LEZIONE 7

G. PARMEGGIANI, 11/3/2021

CODICE: 151181

Abbiamo visto (TEOREMA CINESE DEI RESTI). Dato un sistema di congruenze del tipo:

$$\begin{cases} x \equiv b_1 \bmod n_1 \\ x \equiv b_2 \bmod n_2 \\ \vdots \\ x \equiv b_k \bmod n_k \end{cases}$$

se $MCD(n_i, n_j) = 1 \quad \forall i \neq j$

allora

$\exists\, x_0$ sol. del sistema

e le soluzioni del sistema

sono i numeri interi dell'insieme:

$m = n_1 \cdot n_2 \cdot \ldots \cdot n_k$

$$[x_0]_m = \{ x_0 + mk \mid k \in \mathbb{Z} \}$$

IL CASO $k=2$ (SISTEMI CON 2 CONGRUENZE)

$$(*)\begin{cases} x \equiv b_1 \bmod n_1 \\ x \equiv b_2 \bmod n_2 \end{cases} \qquad MCD(n_1, n_2) = 1$$

$$n = n_1 \cdot n_2$$

Per il teorema cinese dei resti, $\exists\, x_2$ soluzione di $(*)$ e le sol. di $(*)$ sono esattamente gli interi nell'insieme

$$\boxed{\{x_2 + nk \mid k \in \mathbb{Z}\} = [x_2]_n}$$

METODO DI NEWTON PER TROVARE x_2

$\boxed{\text{I}}$ $x_1 = b_1$

$\boxed{\text{II}}$ $x_2 = x_1 + t_2 n_1 \equiv b_2 \bmod n_2$

dove t_2 è un numero intero che cerco in modo tale che

$x_2 \equiv b_2 \bmod n_2$ (incognita t_2)

$x_2 = x_1 + t_2 n_1 \equiv x_1 = b_1 \bmod n_1$

$\boxed{\text{III}}$ x_2 è una soluzione di $(*)$

ES 1

$$\begin{cases} x \equiv \underset{b_1}{4} \bmod \underset{n_1}{\boxed{6}} \\ x \equiv \underset{b_2}{3} \bmod \underset{n_2}{\boxed{5}} \end{cases}$$

$K=2$

- le "congruenze sono già ridotte"
- $MCD(n_1, n_2) = MCD(6,5) = 1$

$\overset{\text{Teo Cinese}}{\Longrightarrow}$ $\exists\, x_2$ sol. del sistema

$\boxed{I}$ $x_1 = 4$

$\boxed{II}$ cerco $t_2 \in \mathbb{Z}$ tale che $x_2 = x_1 + t_2 n_1 \equiv b_2 \bmod n_2$

$$4 + t_2 \cdot 6 \equiv 3 \bmod 5$$

FACENDO I CONTI IN $\mathbb{Z}_5$!

$$[4]_5 + t_2 [6]_5 = [3]_5$$

$$t_2 \cdot 6 \equiv 3 - 4 \bmod 5$$

$$6 t_2 \equiv -1 \bmod 5$$

$[6]_5 = [1]_5$ $\qquad$ $[-1]_5 = [4]_5$

$\Longrightarrow$ $t_2 \equiv 4 \bmod 5 \Rightarrow t_2 = 4 \Rightarrow$

$\Rightarrow x_2 = x_1 + t_2 n_1 = 4 + 4 \cdot 6 = 28$

Per il teorema cinese dei resti tutte le sol. di (*) sono gli interi nell'insieme: $n = n_1 \cdot n_2 = 6 \cdot 5 = 30$

$$\{28 + 30k \mid k \in \mathbb{Z}\}$$

$\boxed{\text{IL CASO. } K=3}$

$$\begin{array}{l} A \to \\ B \to \\ C \to \end{array} \begin{cases} x \equiv b_1 \bmod n_1 \\ x \equiv b_2 \bmod n_2 \\ x \equiv b_3 \bmod n_3 \end{cases} \qquad \begin{array}{l} MCD(n_1, n_2) = 1 \\ MCD(n_1, n_3) = 1 \\ MCD(n_2, n_3) = 1 \end{array}$$

