L’INFINITO MATEMATICO

Enrico Bombieri
IAS, Princeton

COSA È L'INFINITO?

Uno, due, tre. . . infinito è il titolo di un piccolo libro, dedicato per un largo pubblico, scritto nel 1948 dal fisico George Gamow. Lo scopo di questo libro era di guidare il lettore ad una presentazione di vari aspetti della scienza moderna: l'atomo, le galassie e il Big Bang, con la relatività di Einstein guida sicura lungo il difficile percorso.

Il titolo del libro era un riferimento all'ipotetico inizio dell'aritmetica in tribù primitive, con "Uno, due, tre, molti".[a] Studi recenti hanno mostrato che una persona normale non è in grado di avere una visione mentale simultanea accurata di più di sette oggetti. Quindi, dopo un milione di anni di evoluzione, ancora oggi contiamo in realtà "Uno, due,. . . ,sette, molti".

La matematica è lo strumento necessario per capire tutto ciò che è incredibilmente grande. Ci si domanda: può la matematica aiutarci a capire meglio quello strano concetto che è l'infinito? Cosa è l'infinito? Rappresenta l'inaccessibile, la negazione del contare e del misurabile? Oppure dobbiamo considerare l'infinito come una entità completa, perfetta in ogni senso, non migliorabile?

[a]La tribù Pirahã dell'Amazzonia ancora oggi fa di conto soltanto con "Uno, due, molti".

PRIME VEDUTE SULL'INFINITO

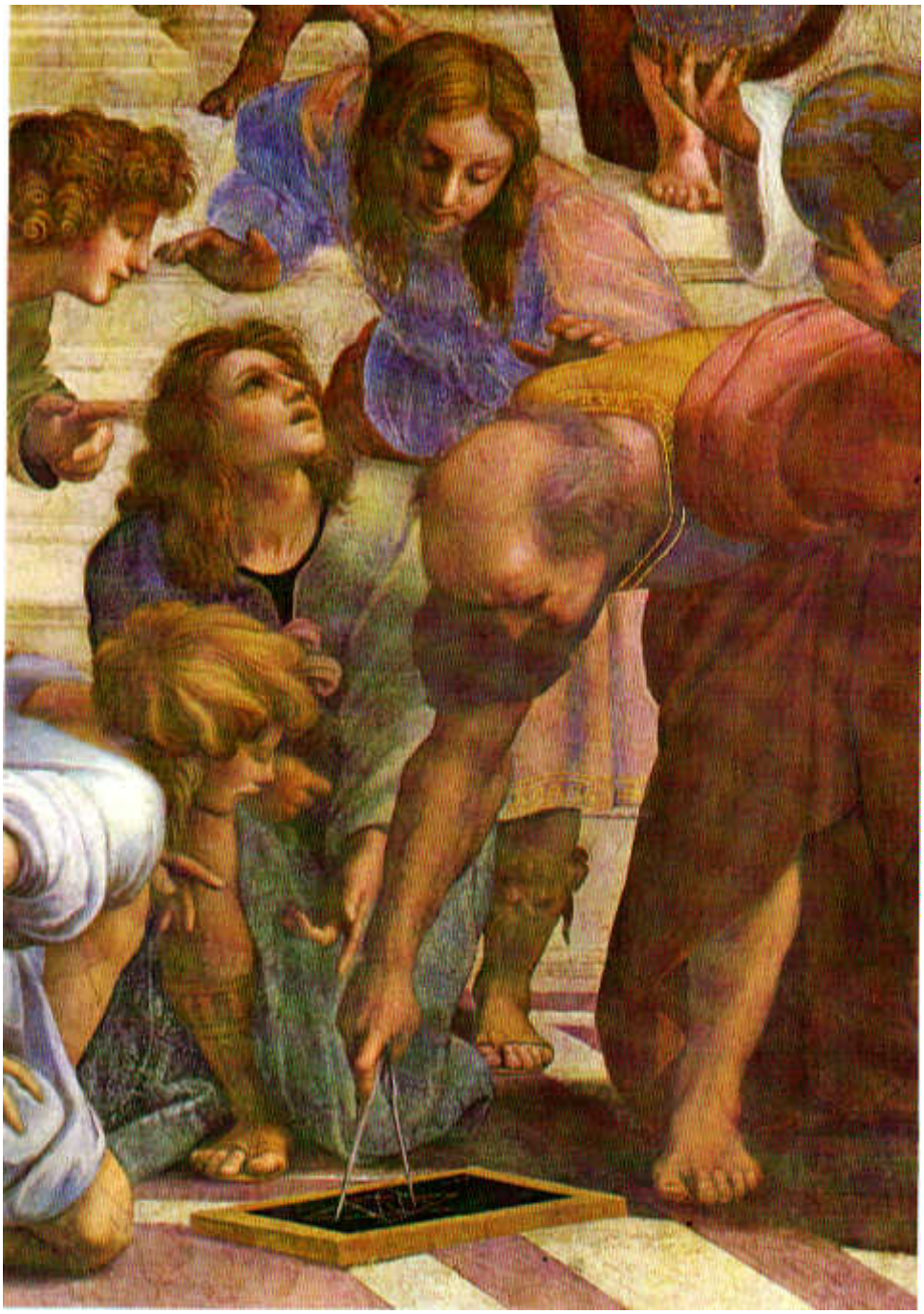
Per Pitagora, la scuola eleatica, e i filosofi Parmenide e Platone, l'infinito era accettato come concetto, ma con un connotato negativo: era inaccessibile; impossibile da descrivere in termini finiti, pertanto caratteristico dell'irrazionale; era senza forma dato che non si poteva aggiungere nulla, né togliere nulla, all'infinito.

La dimostrazione dell'impossibilità del movimento data dal filosofo Zenone con il suo celebre paradosso fu fondata su queste idee.

