Martin Aigner
Günter M. Ziegler

# Proofs from THE BOOK

Martin Aigner
Günter M. Ziegler

# Proofs from THE BOOK

Edizione italiana
a cura di Alfio Quarteroni

Con 250 figure
Comprese le illustrazioni
di Karl H. Hofmann

Springer

MARTIN AIGNER
Freie Universität Berlin
Institut für Mathematik II (WE2)
Arnimallee 3
14195 Berlin, Germany
email: aigner@math.fu-berlin.de

GÜNTER M. ZIEGLER
Technische Universität Berlin
Institut für Mathematik, MA 6-2
Straße des 17. Juni 136
10623 Berlin, Germany
email: ziegler@math.tu-berlin.de

Edizione italiana a cura di:
ALFIO QUARTERONI
MOX, Politecnico di Milano, Milano, Italy
e CMCS-EPFL, Lausanne, Switzerland

Traduzione a cura di:
Silvia Quarteroni
Department of Computer Science
University of York, York, UK



Springer-Verlag fa parte di Springer Science+Business Media

springer.com



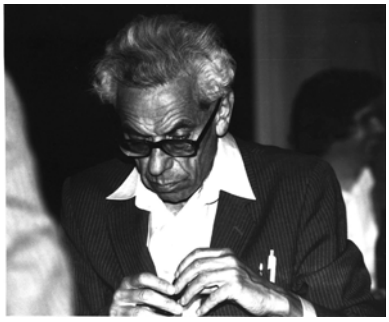
ISBN 10 88-470-0435-7
ISBN 13 978-88-470-0435-7



Riprodotto in copia camera-ready da file originali forniti dagli Autori e rielaborati in italiano dal Traduttore
Progetto grafico della copertina: Deblik, Berlino
Stampato in Italia: Signum, Bollate (Mi)

# Prefazione

Paul Erdős amava parlare del "Libro" in cui Dio conserva le dimostrazioni perfette per i teoremi matematici, seguendo il detto di G. H. Hardy secondo il quale non vi è posto perenne per la matematica brutta. Erdős diceva anche che non è necessario credere in Dio, tuttavia in quanto matematici si deve credere nel Libro. Alcuni anni fa gli suggerimmo di scrivere una prima (e assai modesta) approssimazione del Libro. Egli fu entusiasta dell'idea e, come gli era peculiare, si mise immediatamente al lavoro, riempiendo pagine su pagine con i suoi suggerimenti. Il nostro libro sarebbe dovuto essere pubblicato nel marzo 1998, come strenna per l'85-esimo compleanno di Erdős. Essendo sfortunatamente morto nell'estate del 1996, Paul non compare come co-autore. Tuttavia questo libro è dedicato alla sua memoria.



Paul Erdős

*"Il Libro"*

Non abbiamo alcuna definizione o caratterizzazione di cosa costituisca una *dimostrazione da Libro* (NdT: spesso lasceremo questa espressione nella sua versione originale inglese: *Proof from THE BOOK,* al fine di essere più fedeli al titolo di quest'opera): ci limiteremo qui a proporre alcuni esempi, nella speranza che i nostri lettori condividano il nostro entusiasmo per idee brillanti, astute intuizioni e meravigliose osservazioni. Speriamo che essi gradiscano tutto questo nonostante le imperfezioni della nostra esposizione. La scelta che abbiamo fatto è in larga misura influenzata dallo stesso Paul Erdős. Un buon numero di questi argomenti furono suggeriti direttamente da lui e molte delle dimostrazioni sono riconducibili direttamente a lui o furono abbozzate grazie al suo intuito supremo nel porre la giusta domanda o nel formulare la giusta congettura. Pertanto, questo libro riflette in larga misura il punto di vista di Paul Erdős su cosa debba considerarsi una *Proof from THE BOOK*.

Nella nostra scelta degli argomenti, la limitazione che ci siamo imposti è che qualunque cosa contenuta nel libro sia accessibile a lettori la cui formazione includa solo una modesta quantità di tecniche che si acquisiscono nei corsi di laurea in Matematica. Un po' di algebra lineare, alcuni elementi di base di analisi e teoria dei numeri, ed una salutare cucchiaiata di concetti e ragionamenti elementari di matematica discreta dovrebbero essere sufficienti per capire ed apprezzare tutto quanto vi è in questo libro.

