Martin Aigner · Günter M. Ziegler

Proofs from THE BOOK

Fourth Edition

数学天书中的证明 第4版

Springer

世界图书出版公司
www.wpcbj.com.cn

Martin Aigner
Günter M. Ziegler

Proofs from THE BOOK

Fourth Edition

Including Illustrations by Karl H. Hofmann

Springer

图书在版编目（CIP）数据

数学天书中的证明：第4版 = Proofs from THE BOOK：4th ed：英文/（德）齐格勒（Aigner，M.）著. — 影印本. — 北京：世界图书出版公司北京公司，2013.5
ISBN 978-7-5100-6148-6

Ⅰ.①数… Ⅱ.①齐… Ⅲ.①数学—普及读物—英文 Ⅳ.①O1-49

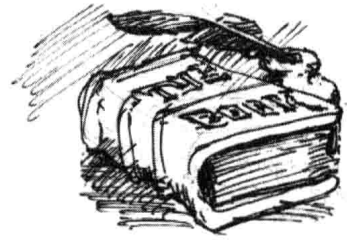
中国版本图书馆CIP数据核字（2013）第088372号

书　　名：	Proofs from THE BOOK 4th ed.
作　　者：	Martin Aigner，Günter M. Ziegler
中 译 名：	数学天书中的证明 第4版
责任编辑：	高蓉　刘慧
出 版 者：	世界图书出版公司北京公司
印 刷 者：	三河市国英印务有限公司
发　　行：	世界图书出版公司北京公司（北京朝内大街137号 100010）
联系电话：	010-64021602，010-64015659
电子信箱：	kjb@ wpcbj. com. cn
开　　本：	16开
印　　张：	18
版　　次：	2013年10月
版权登记：	图字：01-2013-2381
书　　号：	978-7-5100-6148-6　　定　　价：69.00元

Preface

Paul Erdős liked to talk about The Book, in which God maintains the perfect proofs for mathematical theorems, following the dictum of G. H. Hardy that there is no permanent place for ugly mathematics. Erdős also said that you need not believe in God but, as a mathematician, you should believe in The Book. A few years ago, we suggested to him to write up a first (and very modest) approximation to The Book. He was enthusiastic about the idea and, characteristically, went to work immediately, filling page after page with his suggestions. Our book was supposed to appear in March 1998 as a present to Erdős' 85th birthday. With Paul's unfortunate death in the summer of 1996, he is not listed as a co-author. Instead this book is dedicated to his memory.

Paul Erdős



"The Book"

We have no definition or characterization of what constitutes a proof from The Book: all we offer here is the examples that we have selected, hoping that our readers will share our enthusiasm about brilliant ideas, clever insights and wonderful observations. We also hope that our readers will enjoy this despite the imperfections of our exposition. The selection is to a great extent influenced by Paul Erdős himself. A large number of the topics were suggested by him, and many of the proofs trace directly back to him, or were initiated by his supreme insight in asking the right question or in making the right conjecture. So to a large extent this book reflects the views of Paul Erdős as to what should be considered a proof from The Book.

A limiting factor for our selection of topics was that everything in this book is supposed to be accessible to readers whose backgrounds include only a modest amount of technique from undergraduate mathematics. A little linear algebra, some basic analysis and number theory, and a healthy dollop of elementary concepts and reasonings from discrete mathematics should be sufficient to understand and enjoy everything in this book.

We are extremely grateful to the many people who helped and supported us with this project — among them the students of a seminar where we discussed a preliminary version, to Benno Artmann, Stephan Brandt, Stefan Felsner, Eli Goodman, Torsten Heldmann, and Hans Mielke. We thank Margrit Barrett, Christian Bressler, Ewgenij Gawrilow, Michael Joswig, Elke Pose, and Jörg Rambau for their technical help in composing this book. We are in great debt to Tom Trotter who read the manuscript from first to last page, to Karl H. Hofmann for his wonderful drawings, and most of all to the late great Paul Erdős himself.

