Aula 26.05.2020

Inteiros modulo m. 2

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

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

$$\overline{a} = \{a + mk \mid k \in \mathbb{Z}\} = \{b \in \mathbb{Z} \mid b \equiv a \pmod{m}\}$$

- Duas operações em $\mathbb{Z}_m$:

Soma: $\overline{a} \in \mathbb{Z}_m$, $\overline{b} \in \mathbb{Z}_m$

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

produto: $\overline{a} \in \mathbb{Z}_m$, $\overline{b} \in \mathbb{Z}_m$

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

Propriedades:

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

para todos $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$.

Scanned with CamScanner

Divisores de zero e inversos

Def. Um elemento $\bar{a} \in \mathbb{Z}_m$ é <u>invertível</u> se existir $\bar{b} \in \mathbb{Z}_m$ tal que $\bar{a} \cdot \bar{b} = \bar{1}$. Neste caso $\bar{b}$ é chamado <u>inverso</u> de $\bar{a}$.

Exemplos. $\mathbb{Z}_2$: $\bar{0}, \bar{1}$, $\mathbb{Z}_3$: $\bar{0}, \bar{1}, \bar{2}$

invertível

inversíveis

$\mathbb{Z}_4$: $\bar{0}, \bar{1}, \bar{2}, \bar{3}$, $\mathbb{Z}_5$: $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$

inversíveis

inversíveis

$\mathbb{Z}_6$: $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$

inversíveis.

Proposição Seja $\bar{a} \in \mathbb{Z}_m$ elemento não-nulo. Assim

$$\bar{a} \text{ é invertível} \iff mdc(a,m) = 1.$$

Prova

$\bar{a}$ é invertível $\iff$ Existe $\bar{b} \in \mathbb{Z}_m$ t.q. $\bar{a} \cdot \bar{b} = \bar{1}$

$\iff$ $a \cdot x \equiv 1 \pmod{m}$ tem solução

$\iff$ $mdc(a,m) = 1$ $\square$.

Obs $\bar{a}$ é invertível em $\mathbb{Z}_m$ $\iff$ a admite inverso modular modulo m.

Scanned with CamScanner

<u>Corolario</u> Se p um primo, assim todo elemento não-nulo em $\mathbb{Z}_p$ é invertivel.

<u>Prova</u> $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$, se $1 \leq a \leq p-1$

assim $mdc(a, p) = 1 \Rightarrow \bar{a}$ é invertivel $\square$

<u>Obs</u> Se $m > 1$, assim o numero dos elementos invertiveis em $\mathbb{Z}_m$ igual $\varphi(m)$.

<u>Def.</u> Seja $m > 1$, um elemento $\bar{a} \in \mathbb{Z}_m$ é um <u>divisor</u> de <u>zero</u> se $\bar{a} \neq \bar{0}$ e existir $\bar{b} \in \mathbb{Z}_m$ $\bar{b} \neq \bar{0}$ tal que $\bar{a} \cdot \bar{b} = \bar{0}$.

<u>Exemplos</u> 1) Em $\mathbb{Z}_6$: $\bar{2}, \bar{3}, \bar{4}$ são divisor. de zero.

pois $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$

$\bar{4} \cdot \bar{3} = \overline{12} = \bar{0}$

2) Em $\mathbb{Z}_4$: $\bar{2}$ é unico div. de zero: $\bar{2} \cdot \bar{2} = \bar{0}$.

3) Em $\mathbb{Z}_5$ não há divisores de zero.

<u>Proposição 2</u> Seja $m \in \mathbb{Z}$, $m > 1$, e $\bar{a} \in \mathbb{Z}_m$

$\bar{a}$ é divisor de zero em $\mathbb{Z}_m$ $\Longleftrightarrow$ $mdc(a, m) \neq 1$

Scanned with CamScanner

<u>Prova</u> [$\Rightarrow$] Se $\bar{a} \in \mathbb{Z}_m$ divisor de zero, assim existe $\bar{b} \neq \bar{0}$ com $\bar{a} \cdot \bar{b} = \bar{0}$

Assim $\overline{a \cdot b} = \bar{0}$ e $m \mid ab$. Agora se $mdc(a,m) = 1$, assim $m \mid b$, ou $\bar{b} = \bar{0}$, absurdo, portanto $mdc(a,m) \neq 1$.

[$\Leftarrow$] Seja $mdc(a,m) \neq 1$. Se $mdc(a,m) = d > 1$, assim $a = d \cdot a'$ e $m = d \cdot m'$.

Como $d > 1 \Rightarrow 1 \leq m' < m$, assim $\overline{m'} \neq \bar{0}$.

Agora $\bar{a} \cdot \overline{m'} = \overline{am'} = \overline{a' \cdot d \cdot m'} = \overline{a' \cdot m} = \bar{m} = \bar{0}$. $\square$

<u>Corolario</u> Se p é um primo, assim $\mathbb{Z}_p$ não possui os divisores de zero.

<u>Prova</u> Seja $\bar{a} \in \mathbb{Z}_p$, se $mdc(a,p) \neq 1$, assim $mdc(a,p) = p$, ou $p \mid a \Rightarrow \bar{a} = \bar{0}$.

Logo $\mathbb{Z}_p$ não admite div. de zero. $\square$

<u>Proposição</u> Se $\mathbb{Z}_m$ não possui divisores de zero assim m é primo.

<u>Prova</u> Escreva $m = r \cdot s$, com $1 \leq r, s \leq m$

Assim $\bar{0} = \bar{m} = \bar{r} \cdot \bar{s} \Rightarrow \bar{r} = 0$ ou $\bar{s} = 0$

Como $1 \leq r, s \leq m \Rightarrow r = m$ ou $s = m \Rightarrow m$ é primo $\square$

Scanned with CamScanner

Exemplo Busca todos divisores de zero em $\mathbb{Z}_{12}$.

