Lezione 19-10

mercoledì 19 ottobre 2022 09:10

DEF - $\forall m \in \mathbb{Z}$ $\quad \mathbb{Z}_m^* = \{ [a]_m \mid MCD(a,m) = 1 \} \subseteq \mathbb{Z}_m$

ES - $\mathbb{Z}_3^* = \{ [1]_3, [2]_3 \}$

$\mathbb{Z}_3 = \{ [0]_3, [1]_3, [2]_3 \}$

$MCD(1,3) = 1$
$MCD(2,3) = 1$
$MCD(0,3) = 3 \leftarrow$

$\mathbb{Z}_4^* = \{ [1]_4, [3]_4 \}$ perché $MCD(0,4) = 4$
$MCD(2,4) = 2$

$|\mathbb{Z}_m^*|$ = INDICATORE DI GAUSS-EULERO $\varphi(m)$

$\varphi : \mathbb{Z} \to \mathbb{N}$
$m \mapsto |\mathbb{Z}_m^*|$ = il numero di interi positivi che sono coprimi con m (tra 0 e m-1 compresi)

OSS - $\varphi(p) = |\mathbb{Z}_p^*| = |\{ [1]_p, [2]_p, \dots, [p-1]_p \}| = p-1$

$\varphi(p^2) = p^2 - p$

i multipli di p non sono coprimi con p^2

$\varphi(p^n) = p^n - p^{n-1}$

PRIMO TEOREMA di FERMAT sd

Se $p \in \mathbb{N}$ è primo, allora $\forall a \in \mathbb{Z}$ $\quad a^p \equiv a \pmod p$

TEOREMA di FERMAT-EULERO sd

Se $m > 1$ e $a \in \mathbb{Z}$ $MCD(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$

ES $7^4 \equiv 1 \pmod 5$ _

DEF - Dato $m \in \mathbb{Z}$, $a, b \in \mathbb{Z}$ l'equazione $ax \equiv b \pmod m$ è detta

DEF - Dato $m \in \mathbb{Z}$, $a, b \in \mathbb{Z}$ l'equazione $ax \equiv b \pmod{m}$ è detta EQUAZIONE CONGRUENZIALE LINEARE.

TEOREMA

Dato $m \in \mathbb{Z}$, $a, b \in \mathbb{Z}$ l'equazione $ax \equiv b \pmod{m}$ ha soluzione se $MCD(a, m) = 1$.

Se s è soluzione, l'insieme di tutte le soluzioni sarà $S = [s]_m$, cioè $[s]_m = \{ z \in \mathbb{Z} \mid az \equiv b \pmod{m} \}$.

DIM

Sia $MCD(m, a) = 1 \Rightarrow \exists\, u, v \in \mathbb{Z}$ t.c. $1 = au + mv$. Allora ho

$mv = 1 - au \Rightarrow au \equiv 1 \pmod{m} \Rightarrow$ moltiplico per b e ottengo

$bau \equiv b \pmod{m} \Rightarrow a(bu) \equiv b \pmod{m}$

Allora bu è soluzione dell'equazione, e la chiamo s.

- Vediamo che $[s]_m \subseteq \{ z \in \mathbb{Z} \mid az \equiv b \pmod{m} \}$

  Se $t \in [s]_m \Rightarrow \exists\, k \in \mathbb{Z}$ t.c. $t = s + mk \Rightarrow t \equiv s \pmod{m}$

  $\Rightarrow at \equiv as \pmod{m}$ e per ipotesi s è una soluzione $\Rightarrow as \equiv b \pmod{m}$

  $\Rightarrow at \equiv b \pmod{m} \Rightarrow t \in \{ z \in \mathbb{Z} \mid az \equiv b \pmod{m} \}$.

