Def. Um número inteiro c é solução do sistema de equações congruenciais

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ \qquad \vdots \\ a_t x \equiv b_t \pmod{m_t} \end{cases}$$

se $\forall i \leq t$ c é solução da eq. $a_i x \equiv b_i \pmod{m_i}$.

Teorema Chinês do Resto

Sejam $b_1, \dots, b_t, m_1, \dots, m_t \in \mathbb{Z}$, com $m_i > 1$ $\forall i \leq t$.

Se, para todo $i \neq j$, $\mathrm{mdc}(m_i, m_j) = \{\pm 1\}$, então o sistema

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \vdots \\ x \equiv b_t \pmod{m_t} \end{cases}$$

tem soluções.

Além disso, se c é uma solução do sistema, o conjunto das soluções do sistema é

$$S = \{c + mn : n \in \mathbb{Z}\}, \text{ onde } m = m_1 \cdots m_t.$$

Dem. $\forall i = 1, \dots, t$, seja $m_i' = m_1 \cdots m_{i-1} m_{i+1} \cdots m_t$.

$\forall i$, $\mathrm{mdc}(m_i', m_i) = \{\pm 1\}$, então a equação

$$m_i' x \equiv 1 \pmod{m_i} \text{ tem solução } c_i.$$

(Obs.: c_i é o inverso multiplicativo de m_i' na congr. mod m_i).

Seja $\quad c = \sum_{i=1}^{t} b_i m_i' c_i$.

$$\forall j = 1, \dots, t, \quad c = \underbrace{b_j m_j' c_j}_{\equiv\, b_j} + \sum_{\substack{i=1 \\ i \neq j}}^{t} \underbrace{b_i m_i' c_i}_{\equiv\, 0} \equiv b_j \pmod{m_j}$$

pois, na congruência mod m_j, $b_j(m_j' c_j) \equiv b_j \cdot 1 \equiv b_j$ e,

$\forall i \neq j$, $m_j \mid m_i' = m_1 \cdots m_{i-1} m_{i+1} \cdots m_t \Rightarrow m_i' \equiv 0 \pmod{m_j} \Rightarrow$

$$\Rightarrow b_i m_i' c_i \equiv b_i \cdot 0 \cdot c_i \equiv 0 \pmod{m_j}.$$

Logo, c é uma solução do sistema.

$\forall i \leq t$, $m \equiv 0 \pmod{m_i} \Rightarrow c + mn \equiv c \pmod{m_i}$ $\forall i$, $\forall n \in \mathbb{Z}$,

ou seja, $c + mn$ é solução do sistema $\forall n \in \mathbb{Z}$.

Vamos omitir a dem. do fato que toda solução do sistema é deste tipo.

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ x \equiv b_3 \pmod{m_3} \end{cases} \quad mdc(m_1, m_2) = mdc(m_2, m_3) = = mdc(m_1, m_3) = \{\pm 1\}$$

$m = m_1 m_2 m_3$, $m_1' = m_2 m_3$, $m_2' = m_1 m_3$, $m_3' = m_1 m_2$

$m_1' x \equiv 1 \pmod{m_1}$ $\quad m_2' x \equiv 1 \pmod{m_2}$ $\quad m_3' x \equiv 1 \pmod{m_3}$

elas tem soluções pois $mdc(m_1, m_1') = mdc(m_2, m_2') = = mdc(m_3, m_3') = \{\pm 1\}$. Sejem c_1, c_2, c_3 soluções e seja

$$c = b_1 m_1' c_1 + b_2 m_2' c_2 + b_3 m_3' c_3$$

Na congr. mod m_1: $b_1 \underbrace{m_1' c_1}_{\equiv 1} \equiv b_1 \cdot 1 \equiv b_1$

$+$

$b_2 m_2' c_2 = b_2 \underbrace{m_1}_{\equiv 0} m_3 c_2 \equiv b_2 \cdot 0 \cdot m_3 \cdot c_2 \equiv 0$

$+$

$b_3 m_3' c_3 = b_3 \underbrace{m_1}_{\equiv 0} m_2 c_3 \equiv b_3 \cdot 0 \cdot m_2 c_3 \equiv 0$