Siamo estremamente riconoscenti alle tante persone che ci hanno aiutato e sostenuto in questo progetto — tra essi gli studenti di un seminario in cui abbiamo discusso una versione preliminare, Benno Artmann, Stephan Brandt, Stefan Felsner, Eli Goodman, Torsten Heldmann, e Hans Mielke. Ringraziamo Margrit Barrett, Christian Bressler, Ewgenij Gawrilow, Michael Joswig, Elke Pose, e Jörg Rambau per il loro aiuto tecnico nella fase

di composizione di questo testo. Abbiamo un grande debito nei confronti di Tom Trotter che ha letto il manoscritto dalla prima all'ultima pagina, di Karl H. Hofmann per i suoi magnifici disegni, e più di tutti nei confronti del grande Paul Erdős.

Berlino, marzo 1998 *Martin Aigner · Günter M. Ziegler*

# Prefazione alla Seconda Edizione

La prima edizione di questo libro è stata accolta in modo meraviglioso. Inoltre, abbiamo ricevuto un numero inusuale di lettere contenenti commenti e correzioni, alcune scorciatoie, così come suggerimenti interessanti per dimostrazioni alternative e nuovi argomenti da trattare (pur cercando di riportare dimostrazioni *perfette*, tale non è la nostra esposizione).

La seconda edizione ci fornisce l'opportunità di presentare questa nuova versione del nostro libro: esso contiene tre ulteriori capitoli, revisioni sostanziali e nuove dimostrazioni in diversi altri capitoli, molte delle quali basate sui numerosi suggerimenti che abbiamo ricevuto. Abbiamo anche eliminato un capitolo del vecchio libro, quello sul "problema delle tredici sfere", la cui dimostrazione richiedeva dettagli che non abbiamo potuto completare in modo da renderla breve ed elegante.

Ringraziamo tutti i lettori che ci hanno scritto e pertanto ci hanno aiutato—fra essi Stephan Brandt, Christian Elsholtz, Jürgen Elstrodt, Daniel Grieser, Roger Heath-Brown, Lee L. Keener, Christian Lebœuf, Hanfried Lenz, Nicolas Puech, John Scholes, Bernulf Weißbach, e *molti* altri. Grazie di nuovo per l'aiuto e il supporto a Ruth Allewelt e Karl-Friedrich Koch di Springer Heidelberg, a Christoph Eyrich e Torsten Heldmann a Berlino, ed a Karl H. Hofmann per i nuovi splendidi disegni.

Berlino, settembre 2000 *Martin Aigner · Günter M. Ziegler*

# Prefazione alla Terza Edizione

Non avremmo mai sognato, mentre preparavamo la prima edizione di questo libro nel 1998, il grande successo che questo progetto avrebbe avuto, con traduzioni in molte lingue, risposte entusiastiche da tanti lettori, e tanti meravigliosi consigli per miglioramenti, aggiunte, e nuovi argomenti — che potrebbero impegnarci per anni.

Dunque, questa terza edizione offre due nuovi capitoli (sulle identità delle partizioni di Eulero, e sul mescolamento delle carte), tre dimostrazioni sulla serie di Eulero appaiono in un capitolo a parte, e vi è un certo numero di ulteriori miglioramenti come il trattamento di Calkin-Wilf-Newman sulla "enumerazione dei razionali". Questo è tutto, per il momento!

Ringraziamo tutti coloro che hanno sostenuto questo progetto durante gli

ultimi cinque anni e il cui contributo ha reso questa nuova edizione diversa dalle precedenti. In particolare, David Bevan, Anders Björner, Dietrich Braess, John Cosgrave, Hubert Kalf, Günter Pickert, Alistair Sinclair, e Herb Wilf.

Berlino, luglio 2003 *Martin Aigner · Günter M. Ziegler*

# Prefazione all'Edizione Italiana

*Proofs from THE BOOK* è un'opera straordinaria che ha saputo calamitare l'interesse di numerosissimi lettori, matematici e non, come poche altre di argomento matematico apparse in questi ultimi anni. Dall'edizione originale in lingua inglese, pubblicata nel 1998, sono poi state prodotte due altre edizioni in inglese e un numero in continua crescita di traduzioni in altre lingue. L'edizione italiana corrisponde alla traduzione della terza edizione del testo inglese, uscita nel 2004, fatte salve alcune piccole revisioni che ci sono state segnalate dagli stessi autori.

