Aula 20. Inteiros modulo m. II

Lembrete: Dado um inteiro $m > 1$, define

$$\mathbb{Z}_m := \{\overline{0}, \overline{1}, \overline{2}, \ldots \overline{m-1}\},$$

com $\overline{a} = \{a + mk \mid k \in \mathbb{Z}\} = \{b \in \mathbb{Z} \mid b \equiv a (\mathrm{mod}\, m)\}$.

Temos duas operações no conjunto $\mathbb{Z}_m$: **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**:

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

A soma e o produto cumprem as seguintes propriedades padrões:

Proposição 20.1

Para todos $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}$, temos que

1) $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$
2) $\overline{a} + \overline{b} = \overline{b} + \overline{a}$
3) $\overline{a} + \overline{0} = \overline{a}$
4) $\overline{a} + \overline{(-a)} = \overline{0}$
5) $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$
6) $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$
7) $\overline{1} \cdot \overline{a} = \overline{a}$
8) $\overline{a} \cdot (\overline{b} + \overline{a}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$

20.1 Elementos inversíveis

Definição

Um elemento $\overline{a} \in \mathbb{Z}_m$ diz-se *inversível* se existe $\overline{a'} \in \mathbb{Z}_m$ tal que

$$\overline{a}\overline{a'} = \overline{1}.$$

Um elemento $\overline{a'}$ nessas condições diz-se um *inverso* de $\overline{a}$.

Notamos que no $\mathbb{Z}$ os únicos elementos inversíveis de $\mathbb{Z}$ são 1 e -1. Obviamente, $\overline{1}$ e $(\overline{-1})$ são sempre inversíveis em $\mathbb{Z}_m$. Porém, há outros exemplos. Em Z_5 temos que

$$\overline{2} \cdot \overline{3} = \overline{6} = \overline{1}$$

e

$$\overline{4} \cdot \overline{4} = \overline{16} = \overline{1},$$

logo $\overline{2}, \overline{3}$ e $\overline{4}$ são também inversíveis de $\mathbb{Z}_5$: $\overline{2}$ é o inverso de $\overline{3}$ e, reciprocamente, $\overline{4}$ é o seu próprio inverso.

Proposição 20.2

Seja $\overline{a} \in \mathbb{Z}_m$ elemento não-mulo. Assim $\overline{a}$ é invertível se e somente se $\text{mdc}(a, m) = 1$.

Prova

Temos que $\overline{a}$ é invertivel se e somente se existe $\overline{b} \in \mathbb{Z}_m$ tal que

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

ou seja se e somente se a congruencias

$$a \cdot x \equiv 1 (\text{mod}\, m)$$

tem solução. Assim se e somente se $\text{mdc}(a, m) = 1$.

Observação 20.1

Notamos que $\overline{a}$ e invertível em $\mathbb{Z}_m$ se e somente se a amite um inverso modular modulo m.

A demonstração da proposição anterior também sugere um método para determinar o inverso de um dado elemento, como ficará claro no exemplo abaixo.

Exemplo 20.1

Vamos calcular o inverso de $\overline{4}$ em $\mathbb{Z}_{37}$. Pelo Algoritmo de Euclides, determinamos os inteiros de que fala o Teorema de Bézout:

$$-9 \cdot (4) + 1 \cdot (37) = 1$$

Logo, em $\mathbb{Z}_{37}$ temos que $(-\overline{9}) \cdot \overline{4} = \overline{1}$ isto é, o inverso de $\overline{4}$ é $\overline{9} = \overline{28}$

Uma consequência imediata da proposição anterior seguinte:

Corolário 20.1

Se p um primo, assim todo elemento náo-nulo em $\mathbb{Z}_p$ é invertivel.

Prova

Prova $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$, se $1 \leqslant a \leqslant p-1$ assim $\text{mdc}(a, p) = 1 \Rightarrow \overline{a}$ é invertível.

Notamos também o seguinte: o numero dos elementos invertíveis em $\mathbb{Z}_m$ igual o numero dos elementos Se $m > 1$, assim o número dos $1 \leqslant a \leqslant m-1$ com $\text{mdc}(a,m) = 1$ assim igual a $\varphi(m)$.

20.2 *Divisores de zero*

Definição

Um elemento não-nulo $\overline{a} \in \mathbb{Z}_m$ diz-se um *divisor de zero* se existe $\overline{b} \in \mathbb{Z}_m$, também não-nulo, tal que $\overline{a}\overline{b} = \overline{0}$.

