

## Esercizio 1

mercoledì 2 dicembre 2020 08:12

**Esercizio 1.** Si consideri l'insieme  $A = \{a, b, c\}$  dotato della seguente operazione:

$$\begin{aligned} a*a &= a, \quad a*b = b, \quad a*c = c, \\ b*a &= b, \quad b*b = b, \quad b*c = c, \\ c*a &= c, \quad c*b = b, \quad c*c = a. \end{aligned}$$

Si verifichi che  $*$  è un'operazione non associativa e non commutativa, ma dotata di un elemento neutro. Si determini tale elemento.

• **Com?**  $\forall a, b, c \in A$

$$a * b = \underset{b}{b} * a, \quad a * c = \underset{c}{c} * a, \quad b * c = \underset{c}{c} * b$$

(esaminare così)  $\checkmark \quad \checkmark \quad \times \quad$  no commutativa

• **Ass?**  $\forall a, b, c \in A$

$$(a * b) * c = \underset{b}{a} * (\underset{c}{b} * c), \quad (c * b) * a = \underset{b}{c} * (\underset{a}{b} * a)$$

(esaminare così)  $c = c \quad \checkmark \quad b = b \quad \checkmark$

non associative

$$\underline{\underline{c * a * c}} = \underset{a}{c} * \underset{a}{a} * c$$

$$(b * c) * c = \underset{c}{b} * (c * c)$$

$a \neq b$   $\times$

•  $\exists$  neutro t.c.  $a * u = u * a = a$ , se per  $u = \underline{a}$ ,  $\forall a, b, c \in A$

$$\begin{aligned} a * a &= a * a = a \\ b * a &= a * b = b \\ c * a &= a * c = c \end{aligned}$$

## Esercizio 2

mercoledì 2 dicembre 2020 08:29

**Esercizio 2.** Dato il gruppo  $(\mathbb{C}^*, \cdot, 1)$ , e fissato un intero  $n \geq 1$  si consideri l'insieme delle radici  $n$ -esime dell'unità:

$$U_n = \{z \in \mathbb{C} : z^n = 1\}.$$

Si verifichi che  $U_n$  è un sottogruppo di  $(\mathbb{C}^*, \cdot, 1)$ .

E' sottogruppo se:

- 1)  $\lambda \in U_n$ , ovvero  $1 \in U_n$     se:  $U_n = \{z \in \mathbb{C} \mid z^4 = 1\}$ , preso  $z = i$  ho  $i^4 = i^2 \cdot i^2 = -1 \cdot (-1) = +1$
- 2)  $\forall a, b \in U_n \rightarrow a \cdot b \in U_n$

Presi  $z_1$  e  $z_2$  entrambi  $\in U_n$  (ovvero  $z_1 = 1$  e  $z_2 = 1$ )

il loro prodotto  $z_1 \cdot z_2 = z_3 \in U_n$ , in quanto  $z_3$  risulta necessariamente 1

es.  $z_1 = i^4$  e  $z_2 = 2+i^2 \rightarrow (i^4)(2+i^2) = 2i^4 + i^6 = 2 + 1 \cdot i^2 = 2 \cdot 1 = 2$   $\text{U}_n$   
 $\downarrow$   $\downarrow$   $n=4$   $n=1$  ( $\text{U}_n$  diversi per non focalizzare su un  $\text{U}_n$  specifico)

- 3)  $\forall a \in U_n \rightarrow a^{-1} \in U_n$ , per gli stessi motivi del 2), preso

$z_1 = i^4$  e  $z_2 = 2+i^2$  ho necessariamente  $a^{-1} \in U_n$ , in quanto l'inverso di 1 è 1  $\in U_n$

$$z_1^{-1} = \frac{1}{i^4} = 1 \quad z_2^{-1} = \frac{1}{2+i^2} = \frac{1}{2-i^2} = 1$$

l'inverso rispetto al prodotto (operazione inversa) è la divisione, quindi:  
Se  $a = e^i$  ( $1 = e^0$ )  $\bullet z$ ,  
 $\therefore e^{-i} = 1/z$ ,

$U_n$  è sottogruppo di  $(\mathbb{C}^*, \cdot, 1)$

### Esercizio 3

mercoledì 2 dicembre 2020 08:47



(TUTTI)

Esercizio 3. Si consideri  $\mathbb{Z}_{100}$ .

