

# Logica e Reti Logiche

## Episodio 1

### Richiami di matematica: dimostrazioni per assurdo

Francesco Pasquale

5 ottobre 2026

Nella prima parte del corso ci occupiamo di *Logica*. Uno degli obiettivi principali della logica è quello di tentare di formalizzare il concetto di *ragionamento*, ossia il modo in cui partendo da delle “premesse” si giunge a delle “conclusioni”. Usiamo varie forme di ragionamento quotidianamente e in particolare lo facciamo ogni volta che cerchiamo di *dimostrare* una affermazione. Ma cos’è esattamente una *dimostrazione*?

Fra qualche lezione vedremo che in opportuni *sistemi formali* è possibile rendere estremamente precisa la nozione di dimostrazione. Per il momento cominciamo ricordando due tecniche di dimostrazione che sono fondamentali in matematica e che vi troverete spesso ad utilizzare nel vostro percorso di studi in informatica: le dimostrazioni *per assurdo* e le dimostrazioni *per induzione*. In questo episodio ci occupiamo delle dimostrazioni per assurdo, nel prossimo ci occuperemo di quelle per induzione.

## 1 Dimostrazioni per assurdo

Per dimostrare “per assurdo” una certa affermazione  $P$ , si assume che sia vera la sua negazione  $\neg P$  e si cerca di giungere a un “assurdo”. L’assurdo può essere di vari tipi: per esempio, assumendo che  $\neg P$  sia *vera* potremmo

1. Riuscire a dimostrare che  $\neg P$  deve essere anche *falsa*;
2. Trovare un’affermazione  $Q$  che risulta sia vera che falsa;
3. Trovare un’affermazione  $Q$  che non può essere né vera né falsa;
4. Trovare un’affermazione  $Q$  tale che  $Q$  è falsa ma anche  $\neg Q$  è falsa;
5. ...

Come esempio di dimostrazione per assurdo, prendiamo la dimostrazione del *Teorema di Cantor*, che dice che non esiste una *corrispondenza biunivoca* fra l’insieme dei numeri naturali  $\mathbb{N}$  e l’insieme delle parti  $\mathcal{P}(\mathbb{N})$ . Prima di farlo però ricordiamoci brevemente qualche concetto che ci servirà.

**Notazioni.** Con  $\mathbb{N}$  indichiamo l’insieme dei numeri naturali,  $\mathbb{N} = \{1, 2, 3, 4, \dots\}$ . Dato un insieme  $A$ , con  $\mathcal{P}(A)$  indichiamo l’insieme di tutti i sottoinsiemi di  $A$ ,  $\mathcal{P}(A) = \{B : B \subseteq A\}$ . Per esempio, se  $A = \{1, 2, 3\}$ , allora

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

**Esercizio 1.** Se l’insieme  $A$  ha  $n$  elementi, quanti elementi ha l’insieme  $\mathcal{P}(A)$ ?

Talvolta l’insieme delle parti di un insieme  $A$  viene indicato anche con  $2^A$ . L’esercizio precedente vi dice perché.

**Funzioni biunivoche.** Dati due insiemi  $X$  e  $Y$  e una funzione  $f : X \rightarrow Y$ , la funzione  $f$  si dice

- *iniettiva*, se non ci sono due elementi di  $X$  che vengono mappati nello stesso elemento di  $Y$ ,

$f$  iniettiva: per ogni  $x, y \in X$ ,  $x \neq y \Rightarrow f(x) \neq f(y)$ ;

- *suriettiva*, se per ogni elemento  $y \in Y$  c'è un elemento di  $X$  che viene mappato in  $y$ ,

$f$  suriettiva: per ogni  $y \in Y$ , esiste  $x \in X$  tale che  $y = f(x)$ ;

- *biunivoca*, se è sia iniettiva che suriettiva.

Dato un insieme  $A$  indichiamo con  $|A|$  il numero dei suoi elementi.

**Esercizio 2.** Siano  $X$  e  $Y$  due insiemi finiti e sia  $f : X \rightarrow Y$  una funzione. Osservare che

1. Se  $f$  è iniettiva, allora  $|X| \leq |Y|$ ;
2. Se  $f$  è suriettiva allora  $|X| \geq |Y|$ .

Dall'esercizio precedente segue che se  $X$  e  $Y$  sono due insiemi finiti e  $f : X \rightarrow Y$  è una funzione biunivoca, allora  $X$  e  $Y$  devono necessariamente avere lo stesso numero di elementi.

Questo modo di mettere in relazione il numero di elementi di due insiemi può essere esteso anche al caso di insiemi infiniti: se riusciamo a trovare una corrispondenza biunivoca fra due insiemi infiniti  $X$  e  $Y$ , allora  $X$  e  $Y$  devono avere lo stesso numero di elementi (nel caso di insiemi infiniti, diciamo più precisamente che hanno la stessa *cardinalità*).

