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

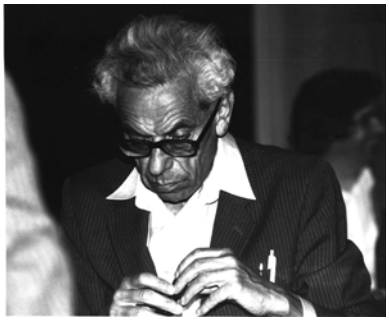
springer.com

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.

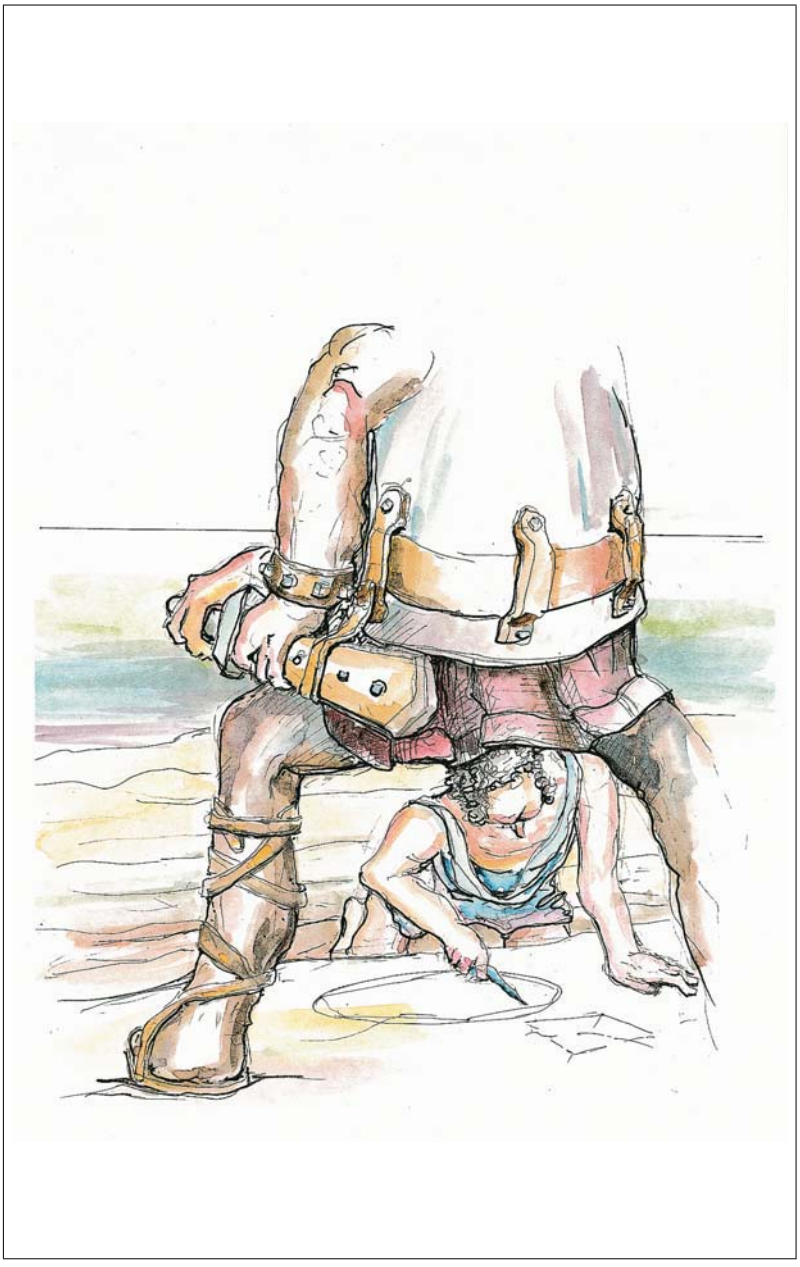
Abbiamo voluto mantenere l'inusuale formato dell'edizione originale inglese con gli ampi margini voluti per dare rilievo ad alcune definizioni ed esempi di particolare interesse, oltre che ai deliziosi schizzi di Karl H. Hofmann; riteniamo che questo libro non sia solo piacevole da leggere, ma anche 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 π"

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

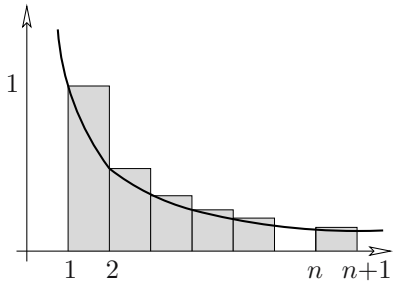
$$a \sim b : \iff ba^{-1} \in U.$$

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.

