

Aula 05.05.2020

Sistemas de Congruências lineares

Considere o sistema:

$$(*) \begin{cases} a_1 \cdot x \equiv b_1 \pmod{m_1} \\ a_2 \cdot x \equiv b_2 \pmod{m_2} \\ \vdots \\ a_k \cdot x \equiv b_k \pmod{m_k} \end{cases} \quad \begin{array}{l} \text{onde } a_1, \dots, a_k \\ b_1, \dots, b_k \\ m_1, \dots, m_k - \text{inteiros} \\ \text{dados,} \\ x - \text{incógnita.} \end{array}$$

Obs. Para existir a solução do (*) é necessário (mas não é suficiente) que $\text{mdc}(a_i, m_i) \mid b_i$ para todo $i=1, \dots, k$.

Seja $d_i = \text{mdc}(a_i, m_i)$ e suponha que $d_i \mid b_i$.

Neste caso congruência linear $a_i x \equiv b_i \pmod{m_i}$ tem mesmas soluções como $x \equiv c_i \pmod{n_i}$

onde $n_i = \frac{m_i}{d_i}$, $c_i = r_i \cdot \frac{b_i}{d_i}$ (com r_i tal que $a_i r_i + m_i s_i = d_i$)

Logo (*) equivalente ao sistema

$$(**) \begin{cases} x \equiv c_1 \pmod{n_1} \\ x \equiv c_2 \pmod{n_2} \\ \vdots \\ x \equiv c_k \pmod{n_k} \end{cases}$$

Se q inteiro tal que $q \equiv c_i \pmod{n_i}$,
 assim $q \equiv t \pmod{n_i}$ para todo i . (3)

$\Rightarrow n_i \mid q - t$. Mas n_i são dois a dois primos
 entre si, assim

$$n_1 \cdots n_k \mid q - t, \text{ ou seja}$$

$$q \equiv t \pmod{n_1 \cdots n_k}.$$

Finalmente, se $q \equiv t \pmod{n_1 \cdots n_k}$ assim

$$n_1 \cdots n_k \mid q - t, \text{ logo } n_i \mid q - t, \text{ e}$$

$$q \equiv c_i \pmod{n_i}$$

□

Exemplos

(a) Resolve
$$\begin{cases} \textcircled{6} x \equiv 2 \pmod{\textcircled{4}} \\ \textcircled{2} x \equiv 1 \pmod{\textcircled{3}} \\ \textcircled{4} x \equiv 2 \pmod{\textcircled{7}} \end{cases}$$

$$\text{mdc}(\textcircled{6}, \textcircled{4}) = \textcircled{2} \Rightarrow 2 = 6 \cdot \textcircled{1} + 4 \cdot (-1)$$

$$\text{mdc}(2, 3) = \textcircled{1} \Rightarrow 1 = 2 \cdot (-1) + 3 \cdot 1$$

$$\text{mdc}(4, 7) = 1 \Rightarrow 1 = 4 \cdot 2 + 7 \cdot (-1)$$

Assim o sistema equivalente ao

$$\begin{cases} x \equiv 1 \cdot \frac{2}{2} \pmod{\frac{4}{2}} \\ x \equiv 2 \cdot \frac{1}{1} \pmod{\frac{3}{1}} \\ x \equiv 2 \cdot \frac{2}{1} \pmod{\frac{7}{1}} \end{cases} \sim \begin{cases} x \equiv \textcircled{1} \pmod{\textcircled{2}} \\ x \equiv \textcircled{2} \pmod{\textcircled{3}} \\ x \equiv \textcircled{4} \pmod{\textcircled{7}} \end{cases} \left| \begin{array}{l} N_1 = 3 \cdot 7 = 21 \\ N_2 = 14 \\ N_3 = 2 \cdot 3 = 6 \end{array} \right.$$

$$\text{mdc}(\underbrace{21}_{N_1}, \underbrace{2}_{n_1}) = 1, \quad 1 = 21 \cdot \underbrace{1}_{r_1} - 2 \cdot 10 \quad (4)$$

$$\text{mdc}(\underbrace{14}_{N_2}, \underbrace{3}_{n_2}) = 1, \quad 1 = 14 \cdot \underbrace{2}_{r_2} - 3 \cdot 9$$

$$\text{mdc}(\underbrace{6}_{N_3}, \underbrace{7}_{n_3}) = 1. \quad 1 = 6 \cdot \underbrace{(-1)}_{r_3} + 7 \cdot 1$$

Assim solução é

$$\begin{aligned} N_1 \cdot r_1 \cdot c_1 + N_2 \cdot r_2 \cdot c_2 + N_3 \cdot r_3 \cdot c_3 &= \\ = 21 \cdot 1 \cdot 1 + 14 \cdot 2 \cdot 2 + 6 \cdot (-1) \cdot 4 &= \\ = 21 + 56 + (-24) = 53 // &- \text{é solução} \end{aligned}$$

É fácil ver que

$$\begin{aligned} 53 &\equiv 1 \pmod{2} \\ 53 &\equiv 2 \pmod{3} \\ 53 &\equiv 4 \pmod{7} \end{aligned}$$

Todas outras soluções (através T. Chin. de Resto) têm forma $53 + 2 \cdot 3 \cdot 7 \cdot t = 53 + 42t //$.

Pergunta: O que acontece se n_i s não foram relativamente primos?

Resposta: O sistema $(*)$ pode ter ou não ter as soluções.