La conseguenza logica di questo punto di vista per l'aritmetica e la geometria era quella di vietare concetti e dimostrazioni che non potevano essere descritti in termini finiti e precisi. La linea retta, con la sua descrizione assegnando la sua direzione e un punto di passaggio, era un buon concetto, e così era per cerchi, triangoli, quadrati, poligoni. Ellissi, parabole, iperbole potevano far parte della geometria dello spazio in quanto sezioni coniche, ma non facevano parte della geometria piana euclidea.

LA VERITÀ RAZIONALE

Raffaello. La scuola di Atene.

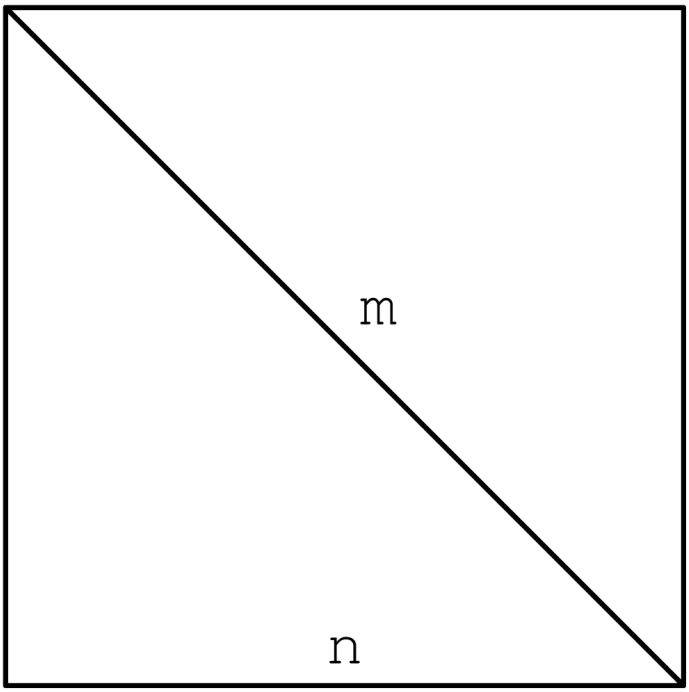


La scuola di Atene. Dettaglio dell’angolo inferiore destro, con Euclide.

LA SCOPERTA DELL'IRRAZIONALE

Supponiamo che la diagonale e il lato di un quadrato siano commensurabili, con un rapporto m/n in numeri interi. Allora per il teorema di Pitagora si ha $m^2 = 2\,n^2$. Quindi m sarebbe pari e pertanto $m = 2p$ con p intero. Allora $4\,p^2 = 2\,n^2$ e in conseguenza $n^2 = 2\,p^2$.

Questa costruzione sarebbe ripetibile all'infinito, con una impossibile **discesa infinita** di numeri interi positivi.



EUCLIDE E I NUMERI PRIMI

Nel nono libro dei suoi celebri *Elementi*, Proposizione (IX.20), Euclide osserva che *“Data una quantità arbitraria di numeri primi esiste un numero primo diverso da questi.”*

Dimostrazione: Consideriamo il prodotto dei numeri primi dati ed aggiungiamo 1. Ottieniamo un numero, più grande di 1, che dà come resto 1 per la divisione con uno qualunque dei numeri primi dati. Tuttavia questo numero si fattorizza come prodotto di numeri primi, necessariamente diversi dai numeri primi dati all’inizio. Q.E.D.

La dimostrazione data è una traduzione di quella di Euclide ed è diversa da quella che si impara sui libri di scuola in quanto Euclide, fedele seguace di Pitagora, evita qualunque riferimento all’infinito.

TRE FAMOSI PROBLEMI DELL'ANTICHITÀ

La diagonale di un quadrato dà una costruzione geometrica del lato di un quadrato con area il doppio dell'area del quadrato iniziale. Allo stesso modo, vi è una semplicissima costruzione con geometria e compasso per determinare la bisettrice di un angolo. Da qui i primi due problemi:

LA DUPLICAZIONE DEL CUBO. Costruire con riga e compasso il lato di un cubo di volume il doppio del volume di un cubo assegnato.
LA TRISEZIONE DELL'ANGOLO. Trisecare un angolo con riga e compasso.
Ecco il terzo:
LA QUADRATURA DEL CERCHIO. Costruire con riga e compasso un quadrato di area uguale a quella di un cerchio assegnato.

Questi tre problemi rimasero insoluti per secoli, sebbene i primi due furono risolti già nell'antichità usando sezioni coniche. Il terzo problema rimase inaccessibile anche con l'aiuto delle sezioni coniche e diventò famoso. Anche Dante lo menziona nella sua splendida conclusione finale della "Commedia".

PARADISO, CANTO XXXIII, 133–145

Dante, davanti all'impossibilità di comprendere il mistero teologico della Trinità fa una similitudine di se stesso con lo studioso di geometria che tenta e ritenta, senza successo, di misurare il cerchio:

Qual è 'l geomètra che tutto s'affige
per misurar lo cerchio, e non ritrova,
pensando, quel principio ond' elli indige,

tal era io a quella vista nova:
veder voleva come si convenne
l'imago al cerchio e come vi s'indova;

ma non eran da ciò le proprie penne:
se non che la mia mente fu percossa
da un fulgore in che sua voglia venne.

A l'alta fantasia qui mancò possa;
ma già volgeva il mio disio e 'l velle,
sì come rota ch'igualmente è mossa,

l'amor che move il sole e l'altre stelle.

Dante ammette l'impossibilità di comprendere da solo il mistero, ma ricevendo l'aiuto divino Dante finalmente completa lo scopo finale del suo viaggio nel mondo ultraterreno.

