

Congruências① Lembretea) Uma congruência linear é equação

$$a \cdot x \equiv b \pmod{n} \quad (*)$$

a, b, n inteiros dados, $n > 0$.

x - incógnito.

b) Solução da (*) é qualquer $r \in \mathbb{Z}$ t.q.

$$a \cdot r \equiv b \pmod{n}.$$

c) [Critério da existência das soluções].

$$\left\{ \begin{array}{l} a \cdot x \equiv b \pmod{n} \\ \text{tem solução} \end{array} \right\} \Leftrightarrow \text{mdc}(a, n) \mid b.$$

① Teorema Sejam $a, b, n \in \mathbb{Z}$, com $n > 0$.Seja $d = \text{mdc}(a, n)$ e suponha que $d \mid b$.Assim congruência (*) tem d soluções
não congruentes dois a dois modulo n, dados por:

$$x_0 = r \cdot b/d, \quad x_1 = r \cdot b/d + n/d, \quad x_2 = r \cdot b/d + 2n/d, \dots$$

$$\dots \quad x_{d-1} = r \cdot b/d + (d-1) \cdot n/d, \quad \text{onde}$$

$$d = a \cdot r + n \cdot s //$$

Prova. Verificamos 3 fatos:

(2)

1) $x_i = r \cdot b/d + i \cdot n/d$ é solução da (*)
para todos $i = 0, 1, \dots, d-1$.

2) $x_i \not\equiv x_j \pmod{n}$, se $i \neq j$

3) Se g é solução de (*) $\Rightarrow$ existe i tal que
 $g \equiv x_i \pmod{n}$.

Escreva $a = a_1 d$, $b = b_1 d$, $n = n_1 d$, assim
 $a/d = a_1$, $b/d = b_1$, $n/d = n_1$ e

$\boxed{x_i = r b_1 + i n_1}$. Como $d = a \cdot r + n \cdot s = 1$
 $1 = a_1 \cdot r + n_1 \cdot s$

1) $a x_i - b = a (r b_1 + i n_1) - b = a_1 d (r b_1 + i n_1) - b_1 d$
 $= d (a_1 r b_1 + i a_1 d n_1 - b_1) =$
 $= d (b_1 (a_1 r - 1) + i a_1 n_1)$
 $= d (b_1 \cdot (-n_1 \cdot s) + i a_1 n_1) = \underbrace{d n_1}_{n} (-b_1 s + i a_1)$

$\Rightarrow n \mid a x_i - b$

$\Rightarrow a \cdot x_i \equiv b \pmod{n}$

$\Rightarrow \{x_i \text{ é solução}\} //$

2) Suponha que $x_i \equiv x_j \pmod{n}$

Com $0 \leq i, j \leq d-1$, ou seja

$$rb_i + i n_1 \equiv rb_j + j n_1 \pmod{n}$$

$$\Rightarrow i n_1 \equiv j n_1 \pmod{n}$$

$$\text{logo } n_1(i-j) = k \cdot n \quad \text{ou} \quad i-j = k \cdot d$$

$$\text{Como } 0 \leq i \leq d-1 \quad \Rightarrow \quad -(d-1) \leq i-j \leq d-1$$

$$-d+1 \leq -j \leq 0 \quad \text{mas} \quad i-j = k \cdot d$$

$$\Rightarrow i = j.$$

3) Seja $g \in \mathbb{Z}$, tal que $a \cdot g \equiv b \pmod{n}$

Assim $a \cdot g - b = t n$ para algum $t \in \mathbb{Z}$

Ou seja (g, t) solução de $a \cdot x + n \cdot y = b$.

Como todas soluções tem forma

$$(rb_i + k n_1, sb_i + k a_1), \quad k \in \mathbb{Z}$$

logo existe $k \in \mathbb{Z}$, t.q. $g = rb_i + k n_1$.

