

ALGEBRA E MATEMATICA DISCRETA

Corsi di laurea : Informatica

Svolgimento degli esercizi per casa 2

I L'indice, se basta

1) L'inverso di 7 modulo 10

II $\text{NCD}(7, 10) = 1 \Rightarrow [7]_{10}^{-1}$.

III Caccia al rimanendo di:

$$7x \equiv 1 \pmod{10}$$

a b n

$$\exists \alpha, \beta \in \mathbb{Z} \mid 1 = \alpha a + \beta n$$

$d = b$ x_0 multiplo di n

$$x_0 = d q = d$$

$d = b \Rightarrow q = 1$

$$\begin{aligned} a &= 7 \\ n &= 10 \end{aligned} \Rightarrow \quad 10 &= 7 \cdot 1 + 3 \quad \Rightarrow \boxed{3 = 10 - 7} \\ &\uparrow \quad \uparrow \quad \uparrow \quad \uparrow \\ n & \quad a \quad q_1 \quad d \end{aligned}$$

$$\begin{aligned} 7 &= 3 \cdot 1 + 1 \quad \Rightarrow \quad 1 = 7 - 3 \cdot 1 = 7 - (10 - 7) \cdot 1 = \\ a &\uparrow \quad \uparrow \quad \uparrow \quad \uparrow \\ q_2 & \quad d \end{aligned}$$

$$\begin{aligned} &= 7 - 10 \cdot 1 + 7 \cdot 1 = \\ &= 7 \cdot 2 - 10 \cdot 1 \end{aligned}$$

$$\Rightarrow \quad 1 = 7 \cdot 3 + 10 \cdot (-2) \quad \Rightarrow x_0 = 3$$

$a \uparrow \quad \uparrow \quad \uparrow \quad \uparrow \quad \uparrow$
 $q_1 \quad d \quad q_2 \quad d \quad m$

IV $[7]_{10}^{-1} = [3]_{10}$

2) L'inverso di 4 modulo 10

NON ESISTE perché $\text{NCD}(4, 10) = 2 \neq 1$.

3) L'inverso di 6 modulo 15

NON ESISTE perché $\text{NCD}(6, 15) = 3 \neq 1$.

4) L'inverso di 8 modulo 15

I) $\text{MCD}(8, 15) = 1 \Rightarrow \exists [8]_{15}^{-1}$

II) Cercare x_0 soluzione di $8x \equiv 1 \pmod{15}$

$$\exists \alpha, \beta \in \mathbb{Z} \mid 1 = \alpha a + \beta b$$

$$\begin{aligned} \left. \begin{array}{l} a=8 \\ m=15 \end{array} \right\} \Rightarrow 15 &= 8 \cdot 1 + 7 \\ &\uparrow \quad \uparrow \quad \uparrow \quad \uparrow \\ &n \quad a \quad q_1 \quad r \\ 8 &= 7 \cdot 1 + 1 \\ &\uparrow \quad \uparrow \quad \uparrow \\ &z_1 \quad q_2 \quad z_2=d \end{aligned} \Rightarrow \boxed{7 = 15 - 8} \quad \begin{aligned} 1 &= 8 - 7 = 8 - (15 - 8) = \\ &\frac{1}{=} 8 - 15 + 8 = \\ &= 8 \cdot 2 - 15 \end{aligned}$$

$$\Rightarrow 1 = 8 \cdot 2 + 15 \cdot (-1) \Rightarrow x_0 = 2$$

III) $[8]_{15}^{-1} = [2]_{15}$

12

Si calcoli il numero degli elementi invertibili di $\mathbb{Z}_{n,k}$: rispett. a:

- 1) $n=3$
- 2) $n=6$
- 3) $n=9$
- 4) $n=12$
- 5) $n=84$
- 6) $n=7^2 \cdot 2^5$

Il numero degli elementi invertibili di \mathbb{Z}_n è $\varphi(n)$, e

- 1) se $n=3$ è $\varphi(n)=\varphi(3)=3-1=2$;
- 2) se $n=6=2 \cdot 3$ è $\varphi(n)=\varphi(6)=6 \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=\cancel{6} \cdot \frac{1}{2} \cdot \cancel{\frac{2}{3}} = 2$
- 3) se $n=9=3^2$ è $\varphi(n)=\varphi(9)=9 \left(1-\frac{1}{3}\right)=\cancel{9} \cdot \frac{2}{3} = 6$
- 4) se $n=12=2^2 \cdot 3$ è $\varphi(n)=\varphi(12)=12 \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=$
 $= \cancel{12} \cdot \frac{1}{2} \cdot \cancel{\frac{2}{3}} = 4$
- 5) se $n=84=2^2 \cdot 3 \cdot 7$ è $\varphi(n)=\varphi(84)=84 \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{7}\right)=$
$$\begin{array}{r} 84 \\ \hline 42 \\ 21 \\ 7 \end{array} \quad | \quad 2 \quad 2 \quad 3$$