Exemplo:

$$1) \begin{cases} x \equiv -1 \pmod{4} \\ x \equiv 2 \pmod{6} \end{cases}$$

Como $x \equiv -1 \pmod{4} \Rightarrow x = 4t - 1, t \in \mathbb{Z}$

$$\begin{aligned} \text{Agora } x \equiv 2 \pmod{6} &\Rightarrow 4t - 1 \equiv 2 \pmod{6} \\ &\Rightarrow 4t \equiv 3 \pmod{6} \end{aligned}$$

mas $4t \equiv 3 \pmod{6}$ não tem soluções, pois $\text{mdc}(4, 6) = 2$ não divide 3, assim o sistema original não tem soluções.

$$2) \begin{cases} x \equiv -1 \pmod{4} \\ x \equiv 3 \pmod{6} \end{cases}$$

De novo $x = 4k - 1$ com $k \in \mathbb{Z}$.

$$\begin{aligned} x \equiv 3 \pmod{6} &\Rightarrow 4k - 1 \equiv 3 \pmod{6} \\ &\Rightarrow 4k \equiv 4 \pmod{6} \end{aligned}$$

Claro que $k \equiv 1$ é solução e outros tem forma $k = 1 + 3e, e \in \mathbb{Z}$.

$$\text{Assim } x = 4(1 + 3e) - 1 = 12e - 3, e \in \mathbb{Z}.$$

Obs. O Teorema Chinês de Resto fornece

o algoritmo pr procurar a solução do sistema, chamado Algoritmo de Gauss

Algoritmo de Gauss

⑥

Sejam $\textcircled{*} \begin{cases} x \equiv c_1 \pmod{n_1} \\ \vdots \\ x \equiv c_k \pmod{n_k} \end{cases}$, com $\text{mdc}(n_i, n_j) = 1$, $i \neq j$.

Seja $N = n_1 \cdot \dots \cdot n_k$, assim

$$x \equiv N_1 \cdot c_1 \cdot d_1 + N_2 \cdot c_2 \cdot d_2 + \dots + N_k \cdot c_k \cdot d_k \pmod{N}$$

é solução, onde $N_i = \frac{N}{n_i}$ e $N_i \cdot d_i \equiv 1 \pmod{n_i}$
 $\nearrow$
inverso modular
de N_i modulo n_i .

Def. (Inverso modular)

Sejam $a, n \in \mathbb{Z}$, com $n > 0$.

O inverso modular de a modulo n
é q.q. inteiro tal que $a \cdot x \equiv 1 \pmod{n}$.

Obs. Inverso modular

de a modulo n existe $\Leftrightarrow \text{mdc}(a, n) = 1$

Como procurar inverso modular?

(7)

1º. Método (Algoritmo de Euclides).

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

$$a \cdot r + n \cdot s = 1, \text{ para alguns } r, s \in \mathbb{Z}$$

$$\Rightarrow a \cdot r \equiv 1 \pmod{n}$$

$\uparrow$
inverso modular de a .

$\Rightarrow r$ (no Teorema de Bezout) é inv. modular de a .

2º. Método ("Preguioso") [Funciona se n é pequeno].

Testar todos r possíveis entre $1, \dots, n-1$

ou testar $a^i = r$, $i = 1, 2, \dots, n-1$.

Exemplo $a = 3$, $n = 20$.

a) $r = 1 \Rightarrow 3 \cdot 1 = 3$ — resto 3

$r = 2 \Rightarrow 3 \cdot 2 = 6$ — resto 6

$\vdots$

$r = 6 \Rightarrow 3 \cdot 6 = 18$ — resto 18

$r = 7 \Rightarrow 3 \cdot 7 = 21$ — resto é 1 //

$\Rightarrow r = 7$ é inverso modular.

b) $3 \cdot 3 = 9$ — resto 9

$3 \cdot 3^2 = 27$ — resto 7

$3 \cdot 3^3 = 81$ — resto 1 //

$\Rightarrow 3^3 = 27 \equiv 7 \pmod{20}$
é inverso de 3 //

Exemplo Seja

$$\begin{cases} x \equiv \textcircled{1}^{=c_1} \pmod{\textcircled{3}^{=n_1}} \\ x \equiv \textcircled{2}^{=c_2} \pmod{\textcircled{4}^{=n_2}} \\ x \equiv \textcircled{3}^{=c_3} \pmod{\textcircled{5}^{=n_3}} \end{cases}$$

Aplicando Alg. de Gauss, temos

$$N = n_1 \cdot n_2 \cdot n_3 = 3 \cdot 4 \cdot 5 = 60$$

$$N_1 = \frac{N}{n_1} = \frac{60}{3} = 20, \quad d_1 = 2, \text{ pois } 2 \cdot 20 \equiv 1 \pmod{3}$$

$$N_2 = \frac{N}{n_2} = \frac{60}{4} = 15, \quad d_2 = 3, \text{ pois } 3 \cdot 15 \equiv 1 \pmod{4}$$

$$N_3 = \frac{N}{n_3} = \frac{60}{5} = 12, \quad d_3 = 3, \text{ pois } 3 \cdot 12 \equiv 1 \pmod{5}$$

$$\Rightarrow x = N_1 \cdot c_1 \cdot d_1 + N_2 \cdot c_2 \cdot d_2 + N_3 \cdot c_3 \cdot d_3 \\ = 20 \cdot 1 \cdot 2 + 15 \cdot 2 \cdot 3 + 12 \cdot 3 \cdot 3 = 238$$

$$\text{ou } x \equiv 58 \pmod{60} //$$

Exercício (p/ casa)

Resolva:

$$a) \begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 3 \pmod{7} \end{cases}$$

$$b) \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 0 \pmod{5} \\ x \equiv 0 \pmod{8} \end{cases}$$

$$c) \begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{7} \end{cases}$$