SATANA, CANTOR E L'INFINITO

ALBERTO SARACCO

SOMMARIO. Il titolo di questo articolo è direttamente ripreso dal titolo del libro di Smullyan [5] sulla logica e i paradossi matematici. All'ultimo capitolo di questo libro è ispirata in linea di massima la conferenza che ho tenuto su questo tema nel corso dello Stage di matematica per studenti delle superiori, riproposta arricchita in questo articolo.

Satana, Cantor e l'Infinito di Smullyan, come d'altronde tutti i suoi titoli divulgativi, è un'ottima lettura per chi fosse interessato a questi temi. Ne consiglio la versione originale inglese [6].

Nel testo sono presenti alcune domande sull'infinito. Le risposte sono (quasi) sempre fornite nelle note. Prima di leggere le note o di andare avanti col testo, consiglio al lettore di pensare al problema, cercare di risolverlo o almeno di farsi un'idea di quale possa essere la risposta.

Nel corso del testo incontreremo alcuni nomi di matematici importanti per la storia dei concetti di numero e di infinito. Da Cantor (che dà il titolo a questo articolo) a Russell (forse più noto come filosofo e vincitore del premio Nobel) faremo una panoramica dei matematici che a cavallo tra 1800 e 1900 hanno scritto i fondamenti della matematica.

Partiremo da concetti molto elementari con cui ogni lettore dovrebbe essere familiare, come quelli di numero o di corrispondenza biunivoca, per poi inoltrarci nel reame dell'infinito, alzando sempre di più il tiro, fino ad arrivare a parlare dell'ipotesi del continuo e ad accennare la differenza tra numeri cardinali e numeri ordinali. L'ultima sezione, quella sull'ipotesi del continuo è probabile che risulti molto ostica e adatta solo al lettore più esperto.

Se a un certo punto vi perdete, non preoccupatevi: in ogni buona conferenza di matematica i primi cinque minuti devono essere comprensibili a tutti, gli ultimi cinque a nessuno! Scherzi a parte, lo scopo di una conferenza o di un testo divulgativo è quello di incuriosire e offrire spunti di riflessione, di fornire al lettore domande, non (tutte le) risposte.

Spero che queste pagine riescano a incuriosirvi, a spingervi a cercare da voi alcune risposte, e a chiarirvi che giocare con l'infinito è pericoloso, e bisogna usare molta cautela quando lo si fa, perfino se si è il Diavolo in persona.

1. Contare

I numeri naturali $(0, 1, 2, 3, 4, \ldots)$ sono un'astrazione. In origine l'uomo non usava i numeri come enti astratti, ma usava parole diverse per indicare una pecora, due pecore, tre pecore e una mucca, due mucche, tre mucche. Ancora oggi, nelle varie lingue, è rimasta traccia di ciò: un gruppo di animali è, di volta in volta, un gregge (di pecore), una mandria (di mucche), un branco (di lupi), un banco (di pesci)...

È stata una grande conquista per l'uomo quando si è capito che i numeri si potevano astrarre. Così il numero 1 indica semplicemente (la classe di equivalenza di) tutti gli insiemi costituiti da un solo elemento, il numero 2 tutti gli insiemi costituiti da due elementi, e così via[1].

Si narra che i pastori, facendo uscire le pecore dal recinto la mattina, mettessero per ogni pecora che usciva un sassolino in un mucchio. La sera, quando le pecore rientravano, per ogni pecora che rientrava toglievano un sassolino dal mucchio. Così, se a sera non restavano più sassolini nel mucchio, le pecore erano rientrate tutte (le pecore uscite erano tante quanti i sassolini nel mucchio, i quali erano tanti quanti le pecore rientrate). In questo modo, tramite una corrispondenza biunivoca tra insiemi[2], non si sapeva quante pecore erano uscite né quante

[1]La definizione di numero come classe di equivalenza di insiemi equipotenti (cioè con lo stesso numero di elementi) è stata data da Gottlob Frege (matematico e filosofo tedesco, 1848–1925) e Bertrand Russell (matematico e filosofo gallese, vincitore del Nobel per la letteratura, 1872–1970). Sebbene sembri una definizione che si morde la coda, ovvero che utilizza il concetto che pretende di definire (*numero*) nella definizione stessa, la definizione può essere resa precisa.

La prima definizione rigorosa del concetto di numero naturale, per quanto strano possa sembrare, è stata data solo nel 1889 da Giuseppe Peano (1858–1932), matematico torinese. Gli assiomi (di Peano) per i numeri naturali sono i seguenti:

(1) Esiste un numero naturale, 0.
(2) Ogni numero naturale a ha un numero naturale successore, denotato come $S(a)$.
(3) Non esiste un numero naturale il cui successore è 0.
(4) Numeri naturali distinti hanno successori pure distinti: se $a \neq b$, allora $S(a) \neq S(b)$.
(5) (principio di induzione) Se una proprietà P è posseduta dallo 0 ed è posseduta anche dal successore di ogni numero naturale che possiede la proprietà P, allora la proprietà P è posseduta da tutti i numeri naturali.

I numeri naturali sono caratterizzati (a meno di isomorfismo) dagli assiomi di Peano.

Al lettore curioso di sapere i retroscena nella storia dei fondamenti della matematica consiglio senza dubbio il bel romanzo grafico *Logicomix* [4].

[2]Il concetto di corrispondenza biunivoca è appunto ciò che permette di rendere rigorosa la definizione di numero secondo Frege e Russell.

pecore erano rientrate, ma solo se erano rientrate tutte quelle che erano uscite (ed effettivamente era la sola cosa che importasse). Dal nome del sassolino (in latino *calculus*) viene la parola *calcolare*.

Il metodo dei pastori, tuttavia, non funzionerebbe se il gregge di pecore fosse infinito.

2. L'infinito

Ma che cosa vuol dire *infinito*?

