C. PARMEGGIANI 8/3/2019

# ALGEBRA E MATEMATICA DISCRETA (parte di Algebra)

## Corso di Laurea: Informatica

---

Risolvere il sistema:

$$(*)\begin{cases} 3x \equiv 4 \bmod 5 \\ 2x \equiv 4 \bmod 6 \end{cases}$$

($a_1 = 3$, $c_1 = 4$, $m_2 = 5$; $a_2 = 2$, $c_2 = 4$, $m_2 = 6$)

SEMPRE CHE ABBIAMO SOLUZIONE!

**1° PASSAGGIO** Sostituisco tutte le congruenze in congruenze che abbiano UNA UNICA CLASSE DI CONGRUENZA COME SOLUZIONE (ossia tali che le loro soluzioni stiano tutte in un'unica classe di congruenza)

Calcolo: $d_1 = MCD(a_1, m_1)$

$d_1 = MCD(3,5) = 1$

SICCOME $d_1 \mid c_1$ ALLORA LA 1ª CONGRUENZA HA SOLUZIONE

SICCOME $d_1 = 1$ NON HO BISOGNO DI SOSTITUIRE LA 1ª CONGRUENZA

$d_2 = MCD(a_2, m_2)$

$d_2 = MCD(2,6) = 2$

SICCOME $d_2 = 2 \mid 4 = c_2$, ALLORA LA 2ª CONGRUENZA HA SOLUZIONE

SICCOME $d_2 = 2$

N.B: Se una sola delle congruenze non avesse avuto soluzione, l'intero sistema non avrebbe avuto soluzione!

Sostituisco $2x \equiv 4 \bmod 6$ con

$$\frac{2x}{2} \equiv \frac{4}{2} \bmod \frac{6}{2}$$ OSSIA $x \equiv 2 \bmod 3$

Ottengo così il sistema equivalente e quello da cui sono partito, ossia equivalente a (*)

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

**2° PASSAGGIO** Risolvo ogni congruenza di (**). So che ogni congruenza di (**) ha soluzioni, e che le sue soluzioni stanno in una unica classe di congruenza.

Risolvo la 1ª: $3x \equiv 4 \bmod 5$ ($a = 3$, $b = 4$, $n = 5$), $1 = d = MCD(a,n) = MCD(4,5)$

cioè $\alpha, \beta \in \mathbb{Z}$ t.c. $1 = d = \alpha a + \beta n = \alpha \cdot 3 + \beta \cdot 5$

Euclide: $5 = 3 \cdot 1 + 2 \Rightarrow \boxed{2 = 5 - 3}$ ($n$, $a$, $q_1$, $z_1$)

$3 = 2 \cdot 1 + 1$ ($a$, $z_1$, $q_2$, $z_2$) $=$

$1 = 3 - 2 = 3 - (5-3) =$

$= 3 - 5 + 3 =$

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

$1 = 3 \cdot 2 + 5 \cdot (-2)$ ($d$, $a$, $\alpha$, $n$, $\beta$)

$\Rightarrow x_0 = \alpha \cdot b$

$= 2 \cdot 4$

$= 8$ è una soluzione:

$b = q \cdot d = q \Rightarrow q = b = 4$ ($d = 1$)

$3x \equiv 4 \bmod 5$ ha infinite soluzioni intere, tutte nell'unica classe di congruenza

$$[8]_5 = [3]_5 = \{3 + 5k \mid k \in \mathbb{Z}\}$$

QUINDI SOSTITUISCO $3x \equiv 4 \bmod 5$ CON

$x \equiv 3 \bmod 5$ ("LA" SOLUZIONE)

RISOLVO LE 2^ : $x \equiv 2 \bmod 3$ PER PURO CASO QUESTA CONGRUENZA È GIÀ RISOLTA!