I TRE FAMOSI PROBLEMI, OGGI

La similitudine di Dante con il problema della quadratura del cerchio risultò alla fine molto appropriata. Infatti, Lindemann nel 1882 dimostrò rigorosamente che è impossibile effettuare la quadratura del cerchio con costruzioni puramente geometriche e in particolare per mezzo della geometria euclidea. Un trionfo della matematica moderna, dato il suo significato storico e le sue conseguenze filosofiche.

Questi tre problemi sono stati per secoli il territorio di caccia di migliaia e migliaia di matematici dilettanti, alla ricerca di soddisfare il proprio ego.[a] Nonostante la soluzione negativa di tutti e tre i problemi, il diluvio di “soluzioni” continua ancora oggi.[b]

[a] Esiste un istruttivo compendio su questo, completo fino all’anno 1872, nel libro: *A budget of paradoxes* di Augustus De Morgan, astronomo reale e tra i fondatori della logica matematica.

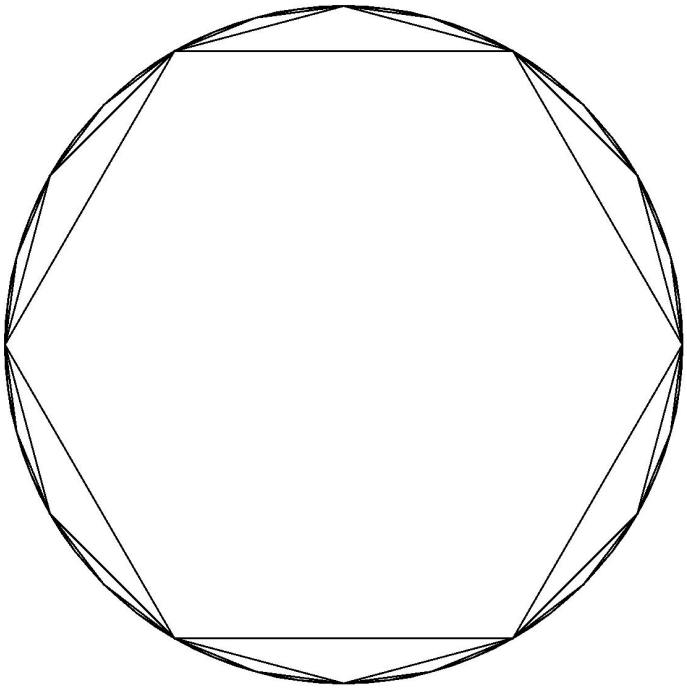
[b] La verità non ha ancora raggiunto i politici americani. Il deputato Daniel Inouye (D-HA) presentò nel 1960 in parlamento un tributo al pittore hawaiano Maurice Kidjel, risolutore di tutti e tre i problemi. Il pittore, fondatore della Kidjel Ratio Company, vendeva un suo libretto e il “calibratore Kidjel” da usare per la soluzione. La società radiofonica KPIX-San Francisco fece in proposito un documentario dal titolo “Il mistero dei secoli”. Il deputato disse (speriamo non corrisponda al vero!) *“The Kidjel solutions are now being taught in hundreds of schools and colleges throughout... the United States and Canada.”*

ARCHIMEDE AND IL CERCHIO

Archimede fece uso del concetto di **limite matematico**. Esiste un frammento di un suo libro con una dimostrazione rigorosa di

$$3\frac{10}{71} < \pi < 3\frac{1}{7}$$

approssimando il cerchio con poligoni, iniziando dall'esagono e raddoppiando quattro volte il numero dei lati:



La formula di Archimede in linguaggio moderno:

$$3 \times 2^n \sin\left(\frac{\pi}{3 \times 2^n}\right) < \pi < 3 \times 2^n \tan\left(\frac{\pi}{3 \times 2^n}\right)$$

ARCHIMEDE E IL PROBLEMA DEI BUOI

Un precursore di questo problema si trova in Omero, *Odissea*, Libro XII, 194–198. la versione di Archimede apparve in un epigramma greco di 24 versi, pubblicato da Gotthold Ephraim Lessing nel 1773, chiamato correntemente il problema dei buoi di Archimede.

Si richiede di trovare la composizione della mandria del Dio Sole, cioè il numero dei tori bianchi, neri, pezzati, e bruni, e il numero delle vacche dei corrispondenti colori, con questi numeri soddisfacenti a nove relazioni. Vi sono otto incognite e sette relazioni lineari (ad esempio, il numero dei tori bianchi è cinque sesti quello dei tori neri, più il numero di quelli bruni). Le ultime due sono quadratiche: la mandria sta perfettamente, senza spazi vuoti, sia in un quadrato che in un triangolo rettangolo isoscele.

La Mandria del Sole. Vaso etrusco. Caere, VI c. A.C. Musée du Louvre.

IL PROBLEMA DEI BUOI, II

La più piccola soluzione ha 206545 cifre!

È possibile che questo strano problema risalga ad Archimede? Improbabile, dato che l'epigramma dice che, per ogni colore, il numero delle vacche è molto maggiore di quello dei tori, mentre la soluzione non verifica ciò. Alcuni letterati ritengono che il testo sia corrotto e hanno proposto versioni alternative.

Un'altra spiegazione, assai divertente, si può dedurre dagli scritti di Archimede. Nel suo trattatto "Sulle spirali", Archimede scrive che informava regolarmente i matematici alessandrini dei suoi nuovi risultati, ma senza spiegazioni. Avendo saputo che alcuni di questi matematici si appropriavano delle sue scoperte, Archimede ci dice che nell'ultima lettera aveva aggiunto due affermazioni false, così che *"... quelli che dicono di scoprire tutto, ma senza dimostrazione, possano essere smascherati avendo scoperto l'impossibile."*

È possibile che Archimede abbia proposto questo problema, con una soluzione che nessuno può scrivere esplicitamente, proprio col proposito di smascherare i suoi falsi amici?

