

Esercizio 1

(1)

(i) $\mathbb{R}^2$ piano affine, $RA(0, \varepsilon)$ con coord (x, y)

$$(x_1, y_1) \sim (x_2, y_2) \Leftrightarrow \exists \lambda \in \mathbb{R} \text{ t.c.}$$

$$(x_2, y_2) = (x_1 + \lambda, y_1 - \lambda)$$

riflessiva con $\lambda = 0$

(OK)

simmetrica

$$\left. \begin{aligned} x_2 &= x_1 + \lambda \\ y_2 &= y_1 - \lambda \end{aligned} \right\} \Rightarrow$$

$$x_1 = x_2 - \lambda$$

$$y_1 = y_2 + \lambda = y_2 - (-\lambda) \quad (\text{OK})$$

transitiva

$$x_2 = x_1 + \lambda$$

$$y_2 = y_1 - \lambda$$

$$\text{e } \left\{ \begin{aligned} x_3 &= x_2 + \mu \\ y_3 &= y_2 - \mu \end{aligned} \right.$$

$$\Rightarrow \left\{ \begin{aligned} x_3 &= x_1 + (\lambda + \mu) \\ y_3 &= y_1 - (\lambda + \mu) \end{aligned} \right. \quad (\text{OK})$$

• Classi di equivalenza:

$$(x_1, y_1) \sim (x_2, y_2) \Leftrightarrow x_2 + y_2 = x_1 + y_1$$

Posto $x_1 + y_1 := c \in \mathbb{R} \Rightarrow$

$$[(x_1, y_1)] = \{ (x, y) \in \mathbb{R}^2 \mid x + y = c \}$$

retta affine in $\mathbb{R}^2$
parallela a $x + y = 0$
e passante per $P_1 = (x_1, y_1)$

• Quoziente $\frac{\mathbb{R}^2}{\sim}$: cerco un modello geometrico

$$\frac{\mathbb{R}^2}{\sim} = \mathbb{R}$$

$$[(x, y)] \longrightarrow c = x + y$$

$\Rightarrow$ le classi sono in biiezione
con $c \in \mathbb{R}$, al variare di c .

(ii) $\mathbb{R}^2$ sp. vettoriale con base $E = \{e_1, e_2\}$ (canonica)

$X := \mathbb{R}^2 \setminus \{0\}$ e su X pongo relazione di proporzionalità

$$\underline{v} \sim \underline{w} \Leftrightarrow \exists \lambda \in \mathbb{R}^* \text{ t.c. } \underline{w} = \lambda \underline{v}$$

Oss (1) $\sim$ è banalmente di equivalenza

(2) $\lambda \in \mathbb{R}^* = \mathbb{R} \setminus \{0\}$, perché $0 \notin X$

(3) Abbiamo escluso 0 perché se $\lambda \neq 0 \Rightarrow \lambda \cdot 0 = 0$

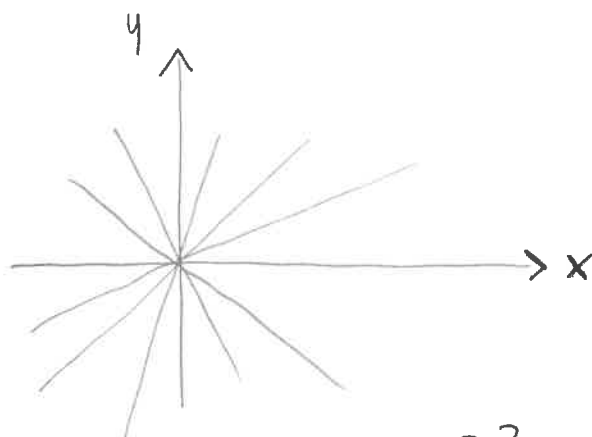
$\sim$ è in relazione solo con se stesso

se non avessi escluso $\lambda = 0 \Rightarrow \forall \underline{v} \in V$ in relazione con $\underline{0} = 0 \cdot \underline{v}$

Perciò $\underline{v} \sim \underline{w} \Leftrightarrow \underline{w} = \lambda \underline{v}, \quad \underline{v}, \underline{w} \in X \text{ e } \lambda \neq 0$

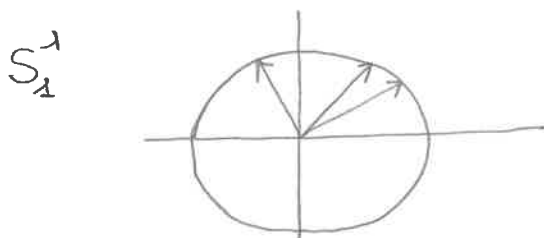
(2)

$$\Rightarrow [\underline{v}] = \text{Span}\{\underline{v}\} \setminus \{0\}$$

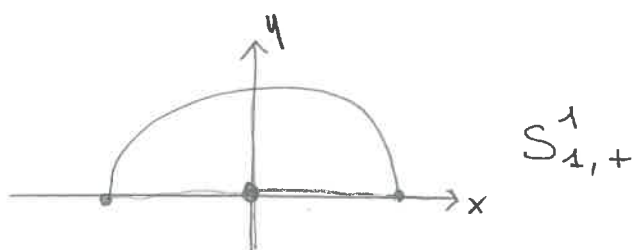


Fascio di rette per $\underline{0} = (0,0) = \mathbb{R}^2 / \sim$

Se $(\mathbb{R}^2, \langle \cdot, \cdot \rangle_{st})$ sostituisco ogni $\underline{v}$ con $\pm \frac{\underline{v}}{\|\underline{v}\|} \Rightarrow$



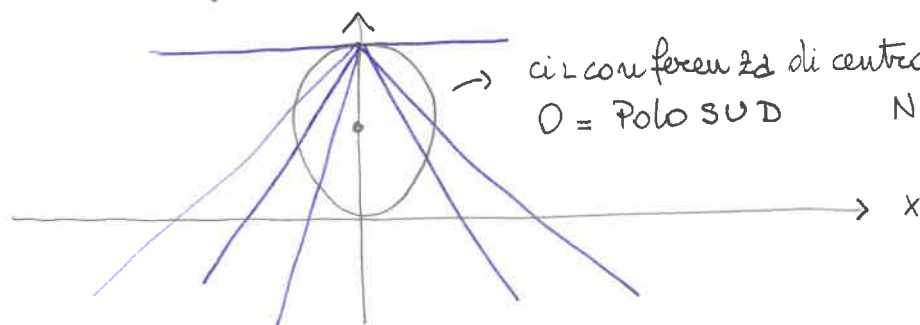
$\frac{\underline{v}}{\|\underline{v}\|} \text{ e } -\frac{\underline{v}}{\|\underline{v}\|}$
ancora in relazione
(anti poles)



$\underline{e}_1 \text{ e } -\underline{e}_1$ ancora da identificare $\rightarrow$ ritrovare S^1