 $= \cancel{84} \cdot \frac{1}{2} \cdot \cancel{\frac{2}{3}} \cdot \cancel{\frac{6}{7}} = 12 \cdot 2 = 24$
- 6) se $n=7^2 \cdot 2^5$ è $\varphi(n)=\varphi(7^2 \cdot 2^5)=7^2 \cdot 2^5 \cdot \left(1-\frac{1}{2}\right)\left(1-\frac{1}{7}\right)=$
 $= \cancel{7^2} \cdot 2^5 \cdot \frac{1}{2} \cdot \cancel{\frac{6}{7}} = 7 \cdot 2^5 \cdot 3$

3 ①

Si risolve il sistema

$$\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 10 \pmod{25} \end{cases}$$

b_1 n_1
 b_2 n_2

Poiché $\text{MCD}(n_1, n_2) = \text{MCD}(6, 25) = 1$, per il teorema chese del resto il sistema ha infinite soluzioni intere, tutte nelle stesse classi di congruenza moduli $m = n_1 \cdot n_2 = 6 \cdot 25 = 150$.

Cerchiamo una partigolare soluzione x_0 .

10 fatti

$$x_1 = 2$$

$$x_2 = x_1 + t_2 u_1 \quad \text{con } t_2 \in \mathbb{Z} \text{ t.c.}$$

$$x_1 + t_2 n_1 \equiv 10 \pmod{25}$$

$$2 + t_2 \cdot 6 \equiv 10 \pmod{25}$$

$$6t_2 \equiv 8 \pmod{25}$$

a b n

$$\begin{aligned} \text{MCD}(a, n) = 1 \Rightarrow \exists \alpha, \beta \in \mathbb{Z} \mid \alpha a + \beta n = 1 \quad \} \Rightarrow t_2 = \alpha q \\ b = qd = q \Rightarrow q = b \\ d = 1 \end{aligned}$$

$$25 = 6 \cdot 4 + 1 \Rightarrow 1 = 25 + 6 \cdot (-4)$$

$$\begin{array}{ccccccc} \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ n & a & q_1 & z_1 & d & n & \alpha \end{array}$$

$$\Rightarrow t_2 = \alpha \cdot q = (-4) \cdot 8 = -32 \pmod{n_2 = 25}$$

$$[-32]_{25} = [-32+25]_{25} = [-7]_{25} = [18]_{25}$$

Prendo $t_2 = 18$

e ottengo

$$\begin{aligned} x_2 &= x_1 + t_2 \cdot u_1 = \\ &= 2 + 18 \cdot 6 = \\ &= 2 + 108 = \\ &= 110 \end{aligned}$$

x_2 è lo x_0 che cercavo: le soluzioni del sistema sono tutte gli interi nelle classi di congruenza

$$[x_2]_n = [110]_{150} = \{ 110 + 150k \mid k \in \mathbb{Z} \}$$

20.10.05

$$\left\{ \begin{array}{l} x \equiv 2 \pmod{6} \\ x \equiv 10 \pmod{25} \end{array} \right. \quad \begin{array}{l} b_1 \\ n_1 \\ \rightarrow \\ 6 \\ \rightarrow \\ u_1 \end{array} \quad \begin{array}{l} b_2 \\ n_2 \\ \rightarrow \\ 25 \\ \rightarrow \\ u_2 \end{array}$$

$$\text{NCD}(m_1, u_2) = 1 \Rightarrow \exists \alpha_1, \alpha_2 \in \mathbb{Z} \mid \alpha_1 u_1 + \alpha_2 u_2 = 1$$