- Vediamo che $\{ z \in \mathbb{Z} \mid az \equiv b \pmod{m} \} \subseteq [s]_m$

  Se $z \in \{ z \in \mathbb{Z} \mid az \equiv b \pmod{m} \} \Rightarrow z$ è soluzione e $az \equiv b \pmod{m}$

  ma s è soluzione $\Rightarrow as \equiv b \pmod{m} \Rightarrow b \equiv as \pmod{m} \Rightarrow$

  $az \equiv as \pmod{m}$. Poiché per ipotesi $MCD(a, m) = 1$, posso semplificare e ottengo $z \equiv s \pmod{m} \Rightarrow z \in [s]_m$

$\square$

ESEMPIO

$\underbrace{12}_{a} x \equiv 7 \pmod{\underbrace{5}_{m}}$ $\qquad MCD(12, 5) = 1$

$12 = 5 \cdot 2 + 2$

$5 = 2 \cdot 2 + 1$

$2 = 1 \cdot 2 + 0$

$$1 = 5 - 2\cdot 2 = 5 + (-2)\cdot 2 =$$
$$= 5 + (-2)\cdot(12 - 5\cdot 2) =$$
$$= 5 + (-2)\cdot(12 + (-2)\cdot 5) =$$
$$= \underbrace{(-2)12}_{u\cdot a} + 5\cdot 5$$

$s = u\cdot b = (-2)\cdot 8 = -16 \rightarrow$ 1 soluzione

L'insieme delle soluzioni è $S = [-16]_5 = [4]_5$

$$-16 \equiv 4 \pmod 5$$
$$-16 = (-4)\cdot 5 + 4$$

$$[-16]_5 = \{-16 + 5\cdot k \mid k \in \mathbb{Z}\} = \{\ldots \underset{k=0}{-16}, \underset{k=1}{-11}, \underset{k=-1}{-21}, \underset{k=3}{-1}, \ldots\}$$

$\boxed{\text{TEOREMA}}$

Sia $m>0$, $a,b \in \mathbb{Z}$ e sia $t \in \mathbb{Z}$ t.c. $t \mid a$, $t \mid b$ e $t \mid m$.

Allora l'equazione $ax \equiv b \pmod m$ ha soluzione $\Longleftrightarrow$ $\left(\frac{a}{t}\right)x \equiv \left(\frac{b}{t}\right) \left(\mathrm{mod}\ \frac{m}{t}\right)$ ha soluzione $s \in \mathbb{Z}$.

NB - L'insieme delle soluzioni sarà

$$S = [s]_{\frac{m}{t}} = [s]_m \cup \left[s + \frac{m}{t}\right]_m \cup \left[s + \frac{2m}{t}\right]_m \cup \ldots \cup \left[s + \frac{(t-1)m}{t}\right]_m$$

NB - Quindi $ax \equiv b \pmod m$ ha soluzione $\Longleftrightarrow$ $\frac{a}{d}x \equiv \frac{b}{d} \left(\mathrm{mod}\ \frac{m}{d}\right)$ ha soluzione, con $d = \mathrm{MCD}(a,m)$ e $d \mid b$

$\boxed{\text{COROLLARIO}}$

Se $\mathrm{MCD}(a,m) \mid b \Longrightarrow ax \equiv b \pmod m$ ha soluzione e la trovo risolvendo $\left(\frac{a}{d}\right)x \equiv \frac{b}{d} \left(\text{mod } \frac{m}{d}\right)$, con $d = MCD(a,m)$.

(perché $MCD\left(\frac{a}{d}, \frac{m}{d}\right) = 1$)

ESEMPIO

$34x \equiv 108 \pmod{500}$

$500 = 34 \cdot 5 + 80$

$34 = 80 \cdot 1 + 4$

$80 = 4 \cdot 20 + 0$

(*) $125 = 21 \cdot 5 + 20$

$21 = 20 \cdot 1 + 1$

$20 = 1 \cdot 20 + 0$

$MCD(500, 34) = 4$. Si ha $4 | 108$ perché $108 = 27 \cdot 4$

$\frac{34}{4} x \equiv \frac{108}{4} \left(\text{mod } \frac{500}{4}\right) \rightsquigarrow 21x \equiv 27 \pmod{\underline{125}}$ $MCD(21, 125) = 1$

Da (*) ho $1 = 21 + (-1) \cdot 20 = 21 + (-1)(125 + (-5)21) =$

$= 21 + (-1)125 + (+5)21 =$

$= (-1)125 + \underbrace{(6)}_{u}21$

$s = 6 \cdot 27 = 162$

$S = [162]_{125} = [37]_{125}$

$= [37]_{500} \cup \left[37 + \frac{500}{4}\right]_{500} \cup \left[37 + \frac{1000}{4}\right]_{500} \cup \left[37 + \frac{1500}{4}\right]_{500}$