Significato geometrico

$\mathbb{R}^2$ come $\mathbb{H}^2_{\mathbb{R}}$



$\rightarrow$ circonferenza di centro $(0,1)$ e raggio 1
 $O = \text{Polo SUD}$ $N = (1,1) = \text{Polo Nord}$

Proiezione stereografica di S^1 su $\mathbb{R}$ (compattificazione ad un punto di $\mathbb{R}$)

S^1 modello di retta proiettiva che completa retta affine $\mathbb{R}$

(iii) $\mathbb{R}^2$, piano affine, $\mathcal{R}A(0, \varepsilon)$

(3)

$X := \mathbb{R}^2 \setminus \{O = (0,0)\}$ e relazione su X

$$(x_1, y_1) \sim (x_2, y_2) \iff \exists \lambda \in \mathbb{R}_{>0} \text{ t.c.}$$

$$x_2 = \lambda x_1$$

$$y_2 = \lambda^{-1} y_1$$

Osservazioni

1. E' bandamente equivalenza, inoltre

2. x_2, x_1 e y_2, y_1 hanno stesso segno perché $\lambda, \lambda^{-1} \in \mathbb{R}_{>0}$
cioè

(x_1, y_1) in $\begin{matrix} \text{I} \\ \text{II} \\ \text{III} \\ \text{IV} \end{matrix}$ quadrante $\Rightarrow$ lo stesso per (x_2, y_2)

3. Ho tolto $O = (0,0)$ perché in relazione solo con se stesso

Classi di $\sim$ equivalenza

Notiamo che

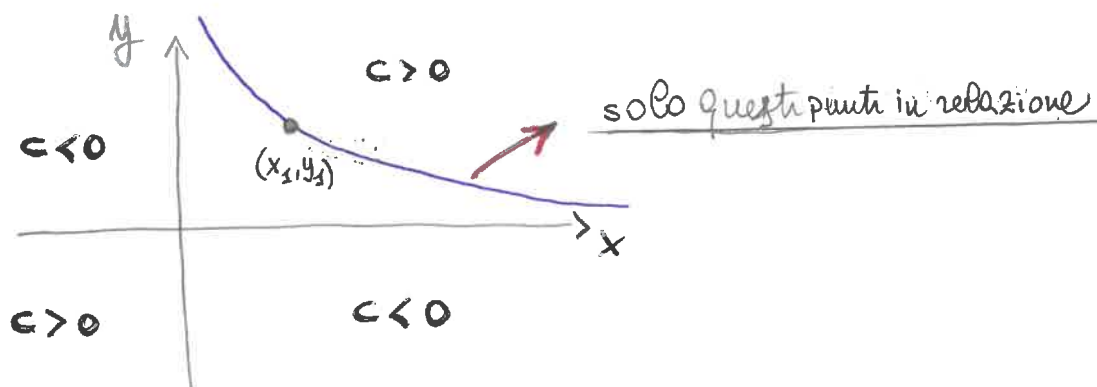
$$(x_1, y_1) \sim (x_2, y_2) \iff x_2 y_2 = x_1 y_1$$

Per $(x_1, y_1) \in X$, posto $x_1 \cdot y_1 := c \in \mathbb{R}$ si ha

Se $c \in \mathbb{R} \setminus \{0\}$

$$[(x_1, y_1)] = \{ (x, y) \in X \mid x \cdot y = c \text{ e } (x, y) \text{ in stesso quadrante di } (x_1, y_1) \}$$

= ramo di iperbole $xy = c = x_1 y_1$ che sta nello stesso quadrante di (x_1, y_1)



Se invece $c = 0$

(4)

$$(x, y) \in X = \mathbb{R}^2 \setminus \{(0, 0)\} \Rightarrow$$

$$xy = 0 \Leftrightarrow \begin{cases} \text{or } x = 0 \text{ e } y \neq 0 \\ \text{or } y = 0 \text{ e } x \neq 0 \end{cases}$$

se $x = 0$ sto prendendo punti sui asse y cioè

$$(0, y_1), (0, y_2) \in \{\text{asse } y\}, \quad y_1, y_2 \neq 0$$

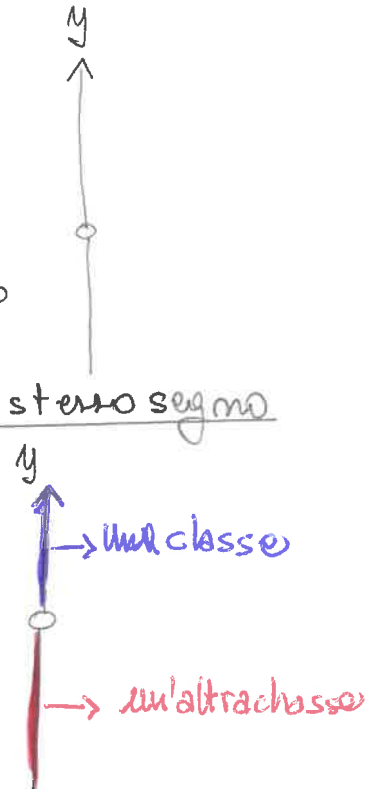
$$(0, y_1) \sim (0, y_2) \Leftrightarrow y_2 = \lambda \cdot y_1, \quad \lambda \in \mathbb{R}_{>0}$$

prendo $\lambda = \frac{y_2}{y_1} \in \mathbb{R}_{>0} \Leftrightarrow y_1, y_2$ obbligatoriamente

Perciò

$$[(0, 1)] = \{(0, y) \mid y \in \mathbb{R}_{>0}\} \Rightarrow$$

$$[(0, -1)] = \{(0, -y) \mid y \in \mathbb{R}_{>0}\}$$



se $y = 0$ analogamente

$$[(1, 0)] = \{(x, 0) \mid x \in \mathbb{R}_{>0}\}$$

$$[(-1, 0)] = \{(-x, 0) \mid x \in \mathbb{R}_{>0}\}$$



Però nessun punto del tipo $(x, 0)$ è in $\sim$ relazione con un punto del tipo $(0, y)$

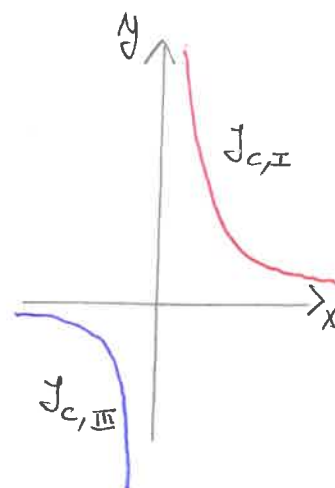
Insieme quoziente modello geometrico
studio applicazione prodotto

(5)

$$\begin{array}{ccc} X & \xrightarrow{\quad \pi \quad} & \mathbb{R} \\ (x, y) & \longmapsto & x \cdot y \end{array}$$