e $z = b_2 \alpha_1 u_1 + b_1 \alpha_2 u_2$ è una soluzione del sistema

$$\begin{array}{l} u_1 = 6 \\ u_2 = 25 \end{array} \Rightarrow \begin{array}{l} 25 = 6 \cdot 4 + 1 \\ \uparrow \quad \uparrow \quad \uparrow \quad \uparrow \\ m_2 \quad u_1 \quad q_1 \quad z_1 \end{array} \Rightarrow 1 = 25 \cdot 1 + 6 \cdot (-4) \quad \begin{array}{l} \uparrow \quad \uparrow \quad \uparrow \quad \uparrow \\ m_2 \quad \alpha_2 \quad u_1 \quad \alpha_1 \end{array}$$

$$\begin{aligned} z &= 10 \cdot (-4) \cdot 6 + 2 \cdot 1 \cdot 25 = \\ &= (-40) \cdot 6 + 50 = \\ &= -240 + 50 = \\ &= -190 \end{aligned}$$

L'insieme delle soluzioni del sistema è l'insieme degli interi nelle classi di congruenza

$$\begin{aligned} [z]_n &= [-190]_{150} = [-190 + 150 \cdot 2]_{150} = [110]_{150} = \\ &= \{ 110 + 150k \mid k \in \mathbb{Z} \} \end{aligned}$$

3. ②

$$\left\{ \begin{array}{l} x \equiv 2 \pmod{4} \\ x \equiv 6 \pmod{7} \\ x \equiv 7 \pmod{9} \end{array} \right. \quad \begin{array}{l} b_1 \\ n_1 \\ \rightarrow \\ 4 \\ \rightarrow \\ u_1 \end{array} \quad \begin{array}{l} b_2 \\ n_2 \\ \rightarrow \\ 7 \\ \rightarrow \\ u_2 \end{array} \quad \begin{array}{l} b_3 \\ n_3 \\ \rightarrow \\ 9 \\ \rightarrow \\ u_3 \end{array}$$

$$\begin{array}{l} \text{Pois} \quad \left. \begin{array}{l} \text{MCD}(n_1, n_2) = \text{MCD}(4, 7) = 1 \\ \text{MCD}(n_1, n_3) = \text{MCD}(4, 9) = 1 \\ \text{MCD}(n_2, n_3) = \text{MCD}(7, 9) = 1 \end{array} \right\} \Rightarrow \end{array}$$

per il teorema chese de' resti
il numero ha cifre intere scritte
insieme, tutte moltiplicate
dai coefficienti inversi moduli

$$\begin{aligned} M &= n_1 \cdot n_2 \cdot n_3 = 4 \cdot 7 \cdot 9 = \\ &= 28 \cdot 9 = 252 \end{aligned}$$

Crea una soluzione x_0 del numero

$$x_1 = 2$$

$$x_2 = x_1 + t_2 n_1 \text{ cerca } t_2 \in \mathbb{Z} \text{ tale che}$$

$$x_1 + t_2 n_1 \equiv 6 \pmod{7}$$

$$2 + t_2 \cdot 4 \equiv 6 \pmod{7}$$

$$4t_2 \equiv 6 - 2 \pmod{7}$$

$$4t_2 \equiv 4 \pmod{7}$$

Prendo $t_2 = 1$

$$\begin{array}{l} x_2 = x_1 + t_2 n_1 = \\ = 2 + 1 \cdot 4 = 2 + 4 = 6 \end{array}$$

$$x_3 = x_2 + t_3 n_1 n_2 \text{ cerca } t_3 \in \mathbb{Z} \text{ tale che}$$

$$x_2 + t_3 \cdot n_1 n_2 \equiv 7 \pmod{9}$$

$$6 + t_3 \cdot 4 \cdot 7 \equiv 7 \pmod{9}$$

$$28t_3 \equiv 7 - 6 \pmod{9}$$

$$28t_3 \equiv 1 \pmod{9}$$

$$[28]_q = [28 - 27]_q = [1]_q$$

$$t_3 \equiv 1 \pmod{9}$$

Prendo $t_3 = 1$

$$\begin{array}{l} x_3 = x_2 + t_3 \cdot n_1 n_2 = \\ = 6 + 1 \cdot 4 \cdot 7 = \\ = 6 + 28 = 34 \end{array}$$

x_3 è la soluzione cercata. Dunque le soluzioni dell'equazione sono tutti i numeri interi dell'insieme:

$$[x_3]_m = [34]_{252} = \{34 + 252k \mid k \in \mathbb{Z}\}$$

3 ③ Risolvere il sistema (*)