- (1) E' vero che se  $\bar{7} \cdot \bar{x} = \bar{7} \cdot \bar{y}$  allora  $\bar{x} = \bar{y}$ ?
- (2) E' vero che se  $\bar{6} \cdot \bar{x} = \bar{6} \cdot \bar{y}$  allora  $\bar{x} = \bar{y}$ ?

$$\mathbb{Z}_{100} = \{\bar{0}, \bar{1}, \dots, \bar{99}\}$$

$$1) \bar{7} \cdot \bar{x} = \bar{7} \cdot \bar{y} \rightarrow \bar{x} \stackrel{?}{=} \bar{y}$$

$$2) \bar{6} \cdot \bar{x} = \bar{6} \cdot \bar{y} \rightarrow \bar{x} \stackrel{?}{=} \bar{y}$$

$$\textcircled{1} \quad 100 \mid \bar{7}(\bar{x} - \bar{y}) \quad \text{allora} \quad \exists k \in \mathbb{Z} \quad \bar{x} - \bar{y} = 100k \quad \text{è multiplo}$$

$$\bar{x} \stackrel{100}{=} \bar{y} \rightarrow \bar{x}'(\bar{x} - \bar{y}) = 100$$

$$\text{ovvero se } \exists k = \bar{x}' \text{ ma } \exists \bar{k} \neq 0 \text{ allora } \bar{x} = \bar{y}$$

$$\text{se } 100 = \bar{k}(\bar{x} - \bar{y}) \quad 100 \neq 0 \text{ dunque } 100 \mid (\bar{x} - \bar{y})$$

$$\text{dunque } \bar{x} = \bar{y}$$

1]  $\bar{7}$  è invertibile in  $\mathbb{Z}_{100}$  ( $\Rightarrow$  si intende rispetto a  $\cdot$ , ovvero  $(\mathbb{Z}_{100}, \cdot, \bar{1})$ )

$$\text{perché } \text{gcd}(7, 100) = 1$$

le somme  
sono tutti invertibili

$$\text{allora } \exists \bar{7}^{-1} \in \mathbb{Z}_{100}$$

$$\bar{7} \cdot \bar{x} = \bar{7} \cdot \bar{y} \rightarrow \bar{7}^{-1} \cdot \bar{7} \cdot \bar{x} = \bar{7}^{-1} \cdot \bar{7} \cdot \bar{y} \rightarrow \bar{1} \cdot \bar{x} = \bar{1} \cdot \bar{y} \rightarrow \bar{x} = \bar{y} \text{ vero}$$

multiplica per uno stesso fattore  
entrambi i membri

2]  $\bar{6}$  non è invertibile in  $\mathbb{Z}_{100}$  perché  $\text{gcd}(6, 100) \neq 1$

non posso usare la tecnica di prima perché  $\nexists \bar{6}^{-1}$  in  $\mathbb{Z}_{100}$

Io posso continuare:

$$\text{scrivo } \bar{x} = \bar{50} + \bar{5} = \bar{5}$$

$$\frac{100}{\text{gcd}} = 50 \quad \hookrightarrow \bar{6} \cdot \bar{x} = \bar{6} \cdot \bar{50} = \bar{300} = \bar{0} = \bar{6} \cdot \bar{5} \quad \text{ma } \bar{x} \neq \bar{5}$$

quindi  $x = y$  falso

## Esercizio 4

mercoledì 2 dicembre 2020 09:02

Esercizio 4. Si consideri  $\mathbb{Z}_{169}$ .

- (1) Determinare, se esiste, l'inverso di  $\bar{15}$ .
- (2) Determinare, se esistono, due elementi distinti  $\bar{x}, \bar{y}$  tali che  $\bar{12} \cdot \bar{x} = \bar{12} \cdot \bar{y}$ .
- (3) Determinare, se esistono, due elementi distinti  $\bar{x}, \bar{y}$  tali che  $\bar{13} \cdot \bar{x} = \bar{13} \cdot \bar{y}$ .

?

$\mathbb{Z}_{169}$  non è primo

$$1) \text{ MCD } (169, 15) : \quad 169 = m \cdot 15 + 4$$

$$15 = 3 \cdot 4 + 3$$

$$4 = 1 \cdot 3 + 1 \rightarrow = \text{MCD}(169, 15) \text{ allora } \bar{15} \text{ invertibile}$$

$$3 = 3 \cdot 1 + 0$$

$$169 \text{ non è primo dunque } \varphi(\bar{15}) = \varphi(13^2) = 13^2 - 13 = 156$$