Se indichiamo con $\mathbb{N}$ l'insieme dei numeri naturali:

$$\mathbb{N} \;=\; \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \ldots, n, \ldots\}\,,$$

allora possiamo dire che un insieme A si dice *finito* con n elementi ($n \in \mathbb{N}$) se può essere messo in corrispondenza biunivoca con l'insieme

$$I_n \;=\; \{l \in \mathbb{N} \mid l < n\} \;=\; \{0, \ldots, n-1\}\,.$$

Si scrive $|A| = n$ (la *cardinalità* di A è n).

Esiste un solo insieme con 0 elementi, l'insieme che non possiede elementi, detto *insieme vuoto* e indicato con $\emptyset$.

Dati due insiemi finiti A (con a elementi) e B (con b elementi) si ha che A può essere messo in corrispondenza biunivoca con un sottoinsieme di B se e solo se $a \leq b$; A può essere messo in corrispondenza biunivoca con un sottoinsieme proprio di B (cioè diverso da B stesso) se e solo se $a < b$.

Un insieme si dice *infinito* se non è finito con n elementi per nessun $n \in \mathbb{N}$.

Esempio 2.1. *L'insieme* $\mathbb{N}$ *è infinito.*

Infatti, supponiamo per assurdo che $\mathbb{N}$ sia finito con n elementi, e sia $m > n$. L'insieme I_m (dei numeri naturali minori di m) può essere messo in corrispondenza biunivoca con un sottoinsieme di $\mathbb{N}$ (è anzi lui stesso un sottoinsieme di $\mathbb{N}$). Pertanto $m \leq n$, assurdo. Quindi $\mathbb{N}$ è un insieme infinito. □

Gli insiemi infiniti hanno molte proprietà sorprendenti. Ad esempio, togliendo un singolo elemento da un insieme infinito A, questo rimane infinito? Sì, no, perché?[3]

[3]Sì, rimane un insieme infinito. Infatti supponiamo per assurdo che $A \setminus \{a\}$, ovvero l'insieme A privato di un suo elemento a sia finito con n elementi. Allora $A \setminus \{a\}$ è in corrispondenza biunivoca con I_n. Associando ad a il numero n, si ottiene che A è in corrispondenza biunivoca con I_{n+1}, ovvero è finito con $n+1$ elementi. Assurdo, quindi $A \setminus \{a\}$ è infinito. □

Lo stesso ragionamento si applica se togliamo un qualsiasi numero finito di elementi dall'insieme A. A privato di questi elementi resta infinito.

3. L'albergo di Hilbert

Gli insiemi infiniti hanno alcune strabilianti proprietà che li differenziano dagli insiemi finiti a cui siamo abituati. Per esplorarle, vi racconto la storia dell'albergo di Hilbert[4].

In un albergo normale, dove c'è un numero finito di camere, se l'albergo è pieno ed arriva un nuovo ospite, questo non può essere alloggiato.

L'albergo di Hilbert è invece un albergo con infinite camere (numerate consecutivamente dai numeri naturali)[5]. Immaginiamo che l'albergo sia pieno ed arrivi un nuovo ospite. Questa volta possiamo alloggiare il cliente imprevisto. Ci basta infatti spostare il cliente alloggiato nella stanza n nella stanza $n+1$. Così facendo resta vuota la prima camera, che possiamo destinare al nuovo ospite.

Sorprendente, vero? Ma non finisce qui. Supponiamo che, ad albergo pieno, arrivi non un nuovo ospite, ma un pullman infinito, con i posti numerati dai numeri naturali, pieno di nuovi clienti che vogliono alloggiare nell'albergo di Hilbert. Si può fare? E se sì, come?[6]

Supponiamo ora che l'albergo sia vuoto (tanto, ormai l'abbiamo capito, vuoto o pieno cambia poco, in un albergo di Hilbert sembra esserci sempre posto) e che arrivino non uno, ma infiniti autobus (numerati coi numeri naturali) con infiniti posti (numerati coi numeri naturali), tutti pieni di clienti per l'albergo. Riusciremo ad alloggiare tutti? Come?[7]

E se togliamo un numero infinito di elementi? Lo scopriremo in seguito.

[4]David Hilbert (1862–1943), matematico tedesco, è stato forse l'ultimo conoscitore di "tutta la matematica". Sono passati alla storia della matematica i *problemi di Hilbert*, ventitre quesiti molto profondi posti da Hilbert nel corso della Esposizione Universale di Parigi del 1900. I ventitre problemi erano, ad avviso di Hilbert, i problemi con cui si sarebbero dovuti confrontare i matematici del secolo che stava iniziando. Molti dei problemi di Hilbert sono stati risolti, alcuni prima, altri dopo, ma sette ancora resistono gli attacchi dei matematici.

[5]Se la cosa vi lascia perplessi, leggete il bel racconto di fantascienza *L'hotel straordinario o il milleunesimo viaggio di Ion il Tranquillo* di Stanislaw Lem, disponibile tra l'altro nella raccolta [1].

[6]Spostiamo il cliente alloggiato nella camera n nella camera $2n$. Ora sono occupate le camere pari e libere le camere dispari. Possiamo quindi far accomodare il nuovo arrivato seduto sul posto n dell'autobus nella camera $2n+1$. □

[7]Si può fare. Ne diamo due diverse dimostrazioni.

Dimostrazione 1. Notiamo che nel primo posto del primo autobus c'è seduto un solo passeggero: lo alloggiamo nella stanza 1.

Nei primi due posti dei primi due autobus sono a questo punto seduti $3 = 2 \cdot 2 - 1$ passeggeri, e li alloggiamo nelle stanze dalla 2 alla 4.

Nei primi tre posti dei primi tre autobus sono a questo punto seduti $5 = 3 \cdot 3 - 4$

4. Insiemi infiniti più grandi e più piccoli

Tutto quanto scoperto sull'albergo di Hilbert sembra miracoloso, vero? Quanto visto mostra in particolare il fatto che gli insiemi infiniti hanno la bizzarra proprietà di poter essere messi in corrispondenza biunivoca con un proprio sottoinsieme proprio, a differenza degli insiemi finiti.

