Esercizio 1. Utilizzando la dimostrazione del teorema cinese del resto determinare l'unica soluzione mod $385 = 5 \cdot 7 \cdot 11$ del sistema cinese

$$(1) \qquad \begin{cases} X \equiv 3(5) \\ X \equiv 4(7) \\ X \equiv 4(11) \end{cases} .$$

$$\begin{cases} X \equiv 3\,(5) \\ X \equiv 4\,(7) \\ X \equiv 4\,(11) \end{cases}$$

il sistema cinese ha soluzione se MCD$(5, 7, 11) = 1$ VERO quindi il sistema ammette soluzione

$R_1 = 7 \cdot 11$

$R_2 = 5 \cdot 11$

$R_3 = 5 \cdot 7$

$77/5 = 15$; $15 \cdot 5 = 75$; $77 - 75 = 2$

$R_1 \tilde{X}_1 \equiv 3(5) \Rightarrow 77\tilde{X}_1 \equiv 3(5) \Rightarrow 2\tilde{X}_1 \equiv 3(5) \Rightarrow \tilde{X}_1 \equiv 3 \cdot 3(5)$

$R_2 \tilde{X}_2 \equiv 4(7) \Rightarrow 55\tilde{X}_2 \equiv 4(7) \Rightarrow 6\tilde{X}_2 \equiv 4(7) \Rightarrow \tilde{X}_2 \equiv 4 \cdot 6\,(7)$

$R_3 \tilde{X}_3 \equiv 4(11) \Rightarrow 35\tilde{X}_3 \equiv 4(11) \Rightarrow 2\tilde{X}_3 \equiv 4(11) \Rightarrow \tilde{X}_3 \equiv 4 \cdot 6(11)$

$\tilde{X}_1 \equiv 9(5) = 4(5)$

$\tilde{X}_2 \equiv 3(7)$

$\tilde{X}_3 \equiv 2(11)$

$\tilde{X} = 77 \cdot 4 + 55 \cdot 3 + 35 \cdot 2$

Esercizio 2. Utilizzando un metodo di sostituzione trovare l'unica soluzione mod $385 = 5 \cdot 7 \cdot 11$ del sistema cinese (1).

Suggerimento. L'idea è di arrivare per successive sostituzioni ad una soluzione scritta nella forma $k + 5 \cdot 7 \cdot 11\ell$, $k < 385$, in modo tale che k sia l'unica soluzione cercata. Procedete come segue: la prima equazione ha soluzione generica $x = 3 + 5t_1$; sostituiamo questa soluzione generica nella seconda equazione; deve essere $3 + 5t_1 \equiv 4(7)$ che possiamo riscrivere come $5t_1 = 1(7)$. Ma 5 e 7 sono comprimi (è qui che utilizziamo l'ipotesi) e quindi 5 ammette un inverso moltiplicativo mod (7) e questo inverso è 3. Ne segue che $t_1 = 3(7)$ e cioè $t_1 = 3 + 7t_2$. Quindi

$$x = 3 + 5(3 + 7t_2) = 18 + 5 \cdot 7t_2$$

(e ora il secondo addendo nel membro a destra fa comparire $5 \cdot 7$). Sostituiamo ora questa espressione nella terza equazione......

$$(1) \qquad \begin{cases} X \equiv 3(5) \\ X \equiv 4(7) \\ X \equiv 4(11) \end{cases} .$$

Esercizio 3. Ho comprato un grosso barattolo di caramelle; il negoziante mi ha assicurato che sono circa mille ma mi ha anche detto che se le metto in fila per 13 ne rimangono 11, se le metto in fila per 11 ne rimangono 7 e ne manca una per riuscire a metterle in fila per 7. Quante caramelle ci sono nel barattolo ?

$$\begin{cases} X \equiv 11\,(13) \\ X \equiv 7\,(11) \\ X \equiv 6\,(7) \end{cases} \longrightarrow$$

QUESTO SISTEMA CINESE HA SOLUZIONI DATO CHE M.C.D.$(13, 11, 7) = 1$

$R_1 = 77$

$R_2 = 91$

$R_3 = 143 = 13 \cdot 11$

$R = 1001$

$77\tilde{x}_1 = 11\,(13) \Rightarrow 12\tilde{x}_1 = 11\,(13) = \tilde{x}_1 \equiv \cancel{132}\,(13) \Rightarrow 2\,(13)$

$91\tilde{x}_2 = 7\,(11) \Rightarrow 3\tilde{x}_2 = 7\,(11) \Rightarrow \tilde{x}_2 \equiv 28\,(11) \Rightarrow \tilde{x}_2 \equiv 6\,(11)$