$$\text{e l'inverso di } \bar{15} \text{ è } \bar{15}^{156-1} = \bar{15}^{155}$$

$$\bar{15} \text{ è invertibile se } \exists y \in \mathbb{Z} \text{ t.c. } \bar{15} \cdot \bar{y} = \bar{1}$$

$$\rightarrow 15 \cdot y = 1 + 169x$$

$$15y - 169x = 1 \text{ equazione di giantea}$$

ottengo  $x$  e  $y$  in funzione di  $n$ ,  $y$  è l'inverso  
naturale fissato

$$2) \quad \bar{x} = \bar{y} \quad \bar{12} \cdot \bar{x} = \bar{12} \cdot \bar{y}$$

$$12 \nu(x-y) = 169 \quad \text{possò trovare } \bar{x} \neq \bar{y} \text{ diverse t.c. ottengo 163}$$

$$\text{ma } 12 \mid 169, \text{ quindi possò avere solo } \bar{x} = \bar{y}$$

$$3) \quad \bar{x} = \bar{y} \quad \bar{13} \cdot \bar{x} = \bar{13} \cdot \bar{y}$$

$$13 \nu(x-y) = 169^{13}$$

$$\nu(x-y) = 13$$

$$\text{possò ottenerlo per } \begin{cases} \bar{x} = \bar{13} \\ \bar{y} = \bar{0} \end{cases} \text{ classi distinte}$$

## Esercizio 5

mercoledì 2 dicembre 2020 09:23

**Esercizio 5.** Calcolare la funzione di Eulero  $\phi(n)$  per  $n = 26, 32, 69, 96, 343, 777$ .

$$1) \quad \varphi(26) \quad 26 \text{ no } p, \quad 26 = 13 \cdot 2 \quad \text{HCD}(13, 2) = 1 \quad \text{allora } \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

$$\varphi(13 \cdot 2) = \varphi(13) \cdot \varphi(2)$$

$$\begin{aligned} & \cdot 13 \text{ e' } p, \quad \varphi(13) = p-1 = 12 \\ & \cdot 2 \text{ e' } p, \quad \varphi(2) = 1 \end{aligned} \quad \rightarrow \varphi(26) = 12 \cdot 1 = \underline{12}$$

$$2) \quad \varphi(32) \quad 32 \text{ no } p, \quad 32 = 16 \cdot 2 \quad \text{HCD}(16, 2) = 8 \neq 1$$

$$\text{allora } 32 = 16 \cdot 2 = \underbrace{(2^4)}_{\text{G.P}} \quad \varphi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right) \quad \text{ha solo un } p \text{ (2)}$$

$$\text{che divide } n$$

$$\rightarrow \varphi(32) = 32 \left(1 - \frac{1}{2}\right) = 32 \cdot \frac{1}{2} = \underline{16}$$

$$3) \quad \varphi(63) \quad 63 \text{ no } p, \quad 63 = 23 \cdot 3 \quad \text{HCD}(23, 3) = 1$$

$$\text{allora } \varphi(63) = \varphi(23 \cdot 3) = \varphi(23) \cdot \varphi(3) = \underline{44}$$

$$\cdot 23 \text{ e' } p, \quad \varphi(23^1) = p-1 = 22$$

$$\cdot 3 \text{ e' } p, \quad \varphi(3^1) = 2$$

$$4) \quad \varphi(36) \quad 36 \text{ no } p, \quad 36 = 32 \cdot 3 = 2^5 \cdot 3 \quad \text{HCD}(32, 3) = 2 \neq 1$$

$$\varphi(36) = 36 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 48 \cdot \frac{2}{3} = \underline{32}$$

$$5) \quad \varphi(343) \quad 343 \text{ no } p, \quad 343 = 7^3 \quad \text{HCD}(13, 7) = 7 \neq 1$$

$$\varphi(343) = 343 \left(1 - \frac{1}{7}\right) = \underline{284}$$

$$6) \quad \varphi(777) \quad 777 \text{ no } p, \quad 777 = 21 \cdot 37 \quad \text{HCD}(777, 21) = 2 \neq 1$$

$$777 = 3 \cdot 7 \cdot 37$$

$$\varphi(777) = 777 \cdot \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{7}\right) \left(1 - \frac{1}{37}\right) = \underline{432}$$