Il postulato di Bertrand

Capitolo 2

Abbiamo visto che la successione dei numeri primi $2, 3, 5, 7, \ldots$ è infinita. Per verificare che le distanze tra numeri primi successivi sono illimitate, si denoti con $N := 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p$ il prodotto di tutti i numeri primi più piccoli di $k + 2$; si noti che nessuno dei k numeri

$$N + 2, N + 3, N + 4, \ldots, N + k, N + (k + 1)$$

è primo, poiché per $2 \leq i \leq k + 1$ sappiamo che i ha un fattore primo minore di $k + 2$ e tale fattore divide anche N, dunque anche $N + i$. Con questa ricetta troviamo, per esempio per $k = 10$, che nessuno dei dieci numeri

$$2312, 2313, 2314, \ldots, 2321$$

è primo.

Non solo, possiamo anche ottenere delle maggiorazioni per le suddette distanze nella successione dei numeri primi. Una famosa maggiorazione stabilisce che "La distanza fra un numero primo ed il suo successivo non può mai superare il più piccolo dei due". Tale enunciato è noto come postulato di Bertrand, poiché fu formulato e verificato empiricamente per $n < 3\,000\,000$ da Joseph Bertrand. Esso fu dimostrato per la prima volta per tutti gli n da Pafnuty Chebyshev nel 1850. Una dimostrazione molto più semplice fu data dal genio indiano Ramanujan. La nostra *Book Proof* è di Paul Erdős: essa è tratta dalla sua prima pubblicazione, apparsa nel 1932, quando Erdős aveva 19 anni.

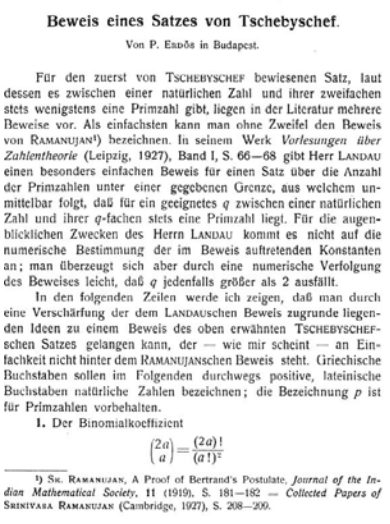
Joseph Bertrand

Il postulato di Bertrand.
Per ogni $n \geq 1$, esiste un numero primo p tale che $n < p \leq 2n$.

■ **Dimostrazione.** Stimeremo la grandezza del coefficiente binomiale $\binom{2n}{n}$ con sufficiente precisione da verificare che se esso non avesse alcun fattore primo nell'intervallo $n < p \leq 2n$, allora sarebbe "troppo piccolo". Il nostro ragionamento si articola in cinque fasi.

(1) Dimostriamo dapprima il postulato di Bertrand per $n < 4000$. A questo scopo non è necessario verificare 4000 casi: è sufficiente (si tratta del "trucco di Landau") controllare che

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001$$



Beweis eines Satzes von Tschebyschef.

Von P. Erdős in Budapest.

Für den zuerst von Tschebyschef bewiesenen Satz, laut dessen es zwischen einer natürlichen Zahl und ihrer zweifachen stets wenigstens eine Primzahl gibt, liegen in der Literatur mehrere Beweise vor. Als einfachsten kann man ohne Zweifel den Beweis von Ramanujan[1]) bezeichnen. In seinem Werk *Vorlesungen über Zahlentheorie* (Leipzig, 1927), Band I, S. 66—68 gibt Herr Landau einen besonders einfachen Beweis für einen Satz über die Anzahl der Primzahlen unter einer gegebenen Grenze, aus welchem unmittelbar folgt, daß für ein geeignetes q zwischen einer natürlichen Zahl und ihrer q-fachen stets eine Primzahl liegt. Für die augenblicklichen Zwecken des Herrn Landau kommt es nicht auf die numerische Bestimmung der im Beweis auftretenden Konstanten an; man überzeugt sich aber durch eine numerische Verfolgung des Beweises leicht, daß q jedenfalls größer als 2 ausfällt.

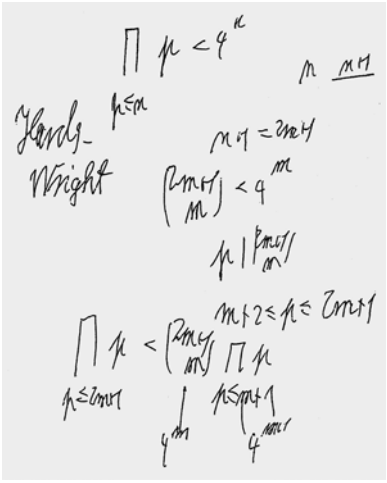
In den folgenden Zeilen werde ich zeigen, daß man durch eine Verschärfung der dem Landauschen Beweis zugrunde liegenden Ideen zu einem Beweis des oben erwähnten Tschebyschefschen Satzes gelangen kann, der — wie mir scheint — an Einfachkeit nicht hinter dem Ramanujanschen Beweis steht. Griechische Buchstaben sollen im Folgenden durchwegs positive, lateinische Buchstaben natürliche Zahlen bezeichnen; die Bezeichnung p ist für Primzahlen vorbehalten.

