1.4. Congruências lineares

Sejam $n \in \mathbb{N}$ e R a relação de congruência módulo n (sobre $\mathbb{Z}$).
Recordemos que R está definida em $\mathbb{Z}$ por: para quaisquer $a, b \in \mathbb{Z}$,

$$aRb \quad \text{se e só se} \quad n|(a-b).$$

Dados $a, b \in \mathbb{Z}$ tais que aRb, dizemos que a é congruente com b módulo n e escrevemos $a \equiv b \,(\mathrm{mod}\, n)$.
A classe (de congruência) módulo n de $a \in \mathbb{Z}$ (i.e. a classe de equivalência de a para a relação de congruência módulo n) é o conjunto

$$[a]_n = \{\ldots,\ a-2n,\ a-n,\ a,\ a+n,\ a+2n, \ldots\} = a + n\mathbb{Z}.$$

Exemplo Para $n = 4$, temos quatro classes distintas:

- $[0]_4 = \{\ldots,\ -8,\ -4,\ 0,\ 4,\ 8, \ldots\} = 4\mathbb{Z}$;
- $[1]_4 = \{\ldots,\ -7,\ -3,\ 1,\ 5,\ 9, \ldots\} = 1 + 4\mathbb{Z}$;
- $[2]_4 = \{\ldots,\ -6,\ -2,\ 2,\ 6,\ 10, \ldots\} = 2 + 4\mathbb{Z}$;
- $[3]_4 = \{\ldots,\ -5,\ -1,\ 3,\ 7,\ 11, \ldots\} = 3 + 4\mathbb{Z}$.

O conjunto quociente $\mathbb{Z}/R$, em que R é a relação de congruência módulo n, é designado por conjunto dos números inteiros módulo n e é denotado por $\mathbb{Z}_n$.

Observação

Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Se $a = nc + b$, com $c \in \mathbb{Z}$, então $a - b = nq$, pelo que $n|(a-b)$, donde $a \equiv b \,(\mathrm{mod}\, n)$ e portanto $[a]_n = [b]_n$.
Em particular, se r é o resto da divisão inteira de a por n, i.e. $a = nq + r$, com $q \in \mathbb{Z}$ e $0 \leq r < n$, então $[a]_n = [r]_n$.

Teorema

Seja $n \in \mathbb{N}$. Então cada inteiro é congruente módulo n precisamente com um dos inteiros $0,\ 1,\ 2, \ldots,\ n-1$, i.e. $\mathbb{Z}_n = \{[0]_n,\ [1]_n, \ldots,\ [n-1]_n\}$.

Exemplo

Seja $n = 13$. O inteiro -15 é congruente módulo 13 com 11, pois $-15 = 13 \times (-2) + 11$. Donde $[-15]_{13} = [11]_{13}$.
O inteiro 25 é congruente módulo 13 com 12, pois $25 = 13 \times 1 + 12$. Assim, $[25]_{13} = [12]_{13}$.

Teorema

Sejam $a, b, c, d \in \mathbb{Z}$ tais que $a \equiv b \,(\mathrm{mod}\, n)$ e $c \equiv d \,(\mathrm{mod}\, n)$. Então, $a + c \equiv b + d \,(\mathrm{mod}\, n)$ e $ac \equiv bd \,(\mathrm{mod}\, n)$.

Este resultado permite-nos definir sem ambiguidade operações de adição $\oplus$ e de multiplicação $\otimes$ em $\mathbb{Z}_n$ do seguinte modo: para quaisquer $a, b \in \mathbb{Z}$,

$$[a]_n \oplus [b]_n = [a+b]_n \quad \text{e} \quad [a]_n \otimes [b]_n = [ab]_n.$$

Teorema

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 $x \oplus x' = \overline{0}$;*
- $x \otimes y = y \otimes x$; $\quad (x \otimes y) \otimes z = x \otimes (y \otimes z)$;
- $x \otimes \overline{1} = x$;
- $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$.

Observação

Seja $n \in \mathbb{N}$.
Se $x = [a]_n$, com $a \in \mathbb{Z}$, então $x' = [-a]_n$ é tal que $x \oplus x' = \overline{0}$. Ao elemento x' chamamos simétrico de x em $\mathbb{Z}_n$ e representamo-lo por $-x$.
Se $x = [0]_n$, então $-x = [0]_n = x$. Se $x = [a]_n$, com $a \in \{1, \ldots, n-1\}$, então $-x = [-a]_n = [n-a]_n$ e temos também $n - a \in \{1, \ldots, n-1\}$.