## Esercizio 6

mercoledì 2 dicembre 2020 09:54

**Esercizio 6.** Calcolare  $\bar{9}^{101}$  e  $\bar{7}^{1000}$  in  $\mathbb{Z}_{26}$ .

$$\bullet \quad \bar{9}^{101} = (\bar{3}^2)^{50} \cdot \bar{3} = \bar{3}^{100} \cdot \bar{3} = (\bar{3}^{10})^5 \cdot \bar{3} = \bar{3}^5 \cdot \bar{3} = \bar{243} \cdot \bar{3} = \bar{8} \cdot \bar{3}$$

$$= \bar{81} = \bar{3}$$

Possiamo utilizzare il teorema di Eulero

$$x \in U(\mathbb{Z}_n) \xrightarrow[\text{t.c.d.}(n, x)=1]{} \bar{x}^{\varphi(n)} = 1 \quad \varphi \text{ di Eulero}$$

$$\varphi(26) = 1 \cdot 12 = 12 \quad 26 = 2 \cdot 13$$

$$\forall x \text{ d.c. } \text{t.c.d.}(x, 26) = 1 \quad \text{allora } x^{12} \equiv 1 \pmod{26}$$

$$\bar{7} \text{ e } \bar{3} \text{ sono invertibili in } \mathbb{Z}_{26} \rightarrow \bar{7}^{12} = \bar{3}^{12} = \bar{1}$$

$$\text{Applico la divisione euclidea } 101 = 8 \cdot 12 + 5 \quad (\text{potenza di 12})$$

$$\begin{aligned} \rightarrow \bar{9}^{101} &= \bar{3}^{8 \cdot 12 + 5} = (\bar{3}^{12})^8 \cdot \bar{3}^5 = (\bar{1})^8 \cdot \bar{3}^5 = \bar{3}^5 = \bar{3}^4 \cdot \bar{3} = (\bar{3}^2)^2 \cdot \bar{3} \\ &= (\bar{81})^2 \cdot \bar{3} = (\bar{3})^2 \cdot \bar{3} = \bar{3} \cdot \bar{3} = \bar{81} = \bar{3} \end{aligned}$$

$$\bullet \quad \bar{7}^{1000} = (\bar{7}^2)^{500} = \bar{49}^{500} \quad 49/26 \text{ ha resto } 23 \quad = \bar{23}^{500} = \bar{523}^{250} = \bar{3}^{250}$$

$$\rightarrow (\bar{3}^2)^{250} = (\bar{3})^{250} = \bar{3}^{25} = \bar{3}^5 = \bar{243} = \bar{3}$$

$$1000 = 83 \cdot 12 + 4 \quad (\bar{7})^{1000} = (\bar{7}^{12})^{83} \cdot \bar{7}^4 = \bar{1} \cdot \bar{7}^4 = \bar{7}^4 = (\bar{7}^2)^2 = (\bar{49})^2$$

$$= (\bar{523})^2 = \bar{3}$$

## Esercizio 7

mercoledì 2 dicembre 2020 10:07

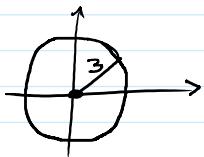
**Esercizio 7.** Provare che l'equazione  $\bar{x}^2 + \bar{y}^2 = \bar{3}$  non ha soluzioni in  $\mathbb{Z}_4$

$$\bar{x}^2 + \bar{y}^2 = \bar{3}$$

$$\mathbb{Z}_4 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3} \}$$

$$\hookrightarrow x^2 + y^2 = 3$$

osservo che qualsiasi sia la classe sostituita a  $\bar{x}$  e  $\bar{y}$ , non posso ottenere  $\bar{3}$ :



- $\bar{0}^2 + \bar{1}^2 \neq \bar{3}$

- $\bar{0}^2 + \bar{3}^2 \neq \bar{3}$

- $\bar{1}^2 + \bar{2}^2 \neq \bar{3}$

In effetti non esistono  $n, m \in \mathbb{Z}$  t.c.  $n^2 + m^2 = 3$

$$y = \pm \sqrt{-x^2 + 3}$$

$$\begin{cases} -x^2 + 3 = y^2 \\ -x^2 + 3 \geq 0 \end{cases} \quad \left\{ \begin{array}{l} x^2 + y^2 - 3 = 0 \\ (x + \sqrt{3})(x - \sqrt{3}) \geq 0 \end{array} \right. \quad \rightarrow \quad -\sqrt{3} \leq x \leq \sqrt{3} \quad (\text{re} \cdot \text{reali})$$

$$\hookrightarrow x^2 \leq 3 \quad \text{per cui l'in quale è il cui quadrato è} \leq 3? \quad \forall n \in \mathbb{Z}$$