*Proofs from THE BOOK* rappresenta un'opera unica nel suo genere. La matematica è una disciplina costruita su teorie codificate in lemmi e teoremi le cui dimostrazioni sono sempre rigorose, spesso avvincenti e creative, talvolta bellissime. È proprio la tensione dei matematici di ogni epoca, che li spinge a cercare dimostrazioni belle, ad aver ispirato gli autori, i quali, immaginano che vi sia UN LIBRO, cioè THE BOOK (forse addirittura di ispirazione divina), che contenga le dimostrazioni più belle della matematica, quelle che rasentano la perfezione. Al fine di essere il più rispettosi possibile del suo solenne significato evocativo, abbiamo voluto mantenere il titolo originale dell'opera anche nell'edizione italiana.

Il testo tocca diversi campi della matematica, quali la teoria dei numeri, la geometria, l'analisi, la combinatoria, la teoria dei grafi, la probabilità; per ognuno di essi vengono scelti dei risultati particolarmente significativi che hanno marcato in modo irreversibile l'evoluzione di una disciplina antichissima e tuttora straordinariamente viva. Vengono proposte le dimostrazioni più geniali, avvincenti e belle – talvolta più dimostrazioni di ogni teorema – che a buon diritto si suppone trovino posto in THE BOOK.

Pur essendo un libro che tratta argomenti non banali di matematica, questo volume non è per soli matematici. Le sue dimostrazioni non richiedono a priori un approfondito bagaglio di conoscenze (in teoria, anche un bravo studente che abbia alle spalle una laurea in discipline scientifiche dovrebbe poterle capire, apprezzare e, soprattutto, gustare). Lo stile espositivo dell'edizione originale è teso alla ricerca dell'essenzialità e del rigore, in atteggiamento quasi riverente verso l'energia dirompente che questi teoremi e queste dimostrazioni sembrano sprigionare. Nella traduzione italiana abbiamo voluto rispettare questa impostazione austera, anche se il desiderio di aderire fedelmente all'originale abbia talvolta imposto la rinuncia alle rotondità tipiche del periodare italiano.

Una caratteristica saliente di quest'opera è la perfetta simbiosi fra dimostra-

zioni di risultati classici, quelli dovuti ad alcuni fra i giganti dello sviluppo delle conoscenze umane di diversi secoli fa – quali ad esempio Euclide, Eulero, Fermat, Bernoulli, Hermite, Cauchy – risultati che hanno segnato nel secolo scorso l'evoluzione verso la matematica moderna – Hilbert, Cantor, Ramanujan, Shannon, Turan, lo stesso Erdős, etc.– e risultati che rappresentano oggi il terminale applicativo di queste straordinarie teorie matematiche che si sono costantemente migliorate e generalizzate nel corso dei secoli. La matematica è infatti un albero vivo percorso in ogni sua componente (sino alle più piccole e moderne ramificazioni) da una linfa che si alimenta con continuità grazie a radici millenarie. Non stupisce allora che in questo libro, le teorie e i teoremi "del passato" trovino applicazione in ambiti di assoluta quotidianità: come può il direttore di un museo disporre il minor numero di guardie con la certezza che ogni sala venga sorvegliata; come assicurarsi che i croupier al casinò (o gli amici al bar) mescolino un mazzo di carte con la certezza che dopo un ben preciso numero di mescolamenti possano considerarsi distribuite in modo casuale; come mettere a punto una strategia che consenta di trovare accoppiamenti stabili fra ragazzi e ragazze oppure uomini e donne appartenenti a due gruppi diversi; a quale numero minimo di colori si debba ricorrere per colorare una carta geografica; come codificare informazioni complesse – audio o video – affinché vengano trasmesse senza errori con i moderni sistemi di telecomunicazione; come completare un quadrato latino, una sorta di predecessore del moderno Sudoku; come spiegare razionalmente il fatto che il direttore del famoso hotel di Hilbert, quello con infinite stanze, possa trovar posto a nuovi ospiti anche quando l'albergo sia al completo; e innumerevoli altri.

Ritengo che questa costante interrelazione ed interposizione fra classico e moderno, teorico e applicato, finito ed infinito, nonché la presenza di numerose illustrazioni del geniale Karl H. Hofmann, non possano non affascinare ed intrigare anche chi, pur non essendo matematico, abbia sempre manifestato curiosità (o interesse) verso la più nobile e fondamentale delle scienze moderne.