Vimos que todos os elementos de $\mathbb{Z}_n$ tem opostos (simétricos) para a adição. Tal não é o caso para a multiplicação em $\mathbb{Z}_n$.
Um elemento $x \in \mathbb{Z}_n$ diz-se invertível se existe $x' \in \mathbb{Z}_n$ (ao qual chamamos inverso de x) tal que $x \otimes x' = \overline{1} = [1]_n$.
Claro que, para $n > 1$, o elemento $\overline{0}$ nunca é invertível. Mas, podemos ter outros elementos não invertíveis.
Por exemplo, para $n = 4$, temos $[3]_4[3]_4 = [9]_4 = [1]_4$, pelo que $[3]_4$ é invertível e o seu inverso é ele próprio. Já o elemento $[2]_4$ não é invertível (visto que $[2]_4[0]_4 = [0]_4$, $[2]_4[1]_4 = [2]_4$, $[2]_4[2]_4 = [4]_4 = [0]_4$ e $[2]_4[3]_4 = [6]_4 = [2]_4$).

O estudo que faremos a seguir, em particular, vai permitir-nos verificar se um elemento de $\mathbb{Z}_n$ é invertível e, nesse caso, determinar o seu inverso.

Definição

Chamamos congruência linear a uma expressão da forma

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

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 $ax \equiv b \pmod{n}$ é um número inteiro α tal que $a\alpha \equiv b \pmod{n}$.

Observação

O inverso (se existir) de $[a]_n \in \mathbb{Z}_n$ é o elemento $[\alpha]_n$, em que $\alpha \in \mathbb{Z}$ é uma solução da congruência linear $ax \equiv 1 \pmod{n}$.

Teorema

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

Demonstração. Uma vez que $a\alpha \equiv b \pmod{n}$ e $\beta \equiv \alpha \pmod{n}$, 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 $a\beta \equiv b \pmod{n}$. □

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 $2x \equiv 1 \pmod{4}$.

  Esta congruência linear não possui soluções em $Z_4 = \{0,\ 1,\ 2,\ 3\}$ (visto que nenhum dos números 2×0, 2×1, 2×2 e 2×3 é congruente com 1 módulo 4). Portanto, não possui quaisquer soluções em $\mathbb{Z}$.

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

  O inteiro $x = 3$ é a única solução da congruência linear em $Z_5 = \{0, 1, 2, 3, 4\}$, pois $2 \times 0 = 0 \equiv 0 \pmod{5}$, $2 \times 1 = 2 \equiv 2 \pmod{5}$, $2 \times 2 = 4 \equiv 4 \pmod{5}$, $2 \times 3 = 6 \equiv 1 \pmod{5}$ e $2 \times 4 = 8 \equiv 3 \pmod{5}$.

  As soluções (em $\mathbb{Z}$) são então todos os elementos do conjunto

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

- Consideremos a congruência linear $4x \equiv 4 \pmod{8}$.

  Os inteiros 1, 3, 5 e 7 são as soluções da congruência linear em Z_8 (exercício). Assim, o conjunto de todas as soluções (em $\mathbb{Z}$) da congruência linear é

  $$[1]_8 \cup [3]_8 \cup [5]_8 \cup [7]_8.$$

Teorema

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 $d|b$ e, neste caso, possui exactamente d soluções em Z_n.

Demonstração.

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

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

Então,

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

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

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

Exemplos

- Determinemos em Z_{15} todas as soluções da congruência linear

  $$13x \equiv 1 \pmod{15}.$$

  Temos $d = \text{mdc}\{13,\ 15\} = 1$. Como $d|1$ (neste caso, $b = 1$), então a congruência linear possui uma única solução em Z_{15}.

  Como $1 = 13 \cdot 7 + 15 \cdot (-6)$ (donde $u = 7$), então $\alpha = \frac{1 \times 7}{1} = 7 \in Z_{15}$ é a única solução de $13x \equiv 1 \pmod{15}$ em Z_{15}.

- Consideremos agora a congruência linear $224x \equiv 154 \pmod{385}$ e determinemos todas as suas soluções em Z_{385}.

  Como $d = \text{mdc}\{224,\ 385\} = 7$ e 7 é um divisor de $b = 154\ (= 7 \times 22)$, então $224x \equiv 154 \pmod{385}$ possui exactamente 7 soluções em Z_{385}. Por outro lado, temos $7 = 224 \cdot (-12) + 385 \cdot 7$ (donde $u = -12$), pelo que

$$\alpha = \frac{154 \times (-12)}{7} = -264,$$

  é uma solução de $224x \equiv 154 \pmod{385}$. Note que $\alpha \notin Z_{385}$.