$\boxed{\text{I}}$ scelgo una sol. di A: $x_1 = b_1$

$\boxed{\text{II}}$ cerco $t_2 \in \mathbb{Z}$ t.c. $x_2 = x_1 + t_2 n_1 \equiv b_2 \bmod n_2$

x_2 è sol. di $\begin{cases} A \\ B \end{cases}$

$\boxed{\text{III}}$ cerco $t_3 \in \mathbb{Z} \mid \quad x_3 = x_2 + t_3 (n_1 \cdot n_2) \equiv b_3 \mod n_3$

x_3 è sol. di $\begin{cases} A \\ B \\ C \end{cases}$

$\underset{\mod n_1}{x_3 \equiv x_2}$ è sol. di A

$$n = n_1 \cdot n_2 \cdot n_3$$

$\underset{\mod n_2}{x_3 \equiv x_2}$ è sol. di B

Per il teorema cinese dei resti le sol. del (*) sono i numeri interi nell'insieme $\{x_3 + nk \mid k \in \mathbb{Z}\}$

Es. 2

$$\begin{cases} x \equiv \underset{b_1}{10} \mod \underset{n_1}{11} \\ x \equiv \underset{b_2}{5} \mod \underset{n_2}{6} \\ x \equiv \underset{b_3}{5} \mod \underset{n_3}{7} \end{cases}$$

$MCD(11,6)=1$
$MCD(11,7)=1$
$MCD(6,7)=1$

$$n = 11 \cdot 6 \cdot 7 = 462$$

$\boxed{I}$ $x_1 = 10$

$\boxed{II}$ cerco $t_2 \in \mathbb{Z}$ | $x_2 = \boxed{x_1 + t_2 n_1} \equiv b_2 \mod n_2$

$$10 + t_2 \cdot 11 \equiv 5 \mod 6$$

$$11 t_2 \equiv 5-10 \mod 6$$

$[11]_6 = [5]_6 \leftarrow 11 t_2 \equiv -5 \mod 6 \rightarrow [-5]_6 = [1]_6$

$\boxed{\begin{array}{l} b=d=1 \\ \Rightarrow q=1 \end{array}}$

$\underset{a}{5} t_2 \equiv \overset{b}{1} \mod \underset{n}{6}$

$1 = d = \alpha a + \beta n = \alpha \cdot 5 + \beta \cdot 6$

$\underset{n}{6} = \underset{a}{5} \cdot \underset{q_1}{1} + \underset{r_1}{1} \Rightarrow 1 = 6 \cdot \underset{\beta}{1} + 5 \cdot \underset{\alpha}{(-1)}$

$x_0 = \alpha q = \alpha = -1$

QUESTO È t_2

Ho trovato una soluzione della congruenza $5t_2 \equiv 1 \mod 6$

(incognita t_2): $t_2 = -1$ ma $[-1]_6 = [5]_6$. $\boxed{\text{PRENDO } t_2 = 5}$

$$x_2 = 10 + t_2 \cdot 11 = 10 + 5 \cdot 11 = 10 + 55 = 65$$

è sol. di (A)
ed anche di (B)

x_2 è sol. $\begin{cases} x \equiv 10 \mod 11 \\ x \equiv 5 \mod 6 \end{cases}$

$\boxed{\text{III}}$ cerco $t_3 \in \mathbb{Z}$ t.c

$$x_3 = \underbrace{x_2}_{65} + t_3(\underset{n_1}{11} \cdot \underset{n_2}{6}) \equiv \underbrace{b_3}_{5} \mod \underbrace{n_3}_{7}$$

$$65 + t_3 \cdot 66 \equiv 5 \mod 7$$

$[66]_7 = [3]_7$ $\quad [-60]_7 = [3]_7$

$$66 t_3 \equiv \overbrace{\boxed{5-65}}^{=-60} \mod 7$$

$$3t_3 \equiv 3 \mod 7$$

$$t_3 = 1$$

$x_3 = 65 + 1 \cdot 66 = 131$ è una sol. di $\begin{cases} A \\ B \\ C \end{cases}$