1. Der Binomialkoeffizient

$$\binom{2a}{a} = \frac{(2a)!}{(a!)^2}$$

[1]) Srr. Ramanujan, A Proof of Bertrand's Postulate, *Journal of the Indian Mathematical Society*, **11** (1919), S. 181—182 — *Collected Papers of* Srinivasa Ramanujan (Cambridge, 1927), S. 208—209.

sia una successione di numeri primi in cui ciascun numero è minore del doppio di quello che lo precede. Pertanto ogni intervallo $\{y : n < y \le 2n\}$, con $n \le 4000$, contiene uno di questi 14 numeri primi.



(2) Proviamo ora che

$$\prod_{p\le x} p \;\le\; 4^{x-1} \qquad \text{per ogni reale } x \ge 2, \tag{1}$$

dove la nostra notazione — qui e nel seguito — significa che il prodotto è esteso a tutti i numeri *primi* $p \le x$. La nostra dimostrazione procede per induzione sul numero di questi numeri primi. Essa non è tratta dalla pubblicazione originale di Erdős, tuttavia è anch'essa dovuta ad Erdős (si veda a margine) ed è una vera *Book Proof*. Innanzitutto osserviamo che se q è il più grande numero primo tale che $q \le x$, allora

$$\prod_{p\le x} p \;=\; \prod_{p\le q} p \qquad \text{e} \qquad 4^{q-1} \;\le\; 4^{x-1}.$$

Pertanto è sufficiente verificare (1) per il caso in cui $x = q$ sia un numero primo. Per $q = 2$ si ha "$2 \le 4$," dunque continuiamo considerando i numeri primi dispari nella forma $q = 2m + 1$. (Qui possiamo assumere, per induzione, che (1) sia valida per tutti gli interi x nell'insieme $\{2, 3, \ldots, 2m\}$.) Per $q = 2m + 1$ scomponiamo il prodotto e calcoliamo

$$\prod_{p\le 2m+1} p \;=\; \prod_{p\le m+1} p \cdot \prod_{m+1<p\le 2m+1} p \;\le\; 4^m \binom{2m+1}{m} \;\le\; 4^m 2^{2m} \;=\; 4^{2m}.$$

Si tratta di passaggi di facile verifica. In effetti,

$$\prod_{p\le m+1} p \;\le\; 4^m$$

si ottiene per induzione.

La disuguaglianza

$$\prod_{m+1<p\le 2m+1} p \;\le\; \binom{2m+1}{m}$$

segue dall'osservazione che $\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}$ è un intero, in cui i numeri primi che consideriamo sono tutti fattori del numeratore $(2m+1)!$, ma non del denominatore $m!(m+1)!$. Infine

$$\binom{2m+1}{m} \;\le\; 2^{2m}$$

vale in quanto

$$\binom{2m+1}{m} \text{ e } \binom{2m+1}{m+1}$$

sono due addendi (identici!) che compaiono in

$$\sum_{k=0}^{2m+1} \binom{2m+1}{k} = 2^{2m+1}.$$

(3)
Dal teorema di Legendre (si veda il riquadro) otteniamo che $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ contiene il fattore primo p esattamente

$$\sum_{k\geq 1}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor\right)$$

volte. Ogni addendo della somma vale al più 1, in quanto si ha

$$\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor \;<\; \frac{2n}{p^k} - 2\left(\frac{n}{p^k}-1\right) \;=\; 2,$$

ed è un numero intero. Inoltre gli addendi si annullano quando $p^k > 2n$. Pertanto $\binom{2n}{n}$ contiene p esattamente

$$\sum_{k\geq 1}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor\right) \;\leq\; \max\{r : p^r \leq 2n\}$$

volte. Ne segue che la più grande potenza di p che divide $\binom{2n}{n}$ non è più grande di $2n$. In particolare, i numeri primi $p > \sqrt{2n}$ compaiono al massimo una sola volta in $\binom{2n}{n}$.
Inoltre — e questo, secondo Erdős, rappresenta la chiave di volta della sua dimostrazione — i numeri primi p che soddisfano $\frac{2}{3}n < p \leq n$ non dividono affatto $\binom{2n}{n}$. In effetti, $3p > 2n$ implica (per $n \geq 3$, e dunque $p \geq 3$) che p e $2p$ sono i soli multipli di p che appaiono come fattori nel numeratore di $\frac{(2n)!}{n!n!}$, mentre abbiamo due p-fattori nel denominatore.