Exemplo 20.2

Por exemplo em $\mathbb{Z}_6 : \overline{2}, \overline{3}, \overline{4}$ sao divisores de zero. pois

$$\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$$
$$\overline{4} \cdot \overline{3} = \overline{12} = \overline{0}$$

Por outro lado em $\mathbb{Z}_4$ único divisor de zero é $\overline{2}$, $\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$.
Observem que em $\mathbb{Z}_4$ não há divisores de zero.

Agora, determinaremos quais são os divisores de zero em Z_m

Proposição 20.3

Um elemento não-nulo $\overline{a}$ de $\mathcal{Z}_m$ é divisor de zero se e somente se $mdc(a,m) \neq 1$.

Prova

Seja $\overline{a}$ um divisor de zero e $\overline{b} \neq \overline{0}$ um elemento de $\mathbb{Z}_m$ tal que

$$\overline{a}\overline{b} = \overline{0}.$$

Como $\overline{a}\overline{b} = \overline{ab} = \overline{0}$, temos que $ab \equiv 0 (\text{mod} m)$, isto é, $m \mid ab$, Supondo por absurdo que $\text{mdc}(a,m) = 1$, pelo Lema de Euclides vem que $m \mid b$, logo, $\overline{b} = \overline{0}$, uma contradição.
Reciprocamente, suponhamos que $\text{mdc}(a,m) = d > 1$. Vamos determinar um elemento $\overline{b} \neq \overline{0}$ em $\mathbb{Z}_m$ tal que $\overline{a}\overline{b} = 0$.
Podemos escrever

$$a = a_1 \cdot d, \qquad m = m_1 \cdot d,$$

em que $0 < m_1 < m$ (já que $d > 1$), logo, $\overline{m}_1 \neq \overline{0}$. Agora, temos que

$$a \cdot m_1 = a \cdot d \cdot m_1 = a_1 \cdot m$$

Logo, em Z_m temos

$$\overline{am}_1 = \overline{a_1 \cdot m} = \overline{0}$$

Assim, basta tomar $b = m_1$.

Corolário 20.2

Se p é um primo, assim $\mathbb{Z}_p$ nao possui os diviso des de zero.

Prova

Seja $\overline{a} \in \mathbb{Z}_p$, se $\text{mdc}(a,p) \neq 1$, assim $\text{mdc}(a,p) = p$, ou seja $p \mid a$. Portanto, $\overline{a} = \overline{0}$. Logo $\mathbb{Z}_p$ não admite divisores de zero.

Proposição 20.4

Se $\mathbb{Z}_m$ nao possui divisores de zero assim m é primo.

Prova

Escreva $m = r \cdot s$ com

$$1 \leqslant r, s \leqslant m.$$

Assim

$$\overline{0} = \overline{m} = \overline{r} \cdot \overline{s}$$

portanto ou $\overline{r} = 0$ ou $\overline{s} = 0$. Como $1 \leqslant r, s \leqslant m$ assim ou $r = m$ ou $s = m$. Logo m é um primo.

Exemplo 20.3

Vamos encontrar todos divisores de zero em $\mathbb{Z}_{12}$. Pelo critério acima, temos que $\overline{a}$ é divisor de zero em $\mathbb{Z}_{12}$ se e somente se $\text{mdc}(a,12) \neq 1$, ou seja se e somente se

$$\overline{a} : \overline{2}, \overline{3}, \overline{4}, \overline{6}, \overline{8}, \overline{9}, \overline{10}.$$

No caso, temos $\overline{2} \cdot \overline{6} = \overline{0}$, $\overline{3} \cdot \overline{4} = \overline{0}$, $\overline{8} \cdot \overline{3} = \overline{0}$, $\overline{3} \cdot \overline{4} = \overline{0}$, $\overline{10} \cdot \overline{6} = \overline{0}$.

Notamos que o numero de divisores de zero em $\mathbb{Z}_m$ igual a

$$m - 1 - \varphi(\text{m}).$$

20.3 *Cancelamento em $\mathbb{Z}_m$*

Vamos lembrar que em $\mathbb{Z}$ se

$$ab = ac,$$

e $a \neq 0$, assim $b = c$. Essa regra chama-se lei de cancelamento.
Podemos notar imediatamente que em $\mathbb{Z}_m$ isso não sempre vale.
Por exemplo, em $\mathbb{Z}_4$

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

mas $\overline{3} \neq \overline{1}$. O "problema" é existencia de divisores de zero, e como $\overline{2}$ é divisor de zero em $\mathbb{Z}_4$ assim a gente não pode cancelar ele. O que vale é o seguinte lema.