$143\tilde{x}_3 = 6\,(7) \Rightarrow 3\tilde{x}_3 = 6\,(7) \Rightarrow \tilde{x}_3 \equiv 30\,(7) = \tilde{x}_3 \equiv 2\,(7)$

$12x_0 + 13y_0 = 1$

$13 - 12 = 1$

$x_0 = -1 = [-1 + 13] = [12]$

$3x_0 + 7y_0 = 1$

$7 - 3 \cdot 2 = 1$

$x_0 = [-2] = [7 - 2] = [5]$

quindi: $\tilde{x} = 77 \cdot 2 + 91 \cdot 6 + 143 \cdot 2 \equiv_{1001} 986$

986 CARAMELLE

Esercizio 4. Risolvere il sistema congruenziale

$$\begin{cases} 4X \equiv 2\,(22) \\ 3X \equiv 2\,(7) \end{cases}$$

$$\begin{cases} \cancel{4}^{2}x \equiv \cancel{2}^{1}(\cancel{22}^{11}) \\ 3x \equiv 2(7) \end{cases}$$

VERIFICHIAMO SE HA POSSIBILI SOLUZIONI

$M.C.D.(2,11) = 1 \mid 1$ ✓

$M.C.D.(3,7) = 1 \mid 2$ ✓

SI

LO RISCRIVO COME UN SISTEMA CINESE DATO CHE $M.C.D(11,7)=1$

$$\begin{cases} 2x \equiv 1(11) \\ 3x \equiv 2(7) \end{cases} \rightarrow \begin{cases} x \equiv 6(11) \\ x \equiv 3(7) \end{cases} \rightarrow \begin{cases} x \equiv 6(11) \\ x \equiv 3(7) \end{cases}$$

$R = 77$

$R_1 = 7$

$R_2 = 11$

$$\begin{cases} 7\tilde{x}_1 \equiv 6(11) \\ 11\tilde{x}_2 \equiv 3(7) \end{cases} \Rightarrow \begin{cases} \cancel{7}\tilde{x}_1 \equiv 48(11) \\ \cancel{11}\tilde{x}_2 \equiv 6(7) \end{cases} \Rightarrow \begin{cases} \tilde{x}_1 \equiv 4(11) \\ \tilde{x}_2 \equiv 6(7) \end{cases}$$

$\tilde{x} = 7(4) + 11(6)$

Quindi $7 \cdot 4 + 11 \cdot 8 \equiv_{77} 94 \equiv_{17} \cancel{17}$

Esercizio **5.** Risolvere il sistema congruenziale

$$\begin{cases} 18X \equiv 12(30) \\ 7X \equiv 4(9) \\ 28X \equiv 14(98) \end{cases}$$

$$\begin{cases} \cancel{18}\,X \equiv \cancel{12}\,(\cancel{30}) \quad (\cancel{9}\ 3,\ \cancel{6}\ 2,\ \cancel{15}\ 5) \\ 7X \equiv 4(9) \\ \cancel{28}\,X \equiv \cancel{14}\,(\cancel{98}) \quad (\cancel{14}\ 2,\ \cancel{7}\ 1,\ \cancel{49}\ 7) \end{cases} \rightarrow \begin{cases} 3X \equiv 2(5) \\ 7X \equiv 4(9) \\ 2X \equiv 1(7) \end{cases} \rightarrow$$

VERIFICO CHE IL SISTEMA ABBIA SOLUZIONI.

$M.C.D(3,5) = 1 \mid 2$

$M.C.D.(7,9) = 1 \mid 4$

$M.C.D.(2,1) = 1 \mid 1$

IL SISTEMA AMMETTE SOLUZIONI.

IL SISTEMA È RIDUCIBILE AD UN SISTEMA CINESE DATO CHE $M.C.D(5,9,7)=1$

$$\begin{cases} 3x \equiv 2\ (5) \\ 7x \equiv 4\ (9) \\ 2x \equiv 1\ (7) \end{cases} \Rightarrow \begin{cases} x \equiv 4\ (5) \\ x \equiv 16\ (9) \\ x \equiv 4\ (7) \end{cases}$$

$9 / 7$

$2 = 9 - 7$

$1 = 7 - 2 \cdot 3$

$1 = 7 - (9 - 7) \cdot 3$

$1 = 7 - 9 \cdot 3 + 7 \cdot 3$

$R_1 = 9 \cdot 7 = 63$
$R_2 = 5 \cdot 7 = 35$
$R_3 = 5 \cdot 9 = 45$
$R = 5 \cdot 9 \cdot 7 = 315$

$63\tilde{X}_I \equiv 4\ (5) \to 3\tilde{X}_I \equiv 4\ (5) \to \tilde{X}_I \equiv 8\ (5) \to \tilde{X}_I \equiv 3\ (5)$