Solução

$\bar{a} \in \mathbb{Z}_{12}$ é div. de zero $\iff mdc(a,12) \neq 1$

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

$\bar{2} \cdot \bar{6} = \bar{0}$, $\bar{3} \cdot \bar{4} = \bar{0}$, $\bar{8} \cdot \bar{3} = \bar{0}$, $\bar{9} \cdot \bar{4} = \bar{0}$, $\overline{10} \cdot \bar{6} = \bar{0}$.

Obs. O numero de divisores de zero em $\mathbb{Z}_m$ igual a $m - 1 - \varphi(m)$, pois

$$\varphi(m) = \#\{1 \leq a \leq m \mid mdc(a,m) = 1\}$$
$$= \#\{\bar{a} \in \mathbb{Z}_m \mid \bar{a} \text{ não é div. de zero}\}.$$

Obs2 Qualquer elemento não-nulo $\bar{a}$ em $\mathbb{Z}_m$ é invertivel ou div. de zero, mas não ambos.

Pois: $mdc(a,m) \geq 1$ e

se $mdc(a,m) = 1 \Rightarrow$ $\bar{a}$ é invertivel

se $mdc(a,m) \neq 1 \Rightarrow$ $\bar{a}$ é div. de zero.

Lema Se $mdc(a,m) = 1$ e $\bar{a} \cdot \bar{b} = \bar{a} \cdot \bar{c} \Rightarrow \bar{b} = \bar{c}$

Scanned with CamScanner

<u>Prova</u> $\overline{a}\cdot\overline{b}=\overline{a}\cdot\overline{c} \Rightarrow a\cdot b\equiv a\cdot c \pmod m$

$\Rightarrow m \mid ab-ac \Rightarrow m \mid a(b-c)$

$\underset{mdc(a,m)=1}{\Rightarrow} m \mid b-c \Rightarrow b\equiv c \pmod m$

$\Rightarrow \overline{b}=\overline{c}$ $\square$

<u>Proposição</u> A propriedade cancelativa do produto vale em $\mathbb{Z}_m \Leftrightarrow m$ é primo.

<u>Prova</u>. [$\Rightarrow$] Se $\overline{a}\cdot\overline{b}=\overline{a}\cdot\overline{c} \Rightarrow \overline{b}\cdot\overline{c}$ para todos não nulos $\overline{a},\overline{b},\overline{c}\in\mathbb{Z}_m$, logo $\mathbb{Z}_m$ não tem divisores de zero, assim m é um primo.

[$\Leftarrow$] Se $m=p$ um primo. Assim $mdc(a,p)=1$ para todo $1\leq a\leq p-1$, assim $\overline{a}\cdot\overline{b}=\overline{a}\cdot\overline{c}$ implique $\overline{b}=\overline{c}$ $\square$

<u>Exemplo</u> Seja $\overline{a}$ invertível e $\overline{b}$ é div de zero em $\mathbb{Z}_m$, mostre que $\overline{a}\cdot\overline{b}$ é div. de zero.

<u>Solução</u> Se $\overline{b}$ é div. de zero $\Rightarrow \overline{b}\neq\overline{0}$ e existe $\overline{c}\neq\overline{0}$ tal que $\overline{b}\cdot\overline{c}=\overline{0}$.

Scanned with CamScanner

Observe que $\bar{a}\cdot\bar{b}$ não nulo, pois

se $\bar{a}\cdot\bar{b} = \bar{a}\cdot\bar{0} = \bar{0} \Rightarrow \bar{b} = \bar{0}$, absurdo.

$\bar{a}$ é invertivel

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

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

<u>Exemplo 2</u> Mostre que o produto de dois elementos inversiveis em $\mathbb{Z}_m$ é invertivel

<u>Solução</u> Se $\bar{a}, \bar{b} \in \mathbb{Z}_m$ invertiveis

$\Rightarrow$ $mdc(a, m) = 1$, $mdc(b, m) = 1$

$\Rightarrow$ $mdc(ab, m) = 1$

$\Rightarrow$ $\overline{ab}$ é invertivel $\Rightarrow$ $\bar{a}\cdot\bar{b}$ é invertivel //

<u>Exemplo 3</u> Quantas soluções tem equação

$$\bar{6}\cdot\bar{x} = \bar{4} \quad \text{em } \mathbb{Z}_7, \mathbb{Z}_8$$

<u>Solução</u>. Temos $6\cdot x \equiv 4 \pmod 7$

Como $mdc(6,7) = 1 \Rightarrow$ há unica solução da congruencia

$\Rightarrow$ unica solução $\bar{x} = \bar{3}$

- $6\cdot x \equiv 4 \pmod 8$ há 2 soluções

$mdc(6,8) = 2 \Rightarrow$ $\bar{x} = \bar{2}$ e $\bar{x} = \bar{6}$ //.

Scanned with CamScanner

Exercício (p/ casa).

a) Encontre elementos invertíveis e divisores de zero em:

$\mathbb{Z}_8$, $\mathbb{Z}_9$, $\mathbb{Z}_{10}$, $\mathbb{Z}_{20}$.

b) Resolve equações

$\overline{2} \cdot \overline{x} = \overline{0}$ em $\mathbb{Z}_7$, $\mathbb{Z}_8$

$\overline{5} \cdot \overline{x} + \overline{3} = \overline{4}$ em $\mathbb{Z}_9$, $\mathbb{Z}_{10}$.

Scanned with CamScanner