Ottengo così il seguente sistema equivalente a (**) (equivalente a (*), che è quello da cui sono partito):

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

($b_1 = 3$, $m_1 = 5$; $b_2 = 2$, $m_2 = 3$)

**3° PASSAGGIO** RISOLVO (***)

SICCOME $MCD(m_1, m_2) = MCD(5,3) = 1$, APPLICO IL TEOREMA CINESE DEI RESTI E, trovata una particolare soluzione $x_0$ di (***)

ovvero che le soluzioni di (***) sono esattamente i numeri interi nelle classi di congruenza $[x_0]_n$ dove $n = n_1 \cdot n_2 = 5 \cdot 3 = 15$:

$$[x_0]_n = [x_0]_{15} = \{x_0 + 15t \mid t \in \mathbb{Z}\}$$

**2° MODO PER TROVARE $x_0$:**

$$\begin{cases} x \equiv 3 \bmod 5 \\ x \equiv 2 \bmod 3 \end{cases}$$

($3 = b_1$, $5 = n_1$, $2 = b_2$, $3 = n_2$)

I $x_1 = 3$

II Cerco $t_2 \in \mathbb{Z}$ tale che $x_1 + t_2 n_1 = x_2$ sia soluzione della 2ª congruenza:

$$3 + t_2 \cdot 5 \equiv 2 \bmod 3 \quad (x_2)$$

$$\Rightarrow \quad 5t_2 \equiv 2 - 3 \bmod 3$$

$$\Rightarrow \quad 5t_2 \equiv -1 \bmod 3$$

$[5]_3 = [5-3]_3 = [2]_3$

$[-1]_3 = [-1+3]_3 = [2]_3$

$$\Rightarrow \quad 2t_2 \equiv 2 \bmod 3$$

risolvo questa congruenza (l'incognita è $t_2$)

$$\Rightarrow \quad t_2 \equiv 1 \bmod 3$$

scelgo $t_2 = 1 \in \mathbb{Z}$ (scelgo $t_2$ nella classe di congruenza modulo 3 che è soluzione di $2t_2 \equiv 2 \bmod 3$)

ALLORA $x_2 = x_1 + t_2 n_1 = 3 + 1 \cdot 5 = 3 + 5 = 8$ è una particolare soluzione del sistema ($x_2$ è la soluzione $x_0$ che sto cercando) e le soluzioni del sistema sono tutti gli interi in

$$[x_2]_{15} = [8]_{15} = \{8 + 15t \mid t \in \mathbb{Z}\}$$

## 2° MODO PER TROVARE $x_0$

$$\begin{cases} x \equiv 3 \bmod 5 \\ x \equiv 2 \bmod 3 \end{cases}$$

($b_1$, $n_1$, $b_2$, $n_2$)

$MCD(n_1, n_2) = 1 \Rightarrow \exists\, \alpha_1, \alpha_2 \in \mathbb{Z}$ t.c. $\alpha_1 n_1 + \alpha_2 n_2 = 1$

e $z = b_2 \alpha_1 n_1 + b_1 \alpha_2 n_2$ è una soluzione del sistema (la $x_0$ che stiamo cercando)

In questo caso $n_1 = 5$, $n_2 = 3$

$5 = 3 \cdot 1 + 2 \Rightarrow 2 = 5 - 3$ ($n_1$, $n_2$, $q_1$, $r_1$)

$3 = 2 \cdot 1 + 1 \Rightarrow 1 = 3 - 2 = 3 - (5-3) = 3 - 5 + 3 = 3 \cdot 2 - 5$ ($n_2$, $r_1$, $q_1$, $r_2$)

$3 \cdot 2 - 5 = 1$ ($n_2$, $\alpha_2$, $n_1$, $\alpha_1 = -1$)

$\Rightarrow 1 = 3 \cdot 2 + 5 \cdot (-1)$ ($\alpha_2$, $\alpha_1$, $n_2$, $n_1$)

$\Rightarrow z = 2 \cdot (-1) \cdot 5 + 3 \cdot 2 \cdot 3 = -10 + 18 = 8$ ($b_2$, $\alpha_1$, $n_1$, $b_1$, $\alpha_2$, $n_2$)

e le soluzioni del sistema sono tutti i numeri interi in

$$[z]_n = [8]_{15} = \{ 8 + 15t \mid t \in \mathbb{Z} \}$$