07/12/2021

$$\begin{cases} 9x \equiv 2 \mod 5 \\ 3x \equiv 4 \mod 13 \\ 2x \equiv 1 \mod 7 \end{cases}$$

deve essere 1

1) sono compatibili?

MCD (9, 5) | 1

2) TEOREMA dei resti?

5 13 7 coprimi? si

SONO nelle condizioni?

(sono semplificabili?)

INVERSO

numero che moltiplicato mi da 1 mod 5

$$\begin{cases} 4x \equiv 2 \mod 5 \\ 3x \equiv 4 \mod 13 \\ 2x \equiv 1 \mod 7 \end{cases} \qquad \begin{cases} x \equiv 2 \cdot 4 \mod 5 \\ x \equiv 4 \cdot 9 \mod 13 \\ x \equiv 1 \cdot 4 \mod 7 \end{cases}$$

$$\begin{cases} x \equiv 3 \mod 5 \\ x \equiv 10 \quad // \quad 13 \\ x \equiv 4 \quad // \quad 7 \end{cases}$$

$N = 455$ prodotto tutti moduli

$N_1 = 91$

$N_2 = 35$

$N_3 = 65$

$$N_i \cdot \bar{x}_i \equiv b_i \mod m_i$$

$91 \cdot \bar{x}_1 \equiv 3 \mod 5 \Rightarrow \bar{x}_1 \equiv 3 \mod 5$

$35 \cdot \bar{x}_2 \equiv 10 \mod 13 \Rightarrow 9\bar{x}_2 \equiv 10 \cdot 3 \mod 13$

$\bar{x}_2 \equiv 30 \mod 13$

$\equiv 4 \quad // \quad //$

$65 \cdot \bar{x}_3 \equiv 4 \mod 7 \Rightarrow 2\bar{x}_3 \equiv 4 \mod 7$

$\Rightarrow x_3 \equiv \frac{4}{2} \, 2 \mod 7$

$$\overline{X} = N_1 \overline{X}_1 + N_2 \overline{X}_2 + N_3 \cdot \overline{X}_3 =$$
$$= 91 \cdot 3 + 35 \cdot 4 + 65 \cdot 2 =$$
$$= 273 + 140 + 130 = 543$$

$$\overline{X} \equiv 543 \mod 455$$
$$\overline{X} \equiv 88 \mod 455$$
$$\boxed{X = 88 + k \cdot 455}$$

quali sono le soluzioni comprese tra 0 e 1000

$k = 0 \Rightarrow 88$

$k = 1 \Rightarrow 543$

$k = 2 \Rightarrow 910 + 88 = 988$

-200 e 0

$k = 88 - 453$ non ci sono soluzioni

$$x \equiv 2 \mod 6$$

$$\begin{cases} x \equiv 2 \mod 2 \\ x \equiv 2 \mod 3 \end{cases} \quad \left.\begin{cases} x \equiv 0 \mod 2 \\ x \equiv 2 \mod 3 \end{cases}\right\} \text{FATTORI COPRIMI}$$

$$X \equiv 7 \mod 12$$

$$\boxed{\cancel{\begin{cases} x \equiv 7 \mod 2 \\ x \equiv 7 \mod 6 \end{cases}}}$$

$$\begin{cases} x \equiv 2 \mod 14 \\ 3x \equiv 2 \mod 5 \\ 5x \equiv 2 \mod 6 \end{cases}$$

NON SONO COPRIMI

NO TEO dei RESTI

sono compatibili?

SONO equivalenti

$$\begin{cases} x \equiv 2 \mod 2 \\ x \equiv 2 \mod 7 \\ 3x \equiv 2 \mod 5 \\ \cancel{5x \equiv 2 \mod 2} \\ 5x \equiv 2 \mod 3 \end{cases}$$

se hanno RISULTATO DIVERSO sono incompatibili

$x \equiv 0 \mod 2$

$x \equiv 0 \mod 2$

$$\begin{array}{r} 14 \\ 15 \\ \hline 70 \\ 140 \\ \hline 210 \end{array}$$

$$\begin{cases} x \equiv 2 \mod 2 \\ x \equiv 2 \mod 7 \\ 3x \equiv 2 \mod 5 \\ 5x \equiv 2 \mod 3 \end{cases}$$

ORA POSSO APPLICARE TEO cinesi

$\rightarrow N = 210$

$$\begin{cases} x \equiv 0 \mod 2 \\ x \equiv 2 \mod 7 \\ x \equiv 2 \cdot 2 \mod 5 \\ x \equiv 2 \cdot 2 \mod 3 \end{cases} \quad \begin{cases} x \equiv 0 \mod 2 \\ x \equiv 2 \mod 7 \\ x \equiv 4 \mod 5 \\ x \equiv 1 \mod 3 \end{cases}$$

