CONGRUENZE MODULO m

$a, b \in \mathbb{Z} \quad m \in \mathbb{N}$

$ax \equiv b \ (m)$ (PENSO IN $\mathbb{Z}$) $\qquad [a]_m \cdot [x]_m = [b]_m$ (PENSO IN $\mathbb{Z}_m$)

$Sol_{\mathbb{Z}} = \{ x \in \mathbb{Z} \mid ax \equiv b \ (m) \} \subseteq \mathbb{Z}$

$Sol_{\mathbb{Z}_m} = \{ [x]_m \in \mathbb{Z}_m \mid [a]_m [x]_m = [b]_m \} \subseteq \mathbb{Z}_m$

$d = (a, m) = MCD(a, m)$

<u>CASO 1</u> $d = 1$ (ovviamente $d = 1 \mid b$)

ESISTE UN' UNICA SOLUZIONE IN $\mathbb{Z}_m$
(ESISTONO ∞ SOLUZIONI IN $\mathbb{Z}$)

$d = 1$ significa che $[a]_m \in \mathbb{Z}_m^*$ ($[a]_m$ invertibile)
esiste $[a]_m^{-1} \in \mathbb{Z}_m$ tale che $[a]_m^{-1} [a]_m = [1]_m$

$[a]_m \cdot [x]_m = [b]_m \longrightarrow [a]_m^{-1} \cdot [a]_m [x]_m = [a]_m^{-1} [b]_m$

$\longrightarrow [1]_m [x]_m = [a]_m^{-1} [b]_m \longrightarrow [x]_m = [a]_m^{-1} [b]_m$

$Sol_{\mathbb{Z}_m} = \{ [a]_m^{-1} \cdot [b]_m \} \subseteq \mathbb{Z}_m$ 1 ELEMENTO DI $\mathbb{Z}_m$

$Sol_{\mathbb{Z}} = [a]_m^{-1} \cdot [b]_m \subseteq \mathbb{Z}$ ∞ ELEMENTI DI $\mathbb{Z}$

PER TROVARE LA SOLUZIONE:

<u>MODO 1</u> A MENTE

<u>MODO 2</u> CERCO $[a]_m^{-1}$ E CALCOLO $[a]_m^{-1} \cdot [b]_m$

CASO 2 $\quad d \neq 1, \ d \mid b$

ESISTONO d SOLUZIONI IN $\mathbb{Z}_m$

(ESISTONO ∞ SOLUZIONI IN $\mathbb{Z}$)

$$Sol_{\mathbb{Z}_m} = \{ [r_1]_m, \dots, [r_d]_m \} \subseteq \mathbb{Z}_m$$

$$Sol_{\mathbb{Z}} = [r_1]_m \cup \dots \cup [r_d]_m \subseteq \mathbb{Z}$$

PER TROVARE LE SOLUZIONI

MODO 1 $\quad$ A MENTE

MODO 2 $\quad$ RIDUCO AD UN SISTEMA EQUIVALENTE

$$ax \equiv b \quad (m)$$

$$\frac{a}{d} x \equiv \frac{b}{d} \quad \left(\frac{m}{d}\right)$$

(PER CAPIRE VEDERE L'ESERCIZIO 1)