$\equiv b_1$

Na congr. mod m_2: $b_1 m_1' c_1 = b_1 \underbrace{m_2}_{\equiv 0} m_3 c_1 \equiv b_1 \cdot 0 \cdot m_3 c_1 \equiv 0$

$+$

$b_2 \underbrace{m_2' c_2}_{\equiv 1} \equiv b_2 \cdot 1 \equiv b_2$

$+$

$b_3 m_3' c_3 = b_3 m_1 \underbrace{m_2}_{\equiv 0} c_3 \equiv b_3 \cdot m_1 \cdot 0 \cdot c_3 \equiv 0$

$\equiv b_2$

Na congr. mod m_3:

$b_1 m_1' c_1 = b_1 m_2 \underbrace{m_3}_{\equiv 0} c_1 \equiv b_1 m_2 \cdot 0 \cdot c_1 \equiv 0$

$+$

$b_2 m_2' c_2 = b_2 m_1 \underbrace{m_3}_{\equiv 0} c_2 \equiv b_2 m_1 \cdot 0 \cdot c_2 \equiv 0$

$+$

$b_3 \underbrace{m_3' c_3}_{\equiv 1} \equiv b_3 \cdot 1 \equiv b_3$

$\equiv b_3$

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

b_i ↓ m_i ↓

$4 = 2^2$

$m = m_1 m_2 m_3 = 4 \cdot 5 \cdot 3 = 60$

$m'_1 = m_2 m_3 = 5 \cdot 3 = 15, \quad m'_2 = m_1 m_3 = 4 \cdot 3 = 12, \quad m'_3 = m_1 m_2 = 4 \cdot 5 = 20$

$m'_1 x \equiv 1 \pmod{m_1} \qquad m'_2 x \equiv 1 \pmod{m_2} \qquad m'_3 x \equiv 1 \pmod{m_3}$

$15x \equiv 1 \pmod{4} \qquad 12x \equiv 1 \pmod{5} \qquad 20x \equiv 1 \pmod{3}$

$3x \equiv 1 \pmod{4} \qquad 2x \equiv 1 \pmod{5} \qquad 2x \equiv 1 \pmod{3}$

Podemos encontrar c_1, c_2 e c_3 solucionando as equações equivalentes, porém na fórmula $c = \sum_{i=1}^{t} b_i m'_i c_i$ devemos usar os próprios m'_1, m'_2, m'_3 (neste caso: 15, 12 e 20).

4	3	1
	1	

$1 = 4 - 3 = 1 \cdot 4 - 1 \cdot 3 \Rightarrow c_1 = -1$

5	2	1
	2	

$1 = 1 \cdot 5 - 2 \cdot 2 \Rightarrow c_2 = -2$

3	2	1
	1	

$1 = 1 \cdot 3 - 1 \cdot 2 \Rightarrow c_3 = -1$

$c = b_1 m'_1 c_1 + b_2 m'_2 c_2 + b_3 m'_3 c_3$

$c = 1 \cdot 15 \cdot (-1) + 3 \cdot 12 \cdot (-2) + 2 \cdot 20 \cdot (-1) =$

$= -15 - 72 - 40 = -127$

$S = \{-127 + 60n : n \in \mathbb{Z}\}.$

$$\begin{cases} x \equiv \overset{b_i}{12} \pmod{\overset{m_i}{7}} \\ x \equiv 11 \pmod 8 \\ x \equiv 10 \pmod 9 \\ x \equiv 74 \pmod 5 \end{cases} \iff \begin{cases} x \equiv \overset{b_i}{5} \pmod{\overset{m_i}{7}} \\ x \equiv 3 \pmod 8 \\ x \equiv 1 \pmod 9 \\ x \equiv 4 \pmod 5 \end{cases}$$

$\boxed{\text{Obs.: Simplificar os } b_i \text{ não tem contraindicações.}}$

Podemos usar o TCR pois 7 e 5 são primos $8=2^3$, $9=3^2$ e são dois a dois primos entre si.