Desidero, insieme a Martin Aigner e Günter M. Ziegler, ringraziare calorosamente Silvia Quarteroni del Computer Science Department dell'Università di York per la traduzione di quest'opera, seguita con passione e cura dei minimi particolari e Gianluigi Rozza dell'École Polytechnique Fédérale di Losanna per essersi occupato con generosità e precisione di tutti gli aspetti relativi alla gestione tecnica dei file ed alla correzione delle bozze. Desidero infine ringraziare i miei colleghi del Politecnico di Milano, i professori Alessandra Cherubini, Daniela Lupo, Marco Fuhrman e Piercesare Secchi, che mi hanno aiutato a trovare la traduzione più appropriata di alcuni termini matematici astrusi in alcuni settori di loro competenza.

Milano, novembre 2005 *Alfio Quarteroni*

# Nota dell'Editore

Paul Erdős era un genio; personaggio istrionico, è rimasto senza lavoro per la maggior parte della sua vita, contando pertanto sull'ospitalità di istituzioni e di colleghi alla cui porta spesso bussava alle ore più improbabili dichiarando che "la sua mente era aperta". Pur avendo condotto una vita errabonda e stravagante, Erdős è considerato una delle menti matematiche più grandiose del XX secolo, che ha fatto della ricerca dell'eleganza la caratteristica preminente del suo lavoro.

Pubblicare un volume di questo tipo, ispirato alla filosofia di vita di Paul Erdős, è stato per Springer una sfida accattivante, poiché è notorio quanto sia difficile promuovere un certo tipo di matematica, cosiddetta "divulgativa". In una recensione di questo volume apparsa su Zentralblatt Math nel 2002, Juergen Appell asseriva che è opportuno ringraziare Springer per l'insolita decisione di pubblicare anche l'edizione tedesca del famoso libro, apparso inizialmente in lingua inglese e venduto con successo in tutto il mondo. Ebbene, dalla data di pubblicazione della prima edizione in inglese ad oggi, il LIBRO, che ha venduto globalmente circa 35.000 copie, è stato tradotto in svariate lingue, precisamente in tedesco, francese, giapponese, polacco, portoghese, ungherese, farsi, mentre sono di imminente pubblicazione le traduzioni in russo, spagnolo, coreano, turco e, probabilmente, anche in cinese.

Non poteva quindi mancare l'edizione italiana. In considerazione del forte significato scientifico, ma anche editoriale, del LIBRO, abbiamo deciso di affidare questa traduzione alle sapienti cure di uno dei nomi di maggiore spessore nell'ambito della matematica italiana ed internazionale, il Prof. Alfio Quarteroni; cogliamo qui l'occasione di ringraziarlo non solo per avere accettato di imbarcarsi in questa avventura impegnativa, ma anche per la precisione e la raffinatezza con cui ha seguito i minimi dettagli dell'operazione.