CASO 3 $\quad d \neq 1, \ d \nmid b$

NON ESISTONO SOLUZIONI IN $\mathbb{Z}_m$

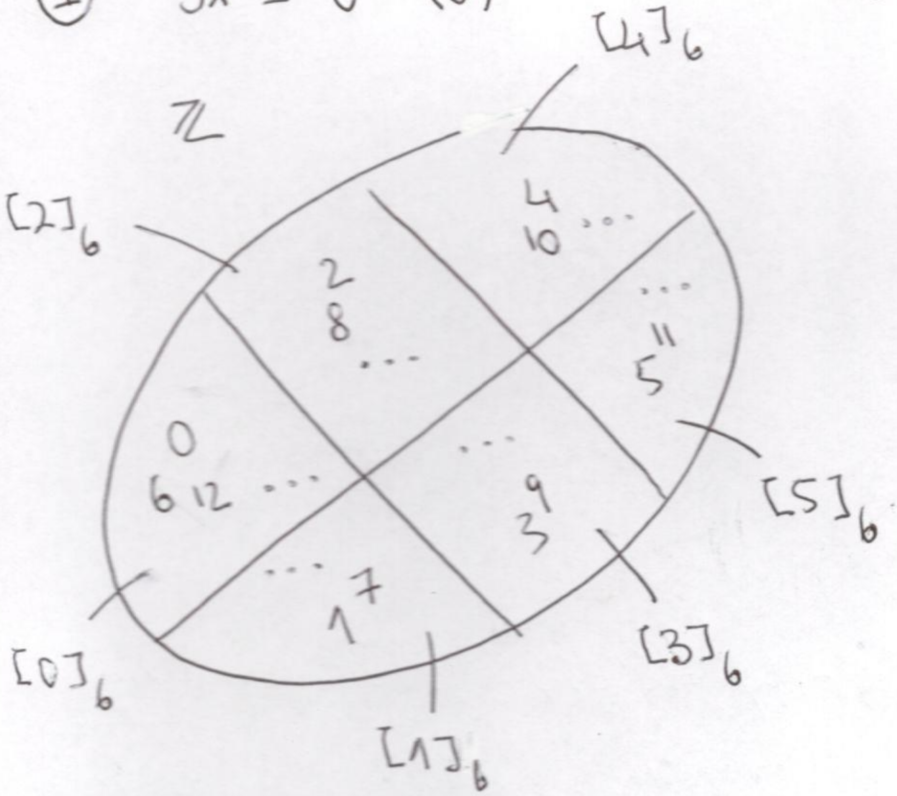
(NON ESISTONO SOLUZIONI IN $\mathbb{Z}$)

$$Sol_{\mathbb{Z}_m} = \emptyset \subseteq \mathbb{Z}_m$$

$$Sol_{\mathbb{Z}} = \emptyset \subseteq \mathbb{Z}$$

$\emptyset$ È L'INSIEME VUOTO

① $3x \equiv 0 \quad (6)$ $\qquad [3]_6 \, [x]_6 = [0]_6$



$$\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$$

$a = 3, \; b = 0, \; m = 6$

$d = (3, 6) = 3 \mid 0 \qquad (0 = 3 \cdot 0)$

<u>CASO 2</u> ESISTONO 3 SOLUZIONI IN $\mathbb{Z}_6$

A MENTE :