Berlin, March 1998 *Martin Aigner · Günter M. Ziegler*

Preface to the Fourth Edition

When we started this project almost fifteen years ago we could not possibly imagine what a wonderful and lasting response our book about The Book would have, with all the warm letters, interesting comments, new editions, and as of now thirteen translations. It is no exaggeration to say that it has become a part of our lives.

In addition to numerous improvements, partly suggested by our readers, the present fourth edition contains five new chapters: Two classics, the law of quadratic reciprocity and the fundamental theorem of algebra, two chapters on tiling problems and their intriguing solutions, and a highlight in graph theory, the chromatic number of Kneser graphs.

We thank everyone who helped and encouraged us over all these years: For the second edition this included Stephan Brandt, Christian Elsholtz, Jürgen Elstrodt, Daniel Grieser, Roger Heath-Brown, Lee L. Keener, Christian Lebœuf, Hanfried Lenz, Nicolas Puech, John Scholes, Bernulf Weißbach, and *many* others. The third edition benefitted especially from input by David Bevan, Anders Björner, Dietrich Braess, John Cosgrave, Hubert Kalf, Günter Pickert, Alistair Sinclair, and Herb Wilf. For the present edition, we are particularly grateful to contributions by France Dacar, Oliver Deiser, Anton Dochtermann, Michael Harbeck, Stefan Hougardy, Hendrik W. Lenstra, Günter Rote, Moritz Schmitt, and Carsten Schultz. Moreover, we thank Ruth Allewelt at Springer in Heidelberg as well as Christoph Eyrich, Torsten Heldmann, and Elke Pose in Berlin for their help and support throughout these years. And finally, this book would certainly not look the same without the original design suggested by Karl-Friedrich Koch, and the superb new drawings provided for each edition by Karl H. Hofmann.

Berlin, July 2009 *Martin Aigner · Günter M. Ziegler*

Table of Contents

Number Theory ____ 1

1. Six proofs of the infinity of primes 3
2. Bertrand's postulate 7
3. Binomial coefficients are (almost) never powers 13
4. Representing numbers as sums of two squares 17
5. The law of quadratic reciprocity 23
6. Every finite division ring is a field 31
7. Some irrational numbers 35
8. Three times $\pi^2/6$ 43

Geometry ____ 51

9. Hilbert's third problem: decomposing polyhedra 53
10. Lines in the plane and decompositions of graphs 63
11. The slope problem 69
12. Three applications of Euler's formula 75
13. Cauchy's rigidity theorem 81
14. Touching simplices 85
15. Every large point set has an obtuse angle 89
16. Borsuk's conjecture 95

Analysis ____ 101

17. Sets, functions, and the continuum hypothesis 103
18. In praise of inequalities 119
19. The fundamental theorem of algebra 127
20. One square and an odd number of triangles 131

21. A theorem of Pólya on polynomials 139
22. On a lemma of Littlewood and Offord 145
23. Cotangent and the Herglotz trick 149
24. Buffon's needle problem 155

Combinatorics 159

25. Pigeon-hole and double counting 161
26. Tiling rectangles 173
27. Three famous theorems on finite sets 179
28. Shuffling cards 185
29. Lattice paths and determinants 195
30. Cayley's formula for the number of trees 201
31. Identities versus bijections 207
32. Completing Latin squares 213