## Esercizio 8

mercoledì 2 dicembre 2020 10:23

~~x~~  
Esercizio 8. Provare che per ogni numero intero dispari  $n$  si ha  $n^2 \equiv 1 \pmod{8}$ .

$$\text{Traduco: } (2n+1)^2 = 8 \cdot m + 1 \rightarrow \text{Pongo } x = (2n+1) \quad x \text{ dispari}$$

dispari<sup>2</sup>      provare resto

$$\text{allora } x^2 = 4n^2 + 4n + 1$$

$$= 4n \underbrace{(n+1)}_{\substack{\text{per 2} \\ \text{perci'}}} + 1$$

perci' → perché moltiplicazione  
di numeri consecutivi  
 $(2 \cdot 3 = 6, 10 \cdot 11 = 110 \dots)$

$$\text{allora } 8 \mid 4n(n+1)$$

$$\text{dove } 2 \mid n(n+1)$$

(2 divide un numero pari)

infine  $4 \cdot \text{pari} = \text{pari}$

$$\text{allora } 4n(n+1) \pmod{8} = 0 \quad (\text{resto della divisione per 8})$$

pari (nelle forme  $2n$ )

$$\text{dunque } 4n(n+1) \underbrace{+ 1}_{\text{dispari (nelle forme } 2n+1\text{)}} \pmod{8} = 1^{0+1}$$

(avanza 1 di resto rispetto alla divisione  
resto zero con un pari)

Vede per ogni  $n$  dispari  $\square$

$\mathbb{Z}_n = \{ \bar{0}, \bar{1}, \dots \}$  classe di resti delle div. per  $n$

$$\bar{0} = \{ b \in \mathbb{Z} \mid a \equiv_n b \}$$

$\cup(\mathbb{Z}_n)$  sono i numeri a f.c. t.c.d. ( $a, n$ ) = 1  
el. invertibili

Es  $\mathbb{Z}_6 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5} \}$

$$\text{t.c.d.}(1, 6) = \text{m.c.d.}(5, 6) = 1$$

### Esercizio 9

venerdì 4 dicembre 2020 08:25

**Esercizio 9.** Calcolare le potenze ottave di tutti gli elementi invertibili di  $\mathbb{Z}_{15}$ .

$\mathbb{Z}_{15}, n = 15$  per essere invertibile  $\text{rgd}(x, 15) = 1$

$$\mathbb{Z}_{15} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{14}\}$$

$$\begin{aligned} 15 &= 3 \cdot 4 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 2 \cdot 1 + 1 \end{aligned}$$

$$\begin{aligned} 16 &= 1 \cdot 13 + 2 \\ 13 &= 6 \cdot 2 + 1 \\ 6 &= 6 \cdot 1 + 0 \end{aligned}$$

Elementi invertibili:  $\bar{4}$  e  $\bar{13}$

dunque:

$$\bar{4}^8 = \overline{65.536} = \overline{604} = \bar{14} \quad \bar{4}^8 = \bar{1}$$

$$\bar{13}^8 = \overline{815.730.721} = \bar{1} \quad \bar{13}^8 = \bar{1}$$

de  $\mathbb{Z}_n$  deve  $n = 15$ :

$$\varphi(n) = \varphi(15) = 8 \text{ in } \mathbb{Z}_{15}$$

$$[x]^{\varphi(n)} = 1$$

in  $\mathbb{Z}_n$

→ dunque ogni classe elevata alla 8 ( $= \varphi(15)$ ) fa 1:

$$[x]^8 = \bar{1}$$

quindi ogni classe di el. invertibili di  $\mathbb{Z}_{15}$

## Esercizio 10

venerdì 4 dicembre 2020 08:53

**Esercizio 10.** Provare che  $\bar{5}$  è invertibile in  $\mathbb{Z}_{48}$  e determinare il suo inverso.

$$\text{MCD}(5, 48) : \quad 48 = 3 \cdot 5 + 3$$

$$3 = 1 \cdot 3 + 0$$

$$3 = 1 \cdot 2 + 1 = \text{MCD}(5, 48) \quad \text{allora } \bar{5} \text{ e' invertibile per Eulero}$$

$$2 = 2 \cdot 1 + 0$$

$$[5]^{-1} = \bar{5}^{\varphi(48)-1} = 5^{\varphi(48)-1} = \bar{5}^{15}$$

$$\varphi(48) = \varphi(6 \cdot 8) \quad \text{MCD}(6, 8) = 2 \neq 1$$

$$48 = 2^4 \cdot 3$$

$$\varphi(48) = 48 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 16$$

## Esercizio 11

venerdì 4 dicembre 2020 09:13

**Esercizio 11.** Calcolare il resto della divisione di  $13^{98}$  per 17.

Si chiede di trovare  $x$  in  $13^{98} \equiv x \pmod{17} \rightarrow \mathbb{Z}_{17}$