$$\begin{cases} 2x \equiv 3 \pmod{9} \\ 5x \equiv 1 \pmod{14} \end{cases}$$

1° PASSO

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

Calcolo $d_1 = \text{MCD}(a_1, m_1) = \text{MCD}(2, 9) = 1$

NON HO BISOGNO DI SOSTituIRE LA 1^ CONGRUENZA

Calcolo $d_2 = \text{MCD}(a_2, m_2) = \text{MCD}(5, 14) = 1$

NON HO BISOGNO DI SOSTituIRE LA 2^ CONGRUENZA

2° PASSO

Risolviamo gli congruenze di (*)

\begin{cases} 2x \equiv 3 \pmod{9} \\ 5x \equiv 1 \pmod{14} \end{cases}

Risolviamo la 1^:

$$2x \equiv 3 \pmod{9}$$

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

Cerco α, β :

$$9 = 2 \cdot 4 + 1 \Rightarrow 1 = 9 \cdot 1 + 2 \cdot (-4)$$

UNA SOLUZIONE DELLA 1^ CONGRUENZA E` $\alpha \cdot q = (-4) \cdot 3 = -12$

perciò $[-12]_q = [-12 + 9 \cdot 2]_q = [-12 + 18]_q = [6]_q$

SOSTITUISCO

$$2x \equiv 3 \pmod{9} \text{ CON}$$

$x \equiv 6 \pmod{9}$ ("LA" SOLUZIONE DELLA CONGRUENZA)

Risolvo le 2^a

$$5x \equiv 1 \pmod{14} \rightarrow n$$

a b

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

Cerco α, β :

$$14 = 5 \cdot 2 + 4 \quad \Rightarrow \quad 4 = 14 - 5 \cdot 2$$

$$S = 4 \cdot 1 + 1 \quad \Rightarrow \quad 1 = S - 4 = S - (14 - 5 \cdot 2) =$$

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

$$= S \cdot 3 - 14$$

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

$$d \nearrow \alpha \nearrow 2 \nearrow m \nearrow \beta$$

UNA SOLUZIONE DELLA 2^a CONGRUENZA E' $d \cdot q = 3 \cdot 1 = 3$

SOSTITUISCO $5x \equiv 1 \pmod{14}$ CON

$x \equiv 3 \pmod{14}$ ("LA" SOLUZIONE DELLA CONGRUENZA)

3° PASSAGGIO

Risolvo (***)

$$\left\{ \begin{array}{l} x \equiv 6 \pmod{9} \\ x \equiv 3 \pmod{14} \end{array} \right.$$

b_1
 b_2

Essendo $\text{MCD}(n_1, n_2) = \text{MCD}(9, 14) = 1$, per il teorema cinese dei resti, (***) ha infinite soluzioni intere, tutte nelle stesse classi di congruenza moduli $m = n_1 \cdot n_2 = 9 \cdot 14 = 126$

CERCO UNA SOLUZIONE DI (***)

1° passo

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

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

$$14 = 9 \cdot 1 + 5 \quad \Rightarrow \quad 5 = 14 - 9$$

$$\begin{aligned}
 14 &= 9 \cdot 1 + 5 & \Rightarrow S = 14 - 9 \\
 9 &= 5 \cdot 1 + 4 & \Rightarrow A = 9 - S \\
 S &= 4 \cdot 1 + 1 & \Rightarrow 1 = 5 - 4 = \\
 &\quad \uparrow \quad \uparrow \quad \uparrow & \quad \downarrow \\
 &z_1 \quad z_2 \quad z_3 & = S - (9 - S) = \\
 && \quad \downarrow \\
 && = S - 9 + S = \\
 && \quad \downarrow \\
 && = S \cdot 2 - 9 = \\
 && \quad \downarrow \\
 && = (14 - 9) \cdot 2 - 9 = \\
 && \quad \downarrow \\
 && = 14 \cdot 2 - 9 \cdot 2 - 9 = \\
 && \quad \downarrow \\
 && = 14 \cdot 2 - 9 \cdot 3
 \end{aligned}$$

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

$$z = b_2 \alpha_1 u_1 + b_1 \alpha_2 u_2 = 3 \cdot (-3) \cdot 9 + 6 \cdot 2 \cdot 14 =$$