ANCORA ARCHIMEDE

Archimede fece uso di un concetto di limite, precursore del calcolo differenziale e integrale. Famoso è il suo teorema che l'area della sfera è i due terzi dell'area del cilindro circonscritto ad essa, un risultato non dimostrabile nello stile di Euclide. Archimede stesso lo considerava il pinnacolo delle sue ricerche.

Archimede morì alla fine dell'assedio di Siracusa nel 212 A.C. Cicerone racconta che quando era questore in Sicilia nel 75 A.C. identificò la tomba di Archimede attraverso i versi di un canzonetta popolare che aveva udito, che dicevano che sulla sua tomba avevano messo una sfera ed un cilindro. Infatti, nel cimitero vi era una colonna, nascosta dai rovi, sulla quale era stata incisa la figura di un cilindro con dentro una sfera.

L'incontro di Archimede con l'infinitamente grande appare nel problema dell' *Arenaria.* Qui Archimede inventa un nuovo sistema di numerazione (iterazione della funzione esponenziale) che gli permette di contare fino a 8×10^{63}, un numero così grande, egli dice, che basta per trovare quanti granelli di sabbia sono necessari per riempire l'universo. Chiaramente, si tratta di una idea rivoluzionaria al tempo di allora.

COSA È L'INFINITO MATEMATICO?

Il pensiero di Aristotele: L'infinito esiste soltanto in un senso implicito ma non può essere mai raggiunto. L'infinito nella matematica non è necessario in quanto i matematici hanno in realtà soltanto bisogno di quantità grandi quanto si voglia, e di costruzioni ripetute quante volte si voglia, ma mai di quantità infinite o di costruzioni infinite quale potrebbe essere il passaggio al limite. L'infinito non fa parte della matematica, è soltanto una conveniente abbreviazione.

Dall'altra parte della barricata c'è Archimede, con il suo teorema della sfera, il suo interesse per numeri estremamente grandi, il suo uso del *metodo di esaustione.* Archimede, di fatto, accetta pienamente l'infinito come concetto che fa parte della matematica.

Il matematico di oggi vede il problema dell'infinito, che è basilare per i fondamenti della matematica, in modo pragmatico.

Il primo scopo del pensiero è la conoscenza.

Come si ottiene la conoscenza ha la sua importanza, ma resta sempre al secondo posto.

La MATEMATICA È UN ESPERIMENTO?

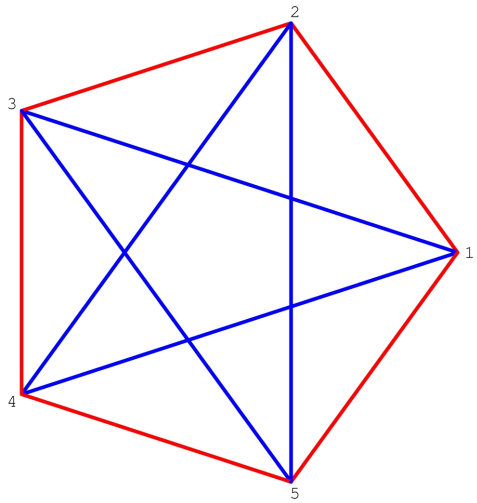
L'esperimento: la verifica del vero o del falso.
Input: uno scritto di matematica.
Il computer (biologico): il cervello (impulsi elettrici attraverso i neuroni).
Il software: Logica a due valori (Vero – Falso).
Output: Vero, Falso, Non Applicabile (per esempio, articolo incomprensibile perchè scritto da cani).

Difficoltà: Il restare sempre nell'ambito del finito (supponendo che ciò sia sempre possibile) comporta serie complicazioni.
Conclusione in stile pragmatico: il rifiuto *a priori* dell'infinito non giova al progresso della matematica.

Un esempio: vi sono proposizioni logiche nell'ambito del calcolo combinatorio sul finito che sono dimostrabili come vere nel modello di Zermelo–Fraenkel della teoria degli insiemi, ma sono indecidibili nel modello "naturale" finitistico dell'aritmetica creato da Giuseppe Peano (modello di tipo "aristotelico", cioè i numeri interi con le operazioni $+$, $-$, $\times$, $:$, unione e intersezione finita, e il principio di induzione completa).

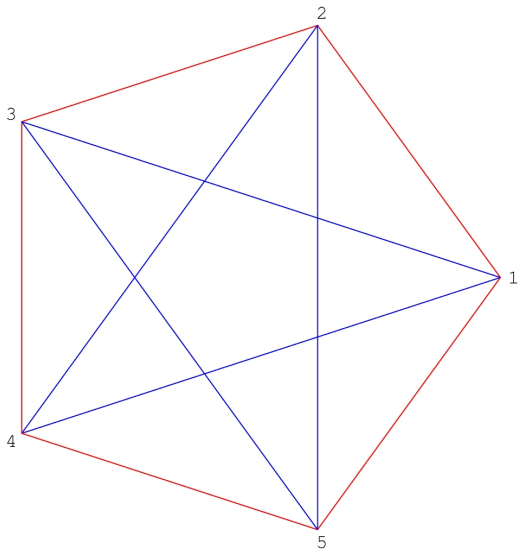
AMICI E SCONOSCIUTI

Il teorema degli *Amici e sconosciuti*: Dato un numero n, in un qualunque gruppo abbastanza grande di persone (la cui soglia si indica con $R(n,n)$) si trovano sempre o n persone che si conoscono già tra loro, oppure n persone che non si sono mai incontrate prima. La domanda: Quanto è grande questa soglia $R(n,n)$? È facilissimo vedere che $R(3,3) = 6$ e meno facile verificare che $R(4,4) = 18$. Oltre, sappiamo ben poco, ad esempio $43 \leq R(5,5) \leq 49$ e $102 \leq R(6,6) \leq 165$.