(4) Ora possiamo stimare $\binom{2n}{n}$. Per $n \geq 3$, usando una minorazione data a pagina 12, otteniamo

$$\frac{4^n}{2n} \;\leq\; \binom{2n}{n} \;\leq\; \prod_{p\leq\sqrt{2n}} 2n \;\cdot \prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p \;\cdot \prod_{n<p\leq 2n} p$$

e pertanto, essendoci non più di $\sqrt{2n}$ numeri primi $p \leq \sqrt{2n}$,

$$4^n \;\leq\; (2n)^{1+\sqrt{2n}} \;\cdot \prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p \;\cdot \prod_{n<p\leq 2n} p \qquad \text{per} \quad n \geq 3. \qquad (2)$$

(5) Supponiamo ora che non vi siano numeri primi p tali che $n < p \leq 2n$, così che il secondo prodotto in (2) valga 1. Sostituendo (1) in (2) otteniamo

$$4^n \;\leq\; (2n)^{1+\sqrt{2n}}\, 4^{\frac{2}{3}n}$$

ovvero

$$4^{\frac{1}{3}n} \;\leq\; (2n)^{1+\sqrt{2n}}, \qquad (3)$$

il che è falso per n sufficientemente grande! In effetti, usando la disuguaglianza $a+1 < 2^a$ (che si dimostra per induzione per tutti i numeri $a \geq 2$) si ottiene

$$2n = \left(\sqrt[6]{2n}\right)^6 < \left(\left\lfloor\sqrt[6]{2n}\right\rfloor + 1\right)^6 < 2^{6\left\lfloor\sqrt[6]{2n}\right\rfloor} \leq 2^{6\sqrt[6]{2n}}, \qquad (4)$$

Teorema di Legendre

Il numero $n!$ contiene il fattore primo p esattamente

$$\sum_{k\geq 1}\left\lfloor\frac{n}{p^k}\right\rfloor$$

volte.

■ **Dimostrazione.** Vi sono esattamente $\lfloor\frac{n}{p}\rfloor$ fattori di $n! = 1\cdot 2\cdot 3\cdot\ldots\cdot n$ divisibili per p, il che si traduce in $\lfloor\frac{n}{p}\rfloor$ p-fattori. Inoltre, $\lfloor\frac{n}{p^2}\rfloor$ fattori di $n!$ sono anche divisibili per p^2, il che si traduce nei successivi $\lfloor\frac{n}{p^2}\rfloor$ fattori primi p di $n!$, etc. □

I seguenti esempi
$\binom{26}{13} = 2^3\cdot 5^2\cdot 7\cdot 17\cdot 19\cdot 23$
$\binom{28}{14} = 2^3\cdot 3^3\cdot 5^2\cdot 17\cdot 19\cdot 23$
$\binom{30}{15} = 2^4\cdot 3^2\cdot 5\cdot 17\cdot 19\cdot 23\cdot 29$
mostrano che fattori primi "molto piccoli" $p < \sqrt{2n}$ possono apparire come potenze più grandi in $\binom{2n}{n}$, "piccoli" numeri primi con $\sqrt{2n} < p \leq \frac{2}{3}n$ appaiono al più una sola volta, mentre fattori nell'intervallo con $\frac{2}{3}n < p \leq n$ non appaiono per nulla

e pertanto per $n \geq 50$ (e quindi $18 < 2\sqrt{2n}$) otteniamo da (3) e (4)

$$2^{2n} \leq (2n)^{3\left(1+\sqrt{2n}\right)} < 2^{\sqrt[6]{2n}\left(18+18\sqrt{2n}\right)} < 2^{20\sqrt[6]{2n}\sqrt{2n}} = 2^{20(2n)^{2/3}}.$$

Ciò implica $(2n)^{1/3} < 20$, e dunque $n < 4000$. □

Si può dedurre anche di più da questo genere di stime: dalla (2) possiamo derivare con gli stessi metodi che

$$\prod_{n<p\leq 2n} p \geq 2^{\frac{1}{30}n} \quad \text{per} \quad n \geq 4000,$$

e dunque che ci sono almeno

$$\log_{2n}\left(2^{\frac{1}{30}n}\right) \;=\; \frac{1}{30}\,\frac{n}{\log_2 n + 1}$$

numeri primi compresi fra n e $2n$.