Questo crea ovviamente dei problemi quando vogliamo definire cosa vuol dire che un insieme A è più piccolo, o contiene meno elementi (o, per dirla in linguaggio matematico, ha cardinalità minore), di un insieme B: $|A| < |B|$.

Se A e B sono finiti abbiamo visto che basta chiedere che

(M) A è in corrispondenza biunivoca con un sottoinsieme proprio di B.

Per insiemi infiniti tale proprietà non basta. Infatti, consideriamo l'insieme dei numeri naturali $\mathbb{N}$ e l'insieme dei numeri pari P

$$P \;=\; \{2n \mid n \in \mathbb{N}\}\,.$$

P è un sottoinsieme proprio di $\mathbb{N}$, ma è anche in corrispondenza biunivoca con tutto $\mathbb{N}$:

$$\mathbb{N} \;\to P: \quad n \mapsto 2n$$

è una tale corrispondenza biunivoca. Inoltre $\mathbb{N}$ è in corrispondenza biunivoca con un sottoinsieme proprio di P (i multipli di 4, Q), tramite la mappa

$$\mathbb{N} \;\to Q: \quad n \mapsto 4n\,.$$

Cosa vuol dire tutto ciò? Se usassimo la nozione valida per gli insiemi finiti, potremmo dedurre che

(1) $|\mathbb{N}| > |P|$;
(2) $|\mathbb{N}| = |P|$;
(3) $|\mathbb{N}| < |P|$.

---

passeggeri, e li alloggiamo nelle stanze dalla 5 alla 9.

E così, dopo $n-1$ passaggi, nei primi n posti dei primi n autobus restano seduti $n^2-(n-1)^2$ passeggeri, e li alloggiamo nelle stanze dalla $(n-1)^2+1$ alla n^2.

Il passeggero seduto nel posto m dell'autobus k viene alloggiato dopo $\max\{m,k\}$ passaggi. Quindi vengono alloggiati tutti, ognuno in una stanza diversa. □

Dimostrazione 2. Ogni passeggero è individuato da due numeri naturali (n,m), dove n individua l'autobus su cui è seduto e m il posto che occupa sull'autobus.

Mandiamo allora il passeggero (n,m) nel posto $2^n \cdot 3^m$. Non solo passeggeri diversi vengono mandati in posti diversi, ma nel nostro albergo restano libere infinite camere, ovvero tutte quelle che hanno un numero che ammette almeno un divisore primo diverso da 2 e 3. □

Ovviamente, se vogliamo che il concetto di cardinalità e quello di maggiore, minore e uguale abbiano un qualche senso, la proprietà (M) non funziona per definire $|A| < |B|$.

Quello che invece va bene è usare la seguente definizione:
$|A| \leq |B|$ *se e solo se* A *è in corrispondenza biunivoca con un sottoinsieme di* B.
Ovviamente ciò implica in particolare, come ci aspettiamo che $A \subset B$ implica $|A| \leq |B|$.
Per quello che abbiamo visto, allora $|\mathbb{N}| \geq |P| \geq |\mathbb{N}|$, ovvero i numeri pari sono tanti quanti i numeri naturali: $|\mathbb{N}| = |P|$.
Per avere il minore stretto dobbiamo avere allora non solo la proprietà (M), ma anche il fatto che B non sia in corrispondenza biunivoca con un sottoinsieme (proprio o meno) di A. Questo secondo fatto, se A è un insieme finito, è conseguenza della proprietà (M), ma non lo è se A è infinito.

5. $\aleph_0$, la cardinalità dell'infinito numerabile

Abbiamo visto la proprietà straordinaria degli insiemi infiniti di poter essere messi in corrispondenza biunivoca con i propri sottoinsiemi. Addirittura questa proprietà è una caratterizzazione degli insiemi infiniti:

Proposizione 5.1. *Un insieme* A *è infinito se e solo se può essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio.*

Una domanda naturale è se esista un infinito solo o più infiniti diversi, ovvero se tutti gli insiemi infiniti sono in corrispondenza biunivoca tra di loro (e quindi con l'insieme dei numeri naturali $\mathbb{N}$) oppure no. In altre parole: dato un qualunque insieme I di clienti arrivi all'albergo di Hilbert, riusciremo sempre ad alloggiarli tutti?
Un insieme infinito che può essere messo in corrispondenza biunivoca con $\mathbb{N}$ si dice *numerabile*.
La questione è dunque: ogni insieme è finito o numerabile? Oppure esistono infiniti non numerabili?
Tale domanda è stata presa in considerazione da Georg Cantor[8] sul finire del XIX secolo.

[8]Georg Cantor (1845–1918), matematico tedesco nato a San Pietroburgo, è considerato il padre della moderna teoria degli insiemi, su cui si basa l'intera matematica.

Prima di rispondere alla domanda di Cantor, vediamo alcuni risultati sulla cardinalità dell'infinito numerabile. Risponderemo alla domanda nella prossima sezione, nel frattempo, provate a pensarci.

Proposizione 5.2. *Un sottoinsieme $A \subset \mathbb{N}$ è finito oppure numerabile.*

Dimostrazione. Sia $A \subset \mathbb{N}$ infinito. Sappiamo già che $|A| \leq |\mathbb{N}|$. Quel che va dimostrato è che $\mathbb{N}$ può essere messo in corrispondenza biunivoca con un sottoinsieme di A, ovvero che esiste una funzione iniettiva (cioè che non assume nessun valore più di una volta) da $\mathbb{N}$ ad A.

Costruiamo la funzione iniettiva $f : \mathbb{N} \to A$ per induzione nel seguente modo:

a) A non è finito, quindi non è vuoto. Sia $a_0 \in A$. Definiamo $f(0) = a_0$;
b) Supponiamo di aver definito $f(i) = a_i$ ($a_i \neq a_j$ se $i \neq j$) per ogni $i \leq n$. Siccome A è infinito, $A_n = A \setminus \{a_i \mid 1 \leq i \leq n\}$ è non vuoto (è addirittura infinito, vedi nota 3). Sia $a_{n+1} \in A_n$. Definiamo $f(n+1) = a_{n+1}$.

