Aula 19. Inteiros modulo m

19.1 Classes de congruência

Lembrete: Se $m > 0$ e a, b inteiros positives assim

$$a \equiv b \pmod{m},$$

se $m \mid (a - b)$

Se $m \in \mathbb{Z}$ com $m > 1$, para todo $a \in \mathbb{Z}$, define

$$\bar{a} := \{b \in \mathbb{Z} \mid b \equiv a (\bmod m)\}.$$

Exemplo 19.1

a) Suponha que $m = 2$ e $a = 1$, assim

$$b \equiv 1 \pmod{2}$$

se e somente se b é impar, logo

$$\bar{a} = \bar{1} = \{\cdots, -7, -5, -3, -1, 1, 3, 5, 7, \ldots\}$$

b) Se $m = 2$ e $a = 4$, assim

$$b \equiv 4 (\bmod 2)$$

se e somente se b é par, logo

$$\bar{4} = \{\cdots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \ldots\}$$

Alem disso notamos que para $m = 2$, temos:

$$\bar{4} = \bar{2} = \bar{0}.$$

c) Se $m = 7$, $a = 11$ assim

$$\bar{a} = \{\ldots - (0, -3, 4, 11, 18, 25, 32, \ldots\}.$$

Proposição 19.1

Seja $m \in \mathbb{Z}$ com $m > 1$. Assim

$$\bar{a} = \{a + km \mid k \in \mathbb{Z}\}$$

Prova

Lembrete: Para mostrar que todis conjuntos X e Y são iguais devemos provar que

$$X \subset Y, \qquad Y \subset X.$$

Assim devemos mostrar que

$$\bar{a} \subset \{a + km \mid k \in \mathbb{Z}\}, \qquad \bar{a} \supset \{a + km \mid k \in \mathbb{Z}\}.$$

[$\subset$]. Suponha que $b \in \bar{a}$. Assim temos que

$$\begin{aligned} a \in \bar{a} &\Rightarrow b \equiv a (\operatorname{mod} m) \\ &\Rightarrow m \mid b - a \Rightarrow m \cdot k = b - a \\ &\Rightarrow b = a + mk \Rightarrow b \in \{a + km \mid k \in \mathbb{Z}\}. \end{aligned}$$

[$\supset$]. Agora suponha que $b \in S = \{a + km \mid k \in \mathbb{Z}\}$. Assim temos que

$$\begin{aligned} b \in S &\Rightarrow b = a + m \cdot k, \quad k \in \mathbb{Z} \\ &\Rightarrow m \mid b - a \\ &\Rightarrow b \equiv a (\operatorname{mod} m) \Rightarrow b \in \bar{a}. \end{aligned}$$

Logo,

$$\bar{a} = \{a + km \mid k \in \mathbb{Z}\}.$$

Proposição 19.2

Temos que

$$\bar{a} = \bar{b} \qquad \Longleftrightarrow \qquad a \equiv b (\operatorname{mod} m).$$

Prova

[$\Rightarrow$]. Seja $c \in \bar{a}$ assim $c \in \bar{b}$ e

$$\begin{cases} c \equiv a (\operatorname{mod} m) \\ c \equiv b (\operatorname{mod} m) \end{cases}$$

Logo, $a \equiv b (\operatorname{mod} m)$.
[$\Leftarrow$]. Temos que

$$c \in \bar{a} \qquad \Longleftrightarrow \qquad \begin{matrix} c \equiv a (\operatorname{mod} m) \\ a \equiv b (\operatorname{mod} m) \end{matrix} \qquad \Longleftrightarrow \qquad c \equiv b (\operatorname{mod} m)$$

Assim

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

Corolário 19.1

Seja $a \in \mathbb{Z}$ e $m > 1$. Se $a, b \in \mathbb{Z}$ com $\bar{a} \neq \bar{b}$, então

$$\bar{a} \cap \bar{b} = \varnothing.$$

Prova

Suponha que $\overline{a} \cap \overline{b} \neq \varnothing$ assim existe $c \in \overline{a}$ e $c \in \overline{b}$. Logo

$$\begin{matrix} c \equiv a(\bmod m) \\ c \equiv b(\bmod m) \end{matrix} \quad \Longleftrightarrow \quad a \equiv b(\bmod m),$$

ou seja

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

Definição

Dado $a \in \mathbb{Z}$, e $m > 1$. $\overline{a}$ e chamado *representante* de a modulo m (ou *classe de congruência* de a modulo m).

Exemplo 19.2

Suponha $m = 3$, assim há 3 representasts

$$\begin{aligned} \overline{0} &= \{\ldots -5, -6, -3, 0, 3, 6, 9, 12, 15, \ldots\} \\ \overline{1} &= \{-8, -5, -2, 1, 4, 7, 10, 13, 16, \ldots\} \\ \overline{2} &= \{-7, -4, -1, 2, 5, 8, 11, 14, 17, \ldots\}. \end{aligned}$$

E, em particular

$$\begin{matrix} \overline{0} = \overline{6}, & \overline{0} = \overline{12}, & \ldots \\ \overline{1} = \overline{4}, & \overline{1} = \overline{7}, & \ldots. \\ \overline{2} = \overline{23}, & \overline{2} = -1, & \ldots. \end{matrix}$$

Notamos que $\overline{0} \cup \overline{1} \cup \overline{2} = \mathbb{Z}$ - todos inteiros.

Definimos o conjunto dos inteiros modulo m, como conjunto de todos classes de congruências diferentes.

