

es: dimostrare che $\forall z \in \mathbb{Z}$:
 $z^3 - z$ è divisibile per 6

• $z > 0 \rightsquigarrow z \in \mathbb{N}$

$z = 1$: $z^3 - z = 1^3 - 1 = 0$ divisibile per 6 ✓

$z > 1$, supponiamo la proprietà vera per z .
Calcoliamo

$$\begin{aligned}(z+1)^3 - (z+1) &= \cancel{z^3} + 3z^2 + 3z + \cancel{1} - z - \cancel{1} \\ &= \underbrace{z^3 - z}_{\text{divisibile per 6}} + \boxed{3z(z+1)} \\ &\quad \text{per ipotesi induttiva}\end{aligned}$$

z pari, $z = 2m \rightsquigarrow \begin{aligned} &3z(z+1) \\ &6m(z+1) \end{aligned}$
divisibile per 6 ✓

z dispari $\Rightarrow z+1$ pari, $z+1 = 2n$
 $\rightsquigarrow \begin{aligned} &3z(z+1) \\ &6nz \end{aligned}$
divisibile per 6

Se $z = 0$ ✓

Se $z \leq -1 \rightsquigarrow -z$ è t.c. $(-z)^3 - (-z)$
è divisibile per 6 ✓

ALGORITMO EUCLIDEO DI DIVISIONE

$\forall a \in \mathbb{N}_0, \forall b \in \mathbb{N}, \exists! q, r \in \mathbb{N}_0$ tali che

$$a = bq + r$$

$q = \text{quoziente}$
 $r = \text{residuo}$

con $0 \leq r < b$

oss: b divisore di $a \iff r = 0$

NOTAZIONE: $b|a \iff a = bq$

PRINCIPIO DEL BUON ORDINAMENTO

$S \subseteq \mathbb{N}_0, S \neq \emptyset \implies S$ ammette un primo elemento.

dim: definiamo

$$S = \{a - qb \mid q \in \mathbb{N}_0\} \subseteq \mathbb{N}_0$$

osserviamo che $a = a - 0 \cdot b \implies a \in S$
 $\implies S \neq \emptyset$

S ha un primo elemento, che chiamiamo r :

$$r \in S \implies r = a - qb$$
$$a = qb + r$$

$0 \leq r < b$: $r \geq 0$ per costruzione \checkmark

Se per assurdo $r \geq b \implies r - b \geq 0$ e

$$r - b = (a - qb) - b = a - (q+1)b \in S$$

ma questo contraddice il primo elem
 $\Rightarrow r < b \checkmark$

Per l'unicit , supponiamo che $\exists q'$ e r' t.c.

$$a = q'b + r' \quad 0 \leq r' < b$$

senza perdere in generalit  $q' < q$

$$q - q' > 0$$

$$a = bq + r = bq' + r'$$

$$\Rightarrow b \leq b(q - q') = r - r' < b \quad \underline{\underline{\text{No}}}$$

$$\Rightarrow r = r' \text{ e } q = q' \quad \#$$

INSIEMI FINITI / INFINITI

$$I_n = \{1, 2, \dots, n\} \subseteq \mathbb{N}$$

$n = |I_n|$ = cardinalità (= num. di elt) di I_n

Def: Sia X un insieme - X si dice
FINITO se o $X = \emptyset$ oppure $\exists n \in \mathbb{N}$ t.c.
 $|X| = |I_n|$ (o meglio se $X \approx I_n$)

↑
equipotente

Altrimenti X si dice INFINITO -

$X \approx Y$ se \exists una applicazione $\varphi: X \rightarrow Y$
(X equipotente a Y) } biettiva

Oss: • ogni sottoinsieme di un insieme
finito è finito -

• se X contiene un insieme infinito Y ,
allora anche X è infinito -

Prop: Sia X un insieme, allora se X
è infinito, esiste un'applicazione
iniettiva $\varphi: \mathbb{N} \hookrightarrow X$ -

→

↪
iniettiva

→
suriettiva

(no dim., ci vuole L'ASSIOMA DELLA SCELTA)

Prop: (CRITERIO DI DEDEKIND)

Sia X un insieme - X è infinito \iff

$X \approx Y$ per qualche sottoinsieme proprio $Y \subseteq X$.