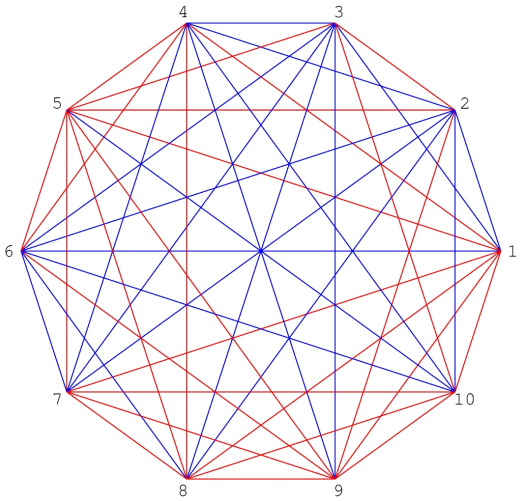


Una dimostrazione che $R(3,3) \geq 6$.

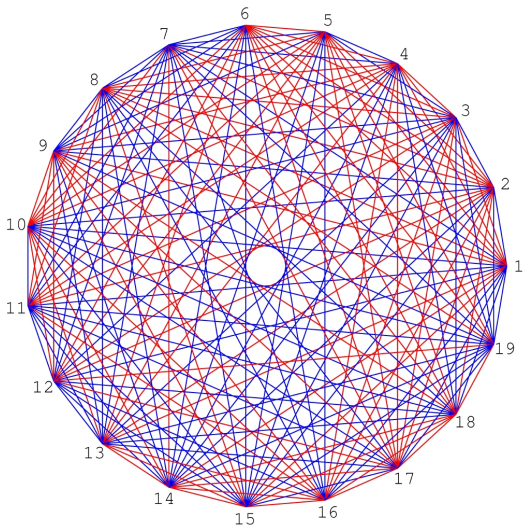
GRAFI A DUE COLORI



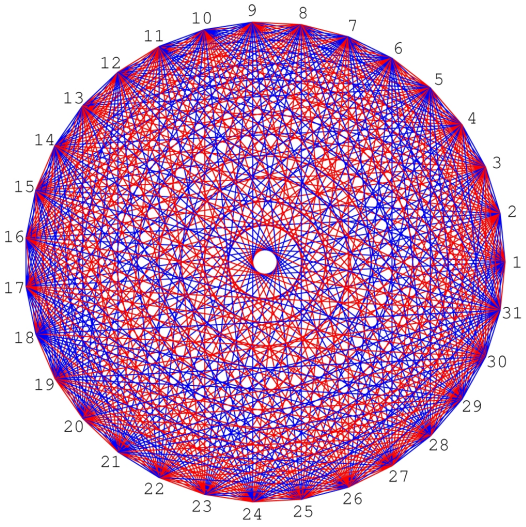
5 vertici, nessun triangolo monocolore



10 vertici, due colori a caso



19 vertici, due colori a caso



31 vertici, due colori a caso

RAMSEY

Siano dati c colori and un intero s. Allora esiste un intero N tale che, comunque si assegni un colore ad ogni sottoinsieme di $\{1, 2, \ldots, N\}$, possiamo trovare un sottoinsieme $S \subset \{1, 2, \ldots, N\}$ con $|S| = s$ elementi che è **omogeneo**, cioè tutti i sottoinsiemi di S con uno stesso numero di elementi hanno lo stesso colore.

PARIS–HARRINGTON

La stessa ipotesi iniziale, una conclusione più forte: Possiamo trovare $S \subset \{1, 2, \ldots, N\}$ omogeneo con $|S| = s$, e inoltre con in più la proprietà che l'elemento minimo di S, diciamo $\min(S)$, è più piccolo di s, vale a dire $|S| > \min(S)$.

Il teorema di Ramsey **è dimostrabile in PA** (doppia induzione del tipo $n \to n + 1$).

Il teorema di Paris–Harrington **non è dimostrabile in PA** ma **è dimostrabile nel modello ZF**. La sua dimostrazione richiede una induzione transfinita (fino all'ordinale ϵ_0).

PARIS–HARRINGTON, CONTINUAZIONE

L'aritmetica di Peano del primo ordine, abbreviata PA, ammette variabili solo su interi. La difficoltà del teorema di Paris–Harrington dipende dal fatto che è indispensabile usare certe proprietà *"intuitive"* di insiemi di interi, ma che non possono essere formulate con gli assiomi alquanto restrittivi di PA.

La dimostrazione usuale del teorema di Paris–Harrington utilizza la sua formulazione *"infinita"*: Ogni colorazione con c colori degli interi ammette un sottoinsieme infinito di interi che è omogeneo. La dimostrazione usa una applicazione **infinita** del principio intuitivo che spezzando un insieme infinito **qualunque** in due parti almeno una rimane infinita.

La dimostrazione che il teorema di Paris–Harrington theorem non è dimostrabile in PA è alquanto difficile. Essa dipende dal fatto che il numero N cresce più rapidamente di qualunque funzione computabile (tecnicamente, primitiva ricorsiva) in PA.

