Lista 5 com respostas

MAT0120 — 1° SEMESTRE DE 2020

Inteiros Módulo m

Exercício 1.
Construa as tabelas de adição e de multiplicação de $\mathbb{Z}_7$ e $\mathbb{Z}_{12}$.

Solução 1.
$\mathbb{Z}_7$:

$+$	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

$\cdot$	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

$\mathbb{Z}_{12}$:

$+$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

$\cdot$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

Exercício 2.
Busque os inversos dos seguintes elementos

a) $\overline{14}$ em $\mathbb{Z}_{15}$;

b) $\overline{38}$ em $\mathbb{Z}_{83}$;

c) $\overline{351}$ em $\mathbb{Z}_{6669}$;

d) $\overline{91}$ em $\mathbb{Z}_{2565}$.

Solução 2.

a)
$$\begin{aligned}
14x &\equiv 1 \pmod{15}\\
-x &\equiv 1 \pmod{15}\\
x &\equiv -1 \pmod{15}\\
x &\equiv 14 \pmod{15}\\
\overline{14}^{-1} &= \overline{14}.
\end{aligned}$$

b)
$$\begin{aligned}
38x &\equiv 1 \pmod{83}\\
76x &\equiv 2 \pmod{83}\\
-7x &\equiv 2 \pmod{83}\\
12\cdot(-7)x &\equiv 24 \pmod{83}\\
-84x &\equiv 24 \pmod{83}\\
-x &\equiv 24 \pmod{83}\\
x &\equiv -24 \pmod{83}\\
x &\equiv 59 \pmod{83}\\
\overline{38}^{-1} &= \overline{59}
\end{aligned}$$

c) $\text{mdc}(351, 6669) = 3 \neq 1$, portanto $\nexists\, \overline{351}^{-1}$

d) Pelo algoritmo de Euclides, temos:

$$1 = 451 \cdot 91 - 16 \cdot 2565$$

$$\overline{1} = \overline{451} \cdot \overline{91}$$
$$\overline{91}^{-1} = \overline{451}$$

Exercício 3.
Mostre

a) $\overline{73} = \overline{-92}$ em $\mathbb{Z}_5$;

b) $\overline{99} = \overline{-87}$ em $\mathbb{Z}_6$;

c) $\overline{3!} = \overline{-2!}$ em $\mathbb{Z}_8$;

d) $\overline{12!} = \overline{15!}$ em $\mathbb{Z}_9$.

Solução 3.
a) Pelo algoritmo da divisão:

$$\left\{\begin{array}{rcl} 73 & = & 5 \cdot 14 + 3 \\ -92 & = & 5 \cdot (-19) + 3 \end{array}\right. \Rightarrow 73 - 5 \cdot 14 = -92 + 5 \cdot 19 \Rightarrow$$
$$\overline{73} - \overline{5 \cdot 14} = \overline{-92} + \overline{5 \cdot 19} \Rightarrow \overline{73} = \overline{-92}.$$

b) Pelo algoritmo da divisão:

$$\left\{\begin{array}{rcl} 99 & = & 6 \cdot 16 + 3 \\ -87 & = & 6 \cdot (-15) + 3 \end{array}\right. \Rightarrow 99 - 6 \cdot 16 = -87 + 6 \cdot 15 \Rightarrow$$
$$\overline{99} - \overline{6 \cdot 16} = \overline{-87} + \overline{6 \cdot 15} \Rightarrow \overline{99} = \overline{-87}.$$

c) Note que $\overline{3!} = \overline{6}$ e $\overline{-2!} = \overline{-2}$. Pelo algoritmo da divisão:

$$\left\{\begin{array}{rcl} 6 & = & 8 \cdot 0 + 6 \\ -2 & = & 8 \cdot (-1) + 6 \end{array}\right. \Rightarrow 6 - 8 \cdot 0 = -2 + 8 \cdot 1 \Rightarrow$$
$$\overline{6} - \overline{8 \cdot 0} = \overline{-2} + \overline{8 \cdot 1} \Rightarrow \overline{6} = \overline{-2}.$$

d) Note que $\overline{12!} = \overline{12 \cdot 11 \cdot 10 \cdot 9 \cdots 1} = \overline{3 \cdot 2 \cdot 1 \cdot 0 \cdots 1} = \overline{0}$ e $\overline{15!} = \overline{15 \cdot 14 \cdots \cdot 9 \cdots 1} = \overline{6 \cdot 5 \cdots 0 \cdots 1} = \overline{0}$.