Pertanto $f : \mathbb{N} \to A$ è iniettiva[9] e quindi $|\mathbb{N}| \leq |A|$. Pertanto A è numerabile. □

La proposizione appena dimostrata ci dice un fatto importantissimo: l'infinito numerabile è il più piccolo infinito esistente. Infatti se A infinito è tale che $|A| \leq |\mathbb{N}|$, allora per definizione A è in corrispondenza biunivoca con un sottoinsieme di $\mathbb{N}$, e pertanto è infinito numerabile.

Per questo motivo, si indica di solito la cardinalità di $\mathbb{N}$ con $\aleph_0$ (aleph con zero[10]), la cardinalità infinita più piccola.

Proposizione 5.3. *L'insieme dei numeri interi $\mathbb{Z}$ è numerabile.*

Dimostrazione. $\mathbb{Z} \supset \mathbb{N}$, quindi è infinito.

Sappiamo già che due coppie di insiemi di numeri naturali sono numerabili (ovvero i passeggeri di due autobus di Hilbert possono essere alloggiati in un albergo di Hilbert).

Quindi $N_\pm = \{+, -\} \times \mathbb{N}$ è numerabile. Ma $\mathbb{Z} \subset N_\pm$ grazie alla funzione che manda 0 in $(+, 0)$, n in $(+, n)$ e $-n$ in $(-, n)$.

[9]Da notare che f non è necessariamente biiettiva tra $\mathbb{N}$ e A, ovvero alcuni (finiti, ma anche infiniti) elementi di A potrebbero non essere nell'immagine della funzione. Un modo naturale per costruire una biiezione tra $\mathbb{N}$ ed A può essere la seguente:

$$f(0) = \min_{a \in A} a\,; \quad f(n+1) = \min_{a \in A_n} a\,,$$

dove A_n è definito come sopra.

[10]Aleph, $\aleph$, è la prima lettera dell'alfabeto ebraico. Con $\aleph_0$ si indica la cardinalità infinita più piccola. Dà anche il titolo ad una raccolta di racconti con ispirazione matematica di Borges [2].

Pertanto $|\mathbb{Z}| \leq |N_{\pm}| = |\mathbb{N}|$, e quindi $\mathbb{Z}$ è numerabile. □

Proposizione 5.4. *L'insieme dei numeri razionali $\mathbb{Q}$ è numerabile.*

Dimostrazione. $\mathbb{Q} \supset \mathbb{N}$, quindi è infinito.

Sappiamo già che un'infinità numerabile di insiemi numerabili è numerabile (ovvero i passeggeri di una quantità numerabile di autobus di Hilbert possono essere alloggiati in un albergo di Hilbert).

Pertanto $\mathbb{N} \times \mathbb{N}$ è numerabile, e così anche $\mathbb{Z} \times \mathbb{Z}$.

Abbiamo che $\mathbb{Q} \subset \mathbb{Z} \times \mathbb{Z}$ grazie alla funzione che a $p/q \in \mathbb{Q}$ ($p, q \in \mathbb{Z}$ coprimi tra loro, $q > 0$) associa la coppia (p, q).

Pertanto $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$, e quindi $\mathbb{Q}$ è numerabile. □

Proposizione 5.5. *Il prodotto cartesiano di un numero arbitrario di copie di $\mathbb{N}$, $\mathbb{N}^n$, è numerabile.*

Dimostrazione. Lasciata per esercizio al lettore[11]. □

6. La scoperta di Cantor

Quanto visto fin'ora (sotto forma di autobus e alberghi, o sotto forma di insiemi di numeri) ha dell'incredibile: i numeri razionali sono tanti quanti i naturali, nonostante tra due naturali ci sia un numero finito di altri naturali e tra due razionali ci sia un numero infinito (di nuovo $\aleph_0$, ovviamente) di altri razionali.

Ma esistono insiemi più grandi di $\mathbb{N}$? La risposta è sì. Anzi, esistono infiniti arbitrariamente grandi, ovvero dato un qualsiasi insieme, c'è un insieme di cardinalità strettamente maggiore.

Anche questa volta per dimostrarlo utilizzeremo una storiella, quella dei club delle Galassie. A molti milioni di anni luce dalla Terra, c'è una zona dell'Universo abitata da un'infinità di alieni A. Gli alieni hanno fondato un certo numero di club in questo modo: ogni sottoinsieme di alieni costituisce uno ed un solo club. L'insieme dei club C è solitamente chiamato dai matematici insieme delle parti (o dei sottoinsiemi) di A e denotato con $\mathcal{P}(A)$. Una piccola precisazione: anche l'insieme

[11]Per la dimostrazione si possono seguire le linee della dimostrazione 2 della nota 7, in cui si dimostrava che $\mathbb{N}^2$ è numerabile. Adattando quella dimostrazione si può dimostrare anche che il prodotto cartesiano di un'infinità numerabile di insiemi numerabili è ancora numerabile.

Un'altra via di dimostrazione può essere quella di utilizzare il fatto che $\mathbb{N}^2$ è numerabile per dimostrare per induzione che se $\mathbb{N}^n$ è numerabile, allora anche $\mathbb{N}^{n+1}$ è numerabile. Questa seconda strada non permette tuttavia di dimostrare il risultato più forte sul prodotto cartesiano di un'infinità numerabile di insiemi numerabili.

I dettagli (e il divertimento della scoperta) li lasciamo davvero al lettore.

vuoto è un sottoinsieme di A e dunque un club di C: un club molto elitario[12]!

Ovviamente i club sono infiniti, e sono almeno tanti quanti gli alieni, dato che ad ogni alieno α possiamo far corrispondere il club formato soltanto da lui: $\{\alpha\}$. Pertanto $|C| \geq |A|$.

Vogliamo dimostrare che $|C| > |A|$, ovvero che non esiste una corrispondenza biunivoca tra A e C. Supponiamo per assurdo che tale corrispondenza esista, ovvero che ci sia il modo di intitolare ogni club ad un alieno diverso (all'alieno α corrisponde biunivocamente il club C_α).