Questa stima non è poi tanto grossolana: il "vero" numero di numeri primi in questo intervallo è all'incirca $n/\log n$. Ciò deriva dal "teorema dei numeri primi", il quale afferma che il limite

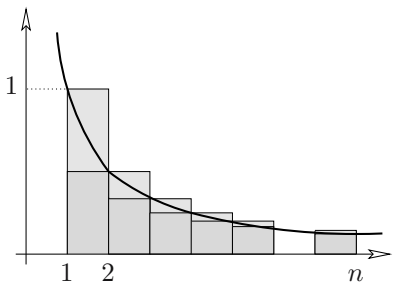
$$\lim_{n\to\infty} \frac{\#\{p \leq n : p \text{ è primo}\}}{n/\log n}$$

esiste, ed è uguale a 1. Questo è un risultato famoso che fu dimostrato per la prima volta da Hadamard e de la Vallée-Poussin nel 1896; Selberg e Erdős trovarono una dimostrazione elementare nel 1948, che pur non facendo uso di tecniche di analisi complessa, è lunga e laboriosa.

Sembra tuttavia che sul teorema dei numeri primi non sia ancora stata detta l'ultima parola: ad esempio la dimostrazione dell'ipotesi di Riemann (si veda a pagina 47), uno dei principali problemi aperti, tuttora irrisolti, della matematica, fornirebbe anche un miglioramento sostanziale della stima del teorema dei numeri primi. Ma ne deriverebbe un decisivo miglioramento anche per il postulato di Bertrand. In effetti, quello che segue è un famoso problema irrisolto:

> *È sempre possibile trovare un numero primo compreso fra n^2 e $(n+1)^2$?*

Per ulteriori informazioni si vedano [3, p. 19] e [4, pp. 248, 257].



Appendice: alcune stime

Stime attraverso integrali

Esiste un metodo molto semplice ma efficace per stimare somme utilizzando integrali (come già visto a pagina 4). Per stimare *i numeri armonici*

$$H_n \;=\; \sum_{k=1}^{n} \frac{1}{k},$$

tracciamo la figura a margine della pagina precedente. Confrontando l'area al di sotto del grafico di $f(t) = \frac{1}{t}$ $(1 \leq t \leq n)$ con l'area dei rettangoli ombreggiati scuri deriviamo che

$$H_n - 1 \;=\; \sum_{k=2}^{n} \frac{1}{k} \;<\; \int_1^n \frac{1}{t}\, dt \;=\; \log n,$$

mentre, confrontandola con l'area dei rettangoli grandi (che includono le parti ombreggiate chiare), otteniamo che

$$H_n - \frac{1}{n} \;=\; \sum_{k=1}^{n-1} \frac{1}{k} \;>\; \int_1^n \frac{1}{t}\, dt \;=\; \log n.$$

Considerando entrambe le disuguaglianze, otteniamo

$$\log n + \frac{1}{n} \;<\; H_n \;<\; \log n \;+\; 1.$$

In particolare, $\lim_{n\to\infty} H_n = \infty$, e l'ordine di infinito di H_n è dato da $\lim_{n\to\infty} \frac{H_n}{\log n} = 1$. Tuttavia si conoscono stime decisamente migliori (si veda [2]), come ad esempio

$$H_n \;=\; \log n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \frac{1}{120n^4} + O\left(\frac{1}{n^6}\right),$$

Qui $O\left(\frac{1}{n^6}\right)$ indica una funzione $f(n)$ tale che la disuguaglianza $f(n) \leq c\frac{1}{n^6}$ sia vera per una opportuna costante c

essendo $\gamma \approx 0.5772$ la "costante di Eulero".

Stima dei fattoriali — formula di Stirling

Lo stesso metodo applicato a

$$\log(n!) \;=\; \log 2 + \log 3 + \ldots + \log n \;=\; \sum_{k=2}^{n} \log k$$

fornisce

$$\log((n-1)!) \;<\; \int_1^n \log t\, dt \;<\; \log(n!),$$

dove l'integrale è facilmente calcolabile, essendo

$$\int_1^n \log t\, dt \;=\; \Big[t \log t - t\Big]_1^n \;=\; n \log n - n + 1.$$

Pertanto otteniamo una minorazione per $n!$

$$n! \;>\; e^{n \log n - n + 1} \;=\; e\Big(\frac{n}{e}\Big)^n$$

e allo stesso tempo una maggiorazione

$$n! \;=\; n\,(n-1)! \;<\; n e^{n \log n - n + 1} \;=\; en\Big(\frac{n}{e}\Big)^n.$$

Un'analisi più attenta è necessaria in questo caso per descrivere il comportamento asintotico di $n!$, come si ottiene dalla *formula di Stirling*

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

Esistono versioni ancora più precise, come ad esempio

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n\left(1+\frac{1}{12n}+\frac{1}{288n^2}-\frac{139}{5140n^3}+O\left(\frac{1}{n^4}\right)\right).$$

Qui $f(n) \sim g(n)$ significa che $\lim_{n\to\infty}\frac{f(n)}{g(n)} = 1$

Stima di coefficienti binomiali

Proprio dalla definizione dei coefficienti binomiali $\binom{n}{k}$ come numero di k-sottoinsiemi di un n-insieme, sappiamo che la successione $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$ di coefficienti binomiali

- ha come somma $\sum_{k=0}^{n}\binom{n}{k} = 2^n$
- è simmetrica: $\binom{n}{k} = \binom{n}{n-k}$.