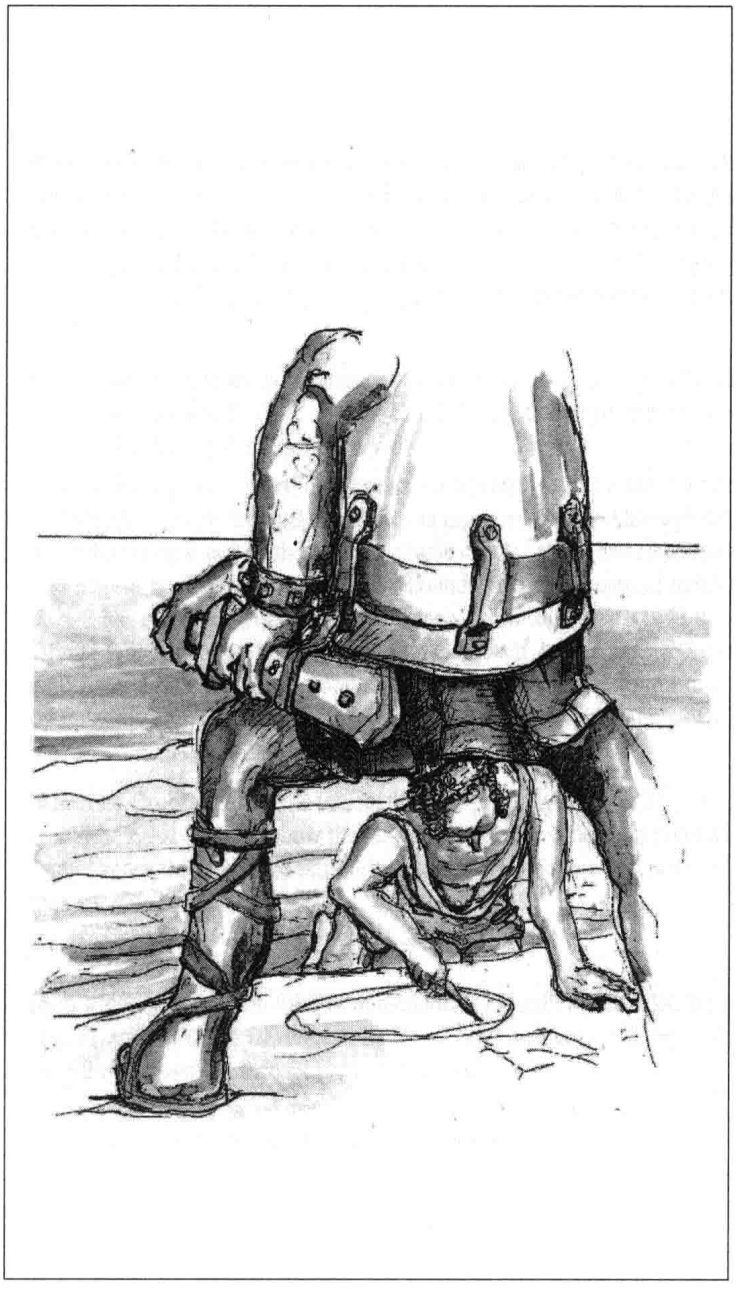
Graph Theory 219

33. The Dinitz problem 221
34. Five-coloring plane graphs 227
35. How to guard a museum 231
36. Turán's graph theorem 235
37. Communicating without errors 241
38. The chromatic number of Kneser graphs 251
39. Of friends and politicians 257
40. Probability makes counting (sometimes) easy 261