Allora ogni alieno α può fare parte o meno del "suo" club C_α. Se un alieno appartiene al suo club, lo chiamiamo *socievole*, altrimenti *asociale*.

Consideriamo N, il club degli asociali, ovvero i cui elementi sono tutti e soli gli alieni asociali. Poiché A e C sono in corrispondenza biunivoca, esiste un alieno α tale che $N = C_\alpha$. Chiediamoci allora se α fa parte del club $N = C_\alpha$.

Se $\alpha \notin N = C_\alpha$, allora per definizione di N è socievole, ma per definizione di asociale è asociale.

Se $\alpha \in N$, allora per definizione di N è asociale, ma per definizione di socievole è socievole.

Assurdo. Quindi tale corrispondenza biunivoca non esiste, e $|C| > |A|$.

La dimostrazione fatta si applica in generale a qualsiasi insieme A di partenza[13], e si dimostra così che:

Proposizione 6.1. *Sia A un insieme qualsiasi. Indicando con $\mathcal{P}(A)$ l'insieme delle parti di A (ovvero l'insieme i cui elementi sono tutti e soli i sottoinsiemi di A) si ha*

$$|A| \ < \ |\mathcal{P}(A)| \, .$$

Di solito la cardinalità dell'insieme delle parti di A si indica[14]

$$|\mathcal{P}(A)| \ = \ 2^{|A|} \, .$$

In particolare abbiamo scoperto che l'insieme dei sottoinsiemi di $\mathbb{N}$ ha cardinalità $2^{\aleph_0} > \aleph_0$.

[12]È il club ideale di Woody Allen: *Non vorrei mai appartenere a un club che vantasse tra i suoi membri un tipo come me.* (Io e Annie)

[13]Anche a insiemi finiti!

[14]Se A ha cardinalità finita n i suoi sottoinsiemi sono effettivamente 2^n. Infatti ogni elemento di A può appartenere o no ad ogni dato sottoinsieme, pertanto i possibili sottoinsiemi di A sono $2 \cdot 2 \cdots 2 = 2^n$.

7. Satana, Cantor e l'Infinito

Per rilassarci un po', raccontiamo ora la storiella che dà il titolo a questo articolo.

Satana era solito tormentare le sue vittime dando loro l'illusione di potersi liberare dalla pena eterna delle fiamme dell'Inferno. Infatti era solito dire alle sue vittime:

Ho pensato ad un sottoinsieme dei numeri naturali. Ogni giorno, da qui all'eternità, potrai nominare un sottoinsieme dei numeri naturali. Se e quando indovinerai, ti lascerò libero di andare in Paradiso.

La cosa sembrava alquanto allettante, e tutti i dannati partecipavano al gioco proposto da Satana. Ma mai nessuno era riuscito a indovinare il sottoinsieme pensato da Satana.

Questo infatti era *l'insieme C di tutti i numeri $n \in \mathbb{N}$ tali che n non appartiene all'insieme nominato l'n-esimo giorno.*

Tale insieme non può mai essere nominato. Infatti, l'insieme C e l'insieme nominato l'n-esimo giorno differiscono (almeno) per l'elemento n, che appartiene a uno ma non all'altro.

Ma, come è noto, il diavolo fa le pentole ma non i coperchi. E così, un bel giorno arrivò all'inferno un allievo di Cantor[15], che era anche un esperto di giurisprudenza e di semantica.

Prima di accettare la generosa offerta di Satana, l'allievo di Cantor mise in chiaro alcuni punti.

AC: *Un insieme può essere descritto in modi diversi. Devo indovinare la tua descrizione dell'insieme o solo l'insieme stesso?*

S: *Ovviamente solo l'insieme. Se diamo due descrizioni diverse dello stesso insieme, vinci.*

AC: *Però a volte è difficile capire che due descrizioni diverse descrivono lo stesso insieme. Supponi che io nomini un insieme e tu dica che non è quello che hai pensato. Se sospetto che in realtà sia lo stesso, ma tu non te ne sia accorto, cosa posso fare?*

S (alquanto indispettito): *Beh, in questo caso ti è concesso sfidarmi. Io aprirò la busta e se tu riuscirai a dimostrare che entrambe le descrizioni descrivono lo stesso insieme, sarai libero. Ma, siccome avrai visto l'insieme che ho scelto, se fallirai, sarai dannato in eterno e non potrai più nominare altri insiemi.*

AC: *Molto bene. Anche questo è chiarito. Ma come faccio a sapere che tu abbia veramente descritto un insieme in quella busta?*

[15]Perché non Cantor stesso? Dato che il povero Cantor già era morto in miseria in un ospedale psichiatrico, probabilmente chi ha inventato la storiella non se l'è sentita di mandarlo anche all'inferno.

S (molto alterato): *Dubiti della mia parola?*

AC: *O, no! Penso che tu creda davvero di aver correttamente descritto un insieme. Ma molto spesso nella storia della matematica qualcosa che sembrava una descrizione genuina si è solo rivelato una pseudodescrizione. Supponi che a un certo punto io sospetti che tu abbia dato una pseudodescrizione. Posso sfidarti?*

S: *Certo! Mi sfidi, apro la busta e se tu dimostri che ho scritto una pseudodescrizione, allora sei libero. Ma ricorda, dopo una sfida non potrai in alcun modo nominare più alcun insieme.*

L'allievo di Cantor, soddisfatto, firmò il contratto col diavolo e nominò subito il suo primo insieme.

AC: *L'insieme C di tutti i numeri $n \in \mathbb{N}$ tali che n non appartiene all'insieme nominato l'n-esimo giorno. E ora, ti sfido, apri la busta!.*

S (perplesso e infastidito): *Uhm... a questo non avevo pensato...*

Aperta la busta, le due descrizioni coincidevano e l'allievo di Cantor stava già cantando vittoria. Ma Satana non è tipo da arrendersi subito, e accusò l'allievo di Cantor di avere barato.