$$[131]_{462} = \{131 + 462k \mid k \in \mathbb{Z}\}$$

In generale se $k \geq 4$ e

$$\begin{array}{l} (1) \to \\ (2) \to \\ \vdots \\ (k) \to \end{array} \begin{cases} x \equiv b_1 \bmod n_1 \\ x \equiv b_2 \bmod n_2 \\ \vdots \\ x \equiv b_k \bmod n_k \end{cases}$$

con $MCD(n_i, n_j) = 1$ $\forall i \neq j$

itero il procedimento:

- $x_1 = b_1$ è sol. di (1)
- impongo che $x_1 + n_1 t_2 = x_2$ sia sol. di (2)
  (cerco $t_2 \in \mathbb{Z}$ | $x_2 = x_1 + n_1 t_2 \equiv b_2 \bmod n_2$)
  allora x_2 è sol. di (1) e di (2)
- impongo che $x_2 + n_1 n_2 t_3 = x_3$ sia sol. di (3)
  (cerco $t_3 \in \mathbb{Z}$ | $x_3 = x_2 + n_1 n_2 t_3 \equiv b_3 \bmod n_3$) allora x_3 è sol. di (1), (2), (3)

$\vdots$

AL PASSAGGIO m-ESIMO ho già x_{m-1} che è sol. di (1), (2), ... ($m-1$)

cerco $t_m \in \mathbb{Z}$ | $x_m = x_{m-1} + (n_1 n_2 \cdots n_{m-1}) t_m \equiv b_m \bmod n_m$

.... x_k è una sol. del sistema

Per il teorema cinese dei resti le soluzioni del sistema sono i numeri interi nell'insieme

$$\{x_k + mt \mid t \in \mathbb{Z}\}$$

dove $m = n_1 n_2 \cdots n_k$

IL CASO $K=2$. METODO DI LAGRANGE PER TROVARE UNA SOLUZIONE

$$\begin{cases} x \equiv b_1 \mod n_1 \\ x \equiv b_2 \mod n_2 \end{cases}$$

$MCD(n_1, n_2) = 1$

$\Rightarrow \exists\, \alpha_1, \alpha_2 \in \mathbb{Z}$ t.c.

$$1 = \alpha_1 n_1 + \alpha_2 n_2$$

$$z = b_2 \alpha_1 n_1 + b_1 \alpha_2 n_2$$

verifico che $z = b_2\alpha_1 n_1 + b_1\alpha_2 n_2$ è una soluzione di

$$\begin{cases} x \equiv b_1 \bmod n_1 \\ x \equiv b_2 \bmod n_2 \end{cases}$$

z è soluzione della 1^a congruenza: da $\alpha_1 n_1 + \alpha_2 n_2 = 1$ ottengo $\alpha_2 n_2 = 1 - \alpha_1 n_1$

per cui $z = b_2\alpha_1 n_1 + b_1\alpha_2 n_2 = b_2\alpha_1 n_1 + b_1(1-\alpha_1 n_1) =$

$\boxed{\alpha_2 n_2 = 1-\alpha_1 n_1}$

$$= \underline{b_2\alpha_1 n_1} + b_1 - \underline{b_1\alpha_1 n_1} \equiv b_1 \bmod n_1$$

multipli di n_1

z è soluzione della 2^a congruenza: da $\alpha_1 n_1 + \alpha_2 n_2 = 1$ ottengo $\alpha_1 n_1 = 1 - \alpha_2 n_2$

$\boxed{\alpha_1 n_1 = 1-\alpha_2 n_2}$

per cui $z = b_2\alpha_1 n_1 + b_1\alpha_2 n_2 = b_2(1-\alpha_2 n_2) + b_1\alpha_2 n_2 =$

$$= b_2 - \underline{b_2\alpha_2 n_2} + \underline{b_1\alpha_2 n_2} \equiv b_2 \bmod n_2$$

multipli di n_2

ES

RISOLVO IL SISTEMA DI PG 3 CON QUESTO METODO

$$(*)\begin{cases} x \equiv \overset{b_1}{4} \mod \overset{n_1}{6} \\ x \equiv \underset{b_2}{3} \mod \underset{n_2}{5} \end{cases}$$

