ESERCIZI EQ. CONGRUENZIALI. $[a]_m = \{a+mq : q\in\mathbb{Z}\}$

(1) $\begin{cases} x\equiv 2 \pmod 3 \\ x\equiv 3 \pmod 5\end{cases}$ Essendo i moduli coprimi $\Rightarrow$ il sistema è compatibile.

Le soluzioni della prima equazione sono della forma
$\rightarrow \underline{\underline{2+3k}}$ $k\in\mathbb{Z}$

Sostituiamo ciò al posto di x nella 2^a equazione:

$$2+3k\equiv 3 \pmod 5$$ $\leftarrow$ ora questa è l'equazione da risolvere.

$$3k\equiv 1 \pmod 5$$

Una soluzione di questa equazione è $k=2$ $\left(\text{poiché } 3\cdot 2=6\in \underset{\{1+5q:q\in\mathbb{Z}\}}{\underset{\parallel}{[1]_5}}\right)$

Quindi una soluzione del sistema è

$$c = 2+3\cdot \underbrace{2}_{k} = 8$$

Tutte le soluzioni del sistema sono nella classe $[8]_{15}$ cioè sono della forma $8+15q,\ q\in\mathbb{Z}$

(2) Determinare tutte le soluzioni del sistema

$$\begin{cases} x\equiv 2 \pmod 3 \\ x\equiv 3 \pmod 5 \\ x\equiv 4 \pmod 7\end{cases}$$

Come calcolato nell'esercizio precedente, le soluzioni delle prime due equazioni sono gli interi
$\rightarrow 8+15q,\ q\in\mathbb{Z}$

Sostituisco ciò nella 3^a equazione:

$$8+15q\equiv 4 \pmod 7$$

ossia $$15q\equiv \underbrace{-4 \pmod 7}_{\{-4+7\cdot k : k\in\mathbb{Z}\}}$$

$q=3 \Rightarrow 15\cdot q = \underset{-4+7\cdot 7}{\underset{\parallel}{45}}$

Questa equazione ha come soluzione $q=3$ $\left(\text{perché } 15\cdot 3 = \underset{(-4+7\cdot 7)}{\underset{\parallel}{45}} \equiv -4 \pmod 7\right)$

Quindi una soluzione del sistema è

$$8+15\cdot 3 = 53$$

Tutte le soluzioni sono i numeri nella classe

$[53]_{105}$ Ossia della forma $53+105\cdot z$, $z\in\mathbb{Z}$.

3 Si consideri il sistema di equazioni congruenziali lineari

$$\begin{cases} \overset{a}{84}x \equiv \overset{b}{108} \pmod{\overset{m}{400}} \\ 33x \equiv 154 \pmod{253} \end{cases}$$

1 Si verifichi che il sistema è compatibile

2 Si determini la minima soluzione positiva del sistema.

1 Vogliamo ridurre innanzitutto le due equazioni ad equazioni del tipo $\begin{cases} x\equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2}\end{cases}$

Per poterle ridurre a ciò, devo andare a trovare le soluzioni di entrambe.

Se per la 1ª eq. trovo che le soluzioni sono nella $[c]_{400}$, questa eq. sarà equivalente ad $x\equiv c \pmod{400}$.

PARTIAMO DALLA PRIMA:

Vediamo se è compatibile, cioè se $MCD(84,400)\mid 108$

$MCD(84,400)$

$$\left.\begin{aligned} 400 &= 84\cdot 4+64 \\ 84 &= 64\cdot 1+20 \\ 64 &= 20\cdot 3+4 \\ 20 &= 4\cdot 5+0 \end{aligned}\right) \Rightarrow MCD(84,400)=4\mid 108 \Rightarrow \text{la } 1^a \text{ eq. è compatibile}$$

Posso dividere tutto per 4:

$$\underbrace{21}_{a}x \equiv \underbrace{27}_{b} \pmod{\underbrace{100}_{m}}$$

$c = \alpha\cdot k$ ($k = \frac{b}{MCD(a,m)}$, α = 1° coeff. di Bézout)

$MCD(a,m) = MCD(21,100)$

$$\left.\begin{aligned} &③\ 100 = 21\cdot 4+16 \\ &②\ 21 = 16\cdot 1+5 \\ &①\ 16 = 5\cdot 3+1 \\ &\quad 5 = 1\cdot 5+0 \end{aligned}\right) \Rightarrow MCD(21,100)=1$$