Pelo algoritmo de divisão $k = q d + r'$, com

$q, r' \in \mathbb{Z}$ e $0 \leq r' \leq d-1$, assim

$$g = rb_i + (q d + r') n_1$$

$$= \underbrace{rb_i + r' n_1}_{x_{r'}} + q \cdot \underbrace{d \cdot n_1}_n, \quad \text{logo } g \equiv x_{r'} \pmod{n}$$

com $0 \leq r' \leq d-1$ $\square$

Corolário

(4)

Se $\text{mdc}(a, n) = 1$ assim:

$a \cdot x \equiv b \pmod{n}$ tem única solução
modulo n .

Exemplo Vamos resolver
 $a = 9, x \equiv b = 21 \pmod{n = 30}$ (**)

Como $\text{mdc}(9, 30) = 3$, e $3 \mid 21$, logo
tem exatamente 3 soluções pois a dois não
congruentes.

Congruência (**) é equivalente a equação

$$9x - 30y = 21$$

$$\text{mdc}(9, 30) = 3 = d$$

$$30 = 9 \cdot 3 + 3 \Rightarrow 3 = 9 \cdot (-3) + 30 \cdot 1$$

$$x_0 = \frac{r \cdot b}{d} = \frac{-3 \cdot 21}{3} = -21$$

$$x_1 = \frac{r \cdot b}{d} + \frac{n}{d} = -21 + \frac{30}{3} = -11$$

$$x_2 = \frac{r \cdot b}{d} + \frac{2n}{d} = -21 + \frac{2 \cdot 30}{3} = -1$$

Or, fazendo deslocamento modulo 30, temos

$$\boxed{9, 19, 29} //$$

Exemplo 2 Suponha

$$a = 6x \equiv 14 \pmod{4}$$

$d = \text{mdc}(6, 4) = 2 \Rightarrow$ há 2 soluções.

$$2 = 1 \cdot 6 + (-1) \cdot 4$$

$$\Rightarrow r = 1, \quad x_1 = \frac{r \cdot b}{d} = \frac{1 \cdot 14}{2} = 7$$

$$x_2 = \frac{r \cdot b}{d} + \frac{n}{d} = 7 + \frac{4}{2} = 9 //$$

Exemplo 3

$$-3x \equiv 18 \pmod{15}$$

$d = \text{mdc}(-3, 15) = 3$, assim há 3 soluções.

$$3 = (-3) \cdot 4 + 15 \cdot 1$$

$$r = 4 \Rightarrow x_0 = \frac{r \cdot b}{d} = \frac{4 \cdot 18}{3} = 24$$

$$x_1 = \frac{r \cdot b}{d} + \frac{n}{d} = 24 + \frac{15}{3} = 29$$

$$x_2 = \frac{r \cdot b}{d} + \frac{2n}{d} = 24 + \frac{2 \cdot 15}{3} = 34 //$$

Exemplo 4 Descreva todos b

(6)

tais que $34 \cdot x \equiv b \pmod{51}$

tem soluções.

Solução $\text{mdc}(34, 51) = 17$

$$51 = 34 \cdot 1 + \textcircled{17} \text{ mdc}$$

$$34 = 17 \cdot 2 + 0$$

Assim,

$$34 \cdot x \equiv b \pmod{51} \Leftrightarrow 17 \mid b$$

tem soluções

$$\Leftrightarrow b = 17 \cdot c, c \in \mathbb{Z}.$$

Ou seja para todos $b = \text{múltiplo de } 17$

$34 \cdot x \equiv b \pmod{51}$ tem solução.

Exemplo 5. Resolva

$$(n-1) \cdot x \equiv b \pmod{n}$$

Solução $(n-1) \equiv (-1) \pmod{n}$

$$\Rightarrow (n-1) \cdot x \equiv (-1)x \pmod{n}$$

$$\Rightarrow -x \equiv b \pmod{n}$$

$$\Rightarrow x \equiv -b \pmod{n}$$

$$\Rightarrow x = -b + t \cdot n, t \in \mathbb{Z}.$$