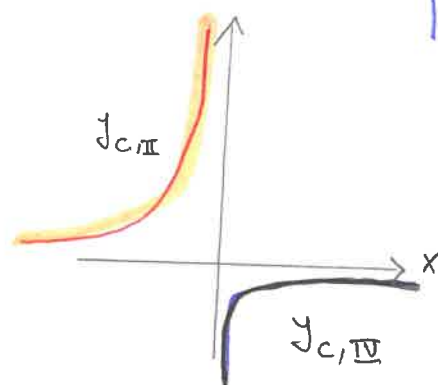
- π suriettiva
- se $c \in \mathbb{R}_{>0}$

$$\pi^{-1}(c) = \{(x, y) \in X \mid x \cdot y = c\} = \underbrace{M_{c, I}}_{\substack{\downarrow \\ \text{una} \\ \text{classe}}} \cup \underbrace{J_{c, III}}_{\substack{\downarrow \\ \text{un'altra} \\ \text{classe}}}$$

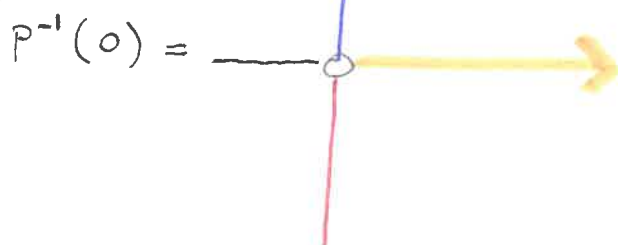


se $c \in \mathbb{R}_{<0}$

$$\pi^{-1}(c) = \underbrace{M_{c, II}}_{\substack{\downarrow \\ \text{una} \\ \text{classe}}} \cup \underbrace{J_{c, IV}}_{\substack{\downarrow \\ \text{un'altra} \\ \text{classe}}}$$



se $c = 0$



4 classi distinte

Per individuare univocamente una classe ho bisogno di:

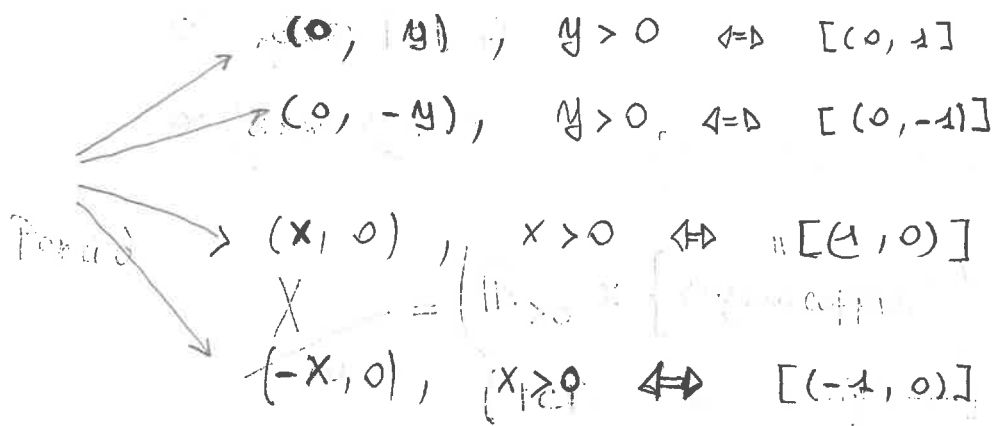
(6)

Se $c \neq 0$

Valore di $|c|$ e segno della coppia (x, y)

$(+, +)$	$xy = c = c , \exists \text{ univ. } (x, y)$
$(+, -)$	$xy = - c , \exists \text{ univ. } (x, y)$
$(-, -)$	$xy = c , \exists \text{ univ. } (x, y)$
$(-, +)$	$xy = - c , \exists \text{ univ. } (x, y)$

Se $c = 0$



Per ciò ponendolo come insieme

$$S := \text{segno coppia} = \{(+, +), (+, -), (-, -), (-, +)\}$$

$$\Rightarrow \frac{X}{\sim} = (\mathbb{R}_{\geq 0} \times S) \quad \text{con } \theta \in S$$

se $c \neq 0$ $\Rightarrow |c| > 0$ e $\theta = (\pm, \pm)$ mi individua quadrante

se $c = 0$ $\Rightarrow$ se $x \neq 0$ allora $\theta = (\pm, \downarrow)$ mi individua semiasse
inutile

se $x = 0 \Rightarrow y \neq 0$ e $\theta = (\downarrow, \pm)$ mi individua semiasse
inutile

(IV) In $\mathbb{R}$ si ha

(7)

$$x \sim y \iff x - y \in \mathbb{Z}$$

$\sim$ è relazione di equivalenza perché proviene dall'azione del gruppo $G = (\mathbb{Z}, +)$ per traslazione interna su $\mathbb{R}$:

$$\begin{aligned} * : \mathbb{Z} \times \mathbb{R} &\longrightarrow \mathbb{R} \\ (m, x) &\longrightarrow x + m \end{aligned}$$

è azione perché

$$\bullet \text{Id}_{\mathbb{Z}} = 0 \text{ e } *(0, x) = x + 0 = x, \forall x \in \mathbb{R}$$

$$\begin{aligned} \bullet *(m+n, x) &= x + (m+n) = (x+m) + n = \\ &= *(n, x+m) = *(n, *(m, x)) \end{aligned}$$

Classi di $\sim$ - equivalenza

$$\forall x \in \mathbb{R}$$

$$[x]_{\sim} = \text{Orbita}_{\mathbb{Z}}(x) = \{x+m \mid m \in \mathbb{Z}\}$$

Quoziente

$$\frac{\mathbb{R}}{\sim} = \frac{\mathbb{R}}{\sim_{\mathbb{Z}}} = [0, 1)$$

equivalentemente

$$S^1 = \{e^{i2\pi\theta} \mid \theta \in [0, 1)\}$$

↓
parametrizzazione
iniettiva di S^1

Svolgimento Es. 2

①

(i) $Z = a_m a_{m-1} a_{m-2} \dots a_0 = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \dots + a_1 \cdot 10 + a_0$ in base 10

Sia $j > 0$ esponente $\Rightarrow$

$$(10^j - 1) = \underbrace{999 \dots 9}_{j \text{ volte}} = 9 \cdot \underbrace{(111 \dots 1)}_{j \text{ volte}}, \text{ i.e. } 3 | 9 | (10^j - 1), \forall j > 0$$

$$\Rightarrow \begin{cases} 10^j - 1 \equiv 0 \pmod{9} \\ 10^j - 1 \equiv 0 \pmod{3} \end{cases} \Rightarrow \boxed{10^j \equiv 1 \pmod{9}} \text{ e anche } \boxed{10^j \equiv 1 \pmod{3}}, \forall j > 0$$

$$\Rightarrow a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \dots + a_1 \cdot 10 + a_0 \equiv a_m \cdot 1 + a_{m-1} \cdot 1 + \dots + a_1 \cdot 1 + a_0$$