Exercício 4.
Em $\mathbb{Z}_{20}$, determine

a) os menores representantes positivos de $\overline{-10}$ e $\overline{-6}$;

b) todos os divisores de zero;

c) todos os elementos inversos com seus inversos;

d) repita os itens b) e c) para $\mathbb{Z}_{10}$ e $\mathbb{Z}_{12}$.

Solução 4.

a)

$$-10 = -1 \cdot 20 + 10 \Rightarrow \overline{-10} = \overline{10}$$

$$-6 = -1 \cdot 20 + 14 \Rightarrow \overline{-6} = \overline{14}$$

b) Precisamos achar os valores de $a < 20$ tais que $\text{mdc}(a, 20) \neq 1$. Logo, os divisores de zero são do tipo $\overline{a}$, que pertencem ao conjunto $\left\{\overline{2}, \overline{4}, \overline{5}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{15}, \overline{16}, \overline{18}\right\}$, pois:

$$\overline{2} \cdot \overline{10} = \overline{0}$$

$$\overline{4} \cdot \overline{5} = \overline{0}$$

$$\overline{6} \cdot \overline{10} = \overline{0}$$

$$\overline{8} \cdot \overline{5} = \overline{0}$$

$$\overline{12} \cdot \overline{5} = \overline{0}$$

$$\overline{14} \cdot \overline{10} = \overline{0}$$

$$\overline{15} \cdot \overline{4} = \overline{0}$$

$$\overline{16} \cdot \overline{5} = \overline{0}$$

$$\overline{18} \cdot \overline{10} = \overline{0}$$

c) Precisamos achar os valores de $a < 20$ tais que $\text{mdc}(a, 20) = 1$. Logo, os elementos inversos são do tipo $\overline{a}$, que pertencem ao conjunto $\left\{\overline{1}, \overline{3}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19}\right\}$, pois:

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

$$\overline{3} \cdot \overline{7} = \overline{1}$$

$$\overline{9} \cdot \overline{9} = \overline{1}$$

$$\overline{11} \cdot \overline{11} = \overline{1}$$

$$\overline{13} \cdot \overline{17} = \overline{1}$$

$$\overline{19} \cdot \overline{19} = \overline{1}$$

d) Em Z_{10}, os divisores de zero pertencem ao conjunto $\left\{\overline{2}, \overline{4}, \overline{5}, \overline{6}, \overline{8}\right\}$, pois:

$$\overline{2} \cdot \overline{5} = \overline{0}$$

$$\overline{4} \cdot \overline{5} = \overline{0}$$

$$\overline{6} \cdot \overline{5} = \overline{0}$$

$$\overline{8} \cdot \overline{5} = \overline{0}$$

Em Z_{10}, os elementos inversos pertencem ao conjunto $\left\{\overline{1}, \overline{3}, \overline{7}, \overline{9}\right\}$, pois:

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

$$\overline{3} \cdot \overline{7} = \overline{1}$$

$$\overline{9} \cdot \overline{9} = \overline{1}$$

Em Z_{12}, os divisores de zero pertencem ao conjunto $\left\{\overline{2},\overline{3},\overline{4},\overline{6},\overline{8},\overline{9},\overline{10}\right\}$, pois:

$$\overline{2}\cdot\overline{6}=\overline{0}$$

$$\overline{3}\cdot\overline{4}=\overline{0}$$

$$\overline{8}\cdot\overline{3}=\overline{0}$$

$$\overline{9}\cdot\overline{4}=\overline{0}$$

$$\overline{10}\cdot\overline{6}=\overline{0}$$

Em Z_{12}, os elementos inversos pertencem ao conjunto $\left\{\overline{1},\overline{5},\overline{7},\overline{11}\right\}$, pois:

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

$$\overline{5}\cdot\overline{5}=\overline{1}$$

$$\overline{7}\cdot\overline{7}=\overline{1}$$

$$\overline{11}\cdot\overline{11}=\overline{1}$$

Exercício 5.
Determine os inversos multiplicativos de $\overline{a}$ em $\mathbb{Z}_n$ e, em seguida, resolva as equações de congruências reduzidas:

a) $a=3, \mathbb{Z}_n=\mathbb{Z}_{10}$ e $3x\equiv 7 \pmod{10}$;

b) $a=6, \mathbb{Z}_n=\mathbb{Z}_{35}$ e $6x-2\equiv 11 \pmod{35}$.

