Teorema 1.4.7

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

$$ax \equiv b \,(mod\, n)$$

- *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 $ax \equiv b \,(\mathrm{mod}\, n)$.

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

Exemplos:

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

Seja $d = \text{mdc}\{2, 500\} = 2$.

$Z_{500} = \{0, 1, 2, 3, 4, \ldots, 499\}$

Como $d = 2$ divide $b = 4$ então a congruência linear tem soluções e tem exactamente $d = 2$ soluções em Z_{500}.

? $\alpha,\ \alpha + m$?

$$2 = \text{mdc}\{2,500\} = 2u + 500v = 2 \times \underset{u}{1} + 500 \times 0$$

$$\alpha = \frac{bu}{d} = \frac{4 \times 1}{2} = 2 \qquad m = \frac{n}{d} = \frac{500}{2} = 250$$

$$\alpha = 2, \quad \alpha + m = 2 + 250 = 252$$

São duas soluções em Z_{500}

Conclusão: $[2]_{500} \cup [252]_{500}$ é o conjunto de todas as soluções em $\mathbb{Z}$

- 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 e 66

são sete solucões não congruentes módulo 385. Como

Encontrar as correspondentes soluções em

$121 \equiv (-264) \pmod{385}$, $176 \equiv (-209) \pmod{385}$,
$231 \equiv (-154) \pmod{385}$, $286 \equiv (-99) \pmod{385}$ 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}.

Congruências lineares equivalentes:

Considere a congruência linear

$$1502x \equiv 1004 \pmod{500}$$

Ora,

$$\begin{array}{r|l} 1502 & 500 \\ \cline{2-2} 2 & 3 \end{array}$$

$$1502 \equiv 2 \pmod{500}$$

$$\begin{array}{r|l} 1004 & 500 \\ \cline{2-2} 4 & 2 \end{array}$$

$$1004 \equiv 4 \pmod{500}$$

Assim,

$$\begin{array}{c} 1502x \equiv 1004 \pmod{500} \\ \Updownarrow \\ 2x \equiv 4 \pmod{500} \end{array}$$

uma vez que as soluções da segunda congruência são as mesmas que as da primeira.

Porquê?

Teorema 1.4.8:

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

$$ax \equiv b \,(\mathrm{mod}\, n) \quad e \quad a'x \equiv b' \,(\mathrm{mod}\, n)$$

possuem exactamente as mesmas soluções.

Demonstração.

$$a \equiv a' \pmod{n} \Leftrightarrow a - a' = k_1 n, \quad k_1 \in \mathbb{Z}$$
$$b \equiv b' \pmod{n} \Leftrightarrow b - b' = k_2 n, \quad k_2 \in \mathbb{Z}$$

Seja α uma solução de $ax \equiv b \pmod{n}$.

Assim,

$$a\alpha \equiv b \pmod{n} \Leftrightarrow a\alpha - b = k_3 n, \quad k_3 \in \mathbb{Z}.$$

Ora,

$$a'\alpha - b' = (a - k_1 n)\alpha - (b - k_2 n) = a\alpha - k_1 n\alpha - b + k_2 n$$
$$= k_3 n - k_1 n\alpha + k_2 n = \underbrace{(k_3 - k_1\alpha + k_2)}_{k_4} n = k_4 n.$$

Então, $a'\alpha \equiv b' \pmod{n}$

Analogamente se conclui que se α é solução de $a'x \equiv b' \pmod{n}$, então também é solução de $ax \equiv b \pmod{n}$. □

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 $a, b \in Z_n$.

Sistemas de congruências:

Sendo $x \in \mathbb{Z}$ e $n, m \in \mathbb{N}$, então

$$[x]_{nm} \subseteq [x]_n \cap [x]_m.$$

$$[3]_{4\times 8} \subseteq [3]_4 \cap [3]_8$$

Considere as duas congruências lineares

$$2x \equiv 2 \pmod 4, \quad 3x \equiv 1 \pmod 8 .$$

3 é solução das duas congrências pois

$$2 \times 3 - 2 = 4 = 4 \times 1 \qquad \text{e} \qquad 3 \times 3 - 1 = 8 = 8 \times 1.$$

Então podemos afirmar que todos os elementos da classe

$$[3]_{32} = 3 + 32\mathbb{Z}$$

são soluções comuns das duas congruências.

Podemos generalizar?

Teorema 1.4.9:

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

$$ax \equiv b \,(\mathrm{mod}\, m) \quad e \quad a'x \equiv b' \,(\mathrm{mod}\, n).$$

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

Demonstração.

Basta atender a que $[\alpha]_{mn} \subseteq [\alpha]_m \cap [\alpha]_n$ □

Lema 1.4.10:

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. □

Exemplo: Considere as congruências lineares

$$x \equiv 5 \pmod{2} \quad \text{e} \quad x \equiv 6 \pmod{3}.$$

Como mdc{2, 3}=1 então existe uma solução comum em Z_6.

Ora,

1= mdc{2, 3}= 2 u + 3 v =2(-1) + 3(1). **(Identidade de Bezout)**

? ?

Assim,

6x2(-1) + 5x3(1) = -12 + 15 =3 é solução das duas congruências.

Conclusão: $[3]_{2\times 3} = [3]_6$ são todas as soluções comuns às duas congruências

Teorema 1.4.11:

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: Considere as congruências lineares

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

$\alpha \in Z_5$ $\quad$ $\alpha' \in Z_4$

Será que têm soluções comuns?

Pelo Teorema, existe $\beta \in Z_{20}$ que é solução comum.

Exemplo: (Cont.)

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 $3x \equiv 6 \pmod 4$ é $\alpha' = 2$.

Seguidamente, calculamos a (única) solução comum em Z_{20}

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

(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.