$\downarrow$
sia (mod 9)
che (mod 3)

$$\Rightarrow Z \equiv a_m + a_{m-1} + \dots + a_1 + a_0 \pmod{9}$$

• Perciò $9 | Z \Leftrightarrow Z \equiv 0 \pmod{9} \Leftrightarrow a_m + a_{m-1} + \dots + a_1 + a_0 \equiv 0 \pmod{9}$

$$\Leftrightarrow 9 | (a_m + a_{m-1} + \dots + a_1 + a_0)$$

• Analogamente (mod 3)

(ii) Per $\forall j > 0$ $\boxed{10^j \equiv 0 \pmod{2}}$ e $\boxed{10^j \equiv 0 \pmod{5}} \Rightarrow$

$$Z = a_m \cdot 10^m + \dots + a_1 \cdot 10 + a_0 \equiv a_0 \pmod{2, 5}$$

Perciò

$$\begin{aligned} 2 | Z &\Leftrightarrow Z \equiv 0 \pmod{2} \Leftrightarrow a_0 \equiv 0 \pmod{2} \Leftrightarrow 2 | a_0 \\ 5 | Z &\Leftrightarrow Z \equiv 0 \pmod{5} \Leftrightarrow a_0 \equiv 0 \pmod{5} \Leftrightarrow 5 | a_0 \end{aligned}$$

(iii) $10^j = 2^j \cdot 5^j \equiv 0 \pmod{2^k} \Leftrightarrow k \leq j$

Perciò

$$Z = a_m 10^m + \dots + a_{k+1} 10^{k+1} + a_k 10^k + \dots + a_1 10 + a_0$$

$$Z \equiv a_k 10^k + a_{k+1} 10^{k+1} + \dots + a_1 10 + a_0 \pmod{2^k}$$

Per tanto

$$2^k | Z \Leftrightarrow Z \equiv 0 \pmod{2^k} \Leftrightarrow a_k a_{k+1} a_{k+2} \dots a_1 a_0 \equiv 0 \pmod{2^k}$$

$$\Leftrightarrow 2^k | a_k a_{k+1} \dots a_1 a_0$$

(iii) $11 \equiv 0 \pmod{11} \Rightarrow 10 \equiv -1 \pmod{11}$

Ma allora

$$10 = (-1) + 11$$

$$\Downarrow$$

$$10^2 = (1) + 11 \cdot k$$

$$\Downarrow$$

$$10^3 = (-1) + 11k$$

$\vdots$

$$10^{2p} \equiv (+1) \pmod{11}$$

$$10^{2p+1} \equiv -1 \pmod{11}$$

Perciò

$$Z = a_m a_{m-1} a_{m-2} \dots a_1 a_0 = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + a_{m-2} \cdot 10^{m-2} + \dots + a_1 \cdot 10 + a_0$$

$$\equiv a_m (-1)^m + a_{m-1} (-1)^{m-1} + \dots + (-1) a_1 + a_0 \pmod{11}$$

Perciò $11 \mid Z \Leftrightarrow Z \equiv 0 \pmod{11} \Leftrightarrow$

$$a_0 - a_1 + a_2 - a_3 + \dots + (-1)^m \cdot a_m \equiv 0 \pmod{11}$$

$$\Leftrightarrow 11 \mid a_0 - a_1 + a_2 - a_3 + \dots + (-1)^m a_m$$

(iv) $(43816)^{20321} \equiv ? \pmod{10}$

• Notare che

$$43816 - 6 = 43810 \equiv 0 \pmod{10}$$

$$\Rightarrow 43816 \equiv 6 \pmod{10}$$

• $\forall k \geq 1 \quad (43816)^k - 6^k = [(43816) - 6] \cdot [(43816)^{k-1} + \dots + 1] = (43810) \cdot [\dots]$

$$\Rightarrow (43816)^k \equiv 6^k \pmod{10} \quad \forall k \geq 1$$

• Inoltre $k \geq 2 \Rightarrow 6^k - 6 = 6 \cdot (6^{k-1} - 1) \Rightarrow$

$$\begin{cases} 5 \mid (6^{k-1} - 1) = (6-1)(6^{k-2} + \dots + 1), \quad k-1 \\ 2 \mid 6 \end{cases}$$

$$\Rightarrow 10 \mid (6^k - 6) \Rightarrow 6^k - 6 \equiv 0 \pmod{10} \Rightarrow 6^k \equiv 6 \pmod{10}, \quad \forall k$$

• Ma allora

$$(43816)^{20321} \equiv 6^{20321} \equiv 6 \pmod{10} \Rightarrow \text{resto divisione} = 6$$

Svolgimento Es. 3

Ricordo: $a x \equiv b \pmod{m}$ comp. $\Leftrightarrow \text{MCD}(a, m) \mid b$

(1)

(i) $9x \equiv 12 \pmod{18}$

comol. provamente che eq. olisfante

$\text{MCD}(9, 18) = 9 \nmid 12 \text{ in } \mathbb{Z} \Rightarrow$ eq. congruenziale
incompatibile $\Rightarrow$ no soluzioni

(ii) $15x \equiv 27 \pmod{39} \Rightarrow$ una fattorizzazione unica in $\mathbb{Z} \Rightarrow$

$15 = 3 \cdot 5$
 $39 = 3 \cdot 13 \Rightarrow \text{MCD}(15, 39) = 3 \mid 27 = 3^3$

$\Rightarrow$ equazione congruenziale compatibile

E' della forma $a x \equiv b \pmod{m}$ con

$a = 15 = a' \cdot c$
 $b = 27 = b' \cdot c$ dove $\begin{cases} a' = 5 \\ c = 3 \\ b' = 9 \end{cases} \Rightarrow \boxed{a' = 5, b' = 9}$

e $d = \text{MCD}(c, m) = \text{MCD}(3, 39) = 3 = c \Rightarrow m = m' \cdot c$
con $\boxed{m' = 13}$

Perciò si ha equivalentemente

$a x \equiv b \pmod{m} \Leftrightarrow \left(\frac{a}{c}\right) x \equiv \left(\frac{b}{c}\right) \pmod{\left(\frac{m}{c}\right)} \Leftrightarrow a' x \equiv b' \pmod{m'}$

coe

a. $\begin{matrix} a' x \equiv b' \pmod{m'} \\ \downarrow \quad \downarrow \quad \downarrow \\ 5 \quad 9 \quad 13 \end{matrix}$

$\Rightarrow$ risolvo quindi l'equazione congruenziale semplificata

$\boxed{5x \equiv 9 \pmod{13}}$

Cerco $x_0 \in \mathbb{Z}$ t.c. $13 \mid (5x_0 - 9)$, i.e. per cui $\exists h \in \mathbb{Z}$ t.c. $5x_0 - 9 = 13h$
 $\Leftrightarrow 9 = 5x_0 + 13(-h)$