Solução 5.

a) Como $\overline{3}\cdot\overline{7}=\overline{1}$, temos:

$$\begin{array}{rcl} 3x & \equiv & 7(\text{mod } 10) \\ 7\cdot 3x & \equiv & 7\cdot 7(\text{mod } 10) \\ x & \equiv & 9(\text{mod } 10). \end{array}$$

b) Como $\overline{6}\cdot\overline{6}=\overline{1}$, temos:

$$\begin{array}{rcl} 6x-2 & \equiv & 11(\text{mod } 35) \\ 6x & \equiv & 13(\text{mod } 35) \\ 6\cdot 6x & \equiv & 6\cdot 13(\text{mod } 35) \\ x & \equiv & 8(\text{mod } 35) \end{array}$$

Exercício 6.
Sejam $\overline{a},\overline{b},\overline{c}\in\mathbb{Z}_m$ com $\text{mdc}(c,m)=1$. Prove que $\overline{a}\cdot\overline{c}=\overline{b}\cdot\overline{c}$ implica que $\overline{a}=\overline{b}$.

Solução 6.
$\overline{a}\cdot\overline{c}=\overline{b}\cdot\overline{c}\Rightarrow\left(\overline{a}-\overline{b}\right)\cdot\overline{c}=\overline{0}$. Como $\text{mdc}(c,m)=1$, então $\overline{c}$ não é nem divisor de zero e nem zero. Logo, $\overline{a}-\overline{b}=\overline{0}$, ou seja, $\overline{a}=\overline{b}$.

Exercício 7.
Sejam p um primo e $\overline{a}, \overline{b} \in \mathbb{Z}_p$. Prove que

a) $\overline{a}^p = \overline{a}$;

b) $(\overline{a} + \overline{b})^p = \overline{a} + \overline{b}$.

Solução 7.
a) Pelo Teorema de Fermat, temos $a^p \equiv a (\text{mod } p)$, ou seja, $\exists k \in Z$ tal que $a^p = a + pk$. Logo:

$$a^p = a + pk$$
$$\overline{a^p} = \overline{a + pk}$$
$$\overline{a}^p = \overline{a} + \overline{p} \cdot \overline{k}$$
$$\overline{a}^p = \overline{a} + \overline{0} \cdot \overline{k}$$
$$\overline{a}^p = \overline{a}$$

b) Pelo Teorema de Fermat, temos $(a + b)^p \equiv a + b (\text{mod } p)$, ou seja, $\exists k \in Z$ tal que $(a + b)^p = a + b + pk$. Logo:

$$(a + b)^p = a + b + pk$$
$$\overline{(a + b)^p} = \overline{a + b + pk}$$
$$\overline{a + b}^p = \overline{a + b} + \overline{p} \cdot \overline{k}$$
$$\overline{a + b}^p = \overline{a + b} + \overline{0} \cdot \overline{k}$$
$$\overline{a + b}^p = \overline{a + b}$$

Exercício 8.
O elemento $\overline{a} \in \mathbb{Z}_m$ chama-se **idempotente** se $\overline{a} \cdot \overline{a} = \overline{a}$.

a) Busque todos idempotentes em $\mathbb{Z}_6$ e $\mathbb{Z}_{12}$.

b) Busque todos idempotentes em $\mathbb{Z}_{10}$ e $\mathbb{Z}_{30}$.

c) Seja p um primo. Mostre que $\overline{0}, \overline{1}$ são os únicos idempotentes em $\mathbb{Z}_p$.

Solução 8.
a) Em $\mathbb{Z}_6$, os elementos idempotentes são: $\overline{0}, \overline{1}, \overline{3}$ e $\overline{4}$.

$$\overline{0} \cdot \overline{0} = \overline{0}$$
$$\overline{1} \cdot \overline{1} = \overline{1}$$
$$\overline{2} \cdot \overline{2} = \overline{4}$$
$$\overline{3} \cdot \overline{3} = \overline{3}$$
$$\overline{4} \cdot \overline{4} = \overline{4}$$

$$\overline{5}\cdot\overline{5}=\overline{1}$$

Em $\mathbb{Z}_{12}$, os elementos idempotentes são: $\overline{0},\overline{1},\overline{4}$ e $\overline{9}$.