About the Illustrations 270

Index 271

Number Theory



1
Six proofs
of the infinity of primes *3*

2
Bertrand's postulate *7*

3
Binomial coefficients
are (almost) never powers *13*

4
Representing numbers
as sums of two squares *17*

5
The law of
quadratic reciprocity *23*

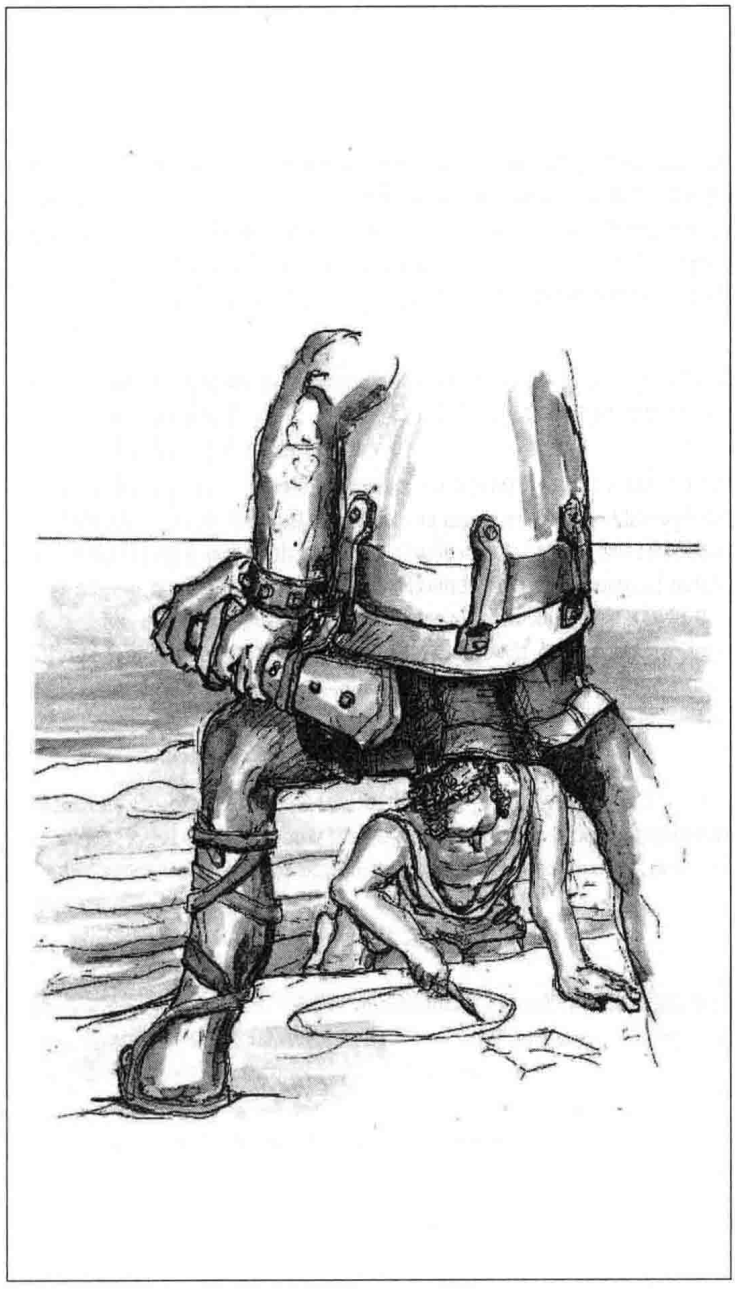
6
Every finite division ring
is a field *31*

7
Some irrational numbers *35*

8
Three times $\pi^2/6$ *43*

"Irrationality and π"

Number Theory



1
Six proofs
of the infinity of primes *3*

2
Bertrand's postulate *7*

3
Binomial coefficients
are (almost) never powers *13*

4
Representing numbers
as sums of two squares *17*

5
The law of
quadratic reciprocity *23*

6
Every finite division ring
is a field *31*

7
Some irrational numbers *35*

8
Three times $\pi^2/6$ *43*

"Irrationality and π"

Six proofs of the infinity of primes

Chapter 1

It is only natural that we start these notes with probably the oldest Book Proof, usually attributed to Euclid (*Elements* IX, 20). It shows that the sequence of primes does not end.

■ **Euclid's Proof.** For any finite set $\{p_1, \ldots, p_r\}$ of primes, consider the number $n = p_1 p_2 \cdots p_r + 1$. This n has a prime divisor p. But p is not one of the p_i: otherwise p would be a divisor of n and of the product $p_1 p_2 \cdots p_r$, and thus also of the difference $n - p_1 p_2 \cdots p_r = 1$, which is impossible. So a finite set $\{p_1, \ldots, p_r\}$ cannot be the collection of *all* prime numbers. □

Before we continue let us fix some notation. $\mathbb{N} = \{1, 2, 3, \ldots\}$ is the set of natural numbers, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ the set of integers, and $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ the set of primes.