$[3]_6 \cdot [0]_6 = [3 \cdot 0]_6 = [0]_6$

$[3]_6 \cdot [2]_6 = [3 \cdot 2]_6 = [6]_6 = [0]_6$

$[3]_6 \cdot [4]_6 = [3 \cdot 4]_6 = [12]_6 = [0]_6$

$$Sol_{\mathbb{Z}_6} = \{[0]_6, [2]_6, [4]_6\} \subseteq \mathbb{Z}_6$$

$$Sol_{\mathbb{Z}} = [0]_6 \cup [2]_6 \cup [4]_6 \subseteq \mathbb{Z}$$

RIDUCO AD UN SISTEMA EQUIVALENTE

$$3x \equiv 0 \quad (6)$$

$$\frac{3}{3} x \equiv \frac{0}{3} \quad \left(\frac{6}{3}\right)$$

$$x \equiv 0 \quad (2)$$

$$Sol_{\mathbb{Z}_2} = \{[0]_2\} \subseteq \mathbb{Z}_2$$

$$Sol_{\mathbb{Z}} = [0]_2 \subseteq \mathbb{Z}$$

<u>OSSERVAZIONE</u> $[0]_2 = [0]_6 \cup [2]_6 \cup [4]_6$

$$Sol_{\mathbb{Z}_6} = \{[0]_6, [2]_6, [4]_6\} \subseteq \mathbb{Z}_6$$

$$Sol_{\mathbb{Z}} = [0]_6 \cup [2]_6 \cup [4]_6 = [0]_2 \subseteq \mathbb{Z}$$

(2) $5x \equiv 2 \ (6)$ $\qquad [5]_6 [x]_6 = [2]_6$

$a = 5 \quad b = 2 \quad m = 6$

$d = (5, 6) = 1$

CASO 1 ESISTE UN'UNICA SOLUZIONE IN $\mathbb{Z}_6$

$[5]_6 \in \mathbb{Z}_6^*$ CERCO $[5]_6^{-1} \in \mathbb{Z}_6$

$[5]_6 \cdot [5]_6 = [5 \cdot 5]_6 = [25]_6 = [1]_6$

$[5]_6^{-1} = [5]_6$

LA SOLUZIONE È $[5]_6^{-1} \cdot [2]_6 = [5]_6 \cdot [2]_6 = [10]_6 = [4]_6$

$5x \equiv 2 \ (6)$ $\qquad [5]_6 \cdot [x]_6 = [2]_6$

$x \equiv 4 \ (6)$ $\qquad [x]_6 = [4]_6$

$Sol_{\mathbb{Z}_6} = \{[4]_6\} \subseteq \mathbb{Z}_6$

$Sol_{\mathbb{Z}} = [4]_6 \subseteq \mathbb{Z}$

(3) $15x \equiv 9 \ (25)$

$a = 15, \ b = 9, \ m = 25$

$d = (15, 25) = 5 \nmid 9$

CASO 3 NON ESISTONO SOLUZIONI IN $\mathbb{Z}_{25}$

$Sol_{\mathbb{Z}_{25}} = \emptyset \subseteq \mathbb{Z}_{25}$

$Sol_{\mathbb{Z}} = \emptyset \subseteq \mathbb{Z}$

(4) $17x \equiv 14 \quad (21)$

$a = 17 \quad b = 14 \quad m = 21$

$d = (17, 21) = 1$

CASO 1 ESISTE UN' UNICA SOLUZIONE IN $\mathbb{Z}_{21}$

$[17]_{21} \in \mathbb{Z}^*_{21}$ CERCO $[17]^{-1}_{21} \in \mathbb{Z}_{21}$

$[5]_{21} \cdot [17]_{21} = [5]_{21} \cdot [-4]_{21} = [5 \cdot (-4)]_{21} =$

$= [-20]_{21} = [1]_{21}$

$[17]^{-1}_{21} = [5]_{21}$

LA SOLUZIONE È $[17]^{-1}_{21} \cdot [14]_{21} = [5]_{21} \cdot [14]_{21} =$

$= [5 \cdot 14]_{21} = [70]_{21} = [7]_{21}$

$Sol_{\mathbb{Z}_{21}} = \{[7]_{21}\} \subseteq \mathbb{Z}_{21}$

$Sol_{\mathbb{Z}} = [7]_{21} \subseteq \mathbb{Z}$

(6) $36x \equiv 10 \quad (12)$

$a = 36 \quad b = 10 \quad m = 12$

$d = (36, 12) = 12 \nmid 10$

CASO 3 NON ESISTONO SOLUZIONI IN $\mathbb{Z}_{12}$

$Sol_{\mathbb{Z}_{12}} = \emptyset \subseteq \mathbb{Z}_{12}$

$Sol_{\mathbb{Z}} = \emptyset \subseteq \mathbb{Z}$

(5) $415x \equiv 21 \quad (18)$

$415 = 23 \cdot 18 + 1$

$415 \equiv 1 \quad (18) \qquad (*)$

$21 \equiv 3 \quad (18) \qquad (**)$

$$415x \equiv 21 \quad (18)$$

$(*)$ $(**)$

$$\Leftrightarrow 1x \equiv 3 \quad (18)$$

$$\Leftrightarrow x \equiv 3 \quad (18)$$

$$Sol_{\mathbb{Z}_{18}} = \{[3]_{18}\} \subseteq \mathbb{Z}_{18}$$

$$Sol_{\mathbb{Z}} = [3]_{18} \subseteq \mathbb{Z}$$

FERMAT 1 | $p \in \mathbb{N}$ primo, $a \in \mathbb{Z} \Rightarrow a^p \equiv a \ (p)$

FERMAT 2 | $p \in \mathbb{N}$ primo, $a \in \mathbb{Z}$, $p \nmid a \Rightarrow a^{p-1} \equiv 1 \ (p)$