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

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

$$\overline{2}\cdot\overline{2}=\overline{4}$$

$$\overline{3}\cdot\overline{3}=\overline{9}$$

$$\overline{4}\cdot\overline{4}=\overline{4}$$

$$\overline{5}\cdot\overline{5}=\overline{1}$$

$$\overline{6}\cdot\overline{6}=\overline{0}$$

$$\overline{7}\cdot\overline{7}=\overline{1}$$

$$\overline{8}\cdot\overline{8}=\overline{4}$$

$$\overline{9}\cdot\overline{9}=\overline{9}$$

$$\overline{10}\cdot\overline{10}=\overline{4}$$

$$\overline{11}\cdot\overline{11}=\overline{1}$$

b) Em $\mathbb{Z}_{10}$, os elementos idempotentes são: $\overline{0},\overline{1},\overline{5}$ e $\overline{6}$.

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

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

$$\overline{2}\cdot\overline{2}=\overline{4}$$

$$\overline{3}\cdot\overline{3}=\overline{9}$$

$$\overline{4}\cdot\overline{4}=\overline{6}$$

$$\overline{5}\cdot\overline{5}=\overline{5}$$

$$\overline{6}\cdot\overline{6}=\overline{6}$$

$$\overline{7}\cdot\overline{7}=\overline{9}$$

$$\overline{8}\cdot\overline{8}=\overline{4}$$

$$\overline{9}\cdot\overline{9}=\overline{1}$$

Em $\mathbb{Z}_{30}$, os elementos idempotentes são:$\overline{0},\overline{1},\overline{6},\overline{10},\overline{15},\overline{16},\overline{21}$ e $\overline{25}$.

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

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

$$\overline{2}\cdot\overline{2}=\overline{4}$$

$$\overline{3}\cdot\overline{3}=\overline{9}$$

$$\overline{4}\cdot\overline{4}=\overline{16}$$

$$\overline{5}\cdot\overline{5}=\overline{25}$$

$$\overline{6}\cdot\overline{6}=\overline{6}$$
$$\overline{7}\cdot\overline{7}=\overline{19}$$
$$\overline{8}\cdot\overline{8}=\overline{4}$$
$$\overline{9}\cdot\overline{9}=\overline{21}$$
$$\overline{10}\cdot\overline{10}=\overline{10}$$
$$\overline{11}\cdot\overline{11}=\overline{1}$$
$$\overline{12}\cdot\overline{12}=\overline{24}$$
$$\overline{13}\cdot\overline{13}=\overline{19}$$
$$\overline{14}\cdot\overline{14}=\overline{16}$$
$$\overline{15}\cdot\overline{15}=\overline{15}$$
$$\overline{16}\cdot\overline{16}=\overline{16}$$
$$\overline{17}\cdot\overline{17}=\overline{19}$$
$$\overline{18}\cdot\overline{18}=\overline{24}$$
$$\overline{19}\cdot\overline{19}=\overline{1}$$
$$\overline{20}\cdot\overline{20}=\overline{10}$$
$$\overline{21}\cdot\overline{21}=\overline{21}$$
$$\overline{22}\cdot\overline{22}=\overline{4}$$
$$\overline{23}\cdot\overline{23}=\overline{19}$$
$$\overline{24}\cdot\overline{24}=\overline{6}$$
$$\overline{25}\cdot\overline{25}=\overline{25}$$
$$\overline{26}\cdot\overline{26}=\overline{16}$$
$$\overline{27}\cdot\overline{27}=\overline{9}$$
$$\overline{28}\cdot\overline{28}=\overline{4}$$
$$\overline{29}\cdot\overline{29}=\overline{1}$$

c) $\overline{a}\cdot\overline{a}=\overline{a}\Rightarrow\overline{a}\cdot(\overline{a}-\overline{1})=\overline{0}$. Como Z_p não possui divisores de zero, então ou $\overline{a}=\overline{0}$ ou $\overline{a}-\overline{1}=\overline{0}$, o que implica que $\overline{a}=\overline{1}$.

Exercício 9.

O elemento $\overline{a}\in\mathbb{Z}_m$ chama-se **nilpotente** se $\overline{a}^k=\overline{0}$ para algum k. Mostre que $\mathbb{Z}_m$ não tem não-nulos nilpotentes se e só se m não tem fator primo em quadrado.

Solução 9.
A sentença é equivalente a: m tem fator primo em quadrado se, e só se, $\mathbb{Z}_m$ tem nilpotentes não-nulos.