Per esempio, abbiamo visto come sia possibile mettere in corrispondenza biunivoca l'insieme dei numeri naturali  $\mathbb{N}$  con alcuni insiemi che all'apparenza potrebbero sembrare “più grandi” o “più piccoli” di  $\mathbb{N}$ . Per esempio, la funzione  $f : \mathbb{N} \rightarrow \{\text{numeri pari}\}$  definita da  $f(n) = 2n$  è una funzione biunivoca fra l'insieme di tutti i numeri naturali e l'insieme dei numeri pari. Quindi, mentre è vero che l'insieme dei numeri pari è un sottoinsieme *proprio* di  $\mathbb{N}$ ,<sup>1</sup> non è vero che l'insieme dei numeri pari contiene “meno elementi” di quanti ne contiene tutto  $\mathbb{N}$ . Entrambi contengono un numero infinito di elementi, e gli infiniti sono dello stesso ordine.

**Esercizio 3.** Trovare una funzione biunivoca da  $\mathbb{N}$  all'insieme dei numeri dispari.

Allo stesso modo non è difficile trovare delle corrispondenze biunivoche fra  $\mathbb{N}$  e

1. L'insieme di tutti i numeri interi  $\mathbb{Z}$  (positivi, negativi e lo zero);
2. L'insieme di tutte le coppie ordinate di numeri interi;
3. L'insieme di tutti i sottoinsiemi finiti di  $\mathbb{N}$ ;
4. ...

Ma se proviamo a cercare una corrispondenza biunivoca fra  $\mathbb{N}$  e l'insieme di tutti i sottoinsiemi di  $\mathbb{N}$  (finiti e infiniti) non ci riusciamo. Il motivo per cui non ci riusciamo è che una tale corrispondenza non esiste.

**Teorema 1.1** (Cantor, 1891). Non esiste una funzione biunivoca fra  $\mathbb{N}$  e  $\mathcal{P}(\mathbb{N})$ .

*Dimostrazione.* Supponiamo “per assurdo” che esista una tale funzione biunivoca, che ad ogni numero naturale  $n \in \mathbb{N}$  associa un sottoinsieme  $A_n \subseteq \mathbb{N}$ . In particolare avremmo che per ogni sottoinsieme  $S$  di  $\mathbb{N}$  deve esistere un numero naturale  $n$  tale che  $A_n = S$  (perché la funzione è *suriettiva*).

---

<sup>1</sup>Dato un insieme  $A$ , un sottoinsieme  $B \subseteq A$  si dice sottoinsieme *proprio* di  $A$  se c'è qualche elemento di  $A$  che non sta in  $B$ .

Osservate che per ogni numero naturale  $n$ , siccome  $A_n$  è un sottoinsieme di numeri naturali,  $A_n$  può contenere oppure non contenere  $n$  stesso. Consideriamo allora l'insieme  $C$  di tutti i numeri naturali  $n$  tali che  $n$  non appartiene ad  $A_n$ ,

$$C = \{n \in \mathbb{N} : n \notin A_n\} \quad (1)$$

Siccome  $C$  è un sottoinsieme di  $\mathbb{N}$ , allora dovrebbe esistere un numero  $k$  tale  $C = A_k$ . A questo punto chiediamoci se  $k$  appartiene o no a  $C$ .

Se  $k \notin C$  allora  $k \notin A_k$  [perchè  $C = A_k$ ]. Ma se  $k \notin A_k$  allora  $k \in C$  [per la definizione di  $C$  in (1)]. Quindi non può essere che  $k \notin C$ . Ma allora dovrebbe essere  $k \in C$ . Però se  $k \in C$  abbiamo lo stesso problema, perché allora  $k \in A_k$  [perchè  $C = A_k$ ] e quindi  $k \notin C$  [per la definizione di  $C$ ]. Quindi non può essere né che  $k \notin C$  né che  $k \in C$ , che è un assurdo.  $\square$

Ora è il turno vostro di fare un po' di lavoro.

**Esercizio 4.** Dimostrare che i numeri primi sono infiniti.

(Suggerimento: Supponete per assurdo che siano finiti. Siano quindi  $p_1, p_2, \dots, p_n$  tutti i numeri primi. Considerate allora il prodotto di tutti i numeri primi e aggiungete uno:  $p_1 p_2 \cdots p_n + 1$ . Riuscite a trovare una qualche contraddizione su questo numero?)

**Esercizio 5.** Dimostrare che  $\sqrt{2}$  non è un numero razionale.

(Suggerimento: Supponete per assurdo che si possa scrivere  $\sqrt{2} = a/b$  con  $a, b \in \mathbb{N}$  e fate vedere che allora  $a$  e  $b$  devono essere entrambi pari. Quindi...)