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

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

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

$z > 1$, suppouiamo la proprietá vera per z.
Calcoliamo

$$(z+1)^3 - (z+1) = z^3 + 3z^2 + 3z + \cancel{1} - z - \cancel{1}$$

$$= \underbrace{z^3 - z}_{\text{divisibile per 6 per ipotesi induttiva}} + \boxed{3z(z+1)}$$

z pari, $z = 2m \rightsquigarrow 3z(z+1)$
$\underbrace{6m(z+1)}_{\text{divisibile per 6}}$ ✓

z dispari $\Longrightarrow z+1$ pari, $z+1 = 2n$

$\rightsquigarrow 3z(z+1)$
$\underbrace{6nz}_{\text{divisibile per 6}}$

se $z = 0$ ✓

se $z \leq -1 \rightsquigarrow -z$ é t.c. $(-z)^3 - (-z)$
é 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 = quoziente
r = resto

con $0 \leq r < b$.

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

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

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:

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

$0 \leq r < b$: $\quad r \geq 0$ per costruzione ✓

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 r primo elem

$\Longrightarrow \quad r < b$ ✓

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

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

Senza perdere in generalità $q' < q$

$q - q' > 0$

$$a = \boxed{bq + r = bq' + r'}$$

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

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

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 $\varphi: X \to Y$ biiettiva
(X equipotente a Y)

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 $\varphi: \mathbb{N} \hookrightarrow X$.

$\longrightarrow$ $\hookrightarrow$ iniettiva $\twoheadrightarrow$ suriettiva

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

Prop: (CRITERIO DI DEDEKIND)
Sia X un insieme. X é 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 é detto:
- numerabile se $X \approx \mathbb{N}$
- al più numerabile se é numerabile o finito
- non numerabile in tutti gli altri casi.

es:
- $\mathbb{N}$ é numerabile
- $\mathbb{N}_0$ é numerabile $\qquad \varphi : \mathbb{N}_0 \to \mathbb{N}$, $\quad n \mapsto n+1$

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

- $\mathbb{Z}$ é numerabile $\qquad \varphi : \mathbb{N} \to \mathbb{Z}$

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

$\dots \quad -3 \quad -2 \quad -1 \quad 0 \quad 1 \quad 2 \quad 3 \quad \dots$

• $\mathbb{Q}$ è numerabile

$$
\begin{array}{cccccc}
1 & 2 & 3 & 4 & 5 & 6 \; \ldots \\
1/2 & \cancel{2/2} & 3/2 & 4/2 & 5/2 & \ldots \\
1/3 & 2/3 & 3/3 & 4/3 & \ldots & \\
1/4 & 2/4 & 3/4 & \ldots & & \\
\vdots & & & & &
\end{array}
$$

<u>esercizio:</u> (per casa)

• l'unione finita di insiemi numerabili è numerabile

• l'unione numerabile di insiemi numerabili è numerabile

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

<u>Prop:</u> $\mathbb{R}$ non è numerabile.

(dim. giovedì)