$(\Rightarrow)$: Suponha que m tem um fator primo p em quadrado. Assim, $m = p \cdot p \cdot m'$ com $m' \in \mathbb{Z}^*$. Seja $a = p \cdot m'$. Logo, $\overline{a}^2 = p \cdot p \cdot m' \cdot m' = \overline{0}$, ou seja, $\overline{a}$ é nilpotente não nulo.

$(\Leftarrow)$: Suponha que m não tem fatores primos ao quadrado, ou seja, $m = p_1 \cdot p_2 \cdots p_k$ com todos os primos distintos entre si. Seja $\overline{a} \in \mathbb{Z}_m^*$, com $\overline{a}^n = 0$. Assim, m divide a^n, ou seja, m divide cada fator p_i de a, ou seja, $\overline{a} = \overline{0}$.

Exercício 10.
Em $\mathbb{Z}_7$, busque os quadrados de todos elementos.

Solução 10.

$$\overline{0} \cdot \overline{0} = \overline{0}$$
$$\overline{1} \cdot \overline{1} = \overline{1}$$
$$\overline{2} \cdot \overline{2} = \overline{4}$$
$$\overline{3} \cdot \overline{3} = \overline{2}$$
$$\overline{4} \cdot \overline{4} = \overline{2}$$
$$\overline{5} \cdot \overline{5} = \overline{4}$$
$$\overline{6} \cdot \overline{6} = \overline{1}$$

Exercício 11.
Busque as raízes em $\mathbb{Z}_7$ de $x^2 + x + \overline{1}$ por completar o quadrado e usando Exercício 10.

$$\begin{aligned} x^2 + x + \overline{1} &= \overline{0} \\ x^2 + 2x + \overline{1} &= x \\ \left(x + \overline{1}\right)^2 &= x \end{aligned}$$

Por inspeção, usando Ex.10 temos $S = \left\{\overline{2}, \overline{4}\right\}$, pois $(\overline{2} + \overline{1}) \cdot (\overline{2} + \overline{1}) = \overline{2}$ e $(\overline{4} + \overline{1}) \cdot (\overline{4} + \overline{1}) = \overline{4}$.

Solução 11.

Exercício 12.
Busque as raízes em $\mathbb{Z}_7$ de $\overline{3}x^2 + \overline{4}x + \overline{3}$ por completar o quadrado e usando Exercício 10.

Solução 12.

$$\begin{aligned} \overline{3}x^2 + \overline{4}x + \overline{3} &= \overline{0} \\ \overline{5} \cdot \left(\overline{3}x^2 + \overline{4}x + \overline{3}\right) &= \overline{5} \cdot \overline{0} \\ x^2 + \overline{6}x + \overline{1} &= \overline{0} \\ \left(x + \overline{3}\right)^2 &= \overline{1} \end{aligned}$$

Por inspeção, $S = \left\{\overline{3}, \overline{5}\right\}$, pois, pelo Ex. 10, temos $(\overline{x} + \overline{3}) = \overline{1}$ ou $(\overline{x} + \overline{3}) = \overline{6}$.

Exercício 13.
Em $\mathbb{Z}_{11}$, busque os quadrados de todos elementos.

Solução 13.

$$\overline{0}\cdot\overline{0}=\overline{0}$$
$$\overline{1}\cdot\overline{1}=\overline{1}$$
$$\overline{2}\cdot\overline{2}=\overline{4}$$
$$\overline{3}\cdot\overline{3}=\overline{9}$$
$$\overline{4}\cdot\overline{4}=\overline{5}$$
$$\overline{5}\cdot\overline{5}=\overline{3}$$
$$\overline{6}\cdot\overline{6}=\overline{3}$$
$$\overline{7}\cdot\overline{7}=\overline{5}$$
$$\overline{8}\cdot\overline{8}=\overline{9}$$
$$\overline{9}\cdot\overline{9}=\overline{4}$$
$$\overline{10}\cdot\overline{10}=\overline{1}$$

Exercício 14.
Busque as raízes em $\mathbb{Z}_{11}$ de $\overline{4}x^2+\overline{6}x+\overline{1}$ por completar o quadrado e usando Exercício 13.

