MAT 0120

Solução - lista 8

1) Demonstração:

Temos que $\mathbb{Z}/_4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ Daí,

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	1	2

Para $\mathbb{Z}/_7\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6\}$. Assim,

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Faça a tabela de $\mathbb{Z}/6\mathbb{Z}$

2) (1) Queremos encontrar os menores representantes positivos de $\overline{(-5)}$ e $\overline{(-4)}$.

Note que $-5 \equiv 19 \pmod{24}$. Daí, pela prop 3.6.2, $\overline{(-5)} = \overline{(19)}$ Veja que 19 é o menor representante positivo pois $\{0, 1, \ldots, 23\}$ é um sistema completo de resíduos módulo 24.

Analogamente, como $-4 \equiv 20 \pmod{24}$, segue que 20 é o menor representante positivo de $\overline{(-4)}$. ■ (2)

(2) Agora, queremos todos os divisores de zero e os elementos inversíveis de $\mathbb{Z}_{24}$.

Obs: Lema 3.6.8: Um elemento não-nulo $\bar{a}$ de $\mathbb{Z}_m$ é divisor de zero se, e somente se, $mdc(a, m) \neq 1$

Assim, veja que $24 = 2^3 \cdot 3$. Portanto o conjunto de divisores de zero $D = (\bar{2}\mathbb{Z} \cup \bar{3}\mathbb{Z}) \cap \{\bar{1}, \ldots, \bar{23}\}$, pois se $x \in \bar{2}\mathbb{Z}$ e $0 < x \leq 23$, então $x = 2k$ e $mdc(x, 24) \geq 2$. Analogamente, se $x \in \bar{3}\mathbb{Z} \cap \{\bar{1}, \ldots, \bar{23}\}$.

Daí, $D = \{\bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}, \bar{12}, \bar{14}, \bar{16}, \bar{18}, \bar{20}, \bar{22}\} \cup \{\bar{3}, \bar{9}, \bar{15}, \bar{18}\}$

Obs: Definição: Um elemento $\bar{a} \in \mathbb{Z}_m$ diz-se inversível se existe $\bar{a}' \in \mathbb{Z}_m$ tal que $\bar{a} \cdot \bar{a}' = \bar{1}$. Um elemento $\bar{a}'$ nessas condições diz-se um inverso de $\bar{a}$.

Note que o inverso é único. De fato se $\bar{a}'$ e $\tilde{\bar{a}}$ são inversos de $\bar{a}$ então

$$\bar{a}' = \bar{a}' \cdot \bar{1} = \bar{a}'(\bar{a} \cdot \tilde{\bar{a}}) = (\bar{a}' \cdot \bar{a})\tilde{\bar{a}} = \bar{1} \cdot \tilde{\bar{a}} = \tilde{\bar{a}}$$

Proposição 3.6.13: Seja $\bar{a}$ um elemento não nulo de

$\mathbb{Z}_m$. Então, $\bar{a}$ é inversível se, e somente se, $mdc(a, m) = 1$

Logo, $I = \{\bar{1}, \dots, \bar{23}\}$ e $D = \{1, 5, 7, 11, 13, 17, 19, 23\}$.

3. Esse item é simples e bastante parecido com o exercício 1.

Exercício 3:

1) Demonstração:

Considere A um anel finito, $A = \{a_1 \leq \dots \leq a_m\}$

Suponha que $\forall a, b, c \; (a \leq b \Rightarrow a + c \leq b + c)$. Assim, para $a_k \in A$

$$a_m + a_k \leq a_m \Rightarrow -a_m + a_m + a_k \leq -a_m + a_m$$

$$\Rightarrow \quad a_k \leq 0. \quad (*)$$

Ou seja, concluímos que todo elemento de A satisfaz $(*)$. No entanto, veja que, para $a_k \neq 0$, se $a_k < 0$ então $-a_k > 0$

$$a_k < 0 \Rightarrow \underbrace{-a_k + a_k}_{0} < -a_k$$

Logo, temos uma contradição.

Exercício 9:

1) $x^{21} - x = \bar{0}$ para $m = 5$

Dem:

$x^{21} - x = 0 \Rightarrow x(x^{20} - 1) = \bar{0} \Rightarrow x = 0$ ou $x^{20} - 1 = 0$, pois $\mathbb{Z}_5$ não possui divisores de zero.

Assim, se $x \neq 0$, pela teorema de fermat,

$x^4 = 1 \Rightarrow (x^4)^5 = x^{20} = 1$.