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
 & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & \\
\end{array}$$

Il triangolo di Pascal

Dall'equazione funzionale $\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}$ si ottiene facilmente che per ogni n i coefficienti binomiali $\binom{n}{k}$ formano una successione simmetrica e *unimodale*: essa cresce verso il centro, di modo che i coefficienti binomiali centrali sono i più grandi della successione

$$1 = \binom{n}{0} < \binom{n}{1} < \ldots < \binom{n}{\lfloor n/2\rfloor} = \binom{n}{\lceil n/2\rceil} > \ldots > \binom{n}{n-1} > \binom{n}{n} = 1.$$

Qui $\lfloor x\rfloor$ risp. $\lceil x\rceil$ indica il numero x arrotondato per difetto risp. per eccesso al più vicino intero.

Dalle formule asintotiche per i fattoriali precedentemente citate si possono ottenere stime molto precise per le grandezze dei coefficienti binomiali. Tuttavia, in questo libro faremo uso solo di stime semplici e molto deboli, quali ad esempio: $\binom{n}{k} \le 2^n$ per ogni k, mentre per $n \ge 2$ abbiamo

$$\binom{n}{\lfloor n/2\rfloor} \ge \frac{2^n}{n},$$

essendo l'uguaglianza valida solo per $n = 2$. In particolare, per $n \ge 1$,

$$\binom{2n}{n} \ge \frac{4^n}{2n}.$$

Questo vale poiché $\binom{n}{\lfloor n/2\rfloor}$, un coefficiente binomiale mediano, è il più grande elemento della successione $\binom{n}{0}+\binom{n}{n}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}$, la cui somma vale 2^n, e la cui media è pertanto $\frac{2^n}{n}$.

D'altro canto, per i coefficienti binomiali abbiamo la maggiorazione:

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} \le \frac{n^k}{k!} \le \frac{n^k}{2^{k-1}},$$

che fornisce una stima ragionevolmente buona per i coefficienti binomiali "piccoli" nella coda della successione, quando n è grande (rispetto a k).

Bibliografia

[1] P. ERDŐS: *Beweis eines Satzes von Tschebyschef,* Acta Sci. Math. (Szeged) **5** (1930-32), 194-198.

[2] R. L. GRAHAM, D. E. KNUTH & O. PATASHNIK: *Concrete Mathematics. A Foundation for Computer Science,* Addison-Wesley, Reading MA 1989.

[3] G. H. HARDY & E. M. WRIGHT: *An Introduction to the Theory of Numbers,* fifth edition, Oxford University Press 1979.

[4] P. RIBENBOIM: *The New Book of Prime Number Records,* Springer-Verlag, New York 1989.

I coefficienti binomiali non sono (quasi) mai potenze

Capitolo 3

Esiste un epilogo al postulato di Bertrand che fornisce uno splendido risultato sui coefficienti binomiali. Nel 1892 Sylvester rafforzò il postulato di Bertrand nel seguente modo:

> *Se $n \geq 2k$, allora almeno uno dei numeri $n, n-1, \ldots, n-k+1$ ha un divisore primo p più grande di k.*

Si noti che per $n = 2k$ si ottiene precisamente il postulato di Bertrand. Nel 1934, Erdős fornì una *Book Proof* breve ed elementare del risultato di Sylvester, seguendo la traccia della sua dimostrazione del postulato di Bertrand. Esiste un enunciato equivalente per il teorema di Sylvester:

> *Il coefficiente binomiale*
>
> $$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} \qquad (n \geq 2k)$$
>
> *ha sempre un fattore primo $p > k$.*

Tenendo a mente questa osservazione, ci interessiamo ad un altro dei gioielli di Erdős. Quando $\binom{n}{k}$ è uguale ad una potenza m^ℓ? È semplice notare che ci sono infinite soluzioni per $k = \ell = 2$, ovvero soluzioni dell'equazione $\binom{n}{2} = m^2$. In effetti, se $\binom{n}{2}$ è un quadrato, allora lo è anche $\binom{(2n-1)^2}{2}$. Per verificarlo, si ponga $n(n-1) = 2m^2$. Ne segue che

$$(2n-1)^2((2n-1)^2-1) = (2n-1)^2 4n(n-1) = 2(2m(2n-1))^2,$$

e pertanto

$$\binom{(2n-1)^2}{2} = (2m(2n-1))^2.$$

A cominciare da $\binom{9}{2} = 6^2$ otteniamo dunque infinite soluzioni — la successiva è $\binom{289}{2} = 204^2$. Ciò tuttavia non fornisce tutte le soluzioni. Ad esempio, $\binom{50}{2} = 35^2$ inizia un'altra serie, e così pure $\binom{1682}{2} = 1189^2$. Per $k = 3$ è noto che $\binom{n}{3} = m^2$ ha come unica soluzione $n = 50$, $m = 140$. Ma ora siamo giunti alla fine. Per $k \geq 4$ ed un qualsiasi $\ell \geq 2$ non esiste alcuna soluzione, come dimostrò Erdős con un'ingegnosa argomentazione.

