Teorema 1.4.2: *Sejam* $a, b, c, d \in \mathbb{Z}$ *tais que*

$$a \equiv b \,(mod\, n) \;\; e \;\; c \equiv d \,(mod\, n).$$

Então,

- $a + c \equiv b + d \,(mod\, n)$
- $ac \equiv bd \,(mod\, n)$.

Operações no conjunto das classes (mod n)

Podem definir-se em $\mathbb{Z}_n$ operações de adição $\oplus$ e de multiplicação $\otimes$, dadas por:

$$[a]_n \oplus [b]_n = [a + b]_n \qquad [a]_n \otimes [b]_n = [ab]_n.$$

Teorema 1.4.3: (Propriedades das operações em classes (mod n))

Sejam $x, y, z \in \mathbb{Z}_n$ *e sejam* $\overline{0} = [0]_n$ *e* $\overline{1} = [1]_n$. *Então:*

- $x \oplus y = y \oplus x; \quad (x \oplus y) \oplus z = x \oplus (y \oplus z);$
- $x \oplus \overline{0} = x;$
- *Existe* $x' \in \mathbb{Z}_n$ *tal que* $x \oplus x' = \overline{0};$

$x = [a]_n$, com $a \in \mathbb{Z}$, então $x' = [-a]_n$ pois $x \oplus x' = \overline{0}$.

Ao elemento x' chamamos simétrico de x em $\mathbb{Z}_n$ e representamo-lo por $-x$.

Exemplo: n=13 $\mathbb{Z}_{13} = \{[0]_{13},\ [1]_{13},\ [2]_{13}, \ldots, [12]_{13}\}$

- $-[0]_{13} = [0]_{13}$
- $-[2]_{13} = [-2]_{13} = [11]_{13}$ pois $-2 = 13(-1) + 11$

Se $a \in \{1, \ldots, n-1\}$ então

– $[a]_n = [-a]_n = [n-a]_n$ e temos também $n - a \in \{1, \ldots, n-1\}$.

Teorema 1.4.3: (continuação)

- $x \otimes y = y \otimes x$; $(x \otimes y) \otimes z = x \otimes (y \otimes z)$;
- $x \otimes \overline{1} = x$;
- $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$.

Definição 1.4.4:

Um elemento $x \in \mathbb{Z}_n$ diz-se invertível se existe $x' \in \mathbb{Z}_n$ tal que

$$x \otimes x' = \overline{1} = [1]_n.$$

Se existir x´, diz-se que x´ é o inverso de x

Exemplos:

n=4 $\mathbb{Z}_4 = \{[0]_4,\ [1]_4,\ [2]_4,\ [3]_4\}$

- $[0]_4$ tem inverso ? Não, pois $[0]_4 \otimes [a]_4 = [0]_4 \neq [1]_4$
- $[3]_4$ tem inverso ? Sim, pois $[3]_4 \otimes [3]_4 = [9]_4 = [1]_4$
- $[2]_4$ tem inverso ?

Não, pois

$$[2]_4 \otimes [0]_4 = [2 \times 0]_4 = [0]_4$$
$$[2]_4 \otimes [1]_4 = [2 \times 1]_4 = [2]_4$$
$$[2]_4 \otimes [2]_4 = [2 \times 2]_4 = [4]_4 = [0]_4$$
$$[2]_4 \otimes [3]_4 = [2 \times 3]_4 = [6]_4 = [2]_4$$

Conclusão: $n \in \mathbb{N} \quad \mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$

Dado $a \in \{0, \ldots, n-1\}$, achar o inverso da classe $[a]_n$ é encontrar um elemento $x \in \{0, \ldots, n-1\}$ tal que

$$[a]_n \otimes [x]_n = [1]_n$$
$$\Updownarrow$$
$$[ax]_n = [1]_n$$
$$\Updownarrow$$
$$\boxed{ax \equiv 1 \pmod{n}}$$

Caso particular de uma congruência linear

Definição 1.4.5:

Chamamos congruência linear a uma expressão da forma

$$\mathbf{ax \equiv b \,(mod\, n)}\ ,$$

em que $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$ (constantes) e x é uma variável inteira (i.e. toma valores em $\mathbb{Z}$).