$35\tilde{X}_{II} \equiv \cancel{16}\ (9) \to 8\tilde{X}_{II} \equiv 7(9) \to \tilde{X}_{II} \equiv 56\ (9) \to \tilde{X}_{II} \equiv 2\ (9)$

$45\tilde{X}_{III} \equiv 4\ (7) \to 3\tilde{X}_{III} \equiv 4\ (7) \to \tilde{X}_{III} \equiv 20\ (7) \to \tilde{X}_{III} \equiv 6\ (7)$

$\tilde{X} = 63 \cdot 3 + 35 \cdot 2 + 45 \cdot 6 \equiv_{315} 529 \equiv_{315} 214$

Esercizio 6. È dato il sistema congruenziale dipendente dal parametro $a \in \mathbb{Z}$:

$$\begin{cases} 3X \equiv 4(10) \\ 2X \equiv 7(9) \\ 5X \equiv a(12) \end{cases}$$

Determinare per quali $a \in \mathbb{Z}$, $1 \leq a \leq 11$, tale sistema è compatibile. Per tali a risolvere il sistema.

Suggerimento: il metodo di sostituzione può essere utile ....

NON SO APPLICARLO :(

(ESERCIZIO GUIDATO)

$$\begin{cases} 3x \equiv 4(10) \\ 2x \equiv 7(9) \\ 5x \equiv a\ (12) \end{cases} \Rightarrow \begin{cases} x \equiv 7 \cdot 4\ (10) \\ x \equiv 5 \cdot 7\ (9) \\ x \equiv a\ (12) \end{cases} \Rightarrow \begin{cases} x \equiv \overset{8}{\cancel{28}}\ (10) \\ x \equiv \overset{8}{\cancel{35}}\ (9) \\ x \equiv 5a\ (12) \end{cases}$$

$1 = 10 - \underbrace{3}_{x_0} \cdot 3$

$2 = 12 - 5 \cdot 2$

$1 = 5 - (12 - 5 \cdot 2) \cdot 2 = (5 \cdot 5 - 12)$

$$\begin{cases} X \equiv 8\ (10) \\ X \equiv 8\ (9) \\ X \equiv 5a\ (12) \end{cases}$$

USIAMO IL METODO DI SOSTITUZIONE.

RISCRIVO LA PRIMA EQUAZIONE COME $X = 8 + 10t_1$

SOSTITUISCO NELLA SECONDA →

$8 + 10t_1 \equiv 8(9) \leftrightarrow 10t_1 \equiv 0(9) \leftrightarrow t_1 \equiv 0(9) \leftrightarrow t_1 \equiv 9t_2$ MULTIPLO DI 9

SOSTITUISCO QUESTO NELLA NELLA PRIMA

$X = 8 + 10 \cdot (9t_2)$

SOSTITUISCO NELLA TERZA

$8 + 10(9t_2) = 5a(12) \Rightarrow 10(9t_2) = 5a - 8(12) \Rightarrow \cancel{90}t_2 = 5a - 8(12) \Rightarrow$

$6t_2 = (5a - 8)(12)$ e questo ammette soluzioni se

M.C.D. $(6, 12) = 6 \mid 5a - 8$ quindi $5a - 8$ deve essere multiplo di 6

$5a - 8 = 6q \rightarrow 5a - 8 \equiv 0(6)$ e questi valori sono

$a = \begin{cases} a = 4 \\ a = 10 \end{cases}$

[...] RIFACCIO...

Esercizio 6. È dato il sistema congruenziale dipendente dal parametro $a \in \mathbb{Z}$:

$$\begin{cases} 3X \equiv 4(10) \\ 2X \equiv 7(9) \\ 5X \equiv a(12) \end{cases}$$

Determinare per quali $a \in \mathbb{Z}$, $1 \leq a \leq 11$, tale sistema è compatibile. Per tali a risolvere il sistema.

Suggerimento: il metodo di sostituzione può essere utile ....

$$\begin{cases} 3X \equiv 4(10) \\ 2X \equiv 7(9) \\ 5X \equiv a(12) \end{cases} \Rightarrow \begin{cases} X \equiv \cancel{28}\ \cancel{18}\ 8\ (10) \\ X \equiv \cancel{35}\ 8\ (9) \\ X \equiv 5a\ (12) \end{cases} \Rightarrow \begin{cases} X \equiv 8\ (10) \\ X \equiv 8\ (9) \\ X \equiv 5a\ (12) \end{cases}$$

USO IL METODO DI SOSTITUZIONE.