$$m = m_1 m_2 m_3 m_4 = 7\cdot 8\cdot 9\cdot 5 = 2520$$

$$m'_1 = m_2 m_3 m_4 = 8\cdot 9\cdot 5 = 360,\quad m'_2 = 7\cdot 9\cdot 5 = 315,\quad m'_3 = 7\cdot 8\cdot 5 = 280,\quad m'_4 = 7\cdot 8\cdot 9 = 504$$

$$m'_1 x \equiv 1 \pmod{m_1},\quad m'_2 x \equiv 1 \pmod{m_2},\quad m'_3 x \equiv 1 \pmod{m_3},\quad m'_4 x \equiv 1 \pmod{m_4}$$

$$360x \equiv 1 \pmod 7,\quad 315x \equiv 1 \pmod 8,\quad 280x \equiv 1 \pmod 9,\quad 504x \equiv 1 \pmod 5$$

$$3x \equiv 1 \pmod 7,\quad 3x \equiv 1 \pmod 8,\quad 1\cdot x \equiv 1 \pmod 9,\quad 4x \equiv 1 \pmod 5$$

$\begin{array}{c|c|c} 7 & 3 & 1 \\ \hline & 2 & \end{array}$ $1 = 1\cdot 7 - 2\cdot 3$ $\quad c_1 = -2$

$\begin{array}{c|c|c|c} 8 & 3 & 2 & 1 \\ \hline & 2 & 1 & \end{array}$ $1 = 3 - 2 = 3 - (8 - 2\cdot 3) =$

$= -1\cdot 8 + 3\cdot 3 \quad c_2 = 3$

$c_3 = 1$

$\begin{array}{c|c|c} 5 & 4 & 1 \\ \hline & 1 & \end{array}$ $1 = 1\cdot 5 - 1\cdot 4 \quad c_4 = -1$

$$c = \sum_{i=1}^{4} b_i m'_i c_i = 5\cdot 360\cdot(-2) + 3\cdot 315\cdot 3 + 1\cdot 280\cdot 1 + 4\cdot 504\cdot(-1) =$$

$$= -2501 \qquad S = \{-2501 + 2520m : m \in \mathbb{Z}\}$$

$ax + by = c$	$ax \equiv c \pmod{b}$ $\quad by \equiv c \pmod{a}$
$123x + 231y = 12$	$123x \equiv 12 \pmod{231}$ $\quad 231y \equiv 12 \pmod{123}$

Elas tem soluções sse $mdc(a,b)$ dividem c

1) Encontro $d \in mdc(a,b)$ com o alg. des div. subseq.
2) Verifico que $d \mid c$ e calculo, no caso, $c/d = h$
3) Encontro u e v t.q. $au + bv = d$
4) $auh + bvh = dh = c \Rightarrow (uh, vh)$ é solução de $ax + by = c$, uh é solução de $ax \equiv c \pmod{b}$ e vh é solução de $by \equiv c \pmod{a}$.

restos →	231	123	108	15	3	0
quocientes →		1	1	7	5	

$d = 3$ $\quad 3 \mid 12$

$h = 4$

$$3 = 108 - 7 \cdot 15 = 231 - 123 - 7(123 - 108) = 231 - 8 \cdot 123 + 7 \cdot 108$$

$$= 231 - 8 \cdot 123 + 7(231 - 123) = \underset{v}{8} \cdot 231 \underset{u}{-15} \cdot 123$$

$u = -15$, $v = 8$ $\qquad 123 \cdot \underbrace{(-15) \cdot 4}_{uh} + 231 \cdot \underbrace{8 \cdot 4}_{vh} = 3 \cdot 4 = 12$

$123x \equiv 12 \pmod{231}$ $\quad uh$ é solução, isto é -60

$$60x - 32y = 12 \qquad d, u, v, h$$

$$dh = 12 \quad e \quad 60u - 32v = d$$

60	32	28	4	0
	1	1	7	

$$d = 4, \quad h = 3$$

$$4 = 32 - 28 = 32 - (60 - 32) = -60 + 2 \cdot 32 = 60 \cdot \underbrace{(-1)}_{u} - 32 \cdot \underbrace{(-2)}_{v}$$

$$(x_0, y_0) = (-3, -6) \qquad b/d = 15 \quad a/d = -8$$

$$S = \{(-3 - 8k, -6 - 15k) : k \in \mathbb{Z}\} =$$

$$= \{(-3 + 8k, -6 + 15k) : k \in \mathbb{Z}\}$$

$$au + bv = d \qquad c = dh$$

$$auh + bvh = dh = c \qquad (x_0, y_0) = (uh, vh)$$