G. PARMEGGIANI 8/3/2019

ALGEBRA E MATEMATICA DISCRETA (parte di Algebra)

Corso di Laurea: Informatica

C'è un 2° modo per risolvere i sistemi di congruenze che soddisfano le ipotesi del teorema cinese dei resti. Noi lo vediamo solo nel caso $k=2$. (si potrebbe generalizzare anche a $k \geq 3$).

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

$\boxed{2° \text{ MODO}}$ (LAGRANGE) per risolvere $(*)$:

$$MCD(n_1,n_2)=1 \underset{\text{Bezout}}{\Longrightarrow} \exists\, \alpha_1, \alpha_2 \in \mathbb{Z} \text{ t.c. } \alpha_1 n_1 + \alpha_2 n_2 = 1$$

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

si ha che z è una soluzione di $(*)$. Infatti:

$$z = b_2\alpha_1 n_1 + b_1 \boxed{\alpha_2 n_2} = b_2 \alpha_1 n_1 + b_1 (1-\alpha_1 n_1) =$$

$\boxed{\begin{array}{l}\alpha_1 n_1 + \alpha_2 n_2 = 1 \\ \Longrightarrow \alpha_2 n_2 = 1 - \alpha_1 n_1\end{array}}$

$$= b_2\alpha_1 n_1 + b_1 - b_1 \alpha_1 n_1 =$$

$$= b_1 + \underbrace{n_1 (b_2\alpha_1 - b_1 \alpha_1)}_{\text{multiplo di } n_1} \equiv b_1 \bmod n_1$$

$\Rightarrow z$ è una soluzione della 1ª congruenza.

Analogamente: $z = b_2 \boxed{\alpha_1 n_1} + b_1 \alpha_2 n_2 =$

$\boxed{\begin{array}{l}\alpha_1 n_1 + \alpha_2 n_2 = 1 \\ \Longrightarrow \alpha_1 n_1 = 1 - \alpha_2 n_2\end{array}}$

$$= b_2(1-\alpha_2 n_2) + b_1\alpha_2 n_2 = b_2 - b_2\alpha_2 n_2 + b_1 \alpha_2 n_2 =$$

$$= b_2 + \underbrace{n_2(-b_2\alpha_2 + b_1\alpha_2)}_{\text{multiplo di } n_2} \equiv b_2 \bmod n_2$$

$\Rightarrow z$ è una soluzione della 2ª congruenza

ESEMPIO Risolviamo in questo modo il sistema

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

(che abbiamo visto la lezione scorsa)

$MCD(n_1,n_2)=1 \Rightarrow \exists\, \alpha_1,\alpha_2 \in \mathbb{Z} \mid \alpha_1 n_1 + \alpha_2 n_2 = 1$

cerco $\alpha_1,\alpha_2 \in \mathbb{Z}$ t.c. $\quad \alpha_1 \cdot \underset{n_1}{6} + \alpha_2 \cdot \underset{n_2}{5} = 1$

$$\underset{n_1}{6} = \underset{n_2}{5} \cdot \underset{q_1}{1} + \underset{r_1}{1} \Rightarrow 1 = 6 - 5 = \underset{n_1}{6} \cdot \underset{\alpha_1}{1} + \underset{n_2}{5} \cdot \underset{\alpha_2}{(-1)}$$

$$z = b_2 \alpha_1 n_1 + b_1 \alpha_2 n_2 = 3 \cdot 1 \cdot 6 + 4 \cdot (-1) \cdot 5 = 18 - 20 = -2$$

$b_1 = 4$
$b_2 = 3$

L'insieme delle soluzioni del sistema è l'insieme dei numeri interi nella classe di congruenza $[z]_n$ dove $z=-2$ ed $n = n_1 \cdot n_2 = 6 \cdot 5 = 30$

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

COME "RIDURRE" UN GENERICO SISTEMA DI CONGRUENZE

$$(*) \begin{cases} a_1 x \equiv c_1 \bmod m_1 \\ a_2 x \equiv c_2 \bmod m_2 \\ \vdots \\ a_k x \equiv c_k \bmod m_k \end{cases} \quad \text{AD UN SISTEMA NELLA FORMA:} \begin{cases} x \equiv b_1 \bmod n_1 \\ x \equiv b_2 \bmod n_2 \\ \vdots \\ x \equiv b_k \bmod n_k \end{cases}$$

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

- "RIDURRE" SIGNIFICA "SOSTITUIRE CON UN SISTEMA EQUIVALENTE"
- "EQUIVALENTE" " "CON LE STESSE SOLUZIONI" (eventualmente con nessuna soluzione)

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

- se $\exists\, d_i$ tale che $d_i \nmid c_i$ allora la congruenza $a_i x \equiv c_i \bmod m_i$ non ha soluzione
  $\Rightarrow$ il sistema non ha soluzione
- se $d_i \mid c_i \ \forall i = 1,\dots,k$ 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

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

N.B. $\frac{a_i}{d_i}, \frac{c_i}{d_i}, \frac{m_i}{d_i} \in \mathbb{Z}$ e

LA CONGRUENZA $\frac{a_i}{d_i} x \equiv \frac{c_i}{d_i} \bmod \frac{m_i}{d_i}$ E' EQUIVALENTE (HA LE STESSE SOLUZIONI)

DELLA CONGRUENZA $a_i x \equiv c_i \bmod m_i$

Siccome MCD $\left(\frac{a_i}{d_i}, \frac{m_i}{d_i}\right) = 1$ (essendo $d_i = \text{MCD}(a_i, m_i)$)

allora le soluzioni di $\frac{a_i}{d_i} x \equiv \frac{c_i}{d_i} \bmod \frac{m_i}{d_i}$ stanno tutte

in un'unica classe di congruenza (modulo $\frac{m_i}{d_i}$).

