L. PARMEGGIANI

ALGEBRA E MATEMATICA DISCRETA

Corso di Laurea: Informatica

SVOLGIMENTO DEGLI ESERCIZI PER CASA 2 (3^ PARTE)

$\boxed{2}$ (5) Risolvere il sistema di congruenze

$$(*)\quad \begin{cases} \overset{a_1=1}{x} \equiv \overset{c_1}{1} \bmod \overset{m_1}{3} \\ \underset{a_2}{2}x \equiv \underset{c_2}{4} \bmod \overset{m_2}{11} \\ \underset{a_3}{2}x \quad \underset{c_3}{3} \bmod \overset{m_3}{10} \end{cases}$$

$\boxed{\text{1° PASSAGGIO}}$ Sostituiamo tutte le congruenze con congruenze in cui le soluzioni stanno tutte nella stessa classe di congruenza.

Calcolo:

$MCD(a_1, m_1) = MCD(1,3) = 1$ NON HO BISOGNO DI SOSTITUIRE LA 1^ CONGRUENZA

$MCD(a_2, m_2) = MCD(2, 11) = 1$ NON HO BISOGNO DI SOSTITUIRE LA 2^ CONGRUENZA

$MCD(a_3, m_3) = MCD(2, 10) = 2 = d$

MA $d = 2 \nmid c_3$ $(c_3 = 3)$ $\Rightarrow$ LA 3^ CONGRUENZA <u>NON</u> HA SOLUZIONE

E QUINDI L'INTERO SISTEMA NON HA SOLUZIONE.

$\boxed{2}$ 6 Risolvere il sistema di congruenze

$$(*)\quad \begin{cases} \overset{a_1}{3}x \equiv \overset{c_1}{4} \bmod \overset{m_1}{5} \\ \overset{a_2}{2}x \equiv \overset{c_2}{4} \bmod \overset{m_2}{8} \\ \underset{a_3=1}{x} \equiv \underset{c_3}{2} \bmod \underset{m_3}{3} \end{cases}$$

$\boxed{\text{1° PASSAGGIO}}$ Sostituiamo tutte le congruenze con congruenze in cui le soluzioni stanno tutte nella stessa classe di congruenza

Calcolo

$MCD(a_1, m_1) = MCD(3, 5) = 1$ NON HO BISOGNO DI SOSTITUIRE LA 1^a CONGRUENZA

$MCD(a_2, m_2) = MCD(2, 8) = 2 \mid 0 = c_2$

SOSTITUISCO LA 2^a CONGRUENZA CON

$$\frac{2x}{2} \equiv \frac{4}{2} \bmod \frac{8}{2}$$ OSSIA CON $x \equiv 2 \bmod 4$

$MCD(a_3, m_3) = MCD(1, 3) = 1$ NON HO BISOGNO DI SOSTITUIRE LA 3^a CONGRUENZA

$\boxed{\text{2° PASSAGGIO}}$ Risolvo ogni congruenza di

$$(**)\quad \begin{cases} 3x \equiv 4 \bmod 5 \\ x \equiv 2 \bmod 4 \\ x \equiv 2 \bmod 3 \end{cases}$$

<u>Risolvo la 1^a</u> $\underset{a}{3}x \equiv \underset{b}{4} \bmod \overset{n}{5}$

$$MCD(a, n) = d = 1 \Rightarrow \begin{cases} \exists\, \alpha, \beta \in \mathbb{Z} \text{ t.c. } \alpha a + \beta n = 1 \\ q = \frac{b}{d} = b \end{cases}$$

Cerco α, β :

$$\underset{n}{5} = \underset{a}{3} \cdot \underset{q_1}{1} + \underset{r_1}{2} \Rightarrow \boxed{2 = 5 - 3}$$

$$\underset{a}{3} = \underset{r_1}{2} \cdot \underset{q_2}{1} + \underset{r_2}{1} \Rightarrow 1 = 3 - 2 = 3 - (5-3) = 3 - 5 + 3 = 3 \cdot 2 - 5$$

$$\Longrightarrow 1 = \underset{a}{3} \cdot \underset{\alpha}{2} + \underset{n}{5} \cdot \underset{\beta}{(-1)}$$

UNA SOLUZIONE DELLA 1^a CONGRUENZA E' $\alpha \cdot q = 2 \cdot 4 = 8$

e siccome $[8]_5 = [8-5]_5 = [3]_5$

SOSTITUISCO $3x \equiv 4 \mod 5$ CON

$x \equiv 3 \mod 5$ ("LA" SOLUZIONE DELLA CONGRUENZA)

LA 2^a E LA 3^a CONGRUENZA SONO GIA' RISOLTE

$\boxed{\text{3° PASSAGGIO}}$ Risolvo (***)

$$\begin{cases} x \equiv \underset{b_1}{3} \mod \underset{n_1}{5} \\ x \equiv \underset{b_2}{2} \mod \underset{n_2}{4} \\ x \equiv \underset{b_3}{2} \mod \underset{n_3}{3} \end{cases}$$

Essendo $MCD(n_1, n_2) = MCD(5,4) = 1$

$MCD(n_1, n_3) = MCD(5,3) = 1$

$MCD(n_2, n_3) = MCD(4,3) = 1$

per il teorema cinese dei resti, (***) ha infinite soluzioni, tutte nella stessa classe di congruenza modulo

$$n = n_1 \cdot n_2 \cdot n_3 = 5 \cdot 4 \cdot 3 = 60$$

CERCO UNA SOLUZIONE DI (***)

$x_1 = 3$

impongo le trovare t_2

$$x_2 = x_1 + t_2 n_1 \equiv 2 \mod 4$$

$$3 + t_2 \cdot 5 \equiv 2 \mod 4$$

$$5t_2 \equiv -1 \mod 4$$

$[5]_4 = [1]_4$ $\qquad$ $[-1]_4 = [3]_4$

$$t_2 \equiv 3 \mod 4$$

QUESTA CONGRUENZA, NELL'INCOGNITA t_2, È CASUALMENTE GIÀ RISOLTA, E POSSO PRENDERE $t_2 = 3$

$$x_2 = 3 + 3 \cdot 5 = 3 + 15 = 18$$

impongo le trovare t_3

$$x_3 = x_2 + t_3 \cdot n_1 \cdot n_2 \equiv 2 \mod 3$$

$$18 + t_3 \cdot 5 \cdot 4 \equiv 2 \mod 3$$

$$20 t_3 \equiv 2 - 18 \mod 3$$

$$20 t_3 \equiv -16 \mod 3$$

$[20]_3 = [20 - 3 \cdot 6]_3 = [2]_3$ $\qquad$ $[-16]_3 = [-16 + 3 \cdot 6]_3 = [2]_3$

$$2t_3 \equiv 2 \mod 3$$

(l'insieme dei numeri interi che sono soluzioni di $2t_3 \equiv 2 \mod 3$ è $[1]_3 = \{1 + 3k \mid k \in \mathbb{Z}\}$)

RISOLVO LA CONGRUENZA NELL'INCOGNITA t_3. "LA" SOLUZIONE È $t_3 \equiv 1 \mod 3$ E POSSO PRENDERE $t_3 = 1$

Allora $x_3 = x_2 + t_3 \cdot n_1 n_2 = 18 + 1 \cdot 5 \cdot 4 = 18 + 20 = 38$

è una soluzione del sistema

QUINDI LE SOLUZIONI DEL SISTEMA SONO TUTTI I NUMERI INTERI NELLA CLASSE DI CONGRUENZA

$$[x_3]_n = [38]_{60} = \{38 + 60k \mid k \in \mathbb{Z}\}$$