Ricavo α: $1=\alpha\cdot 21+\beta\cdot 100$

Ricavo α : $1 = \alpha \cdot 21 + \beta \cdot 100$

$$1 \overset{(1)}{=} 16 + 5 \cdot (-3) \overset{(2)}{=} 16 + (21 + 16(-1))(-3) =$$

$$= 16 + 21(-3) + 16(3) = 16 \cdot 4 + 21 \cdot (-3) \overset{(3)}{=}$$

$$= (100 + 21(-4)) \cdot 4 + 21 \cdot (-3) = 100 \cdot 4 + 21 \cdot (-16) + 21(-3) =$$

$$= \underbrace{(-19)}_{\alpha} \cdot 21 + 4 \cdot 100$$

$$\Rightarrow \alpha = -19$$

$$k = \frac{b}{MCD(21, 100)} = b = 27$$

Una possibile soluzione della 1ª equazione è $c = \alpha \cdot k = -19 \cdot 27 = -513$

Tutte le soluzioni della 1ª equazione sono nella classe

$$[-513]_{100} = [87]_{100}$$

$$-513 + 100 \cdot 6$$

La prima equazione è quindi equivalente a

$$x \equiv 87 \pmod{100}$$

Ora passiamo alla seconda equazione:

$$33x \equiv 154 \pmod{253}$$

Vediamo se è compatibile e cioè se $MCD(33, 253) \mid 154$

$MCD(33, 253)$

$$253 = 33 \cdot 7 + 22$$
$$33 = 22 \cdot 1 + 11$$
$$22 = 11 \cdot 2 + 0$$

$\Rightarrow MCD(33, 253) = 11 \mid 154 \Rightarrow$ è compatibile

Divido tutto per 11:

$$3x \equiv 14 \pmod{23}$$

$c = \alpha \cdot k$ $\qquad$ $MCD(3, 23)$

$$(2)\quad 23 = 3 \cdot 7 + 2$$
$$(1)\quad 3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2 + 0$$

$\Rightarrow MCD(3, 23) = 1$ $\qquad$ $1 = \alpha \cdot 3 + \beta \cdot 23$

$$1 \overset{(1)}{=} 3 + 2(-1) = 3 + (23 + 3 \cdot (-7)) \cdot (-1) =$$

$$1 \overset{(1)}{=} 3+2(-1) = 3 + (23 + 3\cdot(-7))\cdot(-1) =$$

$$= 3 + 23\cdot(-1) + 3\cdot 7 = \underset{\alpha}{8}\cdot 3 + (-1)\cdot 23$$

$$\Rightarrow \alpha = 8 \qquad k = \frac{b}{MCD(3,23)} = b = 14$$

Quindi una soluzione dell'equazione $3x \equiv 14 \pmod{23}$ è

$$c = \alpha \cdot k = 8 \cdot 14 = 112$$

Tutte le soluzioni sono nella classe $[112]_{23} = [20]_{23}$

$112 - 23\cdot 4$

Quindi la 2^a equazione è equivalente a:

$$x \equiv 20 \pmod{23}$$

Pertanto il sistema assegnato inizialmente è equivalente al sistema:

$$(*) \begin{cases} x \equiv 87 \pmod{100} \\ x \equiv 20 \pmod{23} \end{cases}$$

che per il Teorema Cinese del Resto è compatibile perché $MCD(100, 23) = 1 \rightarrow$ moduli sono coprimi.

(2) Nel sistema $(*)$ le soluzioni della prima equazione sono della forma:

$$[87]_{100} = \{87 + 100k : k \in \mathbb{Z}\}$$

Le soluzioni della 2^a equazione sono i numeri che soddisfano:

$$87 + 100k \equiv 20 \pmod{23}$$

che è equivalente a: $100k \equiv -67 \pmod{23}$

MCD (100, 23) per poter ricavare α:

$$\begin{aligned} (3)\quad 100 &= 23\cdot 4 + 8 \\ (2)\quad 23 &= 8\cdot 2 + 7 \\ (1)\quad 8 &= 7\cdot 1 + 1 \\ 7 &= 1\cdot 7 + 0 \end{aligned} \quad \Rightarrow MCD(100,23) = 1$$

$$1 = \alpha\cdot 100 + \beta\cdot 23$$

$$1 \overset{(1)}{=} 8 + 7\cdot(-1) \overset{(2)}{=} 8 + (23 + 8\cdot(-2))\cdot(-1) = 8 + 23\cdot(-1) + 8\cdot 2 =$$