Ora $\text{MCD}(5, 13) = 1 \rightarrow$ cerco iolenti ta' di Bezout per $1 = \text{MCD}(5, 13)$

$\begin{array}{r|l} 13 & 5 \\ \underline{10} & 2 \\ 3 & \end{array} \rightarrow 13 = 5(2) + 3 \text{ (I)}$

$\begin{array}{r|l} 5 & 3 \\ \underline{3} & 1 \\ 2 & \end{array} \rightarrow 5 = 3(1) + 2 \text{ (II)}$

$\begin{array}{r|l} 3 & 2 \\ \underline{2} & 1 \\ 1 & \end{array} \rightarrow 3 = 2(1) + 1 \text{ (III)}$

(2)

$$\begin{aligned} \text{(III)} \rightarrow 1 &= 3(1) + 2(-1) = 3(1) + [5(1) + 3(-1)] \cdot (-1) \\ \text{(II)} \rightarrow 2 &= 5(1) + 3(-1) \quad \text{sostituisco} \quad \downarrow \text{risolvo} \\ 1 &= 3(2) + 5(-1) = 3[13(1) + 5(-2)] + 5(-1) \\ \text{(I)} \rightarrow 3 &= 13(1) + 5(-2) \quad \text{sostituisco} \quad \downarrow \text{risolvo} \\ (*) \quad \boxed{1} &= 13(2) + 5(-5) \quad \text{è una identità di Bezout per } 1 = \text{MCD}(13, 5) \end{aligned}$$

Poiché cerchiamo $x_0 \in \mathbb{Z}$ per cui si abbia

$$g = 5x_0 + 13(-h)$$

Da identità di Bezout $\Rightarrow$ moltiplico per g l'identità (*)

$$\Rightarrow g = 13(18) + 5(-45)$$

Che si rilegge

$$5(-45) - g = 13(-18)$$

$$\Rightarrow x_0 = -45 \quad \text{e} \quad h = -18 \quad \text{sono}$$

$\downarrow$
è una soluzione
di $5x \equiv g \pmod{13}$

$\downarrow$
 $h \in \mathbb{Z}$ che fornisce
 $5x_0 - g = 13h$

$$\boxed{x_0 = -45}$$

è una soluzione particolare di $5x \equiv g \pmod{13}$

Tutte le altre soluzioni di $a'x \equiv b' \pmod{m'}$ sono delle forme

$$\boxed{x = x_0 + h \cdot \left(\frac{m'}{\text{MCD}(a', m')} \right), \quad h \in \mathbb{Z}}$$

Nel nostro caso

$$m' = 13$$

$$a' = 5$$

$$\text{MCD}(13, 5) = 1$$

$\Rightarrow$

$$\boxed{x = -45 + 13h, \quad h \in \mathbb{Z}}$$

tutte le soluzioni in $\mathbb{Z}$ di $a'x \equiv b' \pmod{m'}$

Cerco la prima soluzione "positiva", i.e. per $h \in \mathbb{N}$.

(3)

$$-45 + 13h \geq 0 \quad \text{i.e.} \quad h \geq \frac{45}{13} \sim 3,46$$

per cui mi rivolgo al giusto rappresentante classe resto (mod 13)

$\Rightarrow h_+ :=$ valore che mi dà 1 soluzione positiva

$$= \left\lceil \frac{45}{13} \right\rceil = 4$$

$$\Rightarrow x_0' = -45 + 13 \cdot (4) = -45 + 52 = 7$$

$$x_0' = 7 \quad \underline{\text{è un'altra soluzione di}} \\ 5x \equiv 9 \pmod{13} \quad \text{i.e.} \quad a'x \equiv b' \pmod{m'}$$

(in fatti $5 \cdot 7 - 9 = 35 - 9 = 26 = 13 \cdot 2 \Rightarrow x_0' = 7$ è soluzione)

Posso scrivere tutte le soluzioni in $\mathbb{Z}$ anche utilizzando x_0' , i.e.

$$x = 7 + h \cdot \left(\frac{m'}{\text{HCD}(a', m')} \right) = 7 + 13h, h \in \mathbb{Z}$$

* Se inoltre cerco tutte le incongrue (mod 13)

vuol dire che sto cercando tutte le soluzioni $x \in \mathbb{Z}$ t.c.

$$x = [x] \in \frac{\mathbb{Z}}{13\mathbb{Z}}, \quad \text{i.e.} \quad 0 \leq x \leq 12$$

Ma in $\frac{\mathbb{Z}}{13\mathbb{Z}}$ c'è solo

$$x_0' = 7 \text{ in } \frac{\mathbb{Z}}{13\mathbb{Z}}$$

$\Rightarrow \exists$! soluzioni in fatti le incongrue (mod 13)

sono d soluzioni distinte dove $d = \text{HCD}(a', m') = 1$

$\Rightarrow$! soluzione (mod 13)

$$\begin{aligned} \mathbb{Z}/13\mathbb{Z} \text{ è campo} &\Rightarrow \\ a'x &= b' \text{ in } \mathbb{Z}/13\mathbb{Z} \Rightarrow \\ x &= b' \cdot (a')^{-1} \end{aligned}$$

* Ma invece le soluzioni incongrue (mod 39) di eq. originaria

$$15x \equiv 27 \pmod{39}$$

Sono della forma

$$x = x_0' + h \cdot \left(\frac{39}{\text{HCD}(15, 39)} \right) = 7 + 13h \quad \text{ma con } x \leq 39$$

13 \cdot 3

$$d = \text{HCD}(15, 39) = 3 \Rightarrow \exists 3 \text{ soluzioni incongrue (mod } 39) \quad (4)$$

$$\text{di } 15x \equiv 27 \pmod{39}$$

$$X = 7 + 13h \quad \text{con } h \in \{0, 1, 2 = d-1\}$$

$$\begin{aligned} X'_0 &= 7 \\ X'_1 &= 7 + 13 \cdot 1 = 20 \\ X'_2 &= 7 + 13 \cdot 2 = 33 \end{aligned}$$

3 soluzioni incongrue (mod 39)

equiv. soluzioni in $\mathbb{Z}/39\mathbb{Z}$ di $15 \cdot X = 27$.