Logo, qualquer elemento de $\mathbb{Z}_5$ é solução ■

(2) $x^{12} - x = 0$ para $m = 5$

Demonstração:

Novamente, note que $x^{12} - x = 0 \Leftrightarrow x(x^{11} - 1) = 0$.

Como $\mathbb{Z}_5$ não possui divisores de zero,

$x = 0$ ou $x^{11} = 1$

Se $x \neq 0$, usando o teorema de fermat $x^4 = 1 \Rightarrow$

$x^{12} = 1 \Rightarrow x \cdot x^{11} = 1$. Logo, x^{11} é o inverso de x. Vejo que o inverso de $x \in \mathbb{Z}_5$ é igual a 1 apenas se $x = 1$. Logo, as soluções são 0 e 1 ■

(3) $x^p = \bar{4}$, para p primo positivo.

Demonstração:

Temos que pelo teorema de fermat, $x^p = x$.

Logo $x = \bar{4}$.

(4) $x^{2p} - x^p = 6$

Demonstração:

Temos pelo teo. de fermat que $x^p = x$. Assim

$x^{2p} - x^p = 6 \iff (x^p)^2 - x^p = 6 \iff x^2 - x = 6 \iff$

$x^2 - x - 6 = 0 \iff (x-3)(x-2) = 0 \iff$

$(x-3) = 0$ ou $(x-2) = 0$. Logo, as soluções são $\bar{3}$ e $\bar{2}$.

(5) $x^{4p-4} - x^{2p-2} = \bar{5}$.

Demonstração:

$x^{4p-4} - x^{2p-2} = \bar{5} \iff x^{4(p-1)} - x^{2(p-1)} = \bar{5} \iff$

$(x^{p-1})^4 - (x^{p-1})^2 = \bar{5}$

Se $x \neq \bar{0}$ então pelo teo. do fermat $x^{p-1} = 1$ e

$(x^{p-1})^4 - (x^{p-1})^2 = \bar{1} - \bar{1} = \bar{0} = \bar{5}$

Se $x=0$, então $\bar{0}=\bar{5}$.

Daí, se $p=5$, todo elemento é solução. Se $p\neq 5$, não há soluções.

Exercício 5:

Demonstração:

Consideremos $m|n$ e $f: \mathbb{Z}_n \to \mathbb{Z}_m$
$\bar{x} \mapsto \bar{x}$

(1) Vamos provar que f está bem definida. Isto é, precisamos provar que se $\bar{a}=\bar{b}$, $\bar{a},\bar{b}\in\mathbb{Z}_n$ então $f(\bar{a})=f(\bar{b})$. Como $\bar{a}=\bar{b} \Rightarrow a\equiv b \pmod{n} \Rightarrow$ $n|(a-b)$. Do fato de que $m|n$, segue que

$$m|(a-b) \Rightarrow a\equiv b \pmod{m} \Rightarrow \bar{a}=\bar{b} \Rightarrow$$

$f(\bar{a})=f(\bar{b})$.

(2)

(a) $f(\alpha+\beta)=f(\alpha)+f(\beta)$

Dem:

$$f(\overline{\alpha+\beta}) = \overline{\alpha+\beta} = \bar{\alpha}+\bar{\beta} = f(\bar{\alpha})+f(\bar{\beta}).$$

(b) $f(0) = 0$

Dem: Não há o que fazer

(c) e (d) são análogos

Exercício 6:

Consideremos $\text{mdc}(m, n) = 1$ e $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$

$$\bar{x} \longmapsto (\bar{x}, \bar{x})$$

(a) Sejam $\bar{a} = \bar{b}$, $\bar{a}, \bar{b} \in \mathbb{Z}_{mn}$ Assim,

$a \equiv b \pmod{mn} \iff mn \mid a-b \iff m \mid a-b$ e $n \mid (a-b)$

Logo $\bar{a} = \bar{b}$ (em $\mathbb{Z}_m$) e $\bar{a} = \bar{b}$ (em $\mathbb{Z}_m$). Portanto,

$f(\bar{a}) = (\bar{a}, \bar{a}) = (\bar{b}, \bar{b}) = f(\bar{b})$.

(b) Não há o que fazer

(c) $f(\overline{\alpha+\beta}) = (\overline{\alpha+\beta}, \overline{\alpha+\beta}) = (\bar{\alpha}+\bar{\beta}, \bar{\alpha}+\bar{\beta}) = (\bar{\alpha}, \bar{\alpha}) + (\bar{\beta}, \bar{\beta})$

$f(\bar{\alpha}) + f(\bar{\beta})$

(d) Fiz em uma monitoria.