S: *Hai barato! Hai fatto quello che sostenevi che avrei fatto io: hai fornito una pseudodescrizione di un insieme! Il numero* 1 *non può né appartenere né non appartenere a tale insieme*[16]*, quindi l'insieme che hai nominato non è ben definito!*

AC: *Mi fa molto piacere che tu, così sportivamente, lo ammetta! Dato che abbiamo dato la stessa pseudodescrizione...*

S: *La mia non è una pseudodescrizione! Tu non hai ancora nominato un insieme oggi, dato che hai dato solo una pseudodescrizione. Dovrai nominare un insieme tutti i giorni, da oggi all'eternità. Così il mio insieme sarà perfettamente definito.*

AC: *Purtroppo ti ho sfidato, e per le regole che ci siamo dati non posso più nominare alcun insieme.*

Satana dovette arrendersi, e l'allievo di Cantor fu libero di andare in Paradiso.

In definitiva, la descrizione data da Satana dell'insieme C, *l'insieme di tutti i numeri $n \in \mathbb{N}$ tali che n non appartiene all'insieme nominato l'n-esimo giorno*, è una descrizione o una pseudodescrizione di un insieme? Beh, se effettivamente la vittima avesse nominato uno e un solo sottoinsieme dei numeri naturali ogni giorno, dal primo all'eternità, allora sarebbe stata una descrizione. Altrimenti no. E non ci sarebbe mai stata, da qui all'eternità, la certezza che la frase fosse una

[16]Perché? Al lettore dovrebbe ormai essere chiaro...

descrizione, dato che non si poteva essere certi che in futuro la vittima avrebbe continuato a nominare sottoinsiemi. Quindi in un qualsiasi momento, una sfida a Satana avrebbe rivelato una pseudodescrizione, e non una descrizione di un insieme! Satana aveva fatto davvero un pessimo contratto...

La frase usata da Satana e dall'allievo di Cantor per descrivere C è nota come *procedimento diagonale* di Cantor ed è usata per mostrare che i sottoinsiemi di $\mathbb{N}$ sono più che numerabili. Come?[17]

8. Quanti sono i numeri reali?

Abbiamo visto che gli insiemi di numeri $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ hanno tutti la stessa cardinalità, ovvero sono numerabili.

La stessa cosa vale anche per i numeri algebrici, che sono tutti i numeri $\alpha \in \mathbb{R}$ (o $\alpha \in \mathbb{C}$, se parliamo di numeri algebrici complessi) che soddisfano un equazione polinomiale a coefficienti interi, ovvero tali che esiste un polinomio non nullo

$$P(x) \;=\; a_n x^n + \cdots + a_1 x + a_0, \quad a_0, \ldots, a_n \in \mathbb{Z}, \quad a_n \neq 0$$

tale che

$$P(\alpha) \;=\; a_n \alpha^n + \cdots + a_1 \alpha + a_0 \;=\; 0\,.$$

Perché i numeri algebrici sono numerabili? Provate a pensarci per esercizio, prima di leggere la soluzione nella nota[18].

---

[17]Ormai dovreste essere in grado di rispondere da soli, e quindi vi do solo un suggerimento.

Se esaminate da vicino questo insieme C e il ragionamento per cui non può mai essere nominato, vi accorgerete che è molto simile al problema del *club degli asociali* visto prima.

[18]Chiamiamo A l'insieme dei numeri algebrici (reali o complessi, non importa). Se $\alpha \in A$, allora soddisfa un'equazione polinomiale a coefficienti interi di grado $n > 0$.

Vediamo innanzitutto che i numeri algebrici che verificano le equazioni polinomiali a coefficienti interi di grado al più $n > 0$ fissato (chiamiamo tale insieme A_n) sono numerabili. Questo ci basterà per dimostrare che A è numerabile. Infatti, evidentemente

$$A \;=\; \bigcup_{n=1}^{\infty} A_n$$

ovvero A è un'unione numerabile di insiemi numerabili. Sappiamo già (è il problema degli infiniti autobus che arrivano all'hotel di Hilbert) che tale unione A è numerabile anch'essa.

Le equazioni polinomiali a coefficienti interi di grado al più $n > 0$ sono in corrispondenza biunivoca con $\mathbb{Z}^{n+1}$, facendo corrispondere al polinomio

$$P(x) \;=\; a_n x^n + \cdots + a_1 x + a_0$$

Vediamo ora che i numeri reali non sono numerabili. La cardinalità dei numeri reali è chiamata *cardinalità del continuo* e indicata con $\mathfrak{c}$.

Proposizione 8.1. $\mathfrak{c} = 2^{\aleph_0}$.

Dimostrazione. Dimostreremo le due disuguaglianze.

$\mathfrak{c} \leq 2^{\aleph_0}$, ovvero esiste una funzione iniettiva da $\mathbb{R}$ all'insieme delle parti di un insieme numerabile. Prendiamo $\mathbb{Q}$ come tale insieme e definiamo

$$\begin{aligned} f : \mathbb{R} &\to \mathcal{P}(\mathbb{Q}) \\ f(x) &= \{y \in \mathbb{Q} \mid y \leq x\}. \end{aligned}$$

Dato che tra due numeri reali distinti c'è sempre almeno un razionale, tale funzione è iniettiva.

$\mathfrak{c} \geq 2^{\aleph_0}$, ovvero esiste una funzione iniettiva dall'insieme delle parti di $\mathbb{N}$ in $\mathbb{R}$.

$$g : \mathcal{P}(\mathbb{N}) \to \mathbb{R}$$

è definita nel seguente modo. Se $A \subset \mathbb{N}$, $g(A)$ è quel numero reale $0 \leq x < 2$ nella cui scrittura decimale all'n-esima posizione dopo la virgola c'è una cifra 1 se $n \in A$, una cifra 0 se $n \notin A$. Analogamente, la parte intera di x è 0 se $0 \notin A$, è 1 se $0 \in A$. Tale corrispondenza è evidentemente iniettiva. □

Notiamo che nella dimostrazione precedente non abbiamo esibito una corrispondenza biunivoca tra $\mathbb{R}$ e $\mathcal{P}(A)$, ma solo dimostrato che essa esiste, dato che le cardinalità dei due insiemi sono uguali.