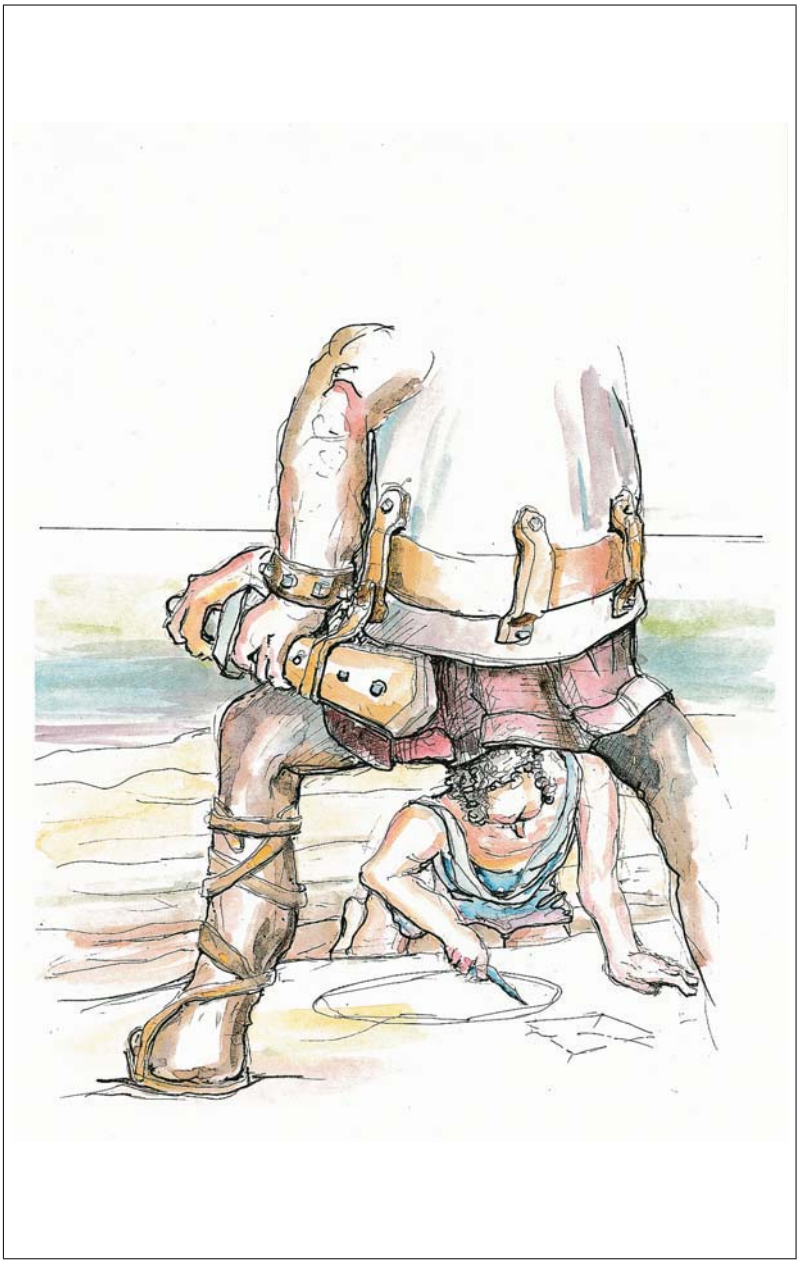
Abbiamo voluto mantenere l'inusuale formato dell'edizione originale inglese con gli ampi margini voluti per dare rilievo ad alcune definizioni ed esempi di particolare interesse, oltre che ai deliziosi schizzi di Karl H. Hofmann; riteniamo che questo libro non sia solo piacevole da leggere, ma anche da tenere in mano e guardare. Ci auguriamo che la nostra traduzione del LIBRO riscuota lo stesso successo avuto all'estero e che sia spunto per i matematici italiani per nuove discussioni su cosa sia bello, cosa sia arguto o cosa sia, come piacerebbe a Erdős, elegante.

Milano, novembre 2005

*Francesca Bonadei*
*Springer-Verlag Italia*

# Sommario

# Teoria dei Numeri





*"Irrazionalità e $\pi$"*

# I numeri primi sono infiniti: sei dimostrazioni

# Capitolo 1

È del tutto naturale incominciare queste note con quella che probabilmente è la più antica *Book Proof*, generalmente attribuita ad Euclide (*Elementi* IX, 20), la quale mostra che la successione dei numeri primi non è limitata.

■ **Dimostrazione di Euclide.** Per ogni insieme finito $\{p_1, \ldots, p_r\}$ di numeri primi, consideriamo il numero $n = p_1 p_2 \cdots p_r + 1$. Questo $n$ ha un divisore primo $p$. Tuttavia $p$ non è uno dei $p_i$: in caso contrario, $p$ sarebbe un divisore di $n$ e del prodotto $p_1 p_2 \cdots p_r$, dunque anche della differenza $n - p_1 p_2 \ldots p_r = 1$, il che è impossibile. Pertanto un insieme finito $\{p_1, \ldots, p_r\}$ non può rappresentare la collezione di *tutti* i numeri primi. □

Prima di continuare, introduciamo alcune notazioni. $\mathbb{N} = \{1, 2, 3, \ldots\}$ è l'insieme dei numeri naturali, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ l'insieme degli interi, $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ quello dei numeri primi.