ovvero  $\text{rcd}(13^{98}, 17) = x$

dividendo la base per 17

$$\text{allora } 13^{98} = ((13^2)^7)^2 = (4^2)^2 = 16$$

$$16 \equiv x \pmod{17} \rightarrow 16 \equiv 1 \pmod{17}$$

$$\text{rcd}(16, 17) = 1$$

$$17 = 1 \cdot 16 + \underline{1}$$

$$16 = 16 \cdot 1 + 0$$

## Esercizio 12

venerdì 4 dicembre 2020 09:25

**Esercizio 12.** Sia  $f : \mathbb{Z}_{1000} \rightarrow \mathbb{Z}_{1000}$  la funzione definita da  $f(\bar{x}) = \bar{7} \cdot \bar{x}$ . Provare che  $f$  è surgettiva.

$$\forall \bar{y} \in \mathbb{Z}_{1000} \quad \exists \bar{x} \in \mathbb{Z}_{1000} : \bar{y} = f(\bar{x}) \quad \text{allora surgettiva}$$

$$f(\bar{x}) : \mathbb{Z}_{1000} \rightarrow \mathbb{Z}_{1000}$$

$$\bar{x} \mapsto \bar{7} \cdot \bar{x}$$

$$\text{allora } \forall \bar{k} \in \mathbb{Z}_{1000} \quad \exists \bar{x} \in \mathbb{Z}_{1000} \text{ t.c.}$$

$$\bar{7} \cdot \bar{x} = \bar{k} \iff 7x \equiv k \pmod{1000}$$

$$\iff 7x - k \equiv 0 \pmod{1000}$$

$$\text{allora } 7x - k \text{ e' divisibile per 1000} : \quad 1000 \mid 7x - k$$

$$\text{allora } \forall k \quad \exists x \text{ t.c. } 7x - k = 1000, \text{ equivale a:}$$

$$\text{RCD}(7, -1) = 1 \quad \text{e } 1 \mid 1000, 1 \mid \forall k \in \mathbb{Z}$$

dunque qualiasi sia  $k$  l'equazione diagona la soluzione (  $f(\bar{x})$  surgettiva )

$$\begin{cases} \text{RCD}(1000, 7) : & 1000 = 142 \cdot 7 + 6 \\ & 7 = 1 \cdot 6 + 1 \end{cases}$$

allora  $\bar{7}$  e' invertibile

$$\begin{aligned} &\text{ci significa che } \bar{7} \cdot (\bar{7})^{-1} = 1 \\ &\text{e } \bar{7} \cdot (\bar{7})^{-1} \cdot \bar{6} = \bar{6} \quad \forall \bar{6} \in \mathbb{Z}_{1000} \quad | \\ &\qquad\qquad\qquad \hookrightarrow \text{surgettiva} \end{aligned}$$

$$\begin{aligned} ax + by &= d \\ \text{se } \text{RCD}(a, b) &\mid d \\ \text{allora le soluzioni} \end{aligned}$$

### Esercizio 13

venerdì 4 dicembre 2020 09:30

**Esercizio 13.** Si consideri il gruppo  $(\mathbb{Z}, +, 0)$ . Il sottoinsieme  $10\mathbb{Z} \cup 15\mathbb{Z}$  è un sottogruppo? E il sottoinsieme  $10\mathbb{Z} \cap 15\mathbb{Z}$ ?

$$\bullet (\mathbb{Z}, +, 0) \supseteq 10\mathbb{Z} \cup 15\mathbb{Z} \quad H$$

1)  $0 \in H \checkmark$

2)  $\forall a, b \in H \rightarrow a + b \in H$

$$10\mathbb{Z} = \{0, 10, 20, \dots\}$$

$$15\mathbb{Z} = \{0, 15, 30, \dots\}$$

$$20 + 15 = 35 \notin H$$

non e' un sottogruppo del gruppo dato

3)  $\forall a \in H \rightarrow a^{-1} \in H$  es. dato  $a^{-1} = -a$  (rispetto alla somma)  $\in H$

$$\bullet (\mathbb{Z}, +, 0) \supseteq 10\mathbb{Z} \cap 15\mathbb{Z} \quad N$$

1)  $0 \in N \checkmark$

2)  $\forall a, b \in N \rightarrow a + b \in N \checkmark$

$$30 + 0 = 30 \in N$$

$$60 + 30 = 150 \in N$$

$$80 + 30 = 120 \in N$$

$$N = \{0, 30, 60, 90, 120, 150, \dots\} = 30\mathbb{Z}$$

3)  $\forall a \in N \rightarrow a^{-1} \in N \checkmark$

l'inverso rispetto alla somma + e' la differenza -

dunque  $30^{-1} = -30 \in N$

$$60^{-1} = -60 \in N$$

E' un sottogruppo.