(iii) $4x \equiv 8 \pmod{14}$

$$\text{HCD}(14, 4) = 2 \mid 8 \Rightarrow \text{compatibile}$$

Cerco soluzioni di

$$2x \equiv 4 \pmod{7} \quad (\text{stesso ragionamento di (ii)})$$

$$\text{cioè } \exists c \in \mathbb{Z} \mid (2x - 4) \text{ in } 7\mathbb{Z}$$

$1 = \text{HCD}(2, 7)$ quindi l'Id Bezout è ovvia

$$1 = 7(-1) + 2(4)$$

$$\Rightarrow 7 \mid (2x - 4) \Leftrightarrow 2x - 4 = 7h \Leftrightarrow$$

$$4 = 2x + 7(-h) \Rightarrow \text{multiplico (*) per 4}$$

$$4 = 7(4) + 2(-12)$$

$$\Rightarrow x_0 = -12 \text{ è una soluzione in } \mathbb{Z}$$

$\Rightarrow$ ogni altra int. della forma

$$X = -12 + h \cdot \frac{m}{\text{HCD}(a, m)} = -12 + h \cdot \frac{7}{\text{HCD}(2, 7)}, \quad h \in \mathbb{Z}$$

$$\Rightarrow x = -12 + 7h, \quad h \in \mathbb{Z} \quad \text{tutte soluz. in } \mathbb{Z} \quad (5)$$

• Se $h = 2 \Rightarrow x_0' = -12 + 14 = 2$ è prima sol. positiva
 (i.e. t.c. $\bar{2} \in \mathbb{Z}/7\mathbb{Z}$ è soluzione di $\bar{2} \cdot x = \bar{4}$ in $\mathbb{Z}/7\mathbb{Z}$)

$\Rightarrow \forall$ soluzione $\bar{x}$ anche scrivibile

$$x = 2 + 7h, \quad h \in \mathbb{Z}$$

* Se cerco soluzioni in congruenza di $2x \equiv 4 \pmod{7}$
 trovo solo $x_0' = 2$

Però io cerco soluzioni in congruenza $(\pmod{14})$ di

$$\underline{4x \equiv 8 \pmod{14}}$$

cioè

$$x = 2 + 7h \leq 14$$

Abbiamo solo 2 in congruenza $(\pmod{14})$

$$\begin{aligned} x_0 &= 2 \\ x_1 &= 9 \end{aligned}$$

infatti $d = \text{HCD}(14, 4) = 2 \Rightarrow$ solo 2 soluz in congruenza

$\Rightarrow$ in $\mathbb{Z}/14\mathbb{Z}$ l'equazione $\bar{4}x = \bar{8}$ ha queste 2 soluz.

Esercizio 4 svolgimento

(1)

(i) Se $m \in \mathbb{Z}$ pari $\Rightarrow m = 2k, k \in \mathbb{Z} \Rightarrow$

$$m^2 = 4k^2 \Rightarrow m \equiv 0 \pmod{4}$$

Se $m \in \mathbb{Z}$ dispari $\Rightarrow m = 2k+1, k \in \mathbb{Z} \Rightarrow$

$$m^2 = (2k+1)^2 = 4k^2 + 4k + 1 \Rightarrow$$

$$m^2 - 1 = 4(k^2 + k) \Rightarrow m^2 - 1 \equiv 0 \pmod{4}$$

$$\Rightarrow m^2 \equiv 1 \pmod{4}$$

(ii) $m = 2h+1, h \in \mathbb{Z}$

Se h è pari i.e. $h = 2r \Rightarrow$

$$m^2 = (4r+1)^2 = 16r^2 + 8r + 1 \Rightarrow$$

$$m^2 - 1 = 8(2r^2 + r) \Rightarrow 8 \mid m^2 - 1 \Rightarrow m^2 - 1 \equiv 0 \pmod{8} \quad \text{ok}$$

Se h è dispari, i.e. $h = 2r+1 \Rightarrow$

$$m = 2(2r+1)+1 \Rightarrow m^2 = 4(2r+1)^2 + 4(2r+1) + 1$$

$$\Rightarrow m^2 - 1 = 4(4r^2 + 4r + 1) + 4(2r+1)$$

$$= 16r^2 + 16r + 4 + 8r + 4$$

$$= 16r(r+1) + 8(r+1) = 8(r+1)[2r+1]$$

$$\Rightarrow 8 \mid m^2 - 1 \Rightarrow m^2 - 1 \equiv 0 \pmod{8} \quad \text{ok}$$

Svolgimento Es. 5

(1)

(i) $m=11$
 $11 \nmid 11 \Rightarrow \mathbb{Z}/11\mathbb{Z}$ è campo in fatti

$\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ è invertibile $\Leftrightarrow \text{HCD}(a, m) = 1$ in $\mathbb{Z}$

$\Rightarrow (\mathcal{U}(\mathbb{Z}/11\mathbb{Z}), \cdot) = (\mathbb{Z}/11\mathbb{Z} \setminus \{\bar{0}\}, \cdot) = \langle \bar{2} \rangle$ ad esempio $\bar{2}$ generatore gruppo moltiplicativo ciclico di ordine 10
 Campo $\Rightarrow$ dominio intero $\Rightarrow$ no zero-divisori $\Rightarrow$ no nilpotenti

$m=15$

$15 = 3 \cdot 5 \Rightarrow \mathbb{Z}/15\mathbb{Z}$ non è campo perché 15 non è primo

$\mathbb{Z}/m\mathbb{Z}$ è campo $\Leftrightarrow \mathbb{Z}/m\mathbb{Z}$ è dominio intero $\Leftrightarrow m \in \mathbb{Z}$ primo

perciò non è dominio intero

$\exists$ zero-divisori e.g. $\bar{3}, \bar{5} \in \mathbb{Z}/15\mathbb{Z} \setminus \{\bar{0}\}$ ma

$$\bar{3} \cdot \bar{5} = \bar{15} = \bar{0} \text{ in } \mathbb{Z}/15\mathbb{Z}$$

Ricordo che

$\bar{m} \in \mathbb{Z}/m\mathbb{Z}$ invertibile $\Leftrightarrow \text{HCD}(m, m) = 1$ in $\mathbb{Z}$

Perciò

$$\mathcal{U}(\mathbb{Z}/15\mathbb{Z}) = \frac{\text{invertibili}}{\text{in } \mathbb{Z}/15\mathbb{Z}} = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\}$$

$$\Rightarrow \mathbb{Z}/15\mathbb{Z} \setminus \mathcal{U}(\mathbb{Z}/15\mathbb{Z}) = \frac{\text{non-invertibili}}{\text{in } \mathbb{Z}/15\mathbb{Z}} = \{\bar{0}, \bar{3}, \bar{5}, \bar{6}, \bar{9}, \bar{10}, \bar{12}\}$$

$$\Rightarrow \frac{\text{zero-divisori}}{\text{in } \mathbb{Z}/15\mathbb{Z}} = \{\bar{3}, \bar{5}, \bar{6}, \bar{9}, \bar{10}, \bar{12}\}$$

Ora

$\bar{x} \in \mathbb{Z}/m\mathbb{Z}$ è nilpotente se

$k = \text{indice nilpotenza}$

$$\bullet \bar{x} \neq \bar{0}$$

$$\bullet \exists k \geq 2 \text{ t.c. } \bar{x}^k = \bar{0} \text{ (k minimo, i.e. } \bar{x}^h \neq \bar{0}, h < k)$$

Pertanto visto che

$$\bar{0} = \bar{x}^k \stackrel{\neq}{=} \bar{x} \cdot \bar{x}^{(k-1)} \Rightarrow$$