↓ ↑
 b₂ ↑
 b₁

$$= -81 + 12 \cdot 14 =$$

$$= -81 + 168 = 87$$

le zanzare del notte non tutti gli altri nelle case

$$[2]_m = [87]_{126} = \{87 + 126k \mid k \in \mathbb{Z}\}$$

201100

per trovare una sbarzone d'

$$\left\{ \begin{array}{l} x \equiv 6 \pmod{9} \\ x \equiv 3 \pmod{4} \end{array} \right.$$

$$x_1 = 6$$

$$x_2 = x_1 + k_2 u_1 \stackrel{\text{imposes } k \text{ have } t_2}{=} 3 \text{ mod } 14$$

$$6 + k_2 \cdot 9 \equiv 3 \pmod{14}$$

$$9t_2 \equiv 3-6 \pmod{14}$$

$$9t_2 \equiv -3 \pmod{14}$$

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

$$9t_2 \equiv 11 \pmod{14}$$

PER TROVARE t_2 DEVO RISOLVERE LA CONGRUENZA:

$$9t_2 \equiv 11 \pmod{14} \quad (t_2 \text{ E' L'INCognITA})$$

$$\text{MCD}(a, n) = \text{MCD}(9, 14) = 1 \Rightarrow \begin{cases} \exists \alpha, \beta \in \mathbb{Z} \mid \alpha a + \beta n = 1 \\ 9 = b/\alpha = b \end{cases}$$

Cerco α, β :

$$\begin{aligned} 14 &= 9 \cdot 1 + 5 & \Rightarrow 5 = 14 - 9 \\ 9 &= 5 \cdot 1 + 4 & \Rightarrow 4 = 9 - 5 \\ 5 &= 4 \cdot 1 + 1 & \Rightarrow 1 = 5 - 4 = \\ && = 5 - (9 - 5) = \\ && = 5 - 9 + 5 = \\ && = 5 \cdot 2 - 9 = \\ && = (14 - 9) \cdot 2 - 9 = \\ && = 14 \cdot 2 - 9 \cdot 2 - 9 = \\ && = 14 \cdot 2 - 9 \cdot 3 \end{aligned}$$

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

$$\begin{matrix} d & \uparrow & \uparrow & \uparrow & \uparrow \\ n & & \beta & a & \alpha \end{matrix}$$

Una scrittura di t_2 è $9t_2 \equiv 11 \pmod{14}$ e $\alpha \cdot q = (-3) \cdot 11 = -33$.

$$\text{Scrumo } [-33]_{14} = [-33 + 14 \cdot 3]_{14} = [-33 + 42]_{14} = [9]_{14}$$

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 classi di congruenza

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

3 **4**

Risolvere il sistema

$$\left\{ \begin{array}{l} 2x \equiv 4 \pmod{22} \rightarrow m_1 \\ 3x \equiv 5 \pmod{15} \rightarrow m_2 \end{array} \right.$$

1° PASSAGGIO

Sottrিere tutte le congruenze con congruenze in cui le divisioni restano tutte nelle stesse classi di congruenza

$$\text{Calcolo } \text{MCD}(a_1, m_1) = \text{MCD}(2, 22) = 2 \mid 4 = c_1$$

SOSTITUISCO LA 1ª CONGRUENZA CON

$$\frac{2x}{2} \equiv \frac{4}{2} \pmod{\frac{22}{2}} \quad \text{ovia cm } x \equiv 2 \pmod{11}$$

$$\text{Calcolo } \text{MCD}(a_2, m_2) = \text{MCD}(3, 5) = 3 = d$$

ma $3 \nmid c_2 \Rightarrow$ LA 2ª CONGRUENZA NON HA SOLUZIONI

QUINDI TUTTO IL SISTEMA NON HA SOLUZIONI

3 (5)

Risolvere il sistema di congruenze

$$\left\{ \begin{array}{l} x \equiv 2 \pmod{3} \\ 2x \equiv 4 \pmod{11} \\ 2x \equiv 3 \pmod{10} \end{array} \right.$$

$\alpha_1 = 1$ c_1 m_1
 $\alpha_2 = 2$ c_2 m_2
 $\alpha_3 = 3$ c_3 m_3

1° PASSAGGIO

Sottriamo tutte le congruenze da congruenze in cui

le soluzioni stanno tutte nelle stesse classi d'equivalenza.