## Esercizio 14

venerdì 4 dicembre 2020 09:43

**Esercizio 14.** Dati due interi  $a, b > 0$  definiamo

$$a\mathbb{Z} + b\mathbb{Z} := \{n \in \mathbb{Z} : n = ar + bs \text{ con } r, s \in \mathbb{Z}\}.$$

Provare che  $a\mathbb{Z} + b\mathbb{Z}$  è un sottogruppo di  $(\mathbb{Z}, +, 0)$  e provare che  $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$  dove  $d = \text{MCD}(a, b)$ .

- $(\mathbb{Z}, +, 0) \supseteq a\mathbb{Z} + b\mathbb{Z} = H$

- 1)  $0 \in H \checkmark$  (dato  $q = 0, r = 0$ )

- 2)  $\forall a, b \rightarrow a + b \in H \checkmark$  e' chiaro perché l'operazione  $a + b$  e' sempre contenuta in  $a\mathbb{Z} + b\mathbb{Z}$  perché  $a + b = a + 0 + b$

- 3)  $\forall a \rightarrow -a \in H \checkmark$  vero, perché negli interi l'inverso delle somme (-)  
e' sempre contenuto

sottogruppo

→ equivale a una diofantica (ha soluzioni  $\forall q, r$  per  $d = ax + by$  dato  $d = \text{MCD}(a, b)$ )

- $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$   $d = \text{MCD}(a, b)$

$$15 = 1 \cdot 10 + 5$$

$$10 = 2 \cdot 5 + 0$$

Provare l'ugualanza con un esempio (se vera allora dovrà valere anche per l'esempio considerato).

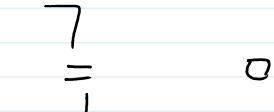
perciò  $a = 10$  e  $b = 15$   $d = 5$

$$10\mathbb{Z} + 15\mathbb{Z} = \{n \in \mathbb{Z} : n = 10r + 15s \text{ con } r, s \in \mathbb{Z}\}$$

$$= \left\{ 0, \frac{-10+15}{25}, 10, 15, 50, 20, \frac{-10+15}{5} \right\}$$

$r=0$	$r=1$	$r=1$	$r=0$	$r=2$	$r=2$	$r=-1$
$s=0$	$s=1$	$s=0$	$s=1$	$s=0$	$s=1$	$s=1$

$$(\text{ordinato}) = \{0, 5, 10, 15, 20, 25 \dots\}$$



$$5\mathbb{Z} = \{0, 5, 10, 15, 20, 25 \dots\}$$



### Esercizio 15

venerdì 4 dicembre 2020 09:55

**Esercizio 15.** Sia  $G$  il gruppo delle applicazioni bigettive da  $\mathbb{Z}$  a  $\mathbb{Z}$  (l'operazione è la composizione). Si consideri il sottoinsieme  $H = \{f \in G : f(n) \geq n \ \forall n \in \mathbb{Z}\}$ . Stabilire se  $H$  è un sottogruppo di  $G$ .

$$G = \{f : \mathbb{Z} \rightarrow \mathbb{Z} \text{ bigettive}\}$$

$$H = \{f \in G : f(n) \geq n \ \forall n \in \mathbb{Z}\} \text{ sono le } f \text{ che rendono l'ordinata maggiore all'escissa}$$

$$1) \lambda \text{ neutro in } G \text{ e } \text{Id} : f \circ \text{Id} = \text{Id} \circ f = f \text{ con } f \in H$$

$$\text{Id} \in H ; \quad \text{Id}(x) \geq x \quad (\text{Id}(x) = x) \quad \checkmark$$

$$2) \forall a, b \in H \rightarrow a + b \in H : \begin{array}{l} f \in H : f(n) \geq n \\ g \in H : g(n) \geq n \end{array} \rightarrow f \circ g \cdot (f \circ g)(n) \geq n ?$$

$$\text{per esempio presa } f = \text{Id} \text{ e } g = n+1 \text{ bigettive e } \in H$$

$$\times \quad g(n) = -n \geq n \text{ no } \forall n, \notin H$$

$$\checkmark \quad g(n) = n+1 \geq n \text{ si } \forall n$$

$$\text{allora } (f \circ g)(n) = f(g(n)) = n+1 \geq n ? \quad \text{si} \quad \checkmark \quad \in H$$

$$\text{vale anche per } g = n-1$$

La proprietà di avere ordinata  $\geq$  esiste viene ereditata dalla funzione composta

per qualsiasi  $f, g \in H$ .