In the following, we will exhibit various other proofs (out of a much longer list) which we hope the reader will like as much as we do. Although they use different view-points, the following basic idea is common to all of them: The natural numbers grow beyond all bounds, and every natural number $n \geq 2$ has a prime divisor. These two facts taken together force $\mathbb{P}$ to be infinite. The next proof is due to Christian Goldbach (from a letter to Leonhard Euler 1730), the third proof is apparently folklore, the fourth one is by Euler himself, the fifth proof was proposed by Harry Fürstenberg, while the last proof is due to Paul Erdős.

■ **Second Proof.** Let us first look at the *Fermat numbers* $F_n = 2^{2^n} + 1$ for $n = 0, 1, 2, \ldots$. We will show that any two Fermat numbers are relatively prime; hence there must be infinitely many primes. To this end, we verify the recursion

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

from which our assertion follows immediately. Indeed, if m is a divisor of, say, F_k and F_n $(k < n)$, then m divides 2, and hence $m = 1$ or 2. But $m = 2$ is impossible since all Fermat numbers are odd.

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

The first few Fermat numbers

To prove the recursion we use induction on n. For $n = 1$ we have $F_0 = 3$ and $F_1 - 2 = 3$. With induction we now conclude

$$\begin{aligned} \prod_{k=0}^{n} F_k &= \Big(\prod_{k=0}^{n-1} F_k\Big) F_n \;=\; (F_n - 2) F_n \;= \\ &= (2^{2^n} - 1)(2^{2^n} + 1) \;=\; 2^{2^{n+1}} - 1 \;=\; F_{n+1} - 2. \end{aligned}$$

□

Lagrange's Theorem

If G is a finite (multiplicative) group and U is a subgroup, then $|U|$ divides $|G|$.

■ **Proof.** Consider the binary relation

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

It follows from the group axioms that $\sim$ is an equivalence relation. The equivalence class containing an element a is precisely the coset

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

Since clearly $|Ua| = |U|$, we find that G decomposes into equivalence classes, all of size $|U|$, and hence that $|U|$ divides $|G|$. □

In the special case when U is a cyclic subgroup $\{a, a^2, \ldots, a^m\}$ we find that m (the smallest positive integer such that $a^m = 1$, called the *order* of a) divides the size $|G|$ of the group.

■ **Third Proof.** Suppose $\mathbb{P}$ is finite and p is the largest prime. We consider the so-called *Mersenne number* $2^p - 1$ and show that any prime factor q of $2^p - 1$ is bigger than p, which will yield the desired conclusion. Let q be a prime dividing $2^p - 1$, so we have $2^p \equiv 1 \pmod{q}$. Since p is prime, this means that the element 2 has order p in the multiplicative group $\mathbb{Z}_q \backslash \{0\}$ of the field $\mathbb{Z}_q$. This group has $q - 1$ elements. By Lagrange's theorem (see the box) we know that the order of every element divides the size of the group, that is, we have $p \mid q - 1$, and hence $p < q$. □

Now let us look at a proof that uses elementary calculus.

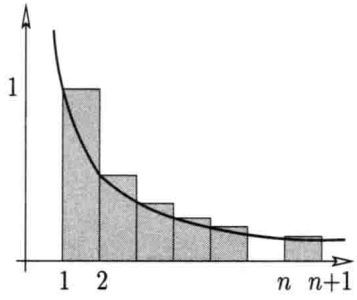
■ **Fourth Proof.** Let $\pi(x) := \#\{p \le x : p \in \mathbb{P}\}$ be the number of primes that are less than or equal to the real number x. We number the primes $\mathbb{P} = \{p_1, p_2, p_3, \ldots\}$ in increasing order. Consider the natural logarithm $\log x$, defined as $\log x = \int_1^x \frac{1}{t} dt$.

