L.PARMEGGIANI 11/3/2019

ALGEBRA E MATEMATICA DISCRETA (parte di Algebra)

Corso di Laurea: Informatica

SVOLGIMENTO DEGLI ESERCIZI PER CASA 2 (2^a PARTE)

$\boxed{2}$ 3 Si risolva il sistema $(*)\begin{cases} 2x \equiv 3 \bmod 9 \\ 5x \equiv 1 \bmod 14 \end{cases}$

a_1, c_1, m_1; a_2, c_2, m_2

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

Calcolo $d_1 = MCD(a_1, m_1) = MCD(2, 9) = 1$

NON HO BISOGNO DI SOSTITUIRE LA 1^a CONGRUENZA

Calcolo $d_2 = MCD(a_2, m_2) = MCD(5, 14) = 1$

NON HO BISOGNO DI SOSTITUIRE LA 2^a CONGRUENZA

$\boxed{2^\circ \text{ PASSAGGIO}}$ Risolvo gli congruenze di $(**)\begin{cases} 2x \equiv 3 \bmod 9 \\ 5x \equiv 1 \bmod 14 \end{cases}$

Risolvo la 1^a: $2x \equiv 3 \bmod 9$ (a, b, n)

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

Cerco α, β: $\underset{n}{9} = \underset{a}{2} \cdot \underset{q_1}{4} + \underset{r_1}{1} \Rightarrow \underset{d}{1} = \underset{n_1}{9} \cdot \underset{\beta}{1} + \underset{a}{2} \cdot \underset{\alpha}{(-4)}$

UNA SOLUZIONE DELLA 1^a CONGRUENZA È $\alpha \cdot q = (-4) \cdot 3 = -12$

e risulta $[-12]_9 = [-12 + 9 \cdot 2]_9 = [-12 + 18]_9 = [6]_9$

SOSTITUISCO $2x \equiv 3 \bmod 9$ CON
$x \equiv 6 \bmod 9$ ("LA" SOLUZIONE DELLA CONGRUENZA)

Risolvo la 2^a $\quad 5x \equiv 1 \mod 14$

$$5 \to a, \quad 1 \to b, \quad 14 \to n$$

$$MCD(a,n)=1 \Rightarrow \begin{cases} \exists \alpha,\beta \in \mathbb{Z} \mid \alpha a + \beta n = 1 \\ q = b/d = b \end{cases}$$

Cerco α, β:

$$\underset{n}{14} = \underset{a}{5}\cdot \underset{q_1}{2} + \underset{r_1}{4} \Rightarrow \boxed{4 = 14 - 5\cdot 2}$$

$$\underset{a}{5} = \underset{r_1}{4}\cdot \underset{q_2}{1} + \underset{r_2}{1} \Rightarrow 1 = 5 - 4 = 5-(14-5\cdot 2) = 5 - 14 + 5\cdot 2 = 5\cdot 3 - 14$$

$$\Rightarrow \underset{d}{1} = \underset{a}{5}\cdot \underset{\alpha}{3} + \underset{n}{14}\cdot \underset{\beta}{(-1)}$$

UNA SOLUZIONE DELLA 2^a CONGRUENZA È $\alpha \cdot q = 3\cdot 1 = 3$

SOSTITUISCO $5x \equiv 1 \mod 14$ CON

$x \equiv 3 \mod 14$ ("LA" SOLUZIONE DELLA CONGRUENZA)

$\boxed{\text{3° PASSAGGIO}}$ Risolvo $(***)$ $\begin{cases} x \equiv \underset{b_1}{6} \mod \underset{n_1}{9} \\ x \equiv \underset{b_2}{3} \mod \underset{n_2}{14} \end{cases}$

Essendo $MCD(n_1,n_2) = MCD(9,14) = 1$, per il teorema cinese dei resti, $(***)$ ha infinite soluzioni intere, tutte nella stessa classe di congruenza modulo $n = n_1 \cdot n_2 = 9\cdot 14 = 126$

CERCO UNA SOLUZIONE DI $(***)$

$\boxed{\text{1° MODO}}$ Cerco $\alpha_1, \alpha_2 \in \mathbb{Z}$ t.c. $\alpha_1 n_1 + \alpha_2 n_2 = 1$ e prendo

$z = b_2 \alpha_1 n_1 + b_1 \alpha_2 n_2$.