$$3) \forall a \in H \rightarrow a^{-1} \in H$$

$$\text{per } f = \text{Id} \quad f^{-1} = \text{Id} \in H \quad \checkmark$$

$$\begin{array}{ccc} f: & n \mapsto n+1 & \\ f^{-1}: & n+1 \mapsto n & \text{ovvero } (n+1)-1 \\ & \downarrow & \\ & n \mapsto n-1 & \end{array}$$

sempre ho dovuto un  $f^{-1} \in H$

allora  $H$  non è sottogruppo di  $G$

$$\text{infatti } f^{-1}(n+1) = n-1 = n \geq n \quad \checkmark$$

$$\text{ma in generale } f^{-1}(n) = n-1 \neq n \quad \times$$

## Esercizio 16

venerdì 4 dicembre 2020 10:22

**Esercizio 16.** Provare che l'insieme delle applicazioni  $f : \mathbb{R} \rightarrow \mathbb{R}$  che si possono scrivere come  $f(x) = ax + b$  per qualche  $a, b \in \mathbb{R}$ ,  $a \neq 0$  forma un sottogruppo del gruppo delle applicazioni bigettive da  $\mathbb{R}$  a  $\mathbb{R}$  (con l'operazione di composizione).

$$G = \{ f : \mathbb{R} \rightarrow \mathbb{R} \text{ bigettive} \}$$

$$H = \{ f : \mathbb{R} \rightarrow \mathbb{R} \mid f(x) = ax + b \text{ per qualche } a, b \in \mathbb{R} \wedge a \neq 0 \}$$

$$1) \exists e \text{ Id}, \text{ Id}(x) = x = ax + b \text{ si per } a=1, b=0 \checkmark$$

$$2) \forall f, g \in H \rightarrow f \circ g \in H$$

$$f = \text{Id} \in H$$

$$g = n+1 \quad g(x) = x+1 = ax+b \text{ si per } a=1, b=1 \in H$$

$$\text{allora } f \circ g \in H? \rightarrow (f \circ g)(x) = f(g(x)) = f(g(x)) = \text{Id}(x+1) = x+1 = ax+b \in H \checkmark \\ \text{si, con } a=1, b=1$$

Significa che la composizione eredita le proprietà delle singole funzioni

$$\text{più in generale se } f(x) = ax + b \text{ e } g(x) = cx + d$$

(funzioni che modificano il numero reale)

$$(f \circ g)(x) = f(g(x)) = f(cx+d) = c(cx+d) + b = cx^2 + cd + b \\ = \underbrace{cx^2}_{a'} + \underbrace{cd + b}_{b'} \quad \text{otteniamo ancora un numero reale nella forma } ax + b$$

quindi ogni  $f \circ g \in H$

$$3) \forall f \in H \rightarrow f^{-1} \in H$$

$$f = \text{Id} \quad f^{-1} = \text{Id} \in H \checkmark$$

$$f = n+1 \quad f^{-1} = n-1 \in H$$

$$\rightarrow f^{-1}(x) = x-1 = ax + b \text{ si per } a=1, b=-1 \checkmark$$

In effetti qualunque  $a \in \mathbb{R}$  contenente  $x$  (perché sceso  $x$  over  $a=0$  ma in  $H$   $a \neq 0$ )

può essere scritto nella forma  $ax + b$  per certi  $a, b \in \mathbb{R}$ ,  $a \neq 0$

come ad esempio  $x+1$  per  $a=b=1$ ,  $-\frac{1}{2}x+6$  per  $a=-\frac{1}{2}$  e  $b=6$

Dunque qualunque  $f$  che opera sul numero reale trasformando in un altro

numero contenente  $x$  (nella forma  $ax + b$ ),  $\in H$  ( $f$  e  $f^{-1}$  vengono quindi inverse)  
Lo chiamo inverso su

poiché sono soddisfatte le 3 condizioni.

H c'è un sottogruppo di  $G$ .