EULERO | $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a,m)=1 \Rightarrow a^{\varphi(m)} \equiv 1 \ (m)$

REGOLE PER CALCOLARE $\varphi(m)$ |

- $p \in \mathbb{N}$ primo $\quad \varphi(p) = p-1 \quad$ (EULERO = FERMAT 2)
- $p \in \mathbb{N}$ primo, $m \in \mathbb{N}$ $\quad \varphi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1)$
- $m \in \mathbb{N}$ qualsiasi $\quad m = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ SCOMPOSIZIONE IN PRIMI

$$\varphi(m) = \varphi(p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_r^{\alpha_r})$$

⑦ $3^{16}x \equiv 2^{18}\,3 \quad (17)$

FERMAT 1: $a = 2 \quad p = 17$

$$2^{17} \equiv 2 \quad (17)$$

$$2^{18} = 2^{17+1} = 2^{17} \cdot 2$$

$$2^{18} \equiv 2 \cdot 2 \quad (17)$$

$$\boxed{2^{18} \equiv 4 \quad (17)} \qquad (*)$$

FERMAT 2: $a = 3 \quad p = 17 \qquad 17 \nmid 3$

$$3^{17-1} \equiv 1 \quad (17)$$

$$\boxed{3^{16} \equiv 1 \quad (17)} \qquad (**)$$

$$3^{16}x \equiv 2^{18} \cdot 3 \quad (17)$$

(*) (**)

$$1 \cdot x \equiv 4 \cdot 3 \quad (17)$$

$$x \equiv 12 \quad (17)$$

$$Sol_{\mathbb{Z}_{17}} = \{[12]_{17}\} \subseteq \mathbb{Z}_{17}$$

$$Sol_{\mathbb{Z}} = [12]_{17} \subseteq \mathbb{Z}$$

(8) $2x \equiv 3^{24} \cdot 24 \quad (23)$

$$\boxed{24 \equiv 1 \quad (23)} \quad (*)$$

FERMAT 1 $\quad a = 3 \quad p = 23$

$$3^{23} \equiv 3 \quad (23)$$

$$3^{24} = 3^{23+1} = 3^{23} \cdot 3$$

$$3^{24} \equiv 3 \cdot 3 \quad (23)$$

$$\boxed{3^{24} \equiv 9 \quad (23)} \quad (**)$$

$$2x \equiv 3^{24} \cdot 24 \quad (23)$$

(*) (**)

$$2x \equiv 9 \cdot 1 \quad (23)$$

$$2x \equiv 9 \quad (23)$$

$(2, 23) = 1$

ESISTE UN'UNICA SOLUZIONE IN $\mathbb{Z}_{23}$

$$Sol_{\mathbb{Z}_{23}} = \{ [16]_{23} \} \subseteq \mathbb{Z}_{23}$$

$$Sol_{\mathbb{Z}} = [16]_{23} \subseteq \mathbb{Z}$$

(9) $x \equiv 190^{592} \quad (17)$

$190 = 11 \cdot 17 + 3$

$\boxed{190 \equiv 3 \quad (17)} \quad (*)$

$$(*)\ \begin{cases} x \equiv 190^{592} \quad (17) \\ x \equiv 3^{592} \quad (17) \end{cases}$$

FERMAT 2: $a = 3 \quad p = 17 \quad 17 \nmid 3$

$3^{17-1} \equiv 1 \quad (17)$

$3^{16} \equiv 1 \quad (17)$

$592 = 37 \cdot 16$

$3^{592} = 3^{16 \cdot 37} = (3^{16})^{37}$

$3^{592} \equiv 1^{37} \quad (17)$

$\boxed{3^{592} \equiv 1 \quad (17)} \quad (**)$

$$(**)\ \begin{cases} x \equiv 3^{592} \quad (17) \\ x \equiv 1 \quad (17) \end{cases}$$

