para todos $\overline{x}, \overline{y} \in \mathbb{Z}_m$: $\overline{x} \otimes \overline{y} = \overline{y} \otimes \overline{x}$.

## Proposição

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

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

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

*iii)* Para todo $\overline{x} \in \mathbb{Z}_m$, $\overline{x} \oplus \overline{0} = \overline{x}$.

*iv)* Para todo $\overline{x} \in \mathbb{Z}_m$, existe $\overline{y} \in \mathbb{Z}_m$ tal que $\overline{x} \oplus \overline{y} = \overline{0}$.

*v)* Para todos $\overline{x}, \overline{y} \in \mathbb{Z}_m$: $\overline{x} \otimes \overline{y} = \overline{y} \otimes \overline{x}$.

*vi)* Para todos $\overline{x}, \overline{y}$ e $\overline{z} \in \mathbb{Z}_m$:

## Proposição

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

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

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

*iii)* Para todo $\overline{x} \in \mathbb{Z}_m$, $\overline{x} \oplus \overline{0} = \overline{x}$.

*iv)* Para todo $\overline{x} \in \mathbb{Z}_m$, existe $\overline{y} \in \mathbb{Z}_m$ tal que $\overline{x} \oplus \overline{y} = \overline{0}$.

*v)* Para todos $\overline{x}, \overline{y} \in \mathbb{Z}_m$: $\overline{x} \otimes \overline{y} = \overline{y} \otimes \overline{x}$.

*vi)* Para todos $\overline{x}, \overline{y}$ e $\overline{z} \in \mathbb{Z}_m$: $(\overline{x} \otimes \overline{y}) \otimes \overline{z} =$

## Proposição

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

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

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

*iii)* Para todo $\overline{x} \in \mathbb{Z}_m$, $\overline{x} \oplus \overline{0} = \overline{x}$.

*iv)* Para todo $\overline{x} \in \mathbb{Z}_m$, existe $\overline{y} \in \mathbb{Z}_m$ tal que $\overline{x} \oplus \overline{y} = \overline{0}$.

*v)* Para todos $\overline{x}, \overline{y} \in \mathbb{Z}_m$: $\overline{x} \otimes \overline{y} = \overline{y} \otimes \overline{x}$.

*vi)* Para todos $\overline{x}, \overline{y}$ e $\overline{z} \in \mathbb{Z}_m$: $(\overline{x} \otimes \overline{y}) \otimes \overline{z} = \overline{x} \otimes (\overline{y} \otimes \overline{z})$.

## Proposição

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

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

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

*iii)* Para todo $\overline{x} \in \mathbb{Z}_m$, $\overline{x} \oplus \overline{0} = \overline{x}$.

*iv)* Para todo $\overline{x} \in \mathbb{Z}_m$, existe $\overline{y} \in \mathbb{Z}_m$ tal que $\overline{x} \oplus \overline{y} = \overline{0}$.

*v)* Para todos $\overline{x}, \overline{y} \in \mathbb{Z}_m$: $\overline{x} \otimes \overline{y} = \overline{y} \otimes \overline{x}$.

*vi)* Para todos $\overline{x}, \overline{y}$ e $\overline{z} \in \mathbb{Z}_m$: $(\overline{x} \otimes \overline{y}) \otimes \overline{z} = \overline{x} \otimes (\overline{y} \otimes \overline{z})$.

*vii)* Para todo $\overline{x} \in \mathbb{Z}_m$:

## Proposição

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

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

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

*iii)* Para todo $\overline{x} \in \mathbb{Z}_m$, $\overline{x} \oplus \overline{0} = \overline{x}$.

*iv)* Para todo $\overline{x} \in \mathbb{Z}_m$, existe $\overline{y} \in \mathbb{Z}_m$ tal que $\overline{x} \oplus \overline{y} = \overline{0}$.

*v)* Para todos $\overline{x}, \overline{y} \in \mathbb{Z}_m$: $\overline{x} \otimes \overline{y} = \overline{y} \otimes \overline{x}$.

*vi)* Para todos $\overline{x}, \overline{y}$ e $\overline{z} \in \mathbb{Z}_m$: $(\overline{x} \otimes \overline{y}) \otimes \overline{z} = \overline{x} \otimes (\overline{y} \otimes \overline{z})$.

*vii)* Para todo $\overline{x} \in \mathbb{Z}_m$: $\overline{x} \otimes \overline{1} = \overline{x}$.

## Proposição

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

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

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

*iii)* Para todo $\overline{x} \in \mathbb{Z}_m$, $\overline{x} \oplus \overline{0} = \overline{x}$.

*iv)* Para todo $\overline{x} \in \mathbb{Z}_m$, existe $\overline{y} \in \mathbb{Z}_m$ tal que $\overline{x} \oplus \overline{y} = \overline{0}$.

*v)* Para todos $\overline{x}, \overline{y} \in \mathbb{Z}_m$: $\overline{x} \otimes \overline{y} = \overline{y} \otimes \overline{x}$.