$MCD(\overset{n_1}{6}, \overset{n_2}{5}) = 1$

$\exists \alpha_1, \alpha_2 \in \mathbb{Z} \mid$

$$\boxed{\alpha_1 n_1 + \alpha_2 n_2 = 1}$$

$\underset{n_1}{6} = \underset{n_2}{5} \cdot \underset{q_1}{1} + \underset{r_1}{1}$

$1 = \underbrace{6}_{n_1} \cdot \underbrace{}_{\alpha_1=1} + \underbrace{5}_{n_2} \cdot \underbrace{(-1)}_{\alpha_2}$

Cerco z una sol. di $(*)$

$$z = b_2 \alpha_1 n_1 + b_1 \alpha_2 n_2$$

$$= 3 \cdot 1 \cdot 6 + 4 \cdot (-1) \cdot 5$$

$$= 18 - 20 = -2$$

$n = n_1 \cdot n_2 = 6 \cdot 5 = 30$

$$[z]_{30} = [-2]_{30} = [28]_{30} = \{28 + 30k \mid k \in \mathbb{Z}\}$$

COME "RIDURRE" UN GENERICO SISTEMA DI CONGRUENZE

$$(*)\begin{cases} a_1 x \equiv c_1 \bmod m_1 \\ a_2 x \equiv c_2 \bmod m_2 \\ \vdots \\ a_k x \equiv c_k \bmod m_k \end{cases}$$

$a_i, c_i \in \mathbb{Z}$
$m_i \in \mathbb{N}, m_i > 0$

AD UN SISTEMA DEL TIPO

$$(**)\begin{cases} x \equiv b_1 \bmod n_1 \\ x \equiv b_2 \bmod n_2 \\ \vdots \\ x \equiv b_k \bmod n_k \end{cases}$$

"RIDURRE" significa "sostituire con un sistema EQUIVALENTE"

"EQUIVALENTE" significa "CON LE STESSE SOLUZIONI" (eventualmente nessuna)

$\boxed{\text{PASSAGGIO 1}}$ calcolo $d_i = MCD(a_i, m_i)$ $\forall i = 1, \dots, k$

- se $\exists d_i \nmid c_i$ allora la congruenza $a_i x \equiv c_i \bmod m_i$ non ha soluzioni $\Rightarrow$ (*) non ha soluzioni

  NON POSSO RIDURRE (*) a un sistema (**)

- se $\boxed{d_i | c_i}$ $\forall i = 1, \dots, k$ allora ogni congruenza di (*) ha soluzione e

  - se $d_i = 1$ MANTENGO la congruenza $a_i x \equiv c_i \bmod m_i$

  - se $d_i \neq 1$ SOSTITUISCO //

  con la congruenza:

$$\boxed{\frac{a_i}{d_i} x \equiv \frac{c_i}{d_i} \bmod \frac{m_i}{d_i}}$$

$d_i = MCD(a_i, m_i)$

questa congruenza è equivalente alla congruenza:

$a_i x \equiv c_i \bmod m_i$

NB $\frac{a_i}{d_i}, \frac{c_i}{d_i}, \frac{m_i}{d_i} \in \mathbb{Z}$

infatti $d_i | a_i$ è $MCD(a_i, m_i)$

$d_i | m_i$

$d_i | c_i$ perché $a_i x \equiv c_i \bmod m_i$ ha soluzioni

siccome $MCD\left(\frac{a_i}{d_i}, \frac{m_i}{d_i}\right) = 1$ perché $d_i = MCD(a_i, m_i)$, allora

→ HA TUTTE LE SOLUZIONI IN UNA UNICA CLASSE DI CONGRUENZA $\boxed{\text{MODULO } \frac{m_i}{d_i}}$