$k = \text{indice nilpotenza}$

nilpotente $\Rightarrow$ zero-divisore

Infatti vale il seguente:

$\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ è nilpotente $\Leftrightarrow$ ogni primo $p \in \mathbb{N}$ s.t. $p \mid m$ t.c. $p \mid a$ in $\mathbb{Z}$

dim
($\Rightarrow$) $\bar{a} \neq \bar{0} \in \mathbb{Z}/m\mathbb{Z}$ nilpotente $\Rightarrow \exists k \geq 2$ t.c. $(\bar{a})^k = \bar{0} \Leftrightarrow$

$$\bar{a}^k = \bar{0} \Leftrightarrow m \mid a^k \text{ in } \mathbb{Z}$$

$$\forall p \text{ primo t.c. } p \mid m \Rightarrow p \mid a^k = \underbrace{a \cdot \dots \cdot a}_{k \text{ volte}}$$

$$Ma p \text{ primo} \Rightarrow p \mid a.$$

($\Leftarrow$) Per fattorizzazione unica in $\mathbb{Z}$, sia

$$m := \prod_{i=1}^r p_i^{e_i} \rightarrow \begin{cases} p_i \text{ primi, } 1 \leq i \leq r \\ p_i \neq p_j, \forall i \neq j \in \{1, \dots, r\} \\ e_i > 0, \forall 1 \leq i \leq r \end{cases}$$

Per hp. $p_i \mid a, \forall i \in \{1, \dots, r\} \Rightarrow$ allora a è della forma

$$a = p_1^{f_1} \cdot \dots \cdot p_r^{f_r} \cdot m, \rightarrow \begin{cases} m \in \mathbb{N} \setminus \{0\} \text{ t.c.} \\ \text{HCD}(p_i, m) = 1, \forall 1 \leq i \leq r \\ f_i > 0, \forall 1 \leq i \leq r \end{cases}$$

• Se fosse $f_i \geq e_i, \forall 1 \leq i \leq r \Rightarrow$

$$\begin{aligned} a &= p_1^{f_1} \cdot p_1^{f_1 - e_1} \cdot \dots \cdot p_r^{f_r} \cdot p_r^{f_r - e_r} \cdot m = \\ &= m \cdot (p_1^{f_1 - e_1} \cdot \dots \cdot p_r^{f_r - e_r}) \cdot m \Rightarrow m \mid a \text{ in } \mathbb{Z} \end{aligned}$$

$$\Rightarrow \bar{a} = \bar{0} \text{ in } \mathbb{Z}/m\mathbb{Z}$$

• Possiamo assumere pertanto che si abbia

$$\begin{aligned} f_i &< e_i \text{ per } 1 \leq i \leq t, \text{ per qualche } t \leq r \\ f_j &\geq e_j \text{ per } t+1 \leq j \leq r \text{ eventualmente} \end{aligned}$$

$\Rightarrow$

$$a = \underbrace{p_1^{f_1} \cdot \dots \cdot p_t^{f_t}}_{\substack{\text{esponenti minori} \\ \text{di } e_i, 1 \leq i \leq t}} \cdot \underbrace{p_{t+1}^{f_{t+1}} \cdot \dots \cdot p_r^{f_r}}_{\substack{\text{esponenti} \\ \text{maggiori di } e_j, t+1 \leq j \leq r}} \cdot m$$

Prendiamo il singolo

(3)

$$p_i^{f_i} \quad 1 \leq i \leq t \quad \text{nella fattorizzazione di } a$$

$$p_i^{e_i} \quad 1 \leq i \leq t \quad \text{nella fattorizzazione di } m$$

Se prendo $m_i = \text{mcm}[e_i, f_i] = \frac{e_i \cdot f_i}{\text{MCD}(e_i, f_i)} \Rightarrow e_i \mid m_i$

Ha $m_i = \left(\frac{e_i}{\text{MCD}(e_i, f_i)} \right) \cdot f_i$

Poniamo

$$k_i := \frac{e_i}{\text{MCD}(e_i, f_i)} \in \mathbb{N} \setminus \{0\}$$

$$\Rightarrow m_i = k_i \cdot f_i \quad \text{ma allora} \quad (p_i^{f_i})^{k_i} = p_i^{f_i k_i} = p_i^{m_i}$$

$$= p_i^{e_i \cdot \hat{k}_i} \quad (p_i^{e_i})^{\hat{k}_i}$$

$$\hat{k}_i := \frac{f_i}{\text{MCD}(e_i, f_i)}$$

Prendendo $\{k_1, \dots, k_t\}$ e considerandone il MASSIMO

e.g. $\text{Max} = k_1 \Rightarrow k_1 = k_j + h_j$ per qualche $h_j \geq 0, 1 \leq j \leq t$

$$(p_1^{f_1})^{k_1} = (p_1^{e_1})^{\hat{k}_1}$$

$$(p_2^{f_2})^{k_2} = (p_2^{f_2})^{k_2 + h_2} = (p_2^{f_2 k_2}) \cdot (p_2^{f_2 h_2}) = (p_2^{e_2})^{\hat{k}_2} \cdot (p_2^{f_2})^{h_2}$$

$$(p_j^{f_j})^{k_j} = (p_j^{f_j})^{k_j + h_j} = (p_j^{f_j k_j}) \cdot (p_j^{f_j h_j}) = (p_j^{e_j})^{\hat{k}_j} \cdot (p_j^{f_j})^{h_j}$$

Pertanto trovata potenza che mi dà

$$a^{k_1} = m \cdot m', \quad m' \in \mathbb{Z} \text{ opportuno}$$

$$\Rightarrow m \mid a \Rightarrow \overline{a^{k_1}} = \overline{0} \text{ in } \mathbb{Z}/m\mathbb{Z} \Rightarrow$$

$$(\overline{a})^{k_1} = \overline{0} \text{ in } \mathbb{Z}/m\mathbb{Z} \text{ anche se } \overline{a} \neq \overline{0} \text{ in } \mathbb{Z}/m\mathbb{Z}$$

$\Rightarrow \overline{a}$ nilpotente

Siccome i primi di 15 sono 3 e 5 $\Rightarrow$

(4)

$$\nexists \bar{a} \in (\mathbb{Z}/15\mathbb{Z} \setminus \{0\}) \setminus U(\mathbb{Z}/15\mathbb{Z}), \text{ i.e. } 1 \leq a < 15,$$

tal che a sia divisibile sia da 3 che da 5 $\Rightarrow \mathbb{Z}/15\mathbb{Z}$ privo di nilpotenti

$\Rightarrow$ tutte gli zero-divisori
in $\mathbb{Z}/15\mathbb{Z}$ non sono
nilpotenti

• $M = 27$

$$27 = 3^3 \Rightarrow$$

no campo

no dominio intero

zero-divisori = nilpotenti

Infatti $\mathbb{Z}/27\mathbb{Z} = \mathbb{Z}/3^3\mathbb{Z} \Rightarrow U(\mathbb{Z}/27\mathbb{Z}) = \{\bar{m} \mid 3 \nmid m \in \mathbb{Z}\} \Rightarrow$

i non invertibili sono $\mathbb{Z}/27\mathbb{Z} \setminus U(\mathbb{Z}/27\mathbb{Z}) = \{\bar{x} \mid 3 \mid x \in \mathbb{Z}\}$ e sono

$$\{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{12}, \bar{15}, \bar{18}, \bar{21}, \bar{24}\} \Rightarrow$$

i non invertibili non-nulli sono tutti nilpotenti perché
tutti divisibili per 3.