Solução 14.

$$\begin{array}{rcl}\overline{4}x^2+\overline{6}x+\overline{1} & = & \overline{0}\\ \overline{3}\cdot\left(\overline{4}x^2+\overline{6}x+\overline{1}\right) & = & \overline{3}\cdot\overline{0}\\ x^2+\overline{7}x+\overline{3} & = & \overline{0}\\ x^2+\overline{6}x+\overline{9} & = & -x+\overline{6}\\ \left(x+\overline{3}\right)^2 & = & -x+\overline{6}\end{array}$$

Por inspeção, $S=\left\{\overline{1},\overline{3}\right\}$.

Exercício 15.
Busque as raízes em $\mathbb{Z}_{11}$ de $\overline{4}x^2+\overline{6}x+\overline{8}$ por completar o quadrado e usando Exercício 13.

Solução 15.

$$\begin{array}{rcl}\overline{4}x^2+\overline{6}x+\overline{8} & = & \overline{0}\\ \overline{3}\cdot\left(\overline{4}x^2+\overline{6}x+\overline{8}\right) & = & \overline{3}\cdot\overline{0}\\ x^2+\overline{7}x+\overline{2} & = & \overline{0}\\ x^2+\overline{6}x+\overline{9} & = & -x+\overline{7}\\ \left(x+\overline{3}\right)^2 & = & -x+\overline{7}\end{array}$$

Por inspeção, $S=\emptyset$.

Exercício 16.
Busque os divisores de zero, em $\mathbb{Z}_m$, e resolva as equações abaixo

a) $\overline{7}x = \overline{0}$, $m = 21$;

b) $\overline{4}x = \overline{10}$, $m = 22$;

c) $\overline{3}x = \overline{6}$, $m = 24$;

d) $\overline{5}x = \overline{0}$, $m = 25$;

Solução 16.
a) $S = \left\{\overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}, \overline{18}\right\}$

b) $S = \left\{\overline{8}, \overline{19}\right\}$

c) $S = \left\{\overline{2}, \overline{10}, \overline{18}\right\}$

d) $S = \left\{\overline{0}, \overline{5}, \overline{10}, \overline{15}, \overline{20}, \right\}$

Exercício 17.
Busque os divisores de zero, em $\mathbb{Z}_m$, para $m = 8, 9, 10, 14, 15, 26, 28$.

Solução 17.
Em $\mathbb{Z}_8 : \overline{2}, \overline{4}, \overline{6}$.

Em $\mathbb{Z}_9 : \overline{3}, \overline{6}$.

Em $\mathbb{Z}_{10} : \overline{2}, \overline{4}, \overline{5}, \overline{6}, \overline{8}$.

Em $\mathbb{Z}_{14} : \overline{2}, \overline{4}, \overline{6}, \overline{7}, \overline{8}, \overline{10}, \overline{12}$.

Em $\mathbb{Z}_{15} : \overline{3}, \overline{5}, \overline{6}, \overline{9}, \overline{10}, \overline{12}$.

Em $\mathbb{Z}_{26} : \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{13}, \overline{14}, \overline{16}, \overline{18}, \overline{20}, \overline{22}, \overline{24}$.

Em $\mathbb{Z}_{28} : \overline{2}, \overline{4}, \overline{6}, \overline{7}, \overline{8}, \overline{10}, \overline{12}, \overline{13}, \overline{14}, \overline{16}, \overline{18}, \overline{20}, \overline{21}, \overline{22}, \overline{24}, \overline{26}$.

Exercício 18.
Ache os divisores de zero e os elementos que tem inversos em $\mathbb{Z}_5$, $\mathbb{Z}_8$, $\mathbb{Z}_{17}$, $\mathbb{Z}_{21}$ e $\mathbb{Z}_{89}$.

Solução 18.
Em $\mathbb{Z}_5, \mathbb{Z}_{17}$ e $\mathbb{Z}_{89}$ não há divisores de zero e todos os elementos são inversíveis.

Em $\mathbb{Z}_8$ os divisores de zero são $\overline{2}, \overline{4}, \overline{6}$ e os elementos inversíveis são $\overline{1}, \overline{3}, \overline{5}$ e $\overline{7}$.

Em $\mathbb{Z}_{21}$ os divisores de zero são $\overline{3}, \overline{6}, \overline{7}, \overline{9}, \overline{12}, \overline{14}, \overline{15}$ e $\overline{18}$ e os elementos inversíveis são $\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{8}, \overline{10}, \overline{11}, \overline{13}, \overline{16}, \overline{17}, \overline{19}$ e $\overline{20}$.