$7 = 1\cdot 7 + 0$, $1 = \alpha\cdot 100 + \beta\cdot 23$

$$1 \overset{(1)}{=} 8 + 7\cdot(-1) \overset{(2)}{=} 8 + (23 + 8\cdot(-2))\cdot(-1) = 8 + 23\cdot(-1) + 8\cdot 2 =$$

$$= 8\cdot 3 + 23\cdot(-1) \overset{(3)}{=} (100 + 23\cdot(-4))\cdot 3 + 23\cdot(-1) =$$

$$= 100\cdot 3 + 23\cdot(-12) + 23\cdot(-1) =$$

$$= \underset{\alpha}{3}\cdot 100 + (-13)\cdot 23$$

$\Rightarrow \alpha = 3$

$$\left[\frac{b}{MCD(100,23)} = \frac{-67}{1} = -67\right]$$

Una soluzione è $k = 3\cdot(-67) = -201$

Quindi una soluzione del sistema è
$87 + 100k = 87 + 100(-201) = -20013$

Per il Teorema Cinese del Resto, tutte le soluzioni del sistema costituiscono la classe

$$[-20013]_{2300} = [687]_{2300}$$
$$= \{-20013 + 2300\cdot 9\}$$

La minima soluzione positiva del sistema è 687.

(4) Si consideri il sistema di equazioni congruenziali lineari

$$\begin{cases} 5x \equiv 7 \pmod 9 \\ 2x \equiv 5 \pmod 7 \\ 6x \equiv 4 \pmod 8 \end{cases}$$

(1) Si verifichi che il sistema è compatibile

(2) Si determinino tutte le soluzioni intere c del sistema tali che $|c| \le 100$.

(1) $5x \equiv 7 \pmod 9 = \{7 + 9k : k \in \mathbb{Z}\}$

- $5x \equiv 7 \pmod 9 \iff x \equiv 5 \pmod 9$ (perchè $5\cdot 5 = 25 = [7]_9$)
  $\uparrow 5$

$2x \equiv 5 \pmod 7 = \{5 + 7\cdot k : k \in \mathbb{Z}\}$
$\uparrow 6\cdot 2 = 12$ $\quad \uparrow 1$

- $2x \equiv 5 \pmod 7 \iff x \equiv 6 \pmod 7$ (perchè $2\cdot 6 = 12 = [5]_7$)

- $2x \equiv 5 \pmod 7 \iff x \equiv 6 \pmod 7$ (perché $2 \cdot 6 = 12 = [5]_7$)

$2x \equiv 2 \pmod 4 = \{2 + 4 \cdot k : k \in \mathbb{Z}\}$
$\uparrow$
$3 \cdot 2 = 6$

- $3x \equiv 2 \pmod 4 \iff x \equiv 2 \pmod 4$

Il sistema assegnato è quindi equivalente al sistema:

$$(*) \begin{cases} x \equiv 5 \pmod 9 \\ x \equiv 6 \pmod 7 \\ x \equiv 2 \pmod 4 \end{cases}$$

Siccome $MCD(9,7) = MCD(9,4) = MCD(7,4) = 1$, per il Teorema Cinese del Resto questo sistema è compatibile.

(2) Le soluzioni della 1ª equazione sono i numeri del tipo
$5 + 9k \;:\; k \in \mathbb{Z}$

Affinché sia soddisfatta anche la 2ª:

$5 + 9k \equiv 6 \pmod 7$

8, 15, 22, ...
cioè $9k \equiv 1 \pmod 7 = \{1 + 7 \cdot q : q \in \mathbb{Z}\}$

Ciò è verificato per $k = 4$ (perché $9 \cdot 4 = 36 = 1 + 7 \cdot 5$)

Quindi una soluzione delle prime 2 equazioni di (*) è

$$5 + 9 \cdot 4 = 41$$

e tutte le soluzioni costituiscono la classe $[41]_{63}$
cioè sono della forma
$41 + 63q, \; q \in \mathbb{Z}$ $\leftarrow$

Affinché una di queste soluzioni soddisfi anche la 3ª equazione di (*) deve aversi che:

$41 + 63q \equiv 2 \pmod 4$

cioè $63q \equiv -39 \pmod 4$
$= \{-39 + 4 \cdot k : k \in \mathbb{Z}\}$

siccome
$-39 \equiv 1 \pmod 4$ $\leftarrow$ $-39 + 4 \cdot 10 = 1$

deve essere $63q \equiv 1 \pmod 4$

$$\{1 + 4 \cdot k : k \in \mathbb{Z}\}$$

$q = 3$

$63 \cdot 3 = 189 = 1 + 188$

Tale equazione è quindi verificata per $q=3$

$\Rightarrow$ Una soluzione del sistema è quindi

$$41 + 63 \cdot 3 = 230$$

Tutte le soluzioni costituiscono $[230]_{252}$ e quindi sono della forma

$$230 + 252z \quad \text{con } z \in \mathbb{Z}.$$

Per $z = -1$ si ottiene la soluzione $c = -22$ che è l'unica con modulo ≤ 100.