Lemma 20.1

Se $\text{mdc}(a, m) = 1$ e $\overline{a} \cdot \overline{b} = \overline{a} \cdot \overline{c}$ assim

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

Prova

Se $\overline{a} \cdot \overline{b} = \overline{a} \cdot \overline{c}$ assim

$$a \cdot b \equiv a \cdot c (\text{mod}\, m).$$

Logo $m \mid (ab - ac)$, ou seja $m \mid a(b - c)$, como $\text{mdc}(a, m) = 1$ assim $m \mid b - c$ logo $b - c \equiv 0 (\text{mod}\, m)$. Portanto, $\overline{b} = \overline{c}$.

Assim, com certas condições (como no lema anterior) podemos cancelar a numa igualdade em $\mathbb{Z}_m$. Alem disso temos o seguinte

Proposição 20.5

A propriedade cancelativa do produto vale em $\mathbb{Z}_m$ se e somente se m é primo.

Prova

Suponhamos inicialmente que m seja primo, e sejam $\vec{a}, \overline{b}, \overline{c}$ elementos de $\mathbb{Z}_m$, com $\overline{a} \neq 0$, tais que

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

Então $\overline{a}(\overline{b} - \overline{c}) = 0$. Como $\overline{a} \neq 0$ e Z_m não tem divisores de zero, deve ser $\overline{b} - \overline{c} = 0$ donde $\overline{b} = \overline{c}$.

Suponhamos que vale a propriedade cancelativa, mostraremos que nesse caso Z_m não contém divisores de zero. Sejam $\overline{a}, \vec{b}$ de $\mathbb{Z}_m$ tais que

$$\overline{a}\overline{b} = \overline{0}.$$

Se $\overline{a} \neq \overline{0}$, escrevemos

$$\overline{a}\overline{b} = \overline{a}\overline{0}$$

e, como podemos cancelar, temos que $\overline{b} = 0$. Assim m é primo.

Exemplo 20.4

Seja $\overline{a}$ é invertível e $\overline{b}$ é divisor de zero em $\mathbb{Z}_m$, vamos mostrar que $\overline{a} \cdot \overline{b}$ e divisor de zero. Como $\overline{b}$ é divisor de zero assim $\overline{b} \neq 0$ e existe $\overline{c} \neq \overline{0}$ tal que:

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

Notamos que $\overline{a} \cdot \overline{b}$ não mulo, pois caso contrario, temos

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

Assim, como $\overline{a}$ é invertivel, cancelando, temos que $\overline{b} = \overline{0}$, é absurdo. Agora

$$(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot \overline{0} = \overline{0}$$

Logo $\overline{a} \cdot \overline{b}$ é divisor de zero.

Exemplo 20.5

Vamos mostrar que o produto de dois elementos inversíveis em $\mathbb{Z}_m$ é invertível. Como $\overline{a}, \overline{b} \in \mathbb{Z}_m$ são invertíveis assim,

$$\text{mdc}(a, m) = 1, \qquad \text{mdc}(b, m) = 1,$$

Logo

$$\text{mdc}(ab, m) = 1$$

Portanto ab é invertível.

Exemplo 20.6

Considere a equação

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

em $\mathbb{Z}_7$, $\mathbb{Z}_8$
Em $\mathbb{Z}_7$ temos que $\text{mdc}(6, 7) = 1$ assim $\overline{6}$ é invertível e seu inverso é $\overline{6}$. Logo multiplicando ambos os lados da equação por $\overline{6}$, temos

$$\overline{6} \cdot \overline{4} = \overline{6} \cdot \overline{6} \cdot \overline{x} = \overline{1} \cdot \overline{x} = \overline{x}$$

assim $\overline{x} = \overline{6}$.
Por outro lado em $\mathbb{Z}_8$ o elemento $\overline{6}$ não é inversivel (ele é divisor de zero). E a equação $\overline{6} \cdot \overline{x} = \overline{4}$ é equivalente a congruencia

$$6x \equiv 4 (\text{mod} 8).$$

Como $\text{mdc}(6, 8) = 2 \mid 4$ assim há 2 soluções

$$\overline{x} = \overline{2}, \qquad \overline{x} = \overline{6}.$$

Exercício 20.1: (Trabalho p/ casa)

Encontre elementos invertíveis e divisores de zero em:

$$\mathbb{Z}_8,\ \mathbb{Z}_{13},\ \mathbb{Z}_{10},\ \mathbb{Z}_{20}.$$

Exercício 20.2: (Trabalho p/ casa)

Resolve as equações

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

em $\mathbb{Z}_7$ e $\mathbb{Z}_8$, e

$$\overline{5} \cdot \overline{x} + \overline{3} = \overline{4}$$

em $\mathbb{Z}_9$, $\mathbb{Z}_{10}$.