$\binom{50}{3} = 140^2$
è l'unica soluzione per $k = 3$, $\ell = 2$

Teorema. *L'equazione $\binom{n}{k} = m^\ell$ non ha soluzioni intere per $\ell \geq 2$ e $4 \leq k \leq n-4$.*

■ **Dimostrazione.** Si noti dapprima che possiamo supporre $n \geq 2k$ dal momento che $\binom{n}{k} = \binom{n}{n-k}$. Supponiamo che il teorema sia falso, e che $\binom{n}{k} = m^\ell$. La dimostrazione, per contraddizione, si articola nelle quattro fasi seguenti.

(1) Secondo il teorema di Sylvester, esiste un fattore primo p di $\binom{n}{k}$ maggiore di k, pertanto p^ℓ divide $n(n-1)\cdots(n-k+1)$. Chiaramente, soltanto uno dei fattori $n-i$ può essere un multiplo di p (essendo $p > k$); possiamo dunque concludere che $p^\ell \mid n-i$ e pertanto

$$n \;\geq\; p^\ell \;>\; k^\ell \;\geq\; k^2.$$

(2) Si consideri un qualunque fattore $n-j$ del numeratore e lo si scriva nella forma $n-j = a_j m_j^\ell$, dove a_j non è divisibile da alcuna potenza ℓ-esima non banale. Grazie a **(1)**, notiamo che a_j ha unicamente divisori primi inferiori o uguali a k. Vogliamo quindi mostrare che $a_i \neq a_j$ se $i \neq j$. Supponiamo al contrario che $a_i = a_j$ per qualche $i < j$. Allora $m_i \geq m_j + 1$ e

$$\begin{aligned} k \;&>\; (n-i)-(n-j) \;=\; a_j(m_i^\ell - m_j^\ell) \;\geq\; a_j((m_j+1)^\ell - m_j^\ell) \\ &>\; a_j \ell m_j^{\ell-1} \;\geq\; \ell(a_j m_j^\ell)^{1/2} \;\geq\; \ell(n-k+1)^{1/2} \\ &\geq\; \ell(\tfrac{n}{2}+1)^{1/2} \;>\; n^{1/2}, \end{aligned}$$

il che contraddice la disuguaglianza $n > k^2$ riportata sopra.

(3) Dimostriamo ora che gli a_i sono gli interi $1, 2, \ldots, k$ in un ordine dato. Secondo Erdős, questo è il punto cruciale della dimostrazione. Poiché sappiamo già che tali numeri sono tutti distinti, è sufficiente dimostrare che

$$a_0 a_1 \cdots a_{k-1} \quad \text{divide} \quad k!.$$

Sostituendo $n-j = a_j m_j^\ell$ nell'equazione $\binom{n}{k} = m^\ell$, otteniamo

$$a_0 a_1 \cdots a_{k-1}(m_0 m_1 \cdots m_{k-1})^\ell \;=\; k! m^\ell.$$

Eliminando i fattori comuni di $m_0 \cdots m_{k-1}$ e m si trova

$$a_0 a_1 \cdots a_{k-1} u^\ell \;=\; k! v^\ell$$

con $\text{mcd}(u, v) = 1$. Resta da dimostrare che $v = 1$. Se così non fosse, v conterrebbe un divisore primo p. Poiché $\text{mcd}(u, v) = 1$, p deve essere un divisore primo di $a_0 a_1 \cdots a_{k-1}$ e pertanto è inferiore o uguale a k. Dal teorema di Legendre (si veda a pagina 2) sappiamo che $k!$ contiene p alla potenza $\sum_{i \geq 1} \lfloor \frac{k}{p^i} \rfloor$. Stimiamo ora l'esponente di p in $n(n-1)\cdots(n-k+1)$. Siano i un intero positivo e $b_1 < b_2 < \ldots < b_s$ i multipli di p^i tra $n, n-1, \ldots, n-k+1$. Allora $b_s = b_1 + (s-1)p^i$ e dunque

$$(s-1)p^i \;=\; b_s - b_1 \;\leq\; n - (n-k+1) \;=\; k-1,$$

il che implica

$$s \;\leq\; \left\lfloor \frac{k-1}{p^i} \right\rfloor + 1 \;\leq\; \left\lfloor \frac{k}{p^i} \right\rfloor + 1.$$