Nel seguito, presenteremo varie altre dimostrazioni (tratte da una lista molto più lunga); speriamo piacciano al lettore tanto quanto piacciono a noi. Nonostante utilizzino diversi punti di vista, l'idea di base è comune a tutte: i numeri naturali crescono al di là di ogni possibile limite e ogni numero naturale $n \geq 2$ ha un divisore primo. Questi due fatti considerati insieme obbligano $\mathbb{P}$ ad essere infinito. La dimostrazione che segue è dovuta a Christian Goldbach (ed è tratta da una lettera a Eulero del 1730), la terza dimostrazione fa parte del folclore, la quarta è dovuta allo stesso Eulero, la quinta fu proposta da Harry Fürstenberg, mentre l'ultima è dovuta a Paul Erdős.

■ **Seconda dimostrazione.** Consideriamo dapprima i *numeri di Fermat* $F_n = 2^{2^n} + 1$ per $n = 0, 1, 2, \ldots$. Mostreremo che ogni coppia di numeri di Fermat è composta da numeri primi fra loro; ne seguirà che debbono esistere infiniti numeri primi. A questo scopo, verifichiamo la relazione ricorsiva

$$\prod_{k=0}^{n-1} F_k \;=\; F_n - 2 \qquad (n \geq 1),$$

dalla quale la nostra tesi segue immediatamente. In effetti, se $m$ ad esempio è un divisore di $F_k$ ed $F_n$ $(k < n)$, allora $m$ divide 2, perciò $m = 1$ o 2. Ma $m = 2$ è impossibile dal momento che tutti i numeri di Fermat sono dispari.

Dimostriamo la precedente relazione ricorsiva procedendo per induzione su $n$. Per $n = 1$ abbiamo $F_0 = 3$ e $F_1 - 2 = 3$. Per induzione concludiamo

$$\begin{aligned} F_0 &= 3 \\ F_1 &= 5 \\ F_2 &= 17 \\ F_3 &= 257 \\ F_4 &= 65537 \\ F_5 &= 641 \cdot 6700417 \end{aligned}$$

I primi sei numeri di Fermat

**Teorema di Lagrange**

*Se $G$ è un gruppo (moltiplicativo) finito e $U$ è un sottogruppo, allora $|U|$ divide $|G|$.*

■ **Dimostrazione.** Consideriamo la relazione binaria

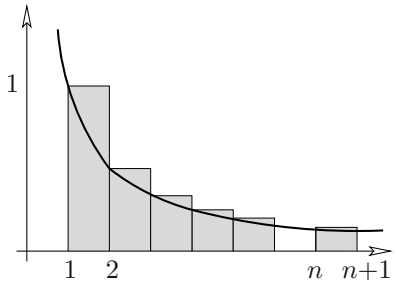
$$a \sim b : \iff ba^{-1} \in U.$$

Segue dagli assiomi di gruppo che $\sim$ è una relazione di equivalenza. La classe di equivalenza che contiene un elemento $a$ è precisamente il coinsieme

$$Ua = \{xa : x \in U\}.$$

Poiché chiaramente $|Ua| = |U|$, troviamo che $G$ si scompone in classi di equivalenza, tutte di grandezza $|U|$, e pertanto che $|U|$ divide $|G|$. □

Nel caso particolare in cui $U$ sia un sottogruppo ciclico, $\{a, a^2, \ldots, a^m\}$ troviamo che $m$ (il più piccolo intero positivo tale che $a^m = 1$, detto l'*ordine* di $a$) divide la cardinalità $|G|$ del gruppo.



Gradini sopra la funzione $f(t) = \frac{1}{t}$

che

$$\prod_{k=0}^{n} F_k \;=\; \Big(\prod_{k=0}^{n-1} F_k\Big)F_n \;=\; (F_n - 2)F_n \;=$$
$$= (2^{2^n} - 1)(2^{2^n} + 1) \;=\; 2^{2^{n+1}} - 1 \;=\; F_{n+1} - 2. \qquad \square$$

■ **Terza dimostrazione.** Supponiamo che $\mathbb{P}$ sia finito e $p$ rappresenti il più grande numero primo. Consideriamo il cosiddetto *numero di Mersenne* $2^p - 1$ e mostriamo che ogni fattore primo $q$ di $2^p - 1$ è maggiore di $p$, il che permetterà di ottenere la conclusione desiderata. Sia $q$ un numero primo divisore di $2^p - 1$, pertanto $2^p \equiv 1 \pmod q$. Essendo $p$ primo, ciò significa che l'elemento 2 ha ordine $p$ nel gruppo moltiplicativo $\mathbb{Z}_q \backslash \{0\}$ del campo $\mathbb{Z}_q$. Questo gruppo ha $q - 1$ elementi. Dal teorema di Lagrange (riportato nel riquadro) sappiamo che l'ordine di ogni elemento divide la cardinalità del gruppo, ovvero abbiamo $p \mid q - 1$, pertanto $p < q$. □

Vediamo ora una dimostrazione che usa l'analisi elementare.