$$14 = 9 \cdot 1 + 5 \implies \boxed{5 = 14 - 9}$$
$$9 = 5 \cdot 1 + 4 \implies \boxed{4 = 9 - 5}$$
$$5 = 4 \cdot 1 + 1 \implies 1 = 5 - 4 =$$

n_1 q_1 r_1 n_2 r_1 q_2 n_1 r_2 r_1 r_2 q_3 r_3

$$= 5 - (9-5) =$$
$$= 5 - 9 + 5 =$$
$$= 5 \cdot 2 - 9 =$$
$$= (14-9) \cdot 2 - 9 =$$
$$= 14 \cdot 2 - 9 \cdot 2 - 9 =$$
$$= 14 \cdot 2 - 9 \cdot 3$$

$$\implies 1 = \underset{m_2}{14} \cdot \underset{\alpha_2}{2} + \underset{m_1}{9} \cdot \underset{\alpha_1}{(-3)}$$

$$z = b_2 \alpha_1 m_1 + b_1 \alpha_2 m_2 = \underset{b_2}{3} \cdot (-3) \cdot 9 + \underset{b_1}{6} \cdot 2 \cdot 14 =$$
$$= -81 + 12 \cdot 14 =$$
$$= -81 + 168 = 87$$

Le soluzioni del sistema sono tutti gli interi nella classe

$$[z]_n = [87]_{126} = \{87 + 126k \mid k \in \mathbb{Z}\}$$

$\boxed{\text{20170100}}$ per trovare una soluzione di $\begin{cases} x \equiv \underset{b_1}{6} \mod \underset{n_1}{9} \\ x \equiv \underset{b_2}{3} \mod \underset{n_2}{14} \end{cases}$

$x_1 = 6$

$x_2 = x_1 + t_2 u_1 \equiv 3 \mod 14$ impongo per trovare t_2

$$6 + t_2 \cdot 9 \equiv 3 \mod 14$$
$$9 t_2 \equiv 3 - 6 \mod 14$$

$9t_2 \equiv -3 \mod 14$

$[-3]_{14} = [-3+14]_{14} = [11]_{14}$

$9t_2 \equiv 11 \mod 14$

PER TROVARE t_2 DEVO RISOLVERE LA CONGRUENZA:

$\underset{a}{9}\, t_2 \equiv \overset{b}{11} \mod \underset{n}{14}$ (t_2 E' L'INCOGNITA)

$MCD(a, n) = MCD(9, 14) = 1 \Rightarrow \begin{cases} \exists\, \alpha, \beta \in \mathbb{Z} \mid \alpha a + \beta n = 1 \\ q = b/d = b \end{cases}$

Cerco α, β:

$\underset{n}{14} = \underset{a}{9} \cdot \underset{q_1}{1} + \underset{r_1}{5} \Rightarrow \boxed{5 = 14 - 9}$

$\underset{a}{9} = \underset{r_1}{5} \cdot \underset{q_2}{1} + \underset{r_2}{4} \Rightarrow \boxed{4 = 9 - 5}$

$\underset{r_1}{5} = \underset{r_2}{4} \cdot \underset{q_3}{1} + \underset{r_3}{1} \Rightarrow 1 = 5 - 4 =$

$= 5 - (9 - 5) =$

$= 5 - 9 + 5 =$

$= 5 \cdot 2 - 9 =$

$= (14 - 9) \cdot 2 - 9 =$

$= 14 \cdot 2 - 9 \cdot 2 - 9 =$

$= 14 \cdot 2 - 9 \cdot 3$

$$\Rightarrow \underset{d}{1} = \underset{n}{14} \cdot \underset{\beta}{2} + \underset{a}{9} \cdot \underset{\alpha}{(-3)}$$

Una soluzione di $9t_2 \equiv 11 \mod 14$ è $\alpha \cdot q = (-3) \cdot 11 = -33$.

Siccome $[-33]_{14} = [-33 + 14 \cdot 3]_{14} = [-33 + 42]_{14} = [9]_{14}$

PRENDO $t_2 = 9$ E OTTENGO

$$x_2 = x_1 + t_2 \cdot n_1 = 6 + 9 \cdot 9 = 6 + 81 = 87$$

Le soluzioni del sistema sono tutti gli interi nella classe di congruenza

$$[x_2]_n = [87]_{126} = \{87 + 126k \mid k \in \mathbb{Z}\}$$

$\boxed{2}$ 4 Risolvere il sistema (*) $\begin{cases} 2x \equiv 4 \bmod 22 \\ 3x \equiv 5 \bmod 15 \end{cases}$

a_1, c_1, m_1, a_2, c_2, m_2

1° PASSAGGIO Sostituisco tutte le congruenze con congruenze in cui le soluzioni stanno tutte nella stessa classe di congruenza

Calcolo $MCD(a_1, m_1) = MCD(2, 22) = 2 \mid 4 = c_1$

SOSTITUISCO LA 1ª CONGRUENZA CON

$$\frac{2x}{2} \equiv \frac{4}{2} \bmod \frac{22}{2}$$ ossia con $x \equiv 2 \bmod 11$

Calcolo $MCD(a_2, m_2) = MCD(3, 5) = 3 = d$

MA $3 \nmid c_2 \Rightarrow$ LA 2ª CONGRUENZA NON HA SOLUZIONI

QUINDI TUTTO IL SISTEMA NON HA SOLUZIONI