Exercício 19.
Resolva, em $\mathbb{Z}_m$, as equações abaixo:

a) $\overline{3}x + \overline{2} = \overline{6}x + \overline{7}$, $m = 8$;

b) $(\overline{2}x + \overline{3})^2 + (\overline{3}x + \overline{2})^2 + \overline{5}x = \overline{0}$, $m = 5$;

c) $\overline{4}x - \overline{7} + \overline{6}x + \overline{2} = \overline{3}x + \overline{5}x$, $m = 12$;

d) $x^{21} - x = \overline{0}$, $m = 5$;

e) $x^{12} - \overline{1} = \overline{0}$, $m = 5$;

f) $x^7 - x = \overline{0}$, $m = 4$.

Solução 19.

a)
$$\begin{aligned} \overline{3}x + \overline{2} &= \overline{6}x + \overline{7} \\ \overline{3}x &= \overline{-5} = \overline{3} \\ \overline{3} \cdot \overline{3}x &= \overline{3} \cdot \overline{3} \\ x &= \overline{1} \end{aligned}$$

b)
$$\begin{aligned} (\overline{2}x + \overline{3})^2 + (\overline{3}x + \overline{2})^2 + \overline{5}x &= \overline{0} \\ (\overline{2}x + \overline{3})^2 + (\overline{3}x + \overline{2})^2 &= \overline{0} \\ \overline{13}x^2 + \overline{24}x + \overline{13} &= \overline{0} \\ \overline{3}x^2 + \overline{4}x + \overline{3} &= \overline{0} \\ \overline{2} \cdot \left(\overline{3}x^2 + \overline{4}x + \overline{3}\right) &= \overline{2} \cdot \overline{0} \\ x^2 + 3x + \overline{1} &= \overline{0} \\ x^2 + 2x + \overline{1} &= -x \\ (x + \overline{1})^2 &= -x \end{aligned}$$

Por inspeção, $S = \left\{\overline{1}\right\}$.

c)
$$\begin{aligned} \overline{4}x - \overline{7} + \overline{6}x + \overline{2} &= \overline{3}x + \overline{5}x \\ \overline{2}x &= \overline{5} \end{aligned}$$

Como $\operatorname{mdc}(2, 12) = 2 \nmid 5$, $S = \emptyset$.

d) $x^{21} - x = x \cdot (x^{20} - \overline{1}) = \overline{0}$. Por inspeção, temos:

$$\begin{aligned} &\overline{0} \cdot \left(\overline{0}^{20} - \overline{1}\right) = \overline{0} \\ &\overline{1} \cdot \left(\overline{1}^{20} - \overline{1}\right) = \overline{0} \\ &\overline{2} \cdot \left(\overline{2}^{20} - \overline{1}\right) = \overline{2} \cdot \left(\overline{4}^{10} - \overline{1}\right) = \overline{2} \cdot \left(\left(\overline{-1}\right)^{10} - \overline{1}\right) = \overline{2} \cdot \left(\overline{1} - \overline{1}\right) = \overline{0} \\ &\overline{3} \cdot \left(\overline{3}^{20} - \overline{1}\right) = \overline{3} \cdot \left(\overline{9}^{10} - \overline{1}\right) = \overline{3} \cdot \left(\left(\overline{-1}\right)^{10} - \overline{1}\right) = \overline{3} \cdot \left(\overline{1} - \overline{1}\right) = \overline{0} \\ &\overline{4} \cdot \left(\overline{4}^{20} - \overline{1}\right) = \overline{4} \cdot \left(\left(\overline{-1}\right)^{20} - \overline{1}\right) = \overline{4} \cdot \left(\overline{1} - \overline{1}\right) = \overline{0} \end{aligned}$$

Logo, $S = Z_5$.

e) Por inspeção, temos:

$$\begin{aligned}
&\overline{0}^{12}-\overline{1}=\overline{0}-\overline{1}=\overline{4}\\
&\overline{1}^{12}-\overline{1}=\overline{1}-\overline{1}=\overline{0}\\
&\overline{2}^{12}-\overline{1}=\overline{4}^{6}-\overline{1}=\left(\overline{-1}\right)^{6}-\overline{1}=\overline{1}-\overline{1}=\overline{0}\\
&\overline{3}^{12}-\overline{1}=\overline{9}^{6}-\overline{1}=\left(\overline{-1}\right)^{6}-\overline{1}=\overline{1}-\overline{1}=\overline{0}\\
&\overline{4}^{12}-\overline{1}=\left(\overline{-1}\right)^{12}-\overline{1}=\overline{1}-\overline{1}=\overline{0}
\end{aligned}$$