Uma solução da congruência linear $ax \equiv b \,(\mathrm{mod}\, n)$ é um número inteiro α tal que $a\alpha \equiv b \,(\mathrm{mod}\, n)$.

Teorema 1.4.6:

Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Se $\alpha \in \mathbb{Z}$ é uma solução da congruência linear $ax \equiv b \,(mod\, n)$, então qualquer $\beta \in [\alpha]_n$ é também uma solução.

Demonstração. Uma vez que $a\alpha \equiv b \,(\mathrm{mod}\, n)$ e $\beta \equiv \alpha \,(\mathrm{mod}\, n)$, então existem $u, v \in \mathbb{Z}$ tais que

$$a\alpha - b = un \quad \text{e} \quad \beta - \alpha = vn.$$

Assim,

$$\begin{aligned} a\beta - b &= a(\alpha + vn) - (a\alpha - un) \\ &= a\alpha + avn - a\alpha + un \\ &= (av + u)n \end{aligned}$$

e portanto $a\beta \equiv b \,(\mathrm{mod}\, n)$. □

Observação:

Para $n \in \mathbb{N}$, definamos

$$Z_n = \{0, 1, \ldots, n-1\}.$$

Uma vez que $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$, o teorema anterior diz-nos que uma congruência linear fica completamente resolvida quando determinarmos as suas soluções em Z_n.

Exemplos:

- Consideremos a congruência linear $2x \equiv 1 \pmod 4$.

Procurar x tal que
2x-1= múltiplo 4

$$\mathbb{Z}_4 = \{[0]_4,\ [1]_4,\ [2]_4,\ [3]_4\} \qquad Z_4 = \{0,\ 1,\ 2,\ 3\}$$

$$2 \times 0 = 0 \not\equiv 1 (\text{mod } 4)$$
$$2 \times 1 = 2 \not\equiv 1 (\text{mod } 4)$$
$$2 \times 2 = 4 \equiv 0 \not\equiv 1 (\text{mod } 4)$$
$$2 \times 3 = 6 \equiv 2 \not\equiv 1 (\text{mod } 4)$$

Portanto, não possui quaisquer soluções em $\mathbb{Z}$.

- Determinemos as soluções da congruência linear $2x \equiv 1 \pmod 5$.

$$\mathbb{Z}_5 = \{[0]_5,\ [1]_5,\ [2]_5,\ [3]_5, [4]_5\}$$

$$Z_5 = \{0, 1, 2, 3, 4\}$$

Procurar x tal que
2x-1= múltiplo 5

$$2 \times 0 = 0 \equiv 0 (\text{mod } 5)$$
$$2 \times 1 = 2 \equiv 2 (\text{mod } 5)$$
$$2 \times 2 = 4 \equiv 4 (\text{mod } 5)$$
$$2 \times 3 = 6 \equiv 1 (\text{mod } 5)$$
$$2 \times 4 = 8 \equiv 3 (\text{mod } 5)$$

O conjunto das soluções é

$$[3]_5 = 3 + 5\mathbb{Z} = \{\ldots, -12, -7, -2, 3, 8, 13, \ldots\}.$$

!!!!!!!!!!!!!!!!!

- Determinemos as soluções da congruência linear $2x \equiv 4 \pmod{500}$.

Teorema 1.4.7

Sejam $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ e $d = mdc\{a, n\}$. Então a congruência linear

$$ax \equiv b \pmod{n}$$

- *tem soluções em $\mathbb{Z}$ se e só se $d|b$;*
- *caso $d|b$, então a congruência linear possui exactamente d soluções em Z_n.*

Notas da demonstração:

mdc{a,n}= au + nv

Igualdade de Bezout

1. Sejam $u, v \in \mathbb{Z}$ tais que $d = au + nv$ e tomemos

$$\alpha = \frac{bu}{d} \in \mathbb{Z} \quad e \quad m = \frac{n}{d} \in \mathbb{Z}.$$

2. $\alpha,\ \alpha + m,\ \alpha + 2m, \ldots,\ \alpha + (d-1)m$

são d soluções não congruentes módulo n de $ax \equiv b \pmod{n}$.

3. Estas d soluções podem não pertencer todas a Z_n, mas atendendo aos teorem anteriores, podemos determinar d soluções em Z_n.