$N_1 = 7 \cdot 5 \cdot 3 = 105$

$N_2 = 2 \cdot 5 \cdot 3 = 30$

$N_3 = 2 \cdot 7 \cdot 3 = 42$

$N_4 = 2 \cdot 7 \cdot 5 = 70$

$105 \bar{X}_1 \equiv 0 \mod 2$

$1 X_1 \equiv 0 \mod 2$

$30 X_2 \equiv 2 \mod 7$

$2 x_2 \equiv 2 \mod 7$

$x_2 \equiv 2 \cdot 4 \mod 7$

$\equiv 1 \mod 7$

$42x_3 \equiv 4 \bmod 5$

$2x_3 \equiv 4 \bmod 5$

$x_3 \equiv 2 \bmod 5$

$70x_4 \equiv 1 \bmod 3$

$x_4 \equiv 1 \bmod 3$

$$\overline{X} \equiv N_1\overline{x}_1 + N_2\overline{x}_2 + N_3\overline{x}_3 + N_4\overline{x}_4$$

$$105\cdot 0 + 30\cdot 1 + 42\cdot 2 + 70\cdot 1$$

$$= 184$$

$$\overline{X} \equiv 184 \bmod 210$$

$$X = 184 + k\cdot 210$$

$$\begin{cases} 3x \equiv 2 \bmod 4 \\ 2x \equiv 1 \quad '' \quad 5 \\ 6x \equiv 1 \quad '' \quad 14 \rightarrow \text{INCOMPATIBILE} \end{cases}$$

IL sistema non è compatibile perché la equazione non è compatibile

FINITO

$$\begin{cases} 3x \equiv 2 \bmod 4 \\ 2x \equiv 1 \quad '' \quad 5 \\ 5x \equiv 1 \quad '' \quad 14 \end{cases}$$

$\leftarrow$ i passaggi di prima solo quando sono due fattori COPRIMI

$$\begin{cases} 5x \equiv 1 \bmod 2 \\ 5x \equiv 1 \bmod 7 \end{cases}$$

?

$3x \equiv 2 \bmod 6$ IMP.

$5x \equiv 1 \bmod 2 \rightarrow \mathbb{Z}_4$

$x \equiv 2 \bmod 4$

$x \equiv 1 \bmod 2$

devo scegliere il MODULO più grande

$\mathbb{Z}_4$

$x \equiv b_1 \mod (n, m)$
$x \equiv b_2 \mod n$

$\Downarrow$

$x \equiv b_1 \mod n$
$x \equiv b_2 \mod n$

?

ES

$$\begin{cases} x \equiv 17 \mod 35 \\ x \equiv 1 \mod 5 \end{cases}$$

$$\cancel{\begin{cases} x \equiv 17 \mod 5 \\ x \equiv 1 \mod 5 \end{cases}}$$ IMP

se

$$\begin{cases} x \equiv 17 \mod 35 \\ \cancel{x \equiv 2 \mod 5} \end{cases}$$

$$\begin{cases} x \equiv \overset{(17)}{2} \mod 5 \\ x \equiv 2 \mod 5 \end{cases}$$

cancello

$x \equiv 2 \mod 5$

$$\begin{cases} x \equiv 2 \mod 14 \\ 3x \equiv 2 \mod 5 \\ 4x \equiv 2 \mod 6 \end{cases} \qquad \begin{cases} x \equiv 2 \mod 14 \\ 3x \equiv 2 \mod 5 \\ 2x \equiv 1 \mod 3 \end{cases}$$

$$\begin{cases} x \equiv 2 \mod 14 \\ x \equiv 4 \mod 5 \\ x \equiv 2 \mod 3 \end{cases} \qquad \begin{array}{l} N = 210 \\ N_1 = 15 \\ N_2 = 42 \\ N_3 = 70 \end{array}$$

$15x_1 \equiv 2 \mod 14$ | $42x_2 \equiv 4 \mod 5$

$x_1 \equiv 2 \mod 14$ | $2x_2 \equiv 4 \mod 5$

$x_2 = 2 \mod 5$

$70x_3 \equiv 2 \mod 3$

$x_3 \equiv 2 \mod 3$

SOL TEO CINESE del SISTEMA $\overline{X} = 2 \cdot 15 + 2 \cdot 42 + 2 \cdot 70 = 254$

$\overline{X} = 254 \mod 210$

$\overline{X} = 44 \mod 210$

SOL GENERALE $X = 44 + k210$

SOL TRA 0 e 200

SOLO $k=0$