Now we compare the area below the graph of $f(t) = \frac{1}{t}$ with an upper step function. (See also the appendix on page 10 for this method.) Thus for $n \le x < n+1$ we have

$$\begin{aligned} \log x &\le 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n-1} + \frac{1}{n} \\ &\le \sum \frac{1}{m}, \text{ where the sum extends over all } m \in \mathbb{N} \text{ which have only prime divisors } p \le x. \end{aligned}$$

Since every such m can be written in a *unique* way as a product of the form $\prod_{p \le x} p^{k_p}$, we see that the last sum is equal to

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



Steps above the function $f(t) = \frac{1}{t}$

The inner sum is a geometric series with ratio $\frac{1}{p}$, hence

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

Now clearly $p_k \ge k + 1$, and thus

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

and therefore

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

Everybody knows that $\log x$ is not bounded, so we conclude that $\pi(x)$ is unbounded as well, and so there are infinitely many primes. □

■ **Fifth Proof.** After analysis it's topology now! Consider the following curious topology on the set $\mathbb{Z}$ of integers. For $a, b \in \mathbb{Z}$, $b > 0$, we set

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

Each set $N_{a,b}$ is a two-way infinite arithmetic progression. Now call a set $O \subseteq \mathbb{Z}$ *open* if either O is empty, or if to every $a \in O$ there exists some $b > 0$ with $N_{a,b} \subseteq O$. Clearly, the union of open sets is open again. If O_1, O_2 are open, and $a \in O_1 \cap O_2$ with $N_{a,b_1} \subseteq O_1$ and $N_{a,b_2} \subseteq O_2$, then $a \in N_{a,b_1 b_2} \subseteq O_1 \cap O_2$. So we conclude that any finite intersection of open sets is again open. So, this family of open sets induces a bona fide topology on $\mathbb{Z}$.

Let us note two facts:

(A) Any nonempty open set is infinite.

(B) Any set $N_{a,b}$ is closed as well.

Indeed, the first fact follows from the definition. For the second we observe

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

which proves that $N_{a,b}$ is the complement of an open set and hence closed.

So far the primes have not yet entered the picture — but here they come. Since any number $n \neq 1, -1$ has a prime divisor p, and hence is contained in $N_{0,p}$, we conclude

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

Now if $\mathbb{P}$ were finite, then $\bigcup_{p\in\mathbb{P}} N_{0,p}$ would be a finite union of closed sets (by (B)), and hence closed. Consequently, $\{1, -1\}$ would be an open set, in violation of (A). □

"Pitching flat rocks, infinitely"

■ **Sixth Proof.** Our final proof goes a considerable step further and demonstrates not only that there are infinitely many primes, but also that the series $\sum_{p\in\mathbb{P}} \frac{1}{p}$ diverges. The first proof of this important result was given by Euler (and is interesting in its own right), but our proof, devised by Erdős, is of compelling beauty.

Let $p_1, p_2, p_3, \ldots$ be the sequence of primes in increasing order, and assume that $\sum_{p\in\mathbb{P}} \frac{1}{p}$ converges. Then there must be a natural number k such that $\sum_{i\geq k+1} \frac{1}{p_i} < \frac{1}{2}$. Let us call $p_1, \ldots, p_k$ the *small* primes, and $p_{k+1}, p_{k+2}, \ldots$ the *big* primes. For an arbitrary natural number N we therefore find

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

Let N_b be the number of positive integers $n \leq N$ which are divisible by at least one big prime, and N_s the number of positive integers $n \leq N$ which have only small prime divisors. We are going to show that for a suitable N

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

which will be our desired contradiction, since by definition $N_b + N_s$ would have to be equal to N.

To estimate N_b note that $\lfloor \frac{N}{p_i} \rfloor$ counts the positive integers $n \leq N$ which are multiples of p_i. Hence by (1) we obtain

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

Let us now look at N_s. We write every $n \leq N$ which has only small prime divisors in the form $n = a_n b_n^2$, where a_n is the square-free part. Every a_n is thus a product of *different* small primes, and we conclude that there are precisely 2^k different square-free parts. Furthermore, as $b_n \leq \sqrt{n} \leq \sqrt{N}$, we find that there are at most $\sqrt{N}$ different square parts, and so

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

Since (2) holds for *any* N, it remains to find a number N with $2^k \sqrt{N} \leq \frac{N}{2}$ or $2^{k+1} \leq \sqrt{N}$, and for this $N = 2^{2k+2}$ will do. □

References

[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.