9. L'ipotesi del continuo

In questa ultima sezione non daremo risposte, ma forniremo solo domande, cercando di far intuire la vastezza dei problemi legati al concetto di infinito. Sarà una sezione con note lunghe, fitte e tecniche. Il lettore più curioso (e meno timoroso) può leggerle: queste forniranno alcune risposte, ma è possibile anche che confondano solo le idee o che facciano nascere altre domande.

---

il punto $(a_0, \ldots, a_n)$. Ognuno di questi polinomi ha al più n radici (distinte). Quindi

$$|A_n| \leq |(\mathbb{Z}^{n+1})^n| = |\mathbb{Z}^{n^2+n}| = \aleph_0,$$

ovvero la cardinalità di A_n è al più numerabile. Che sia infinita è ovvio, dato che tutti i numeri interi $k \in \mathbb{Z}$ sono soluzione dell'equazione di primo grado $x - k = 0$. Pertanto

$$|A_n| = \aleph_0$$

e i numeri algebrici sono numerabili. □

Come abbiamo già detto con $\aleph_0$ si denota la cardinalità infinita più piccola. Analogamente, con $\aleph_1$ si denota la cardinalità infinita che ha solo una cardinalità infinita più piccola di lei stessa, e in generale con $\aleph_n$ la cardinalità infinita che ha esattamente n cardinalità infinite più piccole di lei.

Ci può essere qualcosa come $\aleph_\infty$? Beh, potremmo pensare di sì, in un certo senso, ma –come ormai abbiamo capito– quando abbiamo a che fare con l'infinito dobbiamo fare molta attenzione: ∞, infinito, non è molto ben definito... Stiamo parlando di una cardinalità che abbia esattamente $\aleph_0$ cardinalità infinite più piccole? O di una che ne abbia $\aleph_n$?

E anche in questo caso le cose non son ben definite... La cardinalità immediatamente più grande di $\aleph_{\aleph_0}$ chi è? Ha esattamente $\aleph_0 + 1$ cardinalità infinite più piccole di lei, ma

$$\aleph_0 + 1 = \aleph_0 \,,$$

pertanto la cardinalità infinita immediatamente più grande di $\aleph_{\aleph_0}$ sarebbe $\aleph_{\aleph_0}$ stessa...

C'è qualcosa che non torna. Per aggiustare le cose, servono i numeri ordinali[19] e anche un qualche teorema (o una qualche ipotesi) che ci assicuri che esista sempre una cardinalità infinita immediatamente più grande di un'altra. Infatti chi ci assicura che esista il più piccolo degli insiemi più grandi di un certo insieme fissato?

[19]I numeri ordinali rappresentano un altro modo per distinguere infiniti diversi, in cui conta l'ordine in cui sono presenti gli elementi.

Ad esempio $\mathbb{N}$ e l'insieme $\mathbb{N} \cup \{\omega\}$, dove vale $\omega > n$ per ogni $n \in \mathbb{N}$ hanno la stessa cardinalità $\aleph_0$ (sono in corrispondenza biunivoca), ma non rappresentano lo stesso ordinale dato che non possono essere messi in una corrispondenza biunivoca che *rispetti l'ordine* (infatti il primo insieme non ha un ultimo elemento, mentre il secondo ce l'ha, ω): l'ordinale corrispondente a $\mathbb{N}$ è detto ω, quello corrispondente al secondo insieme $\omega + 1$.

Mentre

$$\aleph_0 + 1 = 1 + \aleph_0 = \aleph_0 \,,$$

per gli ordinali vale

$$\omega + 1 > \omega \,, \quad 1 + \omega = \omega \,.$$

Non è questo il luogo per definire rigorosamente le operazioni tra numeri ordinali. Il lettore interessato ad approfondire questo aspetto o altri dei numeri ordinali e cardinali può leggere l'ultimo capitolo de *Il libro dei numeri* [3].

Due insiemi ben ordinati (ovvero tali che due elementi siano sempre confrontabili e ogni sottoinsieme ammetta minimo) della stessa ordinalità sono anche della stessa cardinalità. Ovvero, l'ordinalità è una relazione d'equivalenza più fine, ovvero che distingue meglio gli insiemi.

Tuttavia per parlare di ordinalità dobbiamo avere insiemi (ben) ordinati, mentre per parlare di cardinalità bastano gli insiemi.

Per capire meglio il problema, qual è il numero reale più piccolo fra i numeri reali più grandi di 0? Ovvero qual è il numero reale strettamente positivo più piccolo? O qual è

$$\min\{x \in \mathbb{R} \mid x > 0\}\,?$$

Risposta: non esiste.

Beh, non c'è ragione di pensare che tale problema non si ponga nel nostro caso.

In particolare non c'è neppure nessuna ragione di supporre che anche solo $\aleph_1$ sia ben definito[20].

Sicuramente ben definiti sono invece i numeri cardinali beth[21], che si definiscono induttivamente nel seguente modo:

$$\left\{ \begin{array}{rcl} \beth_0 & = & \aleph_0 \\ \beth_{n+1} & = & 2^{\beth_n} \end{array} \right\} .$$

Per quanto abbiamo visto (vedi la proposizione 6.1), $\beth_n < \beth_{n+1}$, per ogni $n \in \mathbb{N}$.

---

[20]Nessuna ragione a priori, ovviamente. Ovvero, la tal cosa va dimostrata.

Nell'usuale teoria degli insiemi di Zermelo-Fraenkel (ZF) si può dimostrare che $\aleph_1$ è ben definito.

Se poi si assume come assioma anche l'assioma della scelta (axiom of choice, C, in inglese), allora nella teoria ZFC (Zermelo-Fraenkel + assioma della scelta) si dimostra che la classe dei numeri cardinali è ben ordinata, e pertanto è ben definito $\aleph_n$ per ogni $n \in \mathbb{N}$.