POSSO RISCRIVERE LA PRIMA EQUAZIONE $X = 8 + 10t$

SOSTITUISCO NELLA SECONDA

$8 + 10t \equiv 8(9) \rightarrow$ SOTTRAGGO 8 A DX E SX

$10t \equiv 0(9) \rightarrow t = 9k$

SOSTITUISCO NELLA PRIMA.

$x = 8 + 90k$

SOSTITUISCO NELL' ULTIMA $\rightarrow$ $\boxed{8 + 90k \equiv 5a\ (12)}$

$90k \equiv (5a - 8)\ (12)$

$6k \equiv (5a - 8)\ (12)$

questa equazione ammette soluzioni se MCD $(6, 12) \mid (5a - 8)$

quindi se $6 \mid 5a - 8$ cioè se $5a - 8 = 6f$

($5a - 8$ = MULTIPLO DI 6)

$5a - 8 = 6f \rightarrow 5a - 8 \equiv 0\ (6)$

$* \ 5a \equiv 2\ (6) \rightarrow a \equiv 10\ (6) \rightarrow a \equiv 4\ (6)$

$a = 10 \quad , \quad a = 6$

IL SISTEMA RISULTA RISOLUBILE PER TALI a

VORREI ORA PROVARE A RISOLVERE UNA EQUAZIONE CONGRUENZIALE COL METODO DI SOSTITUZIONE.

Esercizio 1. Utilizzando la dimostrazione del teorema cinese del resto determinare l'unica soluzione mod $385 = 5 \cdot 7 \cdot 11$ del sistema cinese

$$(1) \qquad \begin{cases} X \equiv 3(5) \\ X \equiv 4(7) \\ X \equiv 4(11) \end{cases} .$$

CON METODO DI SOSTITUZIONE.

$$\begin{cases} X \equiv 3(5) \\ X \equiv 4(7) \\ X \equiv 4(11) \end{cases}$$

Posso riscrivere la prima come $x = 3 + 5q$ e sostituisco nella seconda

$3 + 5q = 4\ (7)$

$5q \equiv 1\ (7) \longrightarrow * \ 2 = 7 - 5$

$1 = 5 - 2(7 - 5)$

$1 = 5 + 2 \cdot -7 + 2 \cdot 5$

$x_0 = 3$

$q \equiv 3\ (7)$

$q = 3 + 7k$

sostituendo nelle prime: $x = 3 + 5(3+7k)$

$$x = 3 + 15 + 35k$$

sostituendo nell'ultime: $18 + 35k \equiv 4\ (11)$

$$\cancel{35}k \equiv -14\ (11)$$

$$\cancel{24}$$

$$\cancel{13}$$

$$2k \equiv 5\ (11)$$

$$\cancel{2}k \equiv 5 \cdot 6\ (11)$$

$$k \equiv 30\ (11)$$

$$k \equiv 8\ (11)$$

$$k = 8 + 11z$$

SOSTITUENDO NELLA SECONDA

$$x = 18 + 35(8 + 11z)$$

$$x = 280 + 385z + 18 \Rightarrow x = 298 + 385z$$

$$x = 298\ (385)$$

ERRORI DI CALCOLO
MA IL RAGIONAMENTO DOVREBBE ESSERE GIUSTO.

NB FACCIO UN'ALTRA

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 4 \pmod 7 \\ x \equiv 7 \pmod{11} \end{cases}$$

da: https://www.youtube.com/watch?v=V-nbCG1dGas

$$\begin{cases} x \equiv 3\ (5) \\ x \equiv 4\ (7) \\ x \equiv 7\ (11) \end{cases}$$

$\Rightarrow$ POSSO SCRIVERE LA PRIMA COME $x = 3 + 5y$

- SOSTITUISCO NELLA SECONDA

$$3 + 5y \equiv 4\ (7)$$

$$5y \equiv 1\ (7)$$

$$y \equiv 3\ (7) \qquad y = 3 + 7w$$

RISOSTITUISCO NELLA PRIMA

$X = 3+5(3+7u)$

$X = 3+15+35u$

SOSTITUISCO NELLA TERZA...

$18+35u \equiv 7(11)$

$35u \equiv -11(11)$

$35u \equiv 0(11)$

$2u \equiv 0(11)$

$u = 11K$

SOSTITUISCO NELLA SECONDA...

$X = 3+15+35(11K) = 18+385K$

$X \equiv 18(385)$.

Esercizio 7. Sia p un primo e sia $a \in \mathbb{N}$ tale che $1 \leq a < p^2$. Quali sono gli a privi di inverso aritmetico mod p^2 ?

p e' primo e $a \in \mathbb{N} \mid 1 \leq a < p^2$

$a \equiv \bmod p^2$