$Sol_{\mathbb{Z}_{17}} = \{ [1]_{17} \} \subseteq \mathbb{Z}_{17}$

$Sol_{\mathbb{Z}} = [1]_{17} \subseteq \mathbb{Z}$

(10) $X \equiv 4^{68} \quad (23)$

FERMAT 2: $a = 4 \quad p = 23 \qquad 23 \nmid 4$

$$4^{23-1} \equiv 1 \quad (23)$$

$$4^{22} \equiv 1 \quad (23)$$

$$68 = 3 \cdot 22 + 2$$

$$4^{68} = 4^{22 \cdot 3 + 2} = (4^{22})^3 \cdot 4^2$$

$$4^{68} \equiv 1^3 \cdot 4^2 \quad (23)$$

$$\underline{4^{68} \equiv 16 \quad (23)} \qquad (*)$$

(*) $X \equiv 4^{68} \quad (23)$

$X \equiv 16 \quad (23)$

$$Sol_{\mathbb{Z}_{23}} = \{ [16]_{23} \} \subseteq \mathbb{Z}_{23}$$

$$Sol_{\mathbb{Z}} = [16]_{23} \subseteq \mathbb{Z}$$

11 $\quad X \equiv 523^{321} \quad (100)$

$$523 = 5 \cdot 100 + 23$$

$$\boxed{523 \equiv 23 \quad (100)} \quad (*)$$

(*) $X \equiv 523^{321} \quad (100)$

$X \equiv 23^{321} \quad (100)$

EULERO $\quad a = 23 \quad m = 100 \quad (23,100) = 1$

$$23^{\varphi(100)} \equiv 1 \quad (100)$$

$$\varphi(100) = \varphi(2^2 5^2) = \varphi(2^2)\varphi(5^2) = (2^2-2)(5^2-5) =$$
$$= (4-2)(25-5) = 2 \cdot 20 = 40$$

$$23^{40} \equiv 1 \quad (100)$$

$$321 = 8 \cdot 40 + 1$$

$$23^{321} = (23^8)^{40}\, 23$$

$$23^{321} \equiv 1^{40} \cdot 23 \quad (100)$$

$$\boxed{23^{321} \equiv 23 \quad (100)} \quad (**)$$

(**) $X \equiv 23^{321} \quad (100)$

$X \equiv 23 \quad (100)$

$$Sol_{\mathbb{Z}_{100}} = \{[23]_{100}\} \subseteq \mathbb{Z}_{100}$$

$$Sol_{\mathbb{Z}} = [23]_{100} \subseteq \mathbb{Z}$$

(12) $x \equiv 362971^{29345} \quad (6)$

$362971 = 60495 \cdot 6 + 1$

$\boxed{362971 \equiv 1 \quad (6)}$ (*)

$x \equiv 362971^{29345} \quad (6)$

(*) $x \equiv 1^{29345} \quad (6)$

$x \equiv 1 \quad (6)$

$Sol_{\mathbb{Z}_6} = \{[1]_6\} \subseteq \mathbb{Z}_6$

$Sol_{\mathbb{Z}} = [1]_6 \subseteq \mathbb{Z}$

(13) $x \equiv 29345^{362971} \quad (6)$

$29345 = 4890 \cdot 6 + 5$

$\boxed{29345 \equiv 5 \quad (6)}$ (*)

$x \equiv 29345^{362971} \quad (6)$

(*) $x \equiv 5^{362971} \quad (6)$

EULERO $a = 5, \ m = 6 \quad (5,6) = 1$

$5^{\varphi(6)} \equiv 1 \quad (6)$

$\varphi(6) = \varphi(2 \cdot 3) = \varphi(2)\varphi(3) = (2-1)(3-1) = 1 \cdot 2 = 2$

$5^2 \equiv 1 \quad (6)$

$$362971 = 181485 \cdot 2 + 1$$

$$5^{362971} = (5^2)^{181485} \, 5$$

$$5^{362971} \equiv 1^{181485} \cdot 5 \quad (6)$$

$$\underline{\left| \, 5^{362971} \equiv 5 \quad (6) \right.} \qquad (**)$$

$$x \equiv 5^{362971} \quad (6)$$

(**)

$$x \equiv 5 \quad (6)$$

$$Sol_{\mathbb{Z}_6} = \{ [5]_6 \} \subseteq \mathbb{Z}_6$$

$$Sol_{\mathbb{Z}} = [5]_6 \subseteq \mathbb{Z}$$