

ALGEBRA E MATEMATICA DISCRETA (parte di Algebra)

Corso di Laurea: Informatica

SVOLGIMENTO DEGLI ESERCIZI PER CASA 2 (3^a PARTE)

2 (5) Risolvere il sistema di congruenze

$$\begin{cases}
 x \equiv 1 \pmod{3} & a_1=1, c_1, m_1 \\
 2x \equiv 4 \pmod{11} & a_2, c_2, m_2 \\
 2x \equiv 3 \pmod{10} & a_3, c_3, m_3
 \end{cases}$$

1° PASSAGGIO

Sostituisco tutte le congruenze con congruenze in cui le soluzioni stanno tutte nelle stesse classi di congruenza.

Calcolo:

$$\text{MCD}(a_1, m_1) = \text{MCD}(1, 3) = 1 \quad \text{NON HO BISOGNO DI SOSTITUIRE LA 1^a CONGRUENZA}$$

$$\text{MCD}(a_2, m_2) = \text{MCD}(2, 11) = 1 \quad \text{NON HO BISOGNO DI SOSTITUIRE LA 2^a CONGRUENZA}$$

$$\text{MCD}(a_3, m_3) = \text{MCD}(2, 10) = 2 = d$$

MA $d=2 \nmid c_3 \Rightarrow$ LA 3^a CONGRUENZA NON HA SOLUZIONE
($c_3=3$)

E QUINDI L'INTERO SISTEMA NON HA SOLUZIONE.

2 **6** Risolvere il sistema di congruenze

$$(*) \begin{cases} 3x \equiv 4 \pmod{5} \\ 2x \equiv 4 \pmod{8} \\ x \equiv 2 \pmod{3} \end{cases}$$

$\begin{matrix} \nearrow a_1 & \nearrow c_1 & \nearrow m_1 \\ \nearrow a_2 & \nearrow c_2 & \nearrow m_2 \\ \nearrow a_3=1 & \nearrow c_3 & \nearrow m_3 \end{matrix}$

1° PASSAGGIO

Sostituisco tutte le congruenze con congruenze in cui le soluzioni stanno tutte nelle stesse classi di congruenza

Calcolo

$\text{MCD}(a_1, m_1) = \text{MCD}(3, 5) = 1$ NON HO BISOGNO DI SOSTITUIRE LA 1ª CONGRUENZA

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

SOSTITUISCO LA 2ª CONGRUENZA CON

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

$\text{MCD}(a_3, m_3) = \text{MCD}(1, 3) = 1$ NON HO BISOGNO DI SOSTITUIRE LA 3ª CONGRUENZA

2° PASSAGGIO

Risolvere ogni congruenza di

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

Risolvere la 1ª

$3x \equiv 4 \pmod{5}$

$\begin{matrix} \nearrow a \\ \nearrow b \\ \nearrow m \end{matrix}$

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

CERCO UNA SOLUZIONE DI (x, x, x)

$$x_1 = 3$$

$$x_2 = x_1 + t_2 n_1 \equiv 2 \pmod{4}$$

$$3 + t_2 \cdot 5 \equiv 2 \pmod{4}$$

$$5t_2 \equiv -1 \pmod{4}$$

$$[5]_4 = [1]_4$$

$$[-1]_4 = [3]_4$$

$$t_2 \equiv 3 \pmod{4}$$

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

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

$$x_3 = x_2 + t_3 \cdot n_1 \cdot n_2 \equiv 2 \pmod{3}$$

$$18 + t_3 \cdot 5 \cdot 4 \equiv 2 \pmod{3}$$

$$20t_3 \equiv 2 - 18 \pmod{3}$$

$$20t_3 \equiv -16 \pmod{3}$$

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

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

$$2t_3 \equiv 2 \pmod{3}$$

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

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

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

è una soluzione del sistema

QUINDI LE SOLUZIONI DEL SISTEMA SONO TUTTI

I NUMERI INTERI NELLA CLASSE DI CONGRUENZA

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