• $M = 45$

$$45 = 3^2 \cdot 5 \Rightarrow$$

no campo perché 45 non primo

no dominio intero perché no campo

• $\exists$ zero-divisori non nilpotenti

$$\text{e.g. } \bar{3}, \bar{9}, \bar{5}, \bar{25}, \dots$$

• $\exists$ nilpotenti e unici nilpotenti in $\mathbb{Z}/45\mathbb{Z}$

$$\bar{3} \cdot \bar{5} = \bar{15}, \bar{2} \cdot \bar{3} \cdot \bar{5} = \bar{30}$$

$$\text{perché } \begin{cases} a \equiv 0 \pmod{3} \\ a \equiv 0 \pmod{15} \end{cases} \Rightarrow a \equiv 0 \pmod{\text{m.c.m.}(3,15)}$$

$$\Updownarrow \\ a \equiv 0 \pmod{15}$$

$$a = 0, 15, 30$$

$\Rightarrow$ nilpotenti (quindi non nulli) solo $\bar{a} = \bar{15}$ e $\bar{a} = \bar{30}$

Precisamente

Funzione di Eulero

$$|U(\mathbb{Z}/45\mathbb{Z})| = \varphi(45) = \varphi(3^2 \cdot 5) = \varphi(3^2) \cdot \varphi(5) = (3^2 - 3) \cdot 4 = 6 \cdot 4 = 24$$

$$\Rightarrow |\{\text{non invertibili di } \mathbb{Z}/45\mathbb{Z}\}| = 45 - 24 = 21 \Rightarrow \text{to gli enob zero } \bar{0}$$

$$|\{\text{non invertibili non nulli di } \mathbb{Z}/45\mathbb{Z}\}| = 20 \text{ di cui } 2 \text{ nilpotenti e } 18 \text{ zero-divisori non nilpotenti}$$

$$M = 100$$

$$100 = 2^2 \cdot 5^2$$

- no campo
- no dominio integro
- $\exists$ zero divisori non nilpotenti
e.g. $\overline{2}, \overline{4}, \overline{5}, \overline{25}$
- Nilpotenti
 $\overline{10}, \overline{20}, \overline{30}, \overline{40}, \overline{50}, \overline{60}, \overline{70}, \overline{80}, \overline{90}$

$$M = 121$$

$$121 = 11^2$$

- no campo
- no dominio integro
- Poiché $\mathbb{Z}/11^2\mathbb{Z} \Rightarrow$ tutti gli 0-divisori sono nilpotenti

$$M = 127$$

$$127 \text{ primo}$$

$$\Rightarrow \text{campo} = \text{dominio integro}$$

$$\Rightarrow \nexists \text{ zero-divisori } (\Rightarrow \text{pertanto nemmeno nilpotenti})$$

$$M = 143$$

$$143 = 11 \cdot 13$$

- no campo
- no dominio integro
- $\nexists$ nilpotenti
- $\exists$ zero-divisori
e.g. $\overline{11}, \overline{13}, \overline{22}, \dots$ ecc.

(ii) $625 = 5^4 \Rightarrow$ gli elementi di $U(\mathbb{Z}/625\mathbb{Z})$ sono tutti gli $\bar{x} \in \mathbb{Z}/625\mathbb{Z}$ per cui in $\mathbb{Z}$ si abbia

$$\text{HCD}(x, 625) = 1$$

cioè sono i coprimi con 5, $x \in \mathbb{Z}$ t.c. $5 \nmid x$ e $1 \leq x \leq 624$

Ora i multipli non negativi di 5 e $< 5^4$ sono

$$0.5, 1.5, 2.5, \dots, (5^3 - 1) \cdot 5$$

$\Rightarrow$ sono 5^3 elementi totali

$$\Rightarrow |U(\mathbb{Z}/625\mathbb{Z})| = |\mathbb{Z}/625\mathbb{Z}| - |\{\bar{x} \in \mathbb{Z}/625\mathbb{Z} \mid \bar{x} = 5 \cdot \bar{y}, \exists \bar{y} \in \mathbb{Z}/625\mathbb{Z}\}|$$

$$\varphi(5^3) = 5^4 - 5^3 = 5^3(5-1) = 4 \cdot 5^3 = 500$$

Funzione
di Eulero

$\Rightarrow U(\mathbb{Z}/625\mathbb{Z})$ ha 500 elementi

Tra questi 500 elementi, cerco $\bar{x} \in U(\mathbb{Z}/625\mathbb{Z})$ per cui si abbia $x \equiv 1 \pmod{25}$ in $\mathbb{Z}$

Notare che $x \equiv 1 \pmod{25} \Leftrightarrow \exists h \in \mathbb{Z} \text{ t.c. } (x-1) = 25h \Leftrightarrow x + 25(-h) = 1$

$\Leftrightarrow \text{HCD}(x, 25) = 1$; ma $25 = 5^2 \Rightarrow x$ coprimo con 5

x che soddisfa $x \equiv 1 \pmod{25} \Leftrightarrow \text{t.c. automaticamente } \bar{x} \in U(\mathbb{Z}/625\mathbb{Z})$

* Perciò $x \equiv 1 \pmod{25}$ che cerco è $x = 1 + 25h \in \mathbb{Z} \text{ t.c.}$

$$1 \leq 1 + 25h \leq 624$$

$$0 \leq 25h \leq 623$$

$$0 \leq h \leq \left\lfloor \frac{623}{25} \right\rfloor = 24$$

Pertanto abbiamo

$$\boxed{x = 1 + 25h \text{ con } 0 \leq h \leq 24}$$

ho 25 elementi nel sottoinsieme che sto cercando

$$\{x \in U(\mathbb{Z}/625\mathbb{Z}) \mid x \equiv 1 \pmod{25}\} =$$

$$= \left\{ \begin{array}{l} \overline{1}, \overline{26}, \overline{51}, \overline{76}, \overline{101}, \overline{126}, \overline{151}, \overline{176}, \overline{201}, \\ \overline{226}, \overline{251}, \overline{276}, \overline{301}, \overline{326}, \overline{351}, \overline{401}, \overline{426}, \\ \overline{451}, \overline{476}, \overline{501}, \overline{526}, \overline{551}, \overline{576}, \overline{601} \end{array} \right\}$$