[dim: giovedì]

oss: in particolare, per il criterio,
 $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono tutti infiniti.

Def: X insieme è detto:

- numerabile se $X \approx \mathbb{N}$
- al più numerabile se è numerabile o finito
- non numerabile in tutti gli altri casi.

es:

• \mathbb{N} è numerabile

• \mathbb{N}_0 è numerabile

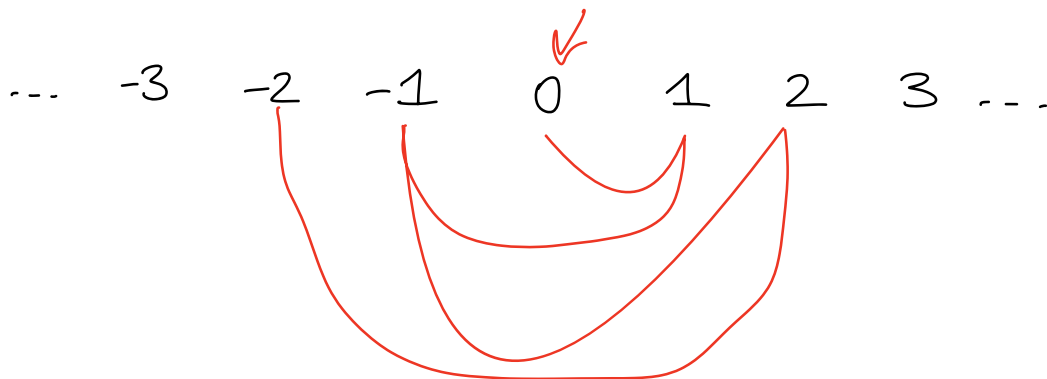
$$q: \mathbb{N}_0 \longrightarrow \mathbb{N}$$
$$n \longmapsto n+1$$

oss: ogni sottoinsieme di un insieme numerabile è al più numerabile.

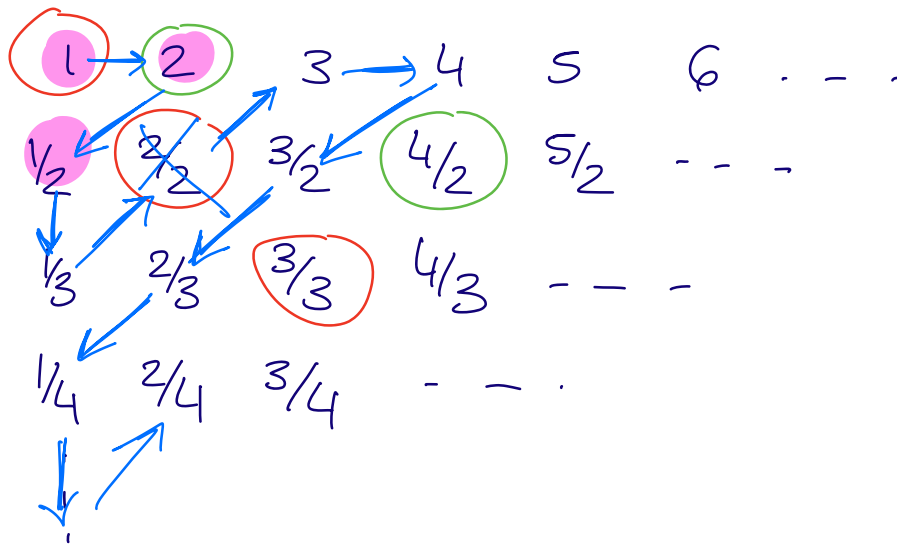
• \mathbb{Z} è numerabile

$$q: \mathbb{N} \longrightarrow \mathbb{Z}$$
$$n=2m \longmapsto m$$

$$n=2m+1 \longmapsto -m$$



- \mathbb{Q} è numerabile



esercizio: (per casa)

- l'unione finita di insiemi numerabili è numerabile
- l'unione numerabile di insiemi numerabili è numerabile

$$\{X_i\}_{i \in \mathbb{N}} \quad \bigcup_{i \in \mathbb{N}} X_i$$

Prop: \mathbb{R} non è numerabile.
(dim. giovedì)