ERDŐS E I NUMERI DI RAMSEY

Anche i più semplici numeri di Ramsey, i numeri $R(n, n)$, sono straordinariamente difficili da determinare. Il famoso matematico ungherese Paul Erdős così ha descritto la situazione: *"Immaginate una flotta di alieni, incredibilmente più potenti di noi, che atterrano sulla Terra e chiedono il valore di $R(5, 5)$, altrimenti distruggeranno il pianeta. In questo caso, dobbiamo mettere a nostra disposizione tutti i computer e tutti i nostri matematici, e tentare di trovare questo numero. Ma se avessero chiesto invece il valore di $R(6, 6)$ allora dovremmo tentare di distruggere gli alieni."*

La situatione per il teorema di Paris–Harrington è assai peggiore. Una descrizione che rende l'idea è che esso è come l'Idra di Lerna, il mostro della mitologia greca a cui ricrescevano due teste ogni volta che se tagliava una. Tentare di risolvere il problema di Paris–Harrington con l'aritmetica di Peano è come uccidere l'Idra, dato che l'esame di ogni caso dà origine a molti sottocasi, e così via all'infinito... Ci vuole la bomba atomica, cioè il modello di Zermelo–Fraenkel.

ERCOLE E L’IDRA

“Ercole e l’Idra”

Attribuito al Pittore dell’Aquila

Greco di Caere, attivo nel 530 – 500 A.C., Etruria, circa 525 A.C.

83.AE.346, Cortesia del J. Paul Getty Museum, Malibu, California

INCERTEZZE SULL'INFINITO

Il diciassettesimo secolo vede l'inizio della matematica moderna.
Il *"metodo di esaustione"* di Archimede viene riscoperto da molti matematici: in Italia, Cavalieri e Torricelli; in Francia, Descartes e Fermat; trovando infine forma generale con Leibniz e Newton con la creazione del calcolo differenziale e integrale.
La derivata, definita come quoziente di due **infinitesimi**, e l'integrale, ottenuto come somma continua di infinitesimi, diedero origine a infinite discussioni. Cosa è in realtà un infinitesimo? L'infinito è un numero o no? È possibile trattare l'infinito come se fosse un numero? I filosofi inglesi Hume e Berkeley rifiutarono drasticamente questi concetti come privi di senso.
I matematici persero il loro tempo con discussioni sulla somma

$$1 - 1 + 1 - 1 + 1 - \dots.$$

Si può dire che, oscillando tra 0 e 1, la somma è la media $1/2$? Ma allora lo stesso punto di vista darebbe

$$1 + 0 - 1 + 1 + 0 - 1 + 0 + \cdots = \frac{2}{3}.$$

EULERO, NUMERI PRIMI, E L'INFINITO. I

Leonardo Eulero, partendo dall'equazione

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1},$$

dove p percorre i numeri primi e $s > 1$, procede coraggiosamente al limite per $s \to 1$, scrivendo l'equazione

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_p \left(1 - \frac{1}{p}\right)^{-1}.$$

A sinistra c'è la serie armonica, divergente a ∞, e perciò l'equazione di Eulero non ha senso. Ma Eulero continua osservando che se la successione dei primi fosse finita allora il termine di destra sarebbe finito, una contraddizione. Pertanto la successione dei numeri primi è infinita. Eulero va molto oltre, scrivendo la formula

$$\sum_p \frac{1}{p} = \log\log\infty.$$

Cosa intendeva Eulero prendendo il logaritmo del logaritmo dell'infinito?

EULERO, NUMERI PRIMI, E L'INFINITO. II

Proviamo a contare come George Gamow: $1+1+1+\cdots=\infty$. Facciamolo usando la serie geometrica

$$1+x+x^2+x^3+\cdots=\frac{1}{1-x}$$

e passando al limite per $x\to 1$.

Prendiamo il logaritmo della serie geometrica:

$$x+\frac{x^2}{2}+\frac{x^3}{3}+\cdots=\log\left(\frac{1}{1-x}\right).$$

Passando al limite per $x\to 1$ si trova (scrivendo imitando lo stile di Eulero)

$$\sum_{n=1}^{\infty}\frac{1}{n}=\log\infty.$$

Prendendo il logaritmo della equazione di Eulero (priva di senso) che lega la serie armonica ad un prodotto sui numeri primi completiamo la linea di pensiero che sta dietro l'affermazione che

$$\sum_{p}\frac{1}{p}=\log\log\infty.$$

Ragionamento privo di senso? No, se eliminiamo l'infinito seguendo Aristotele. Ma invece di una paginetta, questo richiederebbe un piccolo volume...

DIREZIONI E MODE

Due vedute contrastanti: una, che accetta l'infinito come quantità matematica da trattare in modo speciale, l'altra, di tipo aristotelico, che vede l'infinito come una comoda convenzione ma mancante di rigore.

Il *metodo* di Archimede: Un approccio non rigoroso al problema, ma che conduce rapidamente alla conclusione giusta e che può essere reso rigoroso in un secondo tempo. È il prototipo del pragmatismo matematico.

Il punto di vista di Aristotele: L'infinito è una convenzione per tutto ciò che non è limitato *a priori*.

Cominciando con Cauchy all'inizio dell'Ottocento, il punto di vista rigoroso di Aristotele fu accettato. L'insegnamento tradizionale del calcolo infinitesimale, con gli epsilon e delta che indicano quantità arbitrariamente piccole usate per definire i passaggi al limite, ne è l'esempio più semplice.

IL RASOIO DI OCCAM

Dobbiamo allora arrivare alla conclusione che il punto di vista aristotelico ha alla fin fine vinto la battaglia? È l'infinito soltanto una comoda convenzione da evitarsi dato che manca di rigore?

Niente affatto. L'infinito è rientrato in matematica in modo rigoroso, dimostrandosi addirittura essenziale, per coesistere con l'approccio finitistico di Aristotele. Non è più necessario formulare in termini finiti ogni ragionamento matematico. Rifiutare l'infinito in modo sistematico conduce a forzature e contorsioni intellettuali che indicano al matematico che questo rifiuto non è buona cosa.

Lo scopo finale è quello di comprendere, ma occorre una solida base. Occorre procedere col "Rasoio di Occam", il filosofo medioevale:

Scegliere sempre la strada più semplice.

