L. PARTEGGIANI

ALGEBRA E MATEMATICA DISCRETA (parte di Algebra)

Corso di Laurea: Informatica

SVOLGIMENTO DEGLI ESERCIZI PER CASA 2 (2ª PARTE)

2 ③ Si risolva il sistema $(*)\begin{cases} 2x \equiv 3 \bmod 9 \\ 5x \equiv 1 \bmod 14 \end{cases}$ ($a_1=2$, $c_1=3$, $m_1=9$; $a_2=5$, $c_2=1$, $m_2=14$)

1° PASSAGGIO Sostituisco tutte le congruenze con congruenze in cui le soluzioni siano tutte nelle stesse classi di congruenza

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

NON HO BISOGNO DI SOSTITUIRE LA 1ª CONGRUENZA

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

NON HO BISOGNO DI SOSTITUIRE LA 2ª CONGRUENZA

2° PASSAGGIO Risolvo ogni congruenza di $(**)\begin{cases} 2x \equiv 3 \bmod 9 \\ 5x \equiv 1 \bmod 14 \end{cases}$

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

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

Calcolo α, β: $9 = 2 \cdot 4 + 1 \Rightarrow 1 = 9 \cdot 1 + 2 \cdot (-4)$ (n, a, q_1, r_1; d, n_1, β, a, α)

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

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

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

Risolvo la 2ª $\quad 5x \equiv 1 \bmod 14$ (5 = a, 1 = b, 14 = n)

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

Cerco α, β: $\quad 14 = 5 \cdot 2 + 4 \Rightarrow \boxed{4 = 14 - 5 \cdot 2}$ ($n = a \cdot q_1 + r_1$)

$5 = 4 \cdot 1 + 1 \Rightarrow 1 = 5 - 4 = 5 - (14 - 5 \cdot 2) =$ ($a = q \cdot r_1 + q_2 \cdot r_2$)

$= 5 - 14 + 5 \cdot 2 =$

$= 5 \cdot 3 - 14$

$\Rightarrow \quad 1 = 5 \cdot 3 + 14 \cdot (-1)$

$d \quad a \quad \alpha \quad n \quad \beta$

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

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

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

3° PASSAGGIO $\quad$ Risolvo (***)

$$\begin{cases} x \equiv 6 \bmod 9 & (b_1 = 6,\ n_1 = 9) \\ x \equiv 3 \bmod 14 & (b_2 = 3,\ n_2 = 14) \end{cases}$$

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 (***)

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

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

$14 = 9 \cdot 1 + 5 \Rightarrow \boxed{5 = 14 - 9}$ ($n_1 = q_1 \cdot r_1 + r_2$)

$14 = 9 \cdot 1 + 5$ (n_1, q_1, r_1) $\Rightarrow$ $\boxed{5 = 14 - 9}$

$9 = 5 \cdot 1 + 4$ (n_2, r_1, q_2, r_2) $\Rightarrow$ $\boxed{4 = 9 - 5}$

$5 = 4 \cdot 1 + 1$ (r_1, r_2, q_3, r_3) $\Rightarrow$

$$1 = 5 - 4 =$$
$$= 5 - (9 - 5) =$$
$$= 5 - 9 + 5 =$$
$$= 5 \cdot 2 - 9 =$$
$$= (14 - 9) \cdot 2 - 9 =$$
$$= 14 \cdot 2 - 9 \cdot 2 - 9 =$$
$$= 14 \cdot 2 - 9 \cdot 3$$

$\Rightarrow \quad 1 = 14 \cdot 2 + 9 \cdot (-3)$ (n_2, a_2, n_1, a_1)

$$z = b_2 a_1 u_1 + b_1 a_2 u_2 = 3 \cdot (-3) \cdot 9 + 6 \cdot 2 \cdot 14 =$$ (b_2, b_1)
$$= -81 + 12 \cdot 14 =$$
$$= -81 + 168 = 87$$

Le soluzioni del sistema sono tutti gli interi nella classe

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

2ª TODO

per trovare una soluzione di $\begin{cases} x \equiv 6 \bmod 9 \\ x \equiv 3 \bmod 14 \end{cases}$ (b_1, n_1, b_2, n_2)

$x_1 = 6$

$x_2 = x_1 + t_2 u_1 \equiv 3 \bmod 14$ (impongo di trovare t_2)

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

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

$$9t_2 \equiv 11 \mod 14$$

PER TROVARE t_2 DEVO RISOLVERE LA CONGRUENZA:

$$\underbrace{9}_{a} t_2 \equiv \overset{b}{\overbrace{11}} \mod \underbrace{14}_{n} \quad (t_2 \text{ È L'INCOGNITA})$$

$MCD(a,n) = MCD(9,14) = 1 \Rightarrow \exists \alpha, \beta \in \mathbb{Z} \mid \alpha a + \beta n = 1$

$q = b/d = b$

cerco α, β:

$14 = 9 \cdot 1 + 5 \Rightarrow 5 = 14 - 9$ (a, q_1, r_1; n)

$9 = 5 \cdot 1 + 4 \Rightarrow 4 = 9 - 5$ (r_1, q_2, r_2; a)

$5 = 4 \cdot 1 + 1$ (r_2, q_3, r_3; r_1)

$\Rightarrow 1 = 5 - 4 =$

$= 5 - (9-5) =$

$= 5 - 9 + 5 =$

$= 5 \cdot 2 - 9 =$

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

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

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

$$\Rightarrow 1 = 14 \cdot 2 + 9 \cdot (-3)$$

$d \quad n \quad \beta \quad a \quad \alpha$

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

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 nelle classe di congruenza

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

---

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 nelle stesse 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