Relação de Equivalência - Classes de Equivalência nos Inteiros - Continuação

José Antônio O. Freitas

MAT-UnB

27 de agosto de 2020

Como a congruência módulo m é uma relação de equivalência, podemos determinar suas classes de equivalência. Assim, dado $n \in \mathbb{Z}$, temos

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

Denotaremos $C(n)$ por $R_m(n)$ ou $\overline{n}$, quando não houver possibilidade de confusão.
Por exemplo, fixando $m > 1$

$$R_m(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{m}\} = \{x \in \mathbb{Z} \mid x = mk, k \in \mathbb{Z}\} = m\mathbb{Z}$$
$$R_m(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{m}\} = \{x \in \mathbb{Z} \mid x = 1 + km, k \in \mathbb{Z}\}$$
$$R_m(n) = \{x \in \mathbb{Z} \mid x = n + km, k \in \mathbb{Z}\}$$

Proposição

As classes de equivalência definidas pela congruência módulo m 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* $m = 2$, *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 $0, 1, ..., (m-1)$. 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 $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$ *ou* $\mathbb{Z}_m$. *Assim*

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

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

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

Para multiplicação, temos

$\otimes$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Definição

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

$$\overline{a} \oplus \overline{b} = \overline{a+b} \tag{1}$$

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

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

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

■

Exemplo

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

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

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

Exemplo

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

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

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* $\overline{x} \in \mathbb{Z}$, *existe* $\overline{y} \in \mathbb{Z}$ *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* $\overline{x} \in \mathbb{Z}_m$: $\overline{x} \otimes \overline{1} = \overline{x}$.

Prova:

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

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

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

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

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

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

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

■

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.

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

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

■

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

1) *Em* $\mathbb{Z}_4$ *existem dois elementos inversíveis que são* $\overline{1}$, *cujo inverso é* $\overline{1}$, *e o* $\overline{3}$, *cujo inverso é* $\overline{3}$.
2) *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	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{3}$	$\overline{9}$	$\overline{2}$	$\overline{8}$	$\overline{7}$	$\overline{5}$	$\overline{10}$