Logo, $S=\left\{\overline{1},\overline{2},\overline{3},\overline{4}\right\}$.

f) $x^7-x=x\cdot(x^6-\overline{1})=\overline{0}$. Por inspeção, temos:

$$\begin{aligned}
&\overline{0}\cdot\left(\overline{0}^{6}-\overline{1}\right)=\overline{0}\\
&\overline{1}\cdot\left(\overline{1}^{6}-\overline{1}\right)=\overline{0}\\
&\overline{2}\cdot\left(\overline{2}^{6}-\overline{1}\right)=\overline{2}\cdot\left(\overline{4}^{3}-\overline{1}\right)=\overline{2}\cdot\left(\overline{0}^{6}-\overline{1}\right)=\overline{2}\cdot\left(\overline{-1}\right)=\overline{2}\\
&\overline{3}\cdot\left(\overline{3}^{6}-\overline{1}\right)=\overline{3}\cdot\left(\overline{9}^{3}-\overline{1}\right)=\overline{3}\cdot\left(\left(\overline{-1}\right)^{3}-\overline{1}\right)=\overline{3}\cdot\left(\overline{-1}-\overline{1}\right)=\overline{2}
\end{aligned}$$

Logo, $S=\left\{\overline{0},\overline{1}\right\}$.

Exercício 20.
Resolva em $\mathbb{Z}_5$ o sistema abaixo:

$$\begin{cases}\overline{4}x+y & = & \overline{1}\\ x-\overline{2}y & = & \overline{4}.\end{cases}$$

Solução 20.

$$\begin{cases}\overline{2}\cdot\left(\overline{4}x+y\right) & = & \overline{4}\cdot\overline{2}\\ x-\overline{2}y & = & \overline{4}\end{cases}\Rightarrow\begin{cases}\overline{3}x+\overline{2}y & = & \overline{3}\\ x-\overline{2}y & = & \overline{4}\end{cases}\Rightarrow\begin{cases}\overline{4}x & = & \overline{1}\\ x-\overline{2}y & = & \overline{4}\end{cases}\Rightarrow$$

$$\begin{cases}x & = & \overline{4}\\ y & = & \overline{0}\end{cases}$$

Logo, $S=\left\{\overline{4},\overline{0}\right\}$.

Exercício 21.
Resolva em $\mathbb{Z}_4$ o sistema abaixo:

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

Solução 21.
Subtraindo a terceira equação da primeira, temos $\overline{2}z=\overline{0}$, o que implica $z=\overline{0}$ ou $z=\overline{2}$.

Se $z=\overline{0}$, temos:

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

Somando as duas equações, temos $\overline{3}x = \overline{3}$, o que implica que $x = \overline{1}$. Substituindo no sistema acima, temos que $y = \overline{3}$.

Se $z = \overline{2}$, temos:

$$\begin{cases} x + y &= \overline{2} \\ \overline{2}x + \overline{3}y &= \overline{1} \end{cases}.$$

Somando as duas equações, temos $\overline{3}x = \overline{3}$, o que implica que $x = \overline{1}$. Substituindo no sistema acima, temos que $y = \overline{1}$.

Logo $S = \left\{ \left(\overline{1}, \overline{3}, \overline{0}\right), \left(\overline{1}, \overline{1}, \overline{2}\right) \right\}$.

Exercício 22.
Verifique se os elementos abaixo são inversíveis. Em caso afirmativo, determine o inverso.

a) $\overline{97}$ em $\mathbb{Z}_{307}$;

a) $\overline{22}$ em $\mathbb{Z}_{105}$.

Solução 22.

a) Como $\text{mdc}(97, 307) = 1$, então o elemento é inversível. Pelo algoritmo de Euclides, temos: $1 = -6 \cdot 307 + 19 \cdot 97$. Assim, $\overline{1} = \overline{19} \cdot \overline{97}$. Portanto, $\overline{97}^{-1} = \overline{19}$.

b) Como $\text{mdc}(22, 105) = 1$, então o elemento é inversível. Pelo algoritmo de Euclides, temos: $1 = 43 \cdot 22 - 9 \cdot 105$. Assim, $\overline{1} = \overline{43} \cdot \overline{22}$. Portanto, $\overline{22}^{-1} = \overline{43}$.