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

as vezes escrevemos esse conjunto como

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

Exemplo 19.3

$$\begin{aligned} \mathbb{Z}_2 &= \{\overline{0}, \overline{1}\}, \\ \mathbb{Z}_3 &= \{\overline{0}, \overline{1}, \overline{2}\}, \\ \mathbb{Z}_4 &= \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}, \\ &\vdots \\ \mathbb{Z}_{13} &= \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{12}\}. \end{aligned}$$

Exemplo 19.4

Vamos encontra o menor inteiro menor positivo b tal sue

$$\overline{b} = -\overline{21}$$

modulo $m = 8$. Temos que

$$-21 = (-3) \cdot 8 + 3.$$

Ou seja 3 é o resto da divisão de -21 por 8. Logo, temos que

$$\overline{-21} = \overline{3}.$$

19.2 Operações em $\mathbb{Z}_m$

Vamos definir em $\mathbb{Z}_m$ duas operações (some e produto) bem parecidos aos operações em $\mathbb{Z}$. Existe uma forma natural de fazê-lo. Por exemplo, para somar e multiplicar $\overrightarrow{3}$ e $\overline{5}$ em Z_6, faríamos

$$\overline{3} + \overline{5} = \overline{8} = \overline{2}$$
$$\overline{3} \cdot \overline{5} = \overline{15} = \overline{3}.$$

Mais precisamente, temos o seguinte. **Soma:**

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

Produto:

$$\overline{a} \cdot \overline{b} := \overline{ab}$$

Quer dizer, para efetuar a soma de duas classes módulo m, tomamos representantes (quaisquer) a e b dessas classes, fazemos a soma $a + b$ em $\mathbb{Z}$ e consideramos como resultado da soma a classe de $a + b$ módulo m. A operação de produto se faz de forma análoga. Surge agora uma pergunta natural: será que o resultado das operações não depende dos representantes escolhidos? Por exemplo em Z_6, para somar $\overline{3} + \overline{5}$, poderíamos tomar 63 como um representante de $\overline{3}$ e 23 como representante de $\overline{5}$. Será que $\overline{63} + \overline{23} = \overline{86}$ é o mesmo resultado que aquele obtido acima, $\overline{3} + \overline{5} = \overline{2}$? Como $86 \equiv 2 (\mathrm{mod}\, 6)$, o resultado é o mesmo.

Assim mostraremos que as operações são bem-definidas ou seja eles independem das representantes escolhidas. Isto é dados

$$a, b, a', b' \in \mathbb{Z},$$

com

$$\overline{a} = \overline{a'} \qquad \overline{b} = \overline{b}',$$

vamos verificar que

$$\overline{a+b} = a' + b',$$
$$\overline{ab} = \overline{a'.b'}$$

Como $\overline{a} = \overline{a'}, \overline{b} = \overline{b}'$ assim, aplicando Proposição 19.2, temos

$$\begin{aligned} a &\equiv a' \pmod m \\ b &\equiv b' \pmod m \end{aligned}$$

Assim temos que

$$\begin{aligned} a + b &\equiv a' + b' \pmod m \\ ab &\equiv a'b' \pmod m \end{aligned}$$

De novo, aplicando Proposição 19.2, temos

$$\overline{a+b} = \overline{a'+b'} \quad e \quad \overline{ab} = \overline{a'b'}.$$

Isso significue que soma

$$\begin{aligned} + : \mathbb{Z}_m \times \mathbb{Z}_m &\longrightarrow \mathbb{Z}_m \\ (\overline{a}, \overline{b}) &\longmapsto \overline{a} + \overline{b} := \overline{a+b} \end{aligned}$$

e o produto:

$$\begin{aligned} \cdot : \mathbb{Z}_m \times \mathbb{Z}_m &\longrightarrow \mathbb{Z}_m \\ (\overline{a}, \overline{b}) &\longmapsto \overline{a} \cdot \overline{b} := \overline{a \cdot b} \end{aligned}$$

são operações bem definidas.

Exemplo 19.5

Suponha que $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$, neste caso

$$\begin{aligned} \overline{0} &= \{.. - 4, -2, 0; 2, 4, \cdots\} \qquad \text{— inteiros pares} \\ \overline{1} &= \{. - 5, -3, -1, 1, 3, 5, 7, \ldots\} \qquad \text{— inteiros impares} \end{aligned}$$

Soma entre dois inteiros pares é sempre um inteiro par, logo assim

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

Semelhante, soma de dois inteiros impares é inteiro par, ou seja

$$\overline{1} + \overline{1} = \overline{0}.$$

Agora a soma de inteiro impar com um inteiro par é sempre inteiro impar, assim

$$\overline{0} + \overline{1} = \overline{1} + \overline{0} = \overline{1}.$$

O produto de dois inteiros pares é sempre um inteiro par, logo assim

$$\overline{0} \cdot \overline{0} = \overline{0}.$$

Semelhante, o produto de dois inteiros impares é inteiro impar, ou seja

$$\overline{1} \cdot \overline{1} = \overline{0}.$$

Finalmente $\overline{0} \cdot \overline{1} = \overline{1} \cdot \overline{0} = \overline{0}$, pois inteiro impar vezes inteiro par é um inteiro par. Assim temos as seguintes tabelas de soma

$+$	$\overline{0}$	$\overline{0}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

e multiplicação em $\mathbb{Z}_2$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Exercício 19.1: (Trabalho p/ casa)

Encontre $\overline{-81}$ em $\mathbb{Z}_{17}$, $\mathbb{Z}_{21}$ e $\mathbb{Z}_{49}$.

Exercício 19.2: (Trabalho p/ casa)

Descreva soma e produto em $\mathbb{Z}_3$ e $\mathbb{Z}_7$.

Exercício 19.3: (Trabalho p/ casa)

Calcule $\overline{-17} \cdot \overline{21}$ em $\mathbb{Z}_{13}$.

Calcule $\overline{101} \cdot \overline{33}$ em $\mathbb{Z}_6$ e $\mathbb{Z}_8$.