TDN - CONGRUENZE LINEARI

Titolo nota 31/08/2018

Obiettivo Studiare la congruenza

$$ax \equiv b \pmod{m}$$

$\iff m \mid ax - b \iff$ esista $y \in \mathbb{Z}$ t.c.

$$ax - b = my$$

Ovvero: vogliamo risolvere $ax - my = b$

CONDIZIONE DI RISOLUBILITÀ $(a, m) \mid b$

$$ax \equiv b \bmod m \iff_{(a,m)\mid b} \frac{a}{(a,m)} x \equiv \frac{b}{(a,m)} \bmod \frac{m}{(a,m)}$$

con $MCD\left(\frac{a}{(a,m)}, \frac{m}{(a,m)}\right) = 1$

Riscrivo: $cx \equiv d \bmod n$ con $(c, n) = 1$

$\iff c^{-1}cx \equiv c^{-1}d \pmod{n}$

$\iff x \equiv c^{-1}d \pmod{n}$

Esempio $12x \equiv 3 \pmod{51}$

$\iff 4x \equiv 1 \pmod{17}$

$\iff (-4)4x \equiv -4 \pmod{17}$

$x \equiv -4 \pmod{17}$

$$12X \equiv 3 \mod 51 \implies \begin{cases} 12X \equiv 3 \mod 3 \\ 12X \equiv 3 \mod 17 \end{cases}$$

TEOREMA CINESE DEL RESTO

Una congruenza mod $n = p_1^{e_1} \cdots p_r^{e_r}$ è equivalente ad un sistema di r congruenze, una modulo ognuno dei $p_i^{e_i}$ (p_i distinti)

$$X \equiv a \mod (p_1^{e_1} \cdots p_r^{e_r}) \iff \begin{cases} X \equiv a \mod p_1^{e_1} \\ \vdots \\ X \equiv a \mod p_r^{e_r} \end{cases}$$

DIM $\implies$ ovvio

$\impliedby$ Sappiamo che $p_1^{e_1} \mid x-a, \ldots, p_r^{e_r} \mid x-a$

$$\implies p_1^{e_1} \cdots p_r^{e_r} \mid x-a \implies X \equiv a \pmod{p_1^{e_1} \cdots p_r^{e_r}}$$

□

Esempio

$$\begin{cases} X \equiv 2 \mod 7^2 \\ X \equiv 44 \mod 21 \\ X \equiv 5 \mod 9 \end{cases} \qquad \begin{cases} X \equiv 2 \mod 49 \\ X \equiv 44 \mod 7 \\ X \equiv 44 \mod 3 \\ X \equiv 5 \mod 9 \end{cases}$$

$$\begin{cases} X \equiv 2 \mod 49 \\ \cancel{X \equiv 2 \mod 7} \\ \cancel{X \equiv 2 \mod 3} \\ X \equiv 5 \mod 9 \end{cases}$$

$X = 49K + 2$

$X \equiv 149 \mod 9 \cdot 49$

Sostituendo in $X \equiv 5 \mod 9$: $49K + 2 \equiv 5 \mod 9$

$$4K \equiv 49K \equiv 3 \mod 9$$

$$K \equiv -6 \equiv 3 \mod 9$$

$$\Rightarrow X = 49K+2 = 49(9h+3)+2$$

$$= 149 + 49 \cdot 9 \cdot h$$

TCR MARK II

Dato un sistema

$$\begin{cases} X \equiv a_1 \mod m_1 \\ \vdots \\ X \equiv a_r \mod m_r \end{cases},$$

SE i moduli m_i sono a 2 a 2 primi fra loro, le soluzioni sono del tipo

$$X \equiv n \mod \left(\underbrace{mcm(m_1, \dots, m_r)}_{m_1 \cdot \dots \cdot m_r} \right)$$

DIM È sufficiente farlo con 2 equazioni, e si fa esattamente come nell'esempio $\square$

Esempio

$$\begin{cases} X \equiv 2 \mod 7^2 \\ X \equiv 45 \mod 21 \end{cases}$$

$$\begin{cases} X \equiv 2 \mod 49 \\ X \equiv 45 \mod 3 \\ X \equiv 45 \mod 7 \\ \equiv 3 \mod 7 \end{cases}$$

NON COMPATIBILI

$\Rightarrow$ NON CI SONO SOLUZIONI!

Esempio

$$\begin{cases} x \equiv 1 & (3) \\ x \equiv 2 & (5) \\ x \equiv 3 & (7) \end{cases} \iff x \equiv ? \mod 105$$

$$\begin{cases} x \equiv 1 & (3) \\ x \equiv 0 & (5) \\ x \equiv 0 & (7) \end{cases} \qquad \begin{cases} x \equiv 0 & (3) \\ x \equiv 1 & (5) \\ x \equiv 0 & (7) \end{cases} \qquad \begin{cases} x \equiv 0 & (3) \\ x \equiv 0 & (5) \\ x \equiv 1 & (7) \end{cases}$$

$x \equiv 70 \ (3 \cdot 5 \cdot 7)$ $\qquad$ $x \equiv 21 \ (3 \cdot 5 \cdot 7)$ $\qquad$ $x \equiv 15 \ (3 \cdot 5 \cdot 7)$

$$x \equiv 70 \cdot 1 + 21 \cdot 2 + 15 \cdot 3 \mod 105$$

Applicazioni

① Per ogni n esistono n interi positivi consecutivi nessuno dei quali sia un quadrato

Oss Se $p \mid m$ ma $p^2 \nmid m$, certamente m non è un quadrato. Per esempio,

$$m \equiv p \mod p^2$$

$$\begin{cases} m \equiv p_1 \mod p_1^2 \\ m+1 \equiv p_2 \mod p_2^2 \\ \vdots \\ m+(n-1) \equiv p_n \mod p_n^2 \end{cases}$$

Scegliendo i primi p_i tutti diversi, il TCR ci assicura l'esistenza di una soluzione ⇒ VINTO!

② Contare le soluzioni di $x^2 \equiv 1 \mod 105$

└ distinte mod 105

$$x^2 \equiv 1 \ (105) \iff \begin{cases} x^2 \equiv 1 & (3) \\ x^2 \equiv 1 & (5) \\ x^2 \equiv 1 & (7) \end{cases}$$

$$\iff \begin{cases} x \equiv \pm 1 & (3) \\ x \equiv \pm 1 & (5) \\ x \equiv \pm 1 & (7) \end{cases}$$

(8 sistemi)

↕

8 congruenze modulo $3 \cdot 5 \cdot 7$