Ci dà:

$$\text{MCD}(\alpha_1, m_1) = \text{MCD}(1, 3) = 1 \quad \text{NON HO BISOGNO DI SOSTituIRE LA 1^{\Delta} CONGRUENZA}$$

$$\text{MCD}(\alpha_2, m_2) = \text{MCD}(2, 11) = 1 \quad \text{NON HO BISOGNO DI SOSTituIRE LA 2^{\Delta} CONGRUENZA}$$

$$\text{MCD}(\alpha_3, m_3) = \text{MCD}(2, 10) = 2 = d$$

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

E QUINDI L'INTERO SISTEMA NON HA SOLUZIONE.

3 6 Risolvere il sistema di congruenze

$$(x) \left\{ \begin{array}{l} 3x \equiv 4 \pmod{5} \\ 2x \equiv 4 \pmod{8} \\ x \equiv 2 \pmod{3} \\ a_3 = 1 \end{array} \right.$$

1° PASSAGGIO

Sostituisco tutte le congruenze in congruenze in cui le siano state tutte nelle stesse classi di congruenza

Cubo

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

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

SOSTITUISCO LA 2^{a} CONGRUENZA CON

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

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

2° PASSAGGIO

Risolvendo gli congruenze di

$$(**) \left\{ \begin{array}{l} 3x \equiv 4 \pmod{5} \\ x \equiv 2 \pmod{4} \\ x \equiv 2 \pmod{3} \end{array} \right.$$

Risolvendo la 1^{a}

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

$$\text{MCD}(a, m) = d = 1 \Rightarrow$$

$$\left\{ \begin{array}{l} \exists \alpha, \beta \in \mathbb{Z} \text{ t.c. } \alpha e + \beta n = 1 \\ q = \frac{b}{d} = b \end{array} \right.$$

Cerco α, β :

$$S = 3 \cdot 1 + 2 \Rightarrow 2 = S - 3$$
$$3 = 2 \cdot 1 + 1 \Rightarrow 1 = 3 - 2 = 3 - (S - 3) =$$
$$\vdots \quad \vdots \quad \vdots \quad \vdots$$
$$= 3 - S + 3 =$$
$$= 3 \cdot 2 - S$$
$$\Rightarrow 1 = 3 \cdot 2 + S \cdot (-1)$$
$$\uparrow \uparrow \uparrow \uparrow$$
$$\alpha \alpha m \beta$$

UNA SOLUZIONE DELLA 1^ CONGRUENZA E' $a \cdot q = 2 \cdot 4 = 8$

$$\text{e ricorre } [8]_S = [8 - S]_S = [3]_S$$

SOSTITUISCO

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

$x \equiv 3 \pmod{S}$ ("LA" SOLUZIONE
DELLA CONGRUENZA)

LA 2^ E LA 3^ CONGRUENZA SONO GIÀ RISOLTE

3^ PASSAGGIO

RISOLVO (XXX)

$$\left\{ \begin{array}{l} x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{4} \\ x \equiv 2 \pmod{3} \end{array} \right.$$
$$\begin{array}{l} b_1 \\ b_2 \\ b_3 \end{array} \quad \begin{array}{l} n_1 \\ n_2 \\ n_3 \end{array}$$

$$\text{Eseguo } \text{MCD}(n_1, n_2) = \text{MCD}(5, 4) = 1$$

$$\text{MCD}(n_1, n_3) = \text{MCD}(5, 3) = 1$$

$$\text{MCD}(n_2, n_3) = \text{MCD}(4, 3) = 1$$

per il teorema chese dei resti, (XXX) ha infinite soluzioni;

tutte nelle stesse classi di congruenza moduli

$$m = m_1 \cdot m_2 \cdot m_3 = 5 \cdot 4 \cdot 3 = 60$$

CERCO UNA SOLUZIONE DI (XXX)

$$x_1 = 3$$

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

imposto per avere t_2

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

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

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

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

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

QUESTA CONGRUENZA, NELL'INCognITA t_2 , E' ASUALDENTE
GIÀ RISOLTA, E POSSO PRENDERE $t_2 = 3$

$$x_2 = 3 + 3 \cdot 5 = 3 + 15 = 18 \quad \text{imposto per avere } t_3$$

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

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

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

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

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

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

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

{ l'insieme dei numeri interi
soltanto di $2t_3 \equiv 2 \pmod{3}$
è $[1]_3 = \{1 + 3k | k \in \mathbb{Z}\}$ }

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

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

e' una soluzione del sistema

QUINDI LE SOLUZIONI DEL SISTEMA SONO TUTTI
I NUMERI INTERI NELLA CLASSE DI CONGRUENZA

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