$= [37]_{500} \cup [37 + 125]_{500} \cup \ldots$

$z \in [s]_m \iff z = s + m\underline{k}$

$z \in \bigcup_{i=0}^{t-1} \left[s + \frac{im}{t}\right]_m \iff \exists i \in \{0, \ldots, t-1\} \; \exists h \in \mathbb{Z}$ t.c. $z = \underbrace{s + \frac{im}{t} + mh}$

$i=0$

TEOREMA CINESE del RESTO

Sia $m_1, \dots, m_k \in \mathbb{Z}$, $b_1, \dots, b_k \in \mathbb{Z}$ $m_1, \dots, m_k$ sono a 2 a 2 coprimi.

Il sistema $\begin{cases} x \equiv b_1 \pmod{m_1} \\ \vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$ ha soluzione s e

l'insieme di tutte le soluzioni è $S = [s]_{m_1 \cdots m_k}$.

GENERALIZZAZIONE

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$ ha soluzione $\Leftrightarrow$ $\underset{i \neq j}{\mathrm{MCD}}(m_i, m_j) \mid b_i - b_j$

Inoltre:

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ \vdots \\ a_k x \equiv b_k \pmod{m_k} \end{cases}$$ È EQUIVALENTE al SISTEMA $$\begin{cases} x \equiv s_1 \pmod{m_1} \\ \vdots \\ x \equiv s_k \pmod{m_k} \end{cases}$$

dove s_i è la soluzione di $a_i x \equiv b_i \pmod{m_i}$.

ESEMPIO

$$\begin{matrix} \mathrm{I} \\ \mathrm{II} \end{matrix} \begin{cases} x \equiv 4 \pmod 5 \\ x \equiv 3 \pmod 4 \end{cases}$$ $\mathrm{MCD}(5,4) = 1$ ok

1) Risolvo I $x \equiv 4 \pmod 5$

$x = 4 + 5k, \quad k \in \mathbb{Z}$ soluzione generica (classe di 4)

2) Sostituisco in II

$4 + 5k \equiv 3 \pmod 4$

$$4 + 5k \equiv 3 \pmod 4$$

$$5k \equiv -1 \pmod 4$$

$5 \equiv 1 \pmod 4$ $\quad -1 \equiv 3 \pmod 4$ $\quad \Rightarrow \quad k \equiv 3 \pmod 4$

3) Torno in I e sostituisco $k = 3$:

$$x = 4 + 5 \cdot 3 = 19$$

$$S = [19]_{4 \cdot 5} = [19]_{20}$$

ESEMPIO

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 3 \pmod 7 \\ x \equiv 9 \pmod{11} \end{cases}$$

1) $m = m_1 \cdot m_2 \cdot m_3 = 5 \cdot 7 \cdot 11 = 385$

2) $a_1 = \dfrac{m}{m_1} = 7 \cdot 11 = 77$

$a_2 = \dfrac{m}{m_2} = 5 \cdot 11 = 55$

$a_3 = \dfrac{m}{m_3} = 5 \cdot 7 = 35$

3) Scrivo 3 nuove equazioni

$a_1 x \equiv 1 \pmod{m_1} \longrightarrow 77x \equiv 1 \pmod 5 \quad (i)$

$a_2 x \equiv 1 \pmod{m_2} \qquad 55x \equiv 1 \pmod 7 \quad (ii)$

$a_3 x \equiv 1 \pmod{m_3} \qquad 35x \equiv 1 \pmod{11} \quad (iii)$

4) Risolvo le 3 equazioni : (i) ha soluzione $s_1 = 3$

(ii) ha soluzione $s_2 = 6$

(iii) ha soluzione $s_3 = 6$

5) La soluzione è

$$s = a_1 b_1 s_1 + a_2 b_2 s_2 + a_3 b_3 s_3 =$$

$$= 77 \cdot 3 \cdot 3 + 55 \cdot 3 \cdot 6 + 35 \cdot 9 \cdot 6 = 3573$$

$$S = [3573]_{385} = [108]_{385}$$