*vi)* Para todos $\overline{x}, \overline{y}$ e $\overline{z} \in \mathbb{Z}_m$: $(\overline{x} \otimes \overline{y}) \otimes \overline{z} = \overline{x} \otimes (\overline{y} \otimes \overline{z})$.

*vii)* Para todo $\overline{x} \in \mathbb{Z}_m$: $\overline{x} \otimes \overline{1} = \overline{x}$.

$\overline{x} \odot \overline{y} = \overline{x+y} = \overline{y+x} = \overline{y} \odot \overline{x}$

## Definição

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

## Definição

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

## Definição

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

## Definição

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

**Definição**

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

## Definição

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

## Definição

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

## Definição

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

## Proposição

*Se o inverso existe,*

## Definição

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

## Proposição

*Se o inverso existe, então ele é único.*

## Definição

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

## Proposição

*Se o inverso existe, então ele é único.*

## Proposição

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

## Proposição

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

## Proposição

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

## Proposição

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

## Corolário

*Se $m$ é um número primo,*

## Proposição

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

## Corolário

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

## Proposição

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

## Corolário

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

**Proposição**

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

**Corolário**

$\overline{x} + \overline{0} = \overline{x}$

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

## Proposição

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

## Corolário

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

## Exemplos

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

## Proposição

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

## Corolário

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

## Exemplos

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

## Proposição

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

## Corolário

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

## Exemplos

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

## Proposição

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

## Corolário

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

## Exemplos

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

## Proposição

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

## Corolário

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

## Exemplos

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

## Proposição

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

## Corolário

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

## Exemplos

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

## Exemplos

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

## Exemplos

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

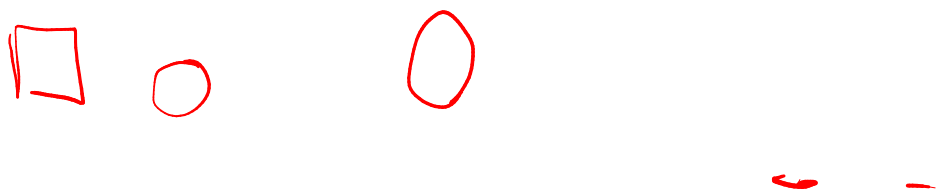
## Exemplos

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

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

| *Elemento* | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ | $\overline{6}$ | $\overline{7}$ | $\overline{8}$ | $\overline{9}$ | $\overline{10}$ |
|---|---|---|---|---|---|---|---|---|---|---|
| *Inverso* | | | | | | | | | | |

$x + (m - x) = m = 0$

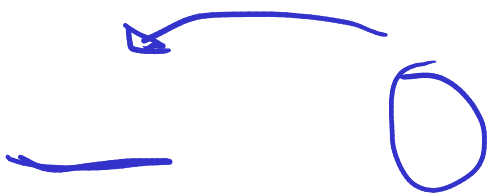


$$\overline{x \cdot y} = \overline{y \cdot x} = \bar{y} \otimes \bar{x}$$

$$\overline{x \cdot y} \otimes \overline{z} = \overline{(x \cdot y) \cdot z} = \overline{x \cdot (yz)} =$$

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

$$\underline{x} = \tau \cdot \underline{x}$$



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

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

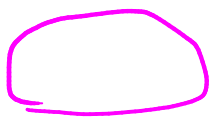
$(\bar{3})^{-1} = \bar{3}$

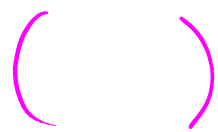
$\bar{2}$

$a \in \mathbb{Z}_m \Rightarrow$ EXISTEM $b, d \in \mathbb{Z}_m$

$\bar{a} \otimes \bar{d} = \bar{1}$ $\qquad$ $\bar{a} \otimes \bar{b} = \bar{1}$

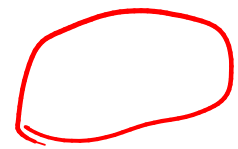
$$\bar{b} = \bar{b} \otimes \bar{1} = \bar{b} \otimes (\bar{a} \otimes \bar{d}) = (\bar{b} \otimes \bar{a}) \otimes \bar{d} = \bar{1} \otimes \bar{d} = \bar{d}$$





$\mathbb{Z}_4$ : $\gcd(2,4) = 2$

$\gcd(1,4) = \gcd(3,4) = 1$



$\overline{1}\ \overline{6}\ \overline{4}\ \overline{3}\ \overline{9}\ \overline{2}\ \overline{8}\ \overline{7}\ \overline{5}\ \overline{10}$

$\overline{2} \otimes \overline{6} = \overline{12} = \overline{1} = \overline{6} \otimes \overline{2}$

$\overline{3} \otimes \overline{4} = \overline{12} = \overline{1} = \overline{4} \otimes \overline{3}$

$\overline{5} \otimes \overline{9} = \overline{45} = \overline{44+1} = \overline{1}$

$\overline{7} \otimes \overline{8} = \overline{56} = \overline{55+1} = \overline{1}$

$\overline{10} \otimes \overline{10} = \overline{100}$

$= \overline{99+1} = \overline{1}$