Pertanto, per ogni i il numero di multipli di p^i tra $n, \ldots, n-k+1$, e quindi tra gli a_j, è limitato da $\lfloor \frac{k}{p^i} \rfloor + 1$. Ragionando come fatto con il teorema di Legendre nel Capitolo 2, ciò implica che l'esponente di p in $a_0 a_1 \cdots a_{k-1}$ vale al più

$$\sum_{i=1}^{\ell-1} \left(\left\lfloor \frac{k}{p^i} \right\rfloor + 1 \right).$$

L'unica differenza è che questa volta la somma si arresta ad $i = \ell - 1$, in quanto gli a_j non contengono alcuna potenza ℓ-esima. Unendo questi due elementi, troviamo che l'esponente di p in v^ℓ vale al massimo

$$\sum_{i=1}^{\ell-1} \left(\left\lfloor \frac{k}{p^i} \right\rfloor + 1 \right) - \sum_{i \geq 1} \left\lfloor \frac{k}{p^i} \right\rfloor \;\leq\; \ell - 1,$$

ottenendo così la contraddizione desiderata, poiché v^ℓ è una potenza ℓ-esima.

Ciò è sufficiente a sistemare il caso $\ell = 2$. In effetti, dal momento che $k \geq 4$, uno degli a_i deve essere uguale a 4, ma gli a_i non contengono quadrati. Passiamo a trattare il caso $\ell \geq 3$.

Notiamo che la nostra analisi finora è in accordo con $\binom{50}{3} = 140^2$, essendo

$$\begin{aligned} 50 &= 2 \cdot 5^2 \\ 49 &= 1 \cdot 7^2 \\ 48 &= 3 \cdot 4^2 \end{aligned}$$

e $5 \cdot 7 \cdot 4 = 140$

(4) Poiché $k \geq 4$, dobbiamo avere $a_{i_1} = 1$, $a_{i_2} = 2$, $a_{i_3} = 4$ per qualche i_1, i_2, i_3, ovvero,

$$n - i_1 = m_1^\ell, \;\; n - i_2 = 2m_2^\ell, \;\; n - i_3 = 4m_3^\ell.$$

Affermiamo che $(n-i_2)^2 \neq (n-i_1)(n-i_3)$. Altrimenti, posto $b = n - i_2$ e $n - i_1 = b - x$, $n - i_3 = b + y$, dove $0 < |x|, |y| < k$, ne deriva che

$$b^2 = (b-x)(b+y) \quad \text{oppure} \quad (y-x)b = xy,$$

dove $x = y$ è chiaramente impossibile. Ora da **(1)** segue

$$|xy| \;=\; b|y-x| \;\geq\; b \;>\; n-k \;>\; (k-1)^2 \;\geq\; |xy|,$$

il che è assurdo.

Pertanto abbiamo che $m_2^2 \neq m_1 m_3$, dove supponiamo che $m_2^2 > m_1 m_3$ (l'altro caso essendo analogo), e procediamo alle ultime catene di diseguaglianze. Otteniamo che

$$\begin{aligned} 2(k-1)n \;&>\; n^2 - (n-k+1)^2 \;>\; (n-i_2)^2 - (n-i_1)(n-i_3) \\ &=\; 4[m_2^{2\ell} - (m_1 m_3)^\ell] \;\geq\; 4[(m_1 m_3 + 1)^\ell - (m_1 m_3)^\ell] \\ &\geq\; 4\ell m_1^{\ell-1} m_3^{\ell-1}. \end{aligned}$$

Poiché $\ell \geq 3$ e $n > k^\ell \geq k^3 > 6k$, ne deriva che

$$\begin{aligned} 2(k-1)n m_1 m_3 \;&>\; 4\ell m_1^\ell m_3^\ell \;=\; \ell(n-i_1)(n-i_3) \\ &>\; \ell(n-k+1)^2 \;>\; 3(n - \frac{n}{6})^2 \;>\; 2n^2. \end{aligned}$$

Ora, poiché $m_i \leq n^{1/\ell} \leq n^{1/3}$ concludiamo che

$$kn^{2/3} \ \geq \ km_1m_3 \ > \ (k-1)m_1m_3 \ > \ n,$$

ovvero $k^3 > n$. Questa contraddizione completa la dimostrazione. □

Bibliografia

[1] P. ERDŐS: *A theorem of Sylvester and Schur,* J. London Math. Soc. **9** (1934), 282-288.

[2] P. ERDŐS: *On a diophantine equation,* J. London Math. Soc. **26** (1951), 176-178.

[3] J. J. SYLVESTER: *On arithmetical series,* Messenger of Math. **21** (1892), 1-19, 87-120; Collected Mathematical Papers Vol. 4, 1912, 687-731.