In questo modo, considerazioni estetiche entrano a fare parte della matematica.

CANTOR E LA TEORIA DEGLI INSIEMI

La rivoluzione che ha permesso all'infinito di far parte della matematica comincia con la nozione di **insieme**, dovuta a Bernard Bolzano nel 1847: **Un insieme è una collezione di oggetti, ma senza alcuna considerazione del loro ordine.**

Ritratto di Bolzano. Áron Pulzer (1839).

Solo più tardi con Georg Cantor vengono poste le fondamenta di una teoria degli insiemi infiniti.

Prima di Cantor l'infinito era semplicemente la negazione del finito. Nella sua memoria del 1874, destinata a cambiare il corso della matematica, Cantor dimostra che vi sono diverse nozioni di infinito, formanti una intera gerarchia.

L'infinito più semplice, $1, 2, 3 \ldots, \infty$ come nel libro di Gamow, viene indicato con il simbolo $\aleph_0$.

LA DIAGONALE DI CANTOR

Una lista numerabile:

$$0.643546675432534645600112\ldots$$
$$\searrow$$
$$0.100053453647545546043860\ldots$$
$$\searrow$$
$$0.000000000000100004534237\ldots$$
$$\searrow$$
$$0.999999999961045674732017\ldots$$
$$\searrow$$
$$0.222955600333054564501179\ldots$$
$$\searrow$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\boxed{diagonal = 0.60095\ldots}$$

Un numero con nessuna cifra uguale alla corrispondente cifra della diagonale non può fare parte della lista.

IL SORGERE DI DIFFICOLTÀ

Il considerare insiemi i cui elementi sono a loro volta insiemi porta a contraddizioni, quali il paradosso di Burali-Forti che sorge quando si parla dell'*insieme composto dalla totalità degli insiemi.*

Il paradosso di Russell, che distrusse gran parte dell'opera di Frege sui fondamenti della logica matematica, consiste nel considerare l'insieme S i cui elementi sono gli insiemi che non contengono se stessi come elemento. Infatti, se S è un elemento di S allora, per definizione di S, S non è un elemento di S. Se invece S non è elemento di S allora S deve essere elemento di S; in tutti e due i casi vi è contraddizione.

Una soluzione: La teoria assiomatica degli insiemi (Zermelo–Fraenkel). Impone restrizioni (assiomi) per la definizione di insieme.

Seconda soluzione: Costruttivismo (Hilbert). Sono permessi solo oggetti finiti e precise regole di deduzione.

Terza soluzione: Intuizionismo (Brouwer). Un oggetto matematico non esiste finchè non è stato costruito.

L'IPOTESI DEL CONTINUO

La teoria di Zermelo–Fraenkel consiste di otto assiomi fondamentali, accettati oggi come fondamento della teoria degli insiemi. Il sesto assioma di ZF è l'esistenza di un insieme infinito.
Un nono assioma, l'assioma C della scelta, che afferma che da una collezioni di insiemi non vuoti si può formare un insieme prendendo un elemento da ciascun insieme, fu aggiunto in seguito, in quello che è chiamato il modello ZFC della teoria degli insiemi.

Nella teoria ZF, il continuo è dato da $2^{\aleph_0}$, la cardinalità dell'insieme di tutti i sottoinsiemi dei numeri naturali. Un famoso problema posto da Cantor era di determinare se il primo numero cardinale infinito non numerabile, indicato con $\aleph_1$, fosse il continuo $2^{\aleph_0}$. L'ipotesi del continuo CH è la validità dell'equazione $\aleph_1 = 2^{\aleph_0}$.

NOTA: Definire $continuum = 2^{\aleph_0}$ come CH è un errore popolare tra i fisici, perpretato anche da Gamow nel suo libro.

Ci sono voluti novanta anni per rispondere all domanda di Cantor. La risposta è che CH è indipendente da ZFC (Kurt Gödel, Paul Cohen).

IL PARADOSSO DI BANACH–TARSKI

Gödel e Cohen dimostrarono che l'assioma della scelta C è indipendente da ZF, quindi se ZF è una teoria non contradditoria allora ZF+C è non contradditoria, ma anche ZF+(negazione di C) è non contradditoria, dando luogo a due teorie matematiche distinte.

L'assioma C è molto conveniente per certi versi ed è accettato dalla maggioranza dei matematici. Però non tutti i matematici sono contenti con C, dato che porta anche a risultati non conformi alla intuizione proveniente dal mondo reale.

Un esempio ben noto è il paradosso di Banach–Tarski: È possibile decomporre la palla di raggio 1 in cinque parti e rimetterle insieme in modo da formare due palle di raggio 1. Strano, ma non cè contraddizione. Le cinque parti, costruite per mezzo dell'assioma della scelta, sono così pazzesche di forma che non si possono nemmeno misurare.

GLI UNIVERSI DI GROTHENDIECK

Come per C, anche CH o la negazione di CH possono essere aggiunti come nuovi assiomi a ZF. Tuttavia l'ultima parola in proposito non è ancora stata scritta e sono state proposte alternative soluzioni.

Il grande De Giorgi ha proposto un sistema di assiomi che tiene conto di altri fattori, che sono chiamati *"qualità"*, che servono a mantenere la teoria dentro i limiti dell'intuizione.

Un'altra soluzione è stata proposta da Grothendieck con la sua teoria degli *"universi"*. In parole povere, un universo U è un insieme nel quale si possono fare tutte le operazioni di ZF senza uscire da U. L'esistenza di un universo U non può essere dedotta da ZF (è risultata equivalente all'esistenza di grandi numeri cardinali fortemente inaccessibili). Gli universi di Grothendieck danno modelli di ZF nei quali ha senso parlare dell'insieme di tutti gli insiemi.