Per chi fosse curioso, l'assioma della scelta afferma semplicemente che *il prodotto di (un numero qualsiasi di) insiemi non vuoti è non vuoto*. Per quanto ovvio e banale ciò possa sembrare, questo assioma è indipendente dalla usuale teoria degli insiemi ZF. E tale innocuo assioma porta con sé interessanti conseguenze molto meno ovvie, come il paradosso di Banach-Tarskii o della *duplicazione dei pani e dei pesci*: *si può "tagliare" una palla in un numero finito di pezzi in modo tale da ottenere, dopo un numero finito di rotazioni e traslazioni, due palle identiche a quella di partenza* (ovviamente tali pezzi saranno alquanto strani). Ed ecco che il principio di conservazione della massa (o del volume) scompare!

In matematica capita che da cose apparentemente *ovvie* ne seguano logicamente altre di decisamente meno ovvie, e a volte paradossali.

L'assioma della scelta è generalmente accettato e usato da tutta la comunità matematica (fondamentalmente perché permette di dimostrare risultati molto utili e potenti), e teorie che non lo comprendono sono abitualmente studiate solo dai logici. Ma questa è un'altra storia...

Tornando ai nostri numeri cardinali, sì, $\aleph_\omega$ esiste (ovviamente in ZFC), e anzi, per ogni numero ordinale α esiste il cardinale $\aleph_\alpha$. La funzione $\aleph$, che ad ogni ordinale α associa il cardinale $\aleph_\alpha$ è una biezione tra i numeri ordinali e i numeri cardinali.

[21]Beth, $\beth$, è la seconda lettera dell'alfabeto ebraico.

Abbiamo visto che $\beth_1$ è la cardinalità del continuo, ovvero dei numeri reali:

$$\beth_1 \;=\; \mathfrak{c} \;=\; |\mathbb{R}|\,.$$

Ma come è collegata la cardinalità del continuo con le cardinalità aleph? Ci sono altri infiniti tra $\aleph_0$ e $\mathfrak{c}$? Un sottoinsieme infinito di $\mathbb{R}$ ha necessariamente la cardinalità di $\mathbb{N}$ o di $\mathbb{R}$ (o sono possibili casi intermedi)?

Per quanto ciò possa sembrare strano, questa domanda non ha risposta nella teoria logica che abitualmente si usa in matematica, ovvero nella teoria degli insiemi ZFC (teoria degli insiemi di Zermelo-Fraenkel con aggiunta dell'assioma della scelta). Si può decidere che la risposta a tali domande è sì (oppure che è no) e ottenere teorie matematiche coerenti.

Addirittura, l'ipotesi $\mathfrak{c} = \aleph_n$ è indipendente da ZFC per ogni $n \in \mathbb{N}$ diverso da 0, ovvero si può supporre che tale uguaglianza sia valida per un $n > 0$ qualsiasi, ottenendo così infinite teorie matematiche diverse, ma tutte coerenti (almeno, se ZFC è coerente)[22].

L'ipotesi $\mathfrak{c} = \aleph_1$ (non ci sono cardinalità intermedie tra quella di $\mathbb{N}$ e quella di $\mathbb{R}$) è la famosa *ipotesi del continuo*.

L'*ipotesi del continuo generalizzata* dice che se A è un insieme infinito tra la cardinalità di A e la cardinalità di $\mathcal{P}(A)$ non vi sono altre cardinalità. In particolare afferma che $\aleph_n = \beth_n$ per ogni $n \in \mathbb{N}$. Anche questa ipotesi è indipendente da ZFC.

Ringraziamenti. Ci tengo a ringraziare Alessandro Zaccagnini, per vari motivi. In primis perché mi ha proposto di scrivere questo articolo, ma soprattutto perché lo ha letto (garantendomi un numero di lettori strettamente positivo!) e mi ha dato utili suggerimenti e spunti per alcune parti del testo e della bibliografia.

Riferimenti bibliografici

[1] Claudio Bartocci (a cura di), *Racconti matematici*, Einaudi, 2006.
[2] Jorge L. Borges, *L'Aleph*, Feltrinelli, 2003.
[3] J. H. Conway and R. K. Guy, *Il libro dei numeri*, Hoepli, 1999.
[4] A. Doxiadis and C. Papadimitriou, *Logicomix*, Guanda Graphic, Guanda, 2010.
[5] Raymond M. Smullyan, *Satana, Cantor e l'infinito e altri inquietanti rompicapi*, Sfide matematiche, RBA Italia, 2008.

[22] Il lettore curioso si chiederà se si può più in generale in ZFC supporre $\mathfrak{c} = \aleph_\alpha$ per ogni ordinale α. La risposta è no; alcune cardinalità, come ad esempio $\aleph_\omega$, sono necessariamente diverse da $\mathfrak{c}$.

$\aleph_\omega \neq \mathfrak{c}$ non vuol tuttavia dire che è necessariamente $\aleph_\omega > \mathfrak{c}$. Si può infatti supporre in ZFC che $\mathfrak{c} = \aleph_{\omega_1}$, dove ω_1 è il più piccolo ordinale non numerabile.

[6] _____, *Satan, Cantor and Infinity. And other mind-boggling puzzles*, Knopf, New York, 1992.

Alberto Saracco
Dipartimento di Matematica e Informatica, Università di Parma, Parco Area delle Scienze 53/A, I-43124 Parma, Italy
alberto.saracco@unipr.it

Stampato in proprio, a cura degli autori, presso il Dipartimento di Matematica e Informatica dell'Università di Parma, Parco Area delle Scienze, 53 A, 43124 - Parma. Adempiuti gli obblighi ai sensi della Legge n.106 del 15.04.2004 "Norme relative al deposito legale dei documenti di interesse culturale destinate all'uso pubblico" (G.U. n. 98 del 27 aprile 2004) e del Regolamento di attuazione emanato con il D.P.R. n. 252 del 3 maggio 2006 (G.U. n. 191 del 18 agosto 2006) entrato in vigore il 2 settembre 2006 [precedente normativa abrogata: Legge n.374 del 2.2.1939, modificato in D.L. n.660 del 31 agosto 1945].

< Esemplare fuori commercio per il deposito legale
agli effetti della legge 15 aprile 2004, n.106 >