

TEOR. CHINESE DEL RESTO : schema risolutorio del sistema

di congruenze lineari

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \vdots \\ x \equiv b_n \pmod{n_n} \end{cases}$$

nelle ipotesi $\text{MCD}(n_i, n_j) = 1 \quad \forall i \neq j$.

Ricordo la notazione: $N_i = \frac{n_1 \cdot n_2 \cdot \dots \cdot n_n}{n_i}$

Lo svolgiamo passo passo sul sistema

$$\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 24 \pmod{25} \\ x \equiv 10 \pmod{11} \end{cases}$$

	b_i	n_i	N_i	$N_i \equiv \bar{N}_i \pmod{n_i}$	$\bar{N}_i \cdot y_i \equiv 1 \pmod{n_i} \Rightarrow \bar{y}_i$	
1	3	4	$25 \cdot 11 = 275$	$275 \equiv -1 \pmod{4}$	$-1 \cdot y_1 \equiv 1 \pmod{4}$	$-1 \text{ oppure } 3$
2	24	25	$4 \cdot 11 = 44$	$44 \equiv -6 \pmod{25}$	$-6 \cdot y_2 \equiv 1 \pmod{25}$	4
3	10	11	$4 \cdot 25 = 100$	$100 \equiv 1 \pmod{11}$	$y_3 \equiv 1 \pmod{11}$	1

$$C = \sum_{i=1}^3 b_i N_i \bar{y}_i = 3 \cdot 275(-1) + 24 \cdot 44 \cdot 4 + 10 \cdot 100 \cdot 1 = \\ = (900 + 75) + (4400 - 175) + 1000 = \\ = 5575$$

$$\underset{n_1 \cdot n_2 \cdot \dots \cdot n_n}{\overset{\text{11}}{\equiv}} \rightarrow 1100 \quad -900 + \underline{75} - \underline{175 + 1000} - 1 = 0 - 1 = -1 \equiv 1099 \pmod{1100}$$

è una soluzione. Tutte e sole le altre hanno la forma

$$x = C + 1100h = -1 + 1100h \quad \text{con } h \in \mathbb{Z}$$

IN OGNI CASO, prima di applicare il metodo chiedersi se è applicabile, cioè:

- $\text{MCD}(n_i, n_j) = 1 \quad \forall i \neq j$? → Se NO cercare di risolvere ogni congruenza e vedere se esistono sol. comuni
- i coefficienti di x sono tutti 1? → Se NO ma $\text{MCD}(\text{coefficienti}) = 1$ risolvere prima: $a_i \cdot z_i \equiv 1 \pmod{n_i}$