Alla fine del $\boxed{\text{PASSAGGIO 1}}$ arrivo SE CIASCUNA CONGRUENZA HA SOL. quindi ad un sistema del tipo

$$(**)\quad \begin{cases} \frac{a_1}{d_1} x \equiv \frac{c_1}{d_1} \bmod \frac{m_1}{d_1} \\ \frac{a_2}{d_2} x \equiv \frac{c_2}{d_2} \bmod \frac{m_2}{d_2} \\ \vdots \\ \frac{a_k}{d_k} x \equiv \frac{c_k}{d_k} \bmod \frac{m_k}{d_k} \end{cases}$$

(dove eventualmente qualche $d_i = 1$) in cui le soluzioni di ciascuna congruenza stanno in un'unica classe di congruenza

$\boxed{\text{PASSAGGIO 2}}$ Risolvo ciascuna congruenza di $(**)$. Se l'unica soluzione mod $\frac{m_i}{d_i}$ della congruenza $\frac{a_i}{d_i} x \equiv \frac{c_i}{d_i} \bmod \frac{m_i}{d_i}$ è $[b_i]_{\frac{m_i}{d_i}}$, alla fine del $\boxed{\text{PASSAGGIO 2}}$ ottengo il sistema equivalente

$$\begin{cases} x \equiv b_1 \bmod \frac{m_1}{d_1} \\ x \equiv b_2 \bmod \frac{m_2}{d_2} \\ \vdots \\ x \equiv b_k \bmod \frac{m_k}{d_k} \end{cases}$$

Posto $n_i = \frac{m_i}{d_i}$, $i = 1, \dots, k$,
SE MCD $(n_i, n_j) = 1 \quad \forall i \neq j$
posso applicare il teorema cinese dei resti ....

ESERCIZIO TIPO 1 (file I19tipo1.pdf)

PER CASA: FINIRE ESERCIZIO 2
(file: I19casaT2.pdf)

MATRICI E LORO OPERAZIONI

Def Una **MATRICE** è una tabella di numeri (o di simboli) disposti in righe ed in colonne, detti **COEFFICIENTI** della matrice

ESEMPIO

$$A = \begin{bmatrix} 2 & 3 & 0 \\ 1 & 4 & 1 \end{bmatrix} \qquad A = \begin{pmatrix} 2 & 3 & 0 \\ 1 & 4 & 1 \end{pmatrix} \qquad A = \begin{matrix} 2 & 3 & 0 \\ 1 & 4 & 1 \end{matrix}$$

tra parentesi quadre... tra parentesi tonde... senza parentesi

Il numero che si trova nella i-esima riga e nella j-esima colonna si chiama COEFFICIENTE di posto (i,j)

A è $m \times n$ se ha m righe e n colonne

$$A = \begin{bmatrix} 2 & 3 & 0 \\ 1 & 4 & 1 \end{bmatrix} \text{ è } 2\times 3 \text{ mentre } B = \begin{bmatrix} 1 & 2 \\ 2 & 7 \\ 0 & 3 \end{bmatrix} \text{ è } 3\times 2$$

Le matrici si indicano con lettere MAIUSCOLE IN STAMPATELLO: $A, B, C, \ldots$

i coefficienti si indicano con lettere MINUSCOLE IN CORSIVO

a_{ij} = il coefficiente di posto (i,j) di A

Per scrivere in modo compatto le matrice

j-esima colonna di A

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1j} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2j} & \cdots & a_{2n} \\ \vdots & & & & & \\ a_{i1} & a_{i2} & \cdots & a_{ij} & \cdots & a_{in} \\ \vdots & & & & & \\ a_{m1} & a_{m2} & \cdots & a_{mj} & \cdots & a_{mn} \end{bmatrix}$$

i-esima riga di A

scrivo $A = (a_{ij})$, $m \times n$ oppure $A = (a_{ij})_{m \times n}$

OPERAZIONI

$\boxed{\text{I}}$ PRODOTTO DI UNA MATRICE PER UNO SCALARE

= NUMERO

Def Data $A = (a_{ij})$, $m \times n$ e dato α scalare, si definisce PRODOTTO DELLO SCALARE α PER LA MATRICE A la matrice $B = (b_{ij})_{m \times n}$ dove $b_{ij} = \alpha \cdot a_{ij}$

Si indica $B = \alpha \cdot A$

ESEMPIO $\alpha = 1 - i$ $\quad A = \begin{bmatrix} 7 & 0 & 3i \\ 1+2i & -i & -4 \end{bmatrix}$

$$\alpha \cdot A = (1-i)\begin{bmatrix} 7 & 0 & 3i \\ 1+2i & -i & -4 \end{bmatrix} =$$

$$= \begin{bmatrix} (1-i)\cdot 7 & (1-i)\cdot 0 & (1-i)\cdot 3i \\ (1-i)(1+2i) & (1-i)\cdot(-i) & (1-i)(-4) \end{bmatrix} =$$

$$= \begin{bmatrix} 7-7i & 0 & 3-3i^2 \\ 1-i+2i-2i^2 & -i+i^2 & -4+4i \end{bmatrix} =$$

$$= \begin{bmatrix} 7-7i & 0 & 3+3i \\ 3+i & -1-i & -4+4i \end{bmatrix}$$