UN SUCCESSO DELLA TEORIA DEGLI INSIEMI

Un esempio importante di equazione diofantea è l'equazione $f(x_1, \ldots, x_n) = 0$, con f polinomio a coefficienti interi, composto da monomi tutti dello stesso grado d, da risolvere in interi non tutti 0.
Sulla base di molti casi, Artin formulò la congettura che se $n > d^2$ allora esistono interi x_i non tutti nulli tali che $f(x_1, \ldots, x_n)$ è divisibile per p^m, per ogni numero primo p ed ogni esponente m. Si parla allora di solubilità p-adica.

La prima grande sorpresa fu la dimostrazione della congettura di Artin fatta da Ax e Kochen nel 1965, ma con la condizione supplementare che il numero primo p deve essere abbastanza grande rispetto al grado d (indipendentemente da come si prenda f).
La seconda sorpresa fu un esempio dato da Guy Terjanan che esiste un polinomio omogeneo di grado 4 in 18 variabili senza soluzioni 2-adiche. Quindi la condizione di Ax e Kochen non può essere evitata.

Il punto di tutto questo è che la dimostrazione di Ax e Kochen dipende in modo essenziale dall'assioma della scelta AC. Soltanto più tardi Paul Cohen (lo stesso della CH) diede una dimostrazione costruttiva.

LA PRESENZA DELL'INFINITO NEL FINITO. I

L'avvento del computer ha portato il punto di vista finitistico di Aristotele assai più vicino al mondo reale. Calcoli impossibili da eseguire in una vita umana sono adesso fattibili in pochi minuti usando il computer. Questo ci porta ad una nuova nozione del finito: da una parte, il finito raggiungibile in tempo reale con il computer, dall'altra il finito impossibilmente grande, esemplificato da semplicissimi programmi il cui tempo di esecuzione supera l'età dell'universo.

Buttiamo giù un numero di 500 cifre e cerchiamo di scomporlo in fattori primi. Supponiamo di essere in grado di consultare l'oracolo di Delfi e di ricevere una risposta. Allora si fa la verifica in una frazione di secondo: basta moltiplicare tra loro i fattori, con un costo di tempo che è solo una potenza del numero delle cifre dell'input. Diciamo che la verifica della fattorizzazione è di classe **P** (polinomiale). Ma il fattorizzare senza l'oracolo è tuttora fuori dalla portata dei nostri computers.

Peter Shor ha dimostrato che la fattorizzazione è in **P** se si usa un (ipotetico) computer quantistico. Le opinioni restano divise se la fattorizzazione con un computer ordinario sia in **P** o no.

LA PRESENZA DELL'INFINITO NEL FINITO. II

Più precisamente, moltiplicare tra loro due numeri si fa con un numero di passi non superiore al quadrato del numero di cifre dei due numeri. Si parla allora di complessità polinomiale.

DEFINIZIONE. *La classe dei problemi risolubili deterministicamente con complessità polinomiale si indica con* **P***. La classe dei problemi la cui soluzione è verificabile (in maniera* ***non deterministica****) con complessità polinomiale si indica con* **NP***.*

Nel 1971 il matematico canadese Stephen Cook fece una scoperta straordinaria, cioè l'esistenza di problemi che sono **NP-completi**: Un problema si dice **NP**-completo se

(i) appartiene alla classe **NP**

(ii) è **NP**-hard, cioè ogni problema in **NP** può essere ridotto a questo, in tempo polinomiale.

LA PRESENZA DELL'INFINITO NEL FINITO. III

La scoperta di Cook ha una conseguenza impensata (da qui l'importanza della scoperta). Se riuscissimo a risolvere un solo problema **NP**-completo in modo deterministico, allora **NP**$=$**P**. Se la verifica di una ipotetica soluzione di un problema è facile, allora la soluzione del problema sarebbe anch'essa facile. Da osservare che "facile" è solamente una cosa teorica, dato che programmi di complessità polinomiale di grado alto non sono utili nella pratica. Quindi anche se fosse **NP**$=$**P** i matematici non perderebbero il posto di lavoro per mancanza di problemi da risolvere...

Ad esempio, il problema di trovare una *clique* di k vertici in un grafo arbitrario (cioè un sottografo completo di k vertici) è **NP**-completo. È chiaro che appartiene a **NP**: L'oracolo ci dice i k vertici del sottografo, e la verifica si fa controllando che tutte le $k(k-1)/2$ connessioni sono presenti.
Trovare i k vertici senza l'aiuto dell'oracolo è un'altra storia, come ci dice la nostra esperienza con il numero di Ramsey $R(6,6)$. (Almeno secondo Erdős.)

CONCLUSIONE

Moltissimi classici problemi di calcolo combinatorio sono **NP**-completi e la maggioranza degli esperti del settore ritiene che **P** non è uguale a **NP**.

Vi sono varianti della questione, una in cui la soluzione non è deterministica al 100%, ma è ottenuta con altissima probabilità aggiungendo un input supplementare di tipo probabilistico con un numero di bit di tipo polinomiale. Questo avviene nella pratica: esiste per esempio un metodo rapido di questo tipo per certificare che un numero è primo, aggiungendo all'input il dato di una curva ellittica scelta a caso.
Un'altra questione è cosa succede se si ammette l'uso di un (ipotetico) computer quantistico.
Tutte queste varianti restano aperte.

Forse la soluzione di questi problemi, con la loro formulazione finita, richiederà una escursione fino all'infinito come per il teorema di Paris–Harrington. Il futuro darà la risposta. Certamente il computer ci ha mostrato, in modo drammatico, la distinzione tra il finito della vita reale, e il finito che va oltre la nostra comprensione, come nel libro *"Uno, due, tre,. . . infinito"* di George Gamow.