■ **Quarta dimostrazione.** Sia $x$ un numero reale e $\pi(x) := \#\{p \le x : p \in \mathbb{P}\}$ il numero di numeri primi minori o uguali a $x$. Ordiniamo in modo crescente i numeri primi $\mathbb{P} = \{p_1, p_2, p_3, \ldots\}$. Consideriamo il logaritmo naturale $\log x$, definito come $\log x = \int_1^x \frac{1}{t} dt$.

Confrontiamo ora l'area soggiacente al grafico di $f(t) = \frac{1}{t}$ con una funzione a gradino maggiorante (si veda anche l'appendice a pagina 10 per questo metodo). Allora per $n \le x < n + 1$ abbiamo

$$\begin{aligned} \log x &\le 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n-1} + \frac{1}{n} \\ &\le \sum \frac{1}{m}, \text{ dove la somma si estende a tutti gli } m \in \mathbb{N} \text{ che} \\ &\qquad \text{hanno solo divisori primi } p \le x. \end{aligned}$$

Poiché ogni $m$ di questo tipo può essere scritto in modo *univoco* come un prodotto della forma $\prod_{p \le x} p^{k_p}$, si vede che quest'ultima somma è uguale a

$$\prod_{\substack{p \in \mathbb{P} \\ p \le x}} \Big(\sum_{k \ge 0} \frac{1}{p^k}\Big).$$

La somma interna è una serie geometrica di ragione $\frac{1}{p}$, pertanto

$$\log x \;\le\; \prod_{\substack{p \in \mathbb{P} \\ p \le x}} \frac{1}{1 - \frac{1}{p}} \;=\; \prod_{\substack{p \in \mathbb{P} \\ p \le x}} \frac{p}{p-1} \;=\; \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}.$$

Poiché, chiaramente, $p_k \ge k + 1$, otteniamo

$$\frac{p_k}{p_k - 1} \;=\; 1 + \frac{1}{p_k - 1} \;\le\; 1 + \frac{1}{k} \;=\; \frac{k+1}{k},$$

e pertanto

$$\log x \;\leq\; \prod_{k=1}^{\pi(x)} \frac{k+1}{k} \;=\; \pi(x)+1.$$

Tutti sanno che $\log x$ non è limitato, dunque $\pi(x)$ è anch'esso illimitato, così possiamo concludere che ci sono infiniti numeri primi. □

■ **Quinta dimostrazione.** Dopo l'analisi, è la volta della topologia! Consideriamo la seguente curiosa topologia sull'insieme $\mathbb{Z}$ degli interi. Per $a, b \in \mathbb{Z}$, $b > 0$, poniamo

$$N_{a,b} = \{a + nb : n \in \mathbb{Z}\}.$$

Ogni insieme $N_{a,b}$ è una progressione aritmetica infinita nei due sensi. Diciamo che un insieme $O \subseteq \mathbb{Z}$ è *aperto* se esso è vuoto, oppure se per ogni $a \in O$ esiste $b > 0$ con $N_{a,b} \subseteq O$. Naturalmente, l'unione di insiemi aperti è ancora un aperto. Se $O_1, O_2$ sono aperti, e $a \in O_1 \cap O_2$ con $N_{a,b_1} \subseteq O_1$ ed $N_{a,b_2} \subseteq O_2$, allora $a \in N_{a,b_1 b_2} \subseteq O_1 \cap O_2$. Dunque concludiamo che ogni intersezione finita di aperti è un aperto. Pertanto, questa famiglia di insiemi aperti induce una topologia in bona fide (NdT: in latino nella versione originale) su $\mathbb{Z}$.

Valgono le due seguenti proprietà:

(A) Ogni insieme aperto non vuoto è infinito.

(B) Ogni insieme $N_{a,b}$ è anche chiuso.

*"Far rimbalzare sassolini all'infinito"*

In effetti, la prima segue dalla definizione. Quanto alla seconda, osserviamo che

$$N_{a,b} \;=\; \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b},$$

il che prova che $N_{a,b}$ è il complementare di un insieme aperto e pertanto è chiuso.