  Seja

$$m = \frac{n}{d} = \frac{385}{7} = 55.$$

  Então, $\alpha + km = -264 + k55$, com $k = 0, 1, 2, 3, 4, 5, 6$, i.e.

$$-264, -209, -154, -99, -44, 11 \text{ e } 66$$

  são sete soluções não congruentes módulo 385. Como
  $121 \equiv (-264) \pmod{385}$, $176 \equiv (-209) \pmod{385}$,
  $231 \equiv (-154) \pmod{385}$, $286 \equiv (-99) \pmod{385}$ e $341 \equiv (-44) \pmod{385}$,
  então

$$11, 66, 121, 176, 231, 286 \text{ e } 341$$

  são as sete soluções de $224x \equiv 154 \pmod{385}$ em Z_{385}.

Proposição

Seja $n \in \mathbb{N}$ e sejam $a, a', b, b' \in \mathbb{Z}$ tais que $a \equiv a' \pmod{n}$ e $b \equiv b' \pmod{n}$. Então, as congruências lineares

$$ax \equiv b \pmod{n} \quad e \quad a'x \equiv b' \pmod{n}$$

possuem exactamente as mesmas soluções.

Observação

O resultado anterior permite-nos concluir que, para estudar todas as congruências lineares do tipo $ax \equiv b \pmod{n}$, com $n \in \mathbb{N}$ e $a, b \in \mathbb{Z}$, basta estudar aquelas em que $a, b \in Z_n$.

Proposição

Sejam $m, n \in \mathbb{N}$ e sejam $a, a', b, b' \in \mathbb{Z}$. Seja α uma solução (comum) das congruências lineares

$$ax \equiv b \pmod{m} \quad e \quad a'x \equiv b' \pmod{n}.$$

Então, qualquer $\beta \in [\alpha]_{mn}$ é ainda uma solução de ambas as congruências lineares.

Lema

Sejam $m, n \in \mathbb{Z}$ tais que $1 = mdc\{m, n\}$ e sejam $b, b' \in \mathbb{Z}$. Então as congruências lineares $x \equiv b \pmod{m}$ e $x \equiv b' \pmod{n}$ têm uma e uma só solução comum em Z_{mn}.

Demonstração. Tomar $u, v \in \mathbb{Z}$ tais que $1 = mu + nv$. Então $\alpha \in Z_{mn}$ tal que $\alpha \equiv (bnv + b'mu) \pmod{mn}$ é a solução pretendida. □

Teorema

Sejam $m, n \in \mathbb{N}$ tais que $1 = mdc\{m, n\}$ e sejam $a, a', b, b' \in \mathbb{Z}$. Se as congruências lineares $ax \equiv b \pmod{m}$ e $a'x \equiv b' \pmod{n}$ têm ambas soluções, então existe uma solução comum a ambas em Z_{mn}.

Demonstração. Sejam α e α' soluções de $ax \equiv b \pmod{m}$ e de $a'x \equiv b' \pmod{n}$, respectivamente. Atendendo ao lema anterior, o sistema de congruência lineares

$$\begin{cases} x \equiv \alpha \pmod{m} \\ x \equiv \alpha' \pmod{n} \end{cases}$$

possui uma (única) solução $\beta \in Z_{mn}$. Claramente, β é também uma solução de $ax \equiv b \pmod{m}$ e de $a'x \equiv b' \pmod{n}$. □

Exemplo

Determinemos em Z_{20} uma solução comum às congruências lineares

$$4x \equiv 12 \pmod{5} \qquad \text{e} \qquad 3x \equiv 6 \pmod{4}.$$

Uma solução de $4x \equiv 2 \pmod{5}$ é $\alpha = 3$ e uma solução de $3x \equiv 2 \pmod{4}$ é $\alpha' = 2$.
Seguidamente, calculamos a (única) solução comum em Z_{20} às congruências

$$x \equiv 3 \pmod{5} \qquad \text{e} \qquad x \equiv 2 \pmod{4}$$

(note-se que $1 = \text{mdc}\{4,\ 5\}$): temos $1 = 5 \cdot 1 + 4 \cdot (-1)$, donde

$$\beta = 2 \cdot 5 \cdot 1 + 3 \cdot 4 \cdot (-1) = -2$$

é uma solução comum.
Como

$$-2 \equiv 18 \pmod{20},$$

então 18 é a (única) solução comum em Z_{20} às congruências $x \equiv 3 \pmod{5}$ e $x \equiv 2 \pmod{4}$ e, consequentemente, também uma solução comum às congruências iniciais.