

Revisão 2

Ex. 1 (Lista 5, Ex. 4).

Em $\mathbb{Z}_{22}$ determine:

- os menores representantes de $\overline{-10}$ e $\overline{-14}$;
- todos div. de zero,
- todos elementos invertíveis e seus inversos.

Solução a) $-10 = 22 \cdot (-1) + 12 \Rightarrow \overline{-10} = \overline{12}$
 $-14 = 22 \cdot (-1) + 8 \Rightarrow \overline{-14} = \overline{8}$ em $\mathbb{Z}_{22}$.

b) Critério: $\overline{a} \in \mathbb{Z}_m$ é div. de zero $\Leftrightarrow \text{mdc}(a, m) \neq 1$

Assim $\overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}, \overline{18}, \overline{20}, \overline{11}$ são div. de zero.

c) Critério: $\overline{a} \in \mathbb{Z}_m$ é invertível $\Leftrightarrow \text{mdc}(a, m) = 1$.

Assim: $\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}, \overline{13}, \overline{15}, \overline{17}, \overline{19}, \overline{21}$ - invertíveis
 $\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow$
 $\overline{1}, \overline{15}, \overline{9}, \overline{19}, \overline{5}, \overline{17}, \overline{3}, \overline{13}, \overline{7}, \overline{21}$ - seus inversos.

Ex. 2 (Lista 5, Ex. 7).

(2)

Seja p um primo e $\bar{a}, \bar{b} \in \mathbb{Z}_p$. Mostre

$$a) \bar{a}^p = \bar{a} \quad b) (\bar{a} + \bar{b})^p = \bar{a} + \bar{b}$$

Solução Pelo Teorema de Fermat

$$a) a^p \equiv a \pmod{p} \Rightarrow \bar{a}^p = \overline{a^p} = \bar{a} \text{ em } \mathbb{Z}_p$$

$$b) (\bar{a} + \bar{b})^p = \bar{a} + \bar{b} \\ \bar{a} = \bar{a}^p, \bar{b} = \bar{b}^p \Rightarrow (\bar{a} + \bar{b})^p = \bar{a}^p + \bar{b}^p \text{ em } \mathbb{Z}_p.$$

Ex. 3 (Lista 5, Ex. 5) Resolva

$$a) 4x = 7 \text{ em } \mathbb{Z}_{15}$$

$$b) 8x + 3 = 10 \text{ em } \mathbb{Z}_{21}$$

Solução a) $\text{mdc}(4, 15) = 1 \Rightarrow \bar{4}$ é invertível em $\mathbb{Z}_{15}$
e seu inverso é $\bar{4}$, pois
 $\bar{4} \cdot \bar{4} = \bar{1}$ em $\mathbb{Z}_{15}$

$$\text{Assim } 4x = 7 \Rightarrow 4 \cdot 4x = 4 \cdot 7 \\ \Rightarrow x = 28 \Rightarrow x = 13 \text{ em } \mathbb{Z}_{15}$$

b) $\text{mdc}(8, 21) = 1 \Rightarrow \bar{8}$ é invertível
e $\bar{8} \cdot \bar{8} = 64 = 1$ em $\mathbb{Z}_{21}$, assim $\bar{8}$ é inverso.

$$\text{Agora } 8x + 3 = 10$$

$$\Rightarrow 8x = 7$$

$$\Rightarrow 8 \cdot 8x = 8 \cdot 7$$

$$\Rightarrow x = 56 = 14 \text{ em } \mathbb{Z}_{21}.$$

Ex. 4 (Lista 5, Ex. 3)

3

O elemento $\bar{a} \in \mathbb{Z}_m$ é chamado nilpotente, se

$\bar{a}^k = \bar{0}$ para algum $k \in \mathbb{Z}$. Mostre que $\mathbb{Z}_m$

não tem nilpotentes não-nulos, se e somente se m não tem fator primo em quadrado.

Solução

[$\Rightarrow$] Temos que $a \in \{0, 1, \dots, m-1\}$ é nilpotente se e somente se $m \mid a^k$.

Se m tem fator primo em quadrado, assim

$m = p^2 \cdot m_1$, com $m_1 \geq 1$. Assim temos que

$$p \cdot m_1 < m \Rightarrow \bar{a} = \overline{p \cdot m_1} \in \mathbb{Z}_m.$$

$$\text{Agora } \bar{a} \cdot \bar{a} = \overline{p^2 \cdot m_1 \cdot m_1} = \overline{m \cdot m_1} = \bar{0}$$

Assim $\bar{a}$ é nilpotente.

[$\Leftarrow$] Contrário, seja $m = p_1 \cdots p_s$ com $p_i \neq p_j$ e seja

$\bar{a}^k = \bar{0}$, com $1 \leq a < m$. Assim $m \mid a^k$

portanto $p_i \mid a$ e $a = p_1 \cdots p_s \cdot d > m$

Contradição.

Ex. 5 Resolva

$$(\bar{2} \cdot x + \bar{3})^2 + (\bar{3} \cdot x + \bar{2})^2 + \bar{5} \cdot x = \bar{0} \quad \text{em } \mathbb{Z}_5$$

(4)

Temos que

$$\overline{5} = \overline{0}, \quad \overline{2} = -\overline{3} \quad \text{e} \quad \overline{3} = -\overline{2} \quad \text{em } \mathbb{Z}_5, \text{ assim}$$

$$(\overline{2}x + \overline{3})^2 + (\overline{3}x + \overline{2})^2 + \overline{5} \cdot x = \overline{0} \quad \Leftrightarrow$$

$$(\overline{2}x + \overline{3})^2 + (-\overline{2}x - \overline{3})^2 + \overline{0} = \overline{0} \quad \Leftrightarrow$$

$$(\overline{2}x + \overline{3})^2 + (\overline{2}x + \overline{3})^2 = \overline{0} \quad \Leftrightarrow \quad \overline{2} \cdot (\overline{2}x + \overline{3})^2 = \overline{0}$$

$\overline{2}$ não é div. de zero em $\mathbb{Z}_5$ assim

$$\overline{2} \cdot x + \overline{3} = \overline{0} \quad \Rightarrow \quad \overline{2}x = -\overline{3} = \overline{2}$$

$$\Rightarrow \boxed{x = \overline{1}} //$$

Ex. 6 Resolva em $\mathbb{Z}_4$

$$\begin{cases} x + y + z = \overline{0} \\ \overline{2}x + \overline{3}y + \overline{3}z = \overline{3} \\ x + y + \overline{3}z = \overline{0} \end{cases}$$

Solução Temos que $\overline{2} \cdot z = \overline{0}$, assim

$$z = \overline{0} \quad \text{ou} \quad z = \overline{2}$$

$$\text{Se } z = \overline{0}, \text{ assim temos } \begin{cases} x + y = \overline{0} \\ \overline{2}x + \overline{3}y = \overline{3} \end{cases} \Rightarrow \begin{matrix} y = \overline{3} \\ x = -\overline{3} = \overline{1} \end{matrix}$$

$$\text{Se } z = \overline{2}, \text{ assim temos } \begin{cases} x + y = \overline{2} \\ 2x + 3y = \overline{1} \end{cases} \Rightarrow \begin{matrix} x = \overline{1} \\ y = \overline{1} \end{matrix}$$

Assim $x = \overline{1}, y = \overline{3}, z = \overline{0}$, ou $x = \overline{1}, y = \overline{1}, z = \overline{2}$.