Sino ad ora i numeri non sono ancora entrati in scena — ma eccoli arrivare. Poiché ogni numero $n \neq 1, -1$ ha un divisore primo $p$, e dunque è contenuto in $N_{0,p}$, concludiamo che

$$\mathbb{Z} \setminus \{1, -1\} \;=\; \bigcup_{p \in \mathbb{P}} N_{0,p}.$$

Ora se $\mathbb{P}$ fosse finito, allora $\bigcup_{p\in\mathbb{P}} N_{0,p}$ sarebbe l'unione finita di insiemi chiusi (grazie a (B)), pertanto sarebbe chiuso. Conseguentemente, l'insieme $\{1, -1\}$ sarebbe aperto, ma ciò violerebbe (A). □

■ **Sesta dimostrazione.** La nostra dimostrazione finale si spinge considerevolmente oltre e dimostra non solo che esistono infiniti numeri primi, ma anche che la serie $\sum_{p\in\mathbb{P}} \frac{1}{p}$ diverge. Questo importante risultato fu formulato per la prima volta da Eulero (il che lo rende già di per sé interessante), ma la nostra dimostrazione, concepita da Erdős, è di una bellezza travolgente.

Sia $p_1, p_2, p_3, \ldots$ la successione dei numeri primi in ordine crescente, e supponiamo che $\sum_{p\in\mathbb{P}} \frac{1}{p}$ converga. Allora deve esistere un numero naturale $k$ tale che $\sum_{i\geq k+1} \frac{1}{p_i} < \frac{1}{2}$. Chiamiamo $p_1, \ldots, p_k$ i numeri primi *piccoli*, e $p_{k+1}, p_{k+2}, \ldots$ i *grandi*. Per un arbitrario numero naturale $N$ troviamo

$$\sum_{i\geq k+1} \frac{N}{p_i} \;<\; \frac{N}{2}. \tag{1}$$

Sia $N_b$ il numero degli interi positivi $n \leq N$ che sono divisibili per almeno un numero primo grande, e $N_s$ il numero di interi positivi $n \leq N$ che hanno soltanto divisori primi piccoli. Vogliamo mostrare che per un opportuno $N$

$$N_b + N_s \;<\; N,$$

il che rappresenterà la contraddizione cercata, in quanto per definizione $N_b + N_s$ dovrebbe essere uguale ad $N$.

Per stimare $N_b$ notiamo che $\lfloor \frac{N}{p_i} \rfloor$ conta il numero di interi positivi $n \leq N$ che sono multipli di $p_i$. Pertanto dalla (1) troviamo

$$N_b \;\leq\; \sum_{i\geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor \;<\; \frac{N}{2}. \tag{2}$$

Consideriamo ora $N_s$. Scriviamo ogni $n \leq N$ che ha solo divisori primi piccoli nella forma $n = a_n b_n^2$, dove $a_n$ è la parte non quadrata. Ogni $a_n$ è perciò il prodotto di numeri primi piccoli *diversi* fra loro, e concludiamo che esistono precisamente $2^k$ parti non quadrate. Inoltre, poiché $b_n \leq \sqrt{n} \leq \sqrt{N}$, troviamo che ci sono al più $\sqrt{N}$ diverse parti quadrate, e pertanto

$$N_s \;\leq\; 2^k\sqrt{N}.$$

Poiché (2) vale per *ogni* $N$, resta da trovare un numero $N$ per il quale $2^k\sqrt{N} \leq \frac{N}{2}$ oppure $2^{k+1} \leq \sqrt{N}$, e a tale scopo è sufficiente prendere $N = 2^{2k+2}$. □

## Bibliografia


[1] B. ARTMANN: *Euclid — The Creation of Mathematics,* Springer-Verlag, New York 1999.

[2] P. ERDŐS: *Über die Reihe* $\sum \frac{1}{p}$, Mathematica, Zutphen B **7** (1938), 1-2.

[3] L. EULER: *Introductio in Analysin Infinitorum,* Tomus Primus, Lausanne 1748; Opera Omnia, Ser. 1, Vol. 8.

[4] H. FÜRSTENBERG: *On the infinitude of primes,* Amer. Math. Monthly **62** (1955), 353.