

Relação de Equivalência - Classes de Equivalência nos Inteiros - Continuação

José Antônio O. Freitas

MAT-UnB

27 de agosto de 2020

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência,

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência.

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, dado $n \in \mathbb{Z}$, temos

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, dado $n \in \mathbb{Z}$, temos

$$\bar{n} =$$

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, dado $n \in \mathbb{Z}$, temos

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

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, dado $n \in \mathbb{Z}$, temos

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

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, dado $n \in \mathbb{Z}$, temos

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

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, dado $n \in \mathbb{Z}$, temos

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

Vamos denotar $C(n)$

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, 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 $R_m(n)$

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, 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} ,

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, 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.

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, 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.

Por exemplo, fixando $m > 1$

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, 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.

Por exemplo, fixando $m > 1$

$$R_m(0) =$$

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, 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.

Por exemplo, fixando $m > 1$

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

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, 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.

Por exemplo, fixando $m > 1$

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

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, 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.

Por exemplo, fixando $m > 1$

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

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, 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.

Por exemplo, fixando $m > 1$

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

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, 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.

Por exemplo, fixando $m > 1$

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

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, 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.

Por exemplo, fixando $m > 1$

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

$$R_m(1) =$$

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, 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.

Por exemplo, fixando $m > 1$

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

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

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, 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.

Por exemplo, fixando $m > 1$

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

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

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, 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.

Por exemplo, fixando $m > 1$

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

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

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, 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.

Por exemplo, fixando $m > 1$

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

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

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, 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.

Por exemplo, fixando $m > 1$

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

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

\vdots

$$R_m(n) =$$

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, 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.

Por exemplo, fixando $m > 1$

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

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

\vdots

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

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, 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.

Por exemplo, fixando $m > 1$

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

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

\vdots

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

Sabemos, pela aula anterior, que a congruência módulo m é uma relação de equivalência, assim vamos determinar suas classes de equivalência. Para isso, 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.

Por exemplo, fixando $m > 1$

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

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

\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.

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, 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

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

Queremos 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	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

Para multiplicação, temos

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

Definição

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

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

$$\bar{a} \otimes \bar{b} = \overline{ab}. \quad (2)$$

Proposição

As operações de soma e produto definidas em (1) e (2) são independentes dos representantes das classes.

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

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

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



Exemplo

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

Tabela: Soma em \mathbb{Z}_4

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

Exemplo

Tabela: Multiplicação em \mathbb{Z}_4

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

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 $\bar{x} \in \mathbb{Z}$, existe $\bar{y} \in \mathbb{Z}$ 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) $\bar{x} \oplus \bar{y} = \overline{x + y} = \overline{y + x} = \bar{y} \oplus \bar{x}.$
- 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) $(\bar{x} \otimes \bar{y}) \otimes \bar{z} = \overline{x \cdot y} \otimes \bar{z} = \overline{(x \cdot y) \cdot z} = \overline{x \cdot (y \cdot z)} = \bar{x} \otimes \overline{y \cdot z} = \bar{x} \otimes (\bar{y} \otimes \bar{z}).$
- vii) $\bar{x} \otimes \bar{1} = \overline{x \cdot 1} = \bar{x}.$



Definição

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

$$\begin{aligned}\bar{b} &= \bar{b} \otimes \bar{1} = \bar{b} \otimes (\bar{a} \otimes \bar{d}) \\ &= (\bar{b} \otimes \bar{a}) \otimes \bar{d} = \bar{1} \otimes \bar{d} = \bar{d}\end{aligned}$$



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