Bertrand's postulate

Chapter 2

We have seen that the sequence of prime numbers $2, 3, 5, 7, \ldots$ is infinite. To see that the size of its gaps is not bounded, let $N := 2 \cdot 3 \cdot 5 \cdots p$ denote the product of all prime numbers that are smaller than $k+2$, and note that none of the k numbers

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

is prime, since for $2 \leq i \leq k+1$ we know that i has a prime factor that is smaller than $k+2$, and this factor also divides N, and hence also $N+i$. With this recipe, we find, for example, for $k = 10$ that none of the ten numbers

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

is prime.

But there are also upper bounds for the gaps in the sequence of prime numbers. A famous bound states that "the gap to the next prime cannot be larger than the number we start our search at." This is known as Bertrand's postulate, since it was conjectured and verified empirically for $n < 3\,000\,000$ by Joseph Bertrand. It was first proved for all n by Pafnuty Chebyshev in 1850. A much simpler proof was given by the Indian genius Ramanujan. Our Book Proof is by Paul Erdős: it is taken from Erdős' first published paper, which appeared in 1932, when Erdős was 19.

Joseph Bertrand

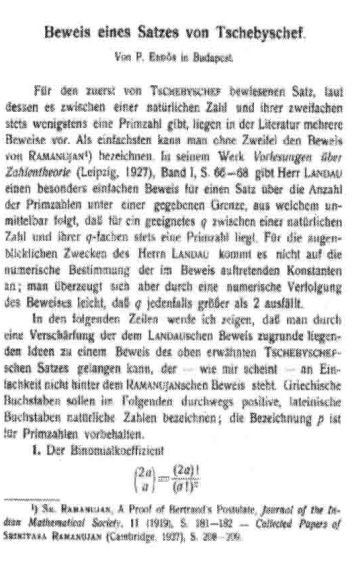
Bertrand's postulate.
For every $n \geq 1$, there is some prime number p with $n < p \leq 2n$.

■ **Proof.** We will estimate the size of the binomial coefficient $\binom{2n}{n}$ carefully enough to see that if it didn't have any prime factors in the range $n < p \leq 2n$, then it would be "too small." Our argument is in five steps.

(1) We first prove Bertrand's postulate for $n < 4000$. For this one does not need to check 4000 cases: it suffices (this is "Landau's trick") to check that

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

is a sequence of prime numbers, where each is smaller than twice the previous one. Hence every interval $\{y : n < y \leq 2n\}$, with $n \leq 4000$, contains one of these 14 primes.



Beweis eines Satzes von Tschebyschef.

Von P. Erdős in Budapest.

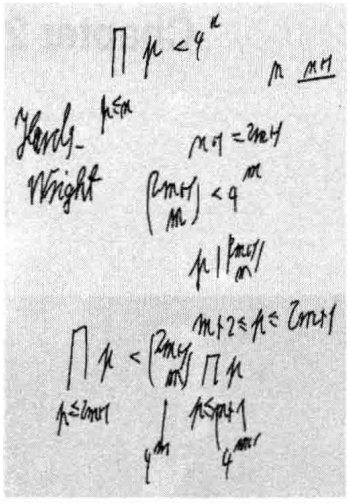
Für den zuerst von TSCHEBYSCHEF bewiesenen Satz, laut dessen es zwischen einer natürlichen Zahl und ihrer zweifachen stets wenigstens eine Primzahl gibt, liegen in der Literatur mehrere Beweise vor. Als einfachsten kann man ohne Zweifel den Beweis von RAMANUJAN[4]) bezeichnen. In seinem Werk *Vorlesungen 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 Einfachheit 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

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

[4]) SR. 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.



(2) Next we prove that

$$\prod_{p\le x} p \;\le\; 4^{x-1} \qquad \text{for all real } x \ge 2, \tag{1}$$

where our notation — here and in the following — is meant to imply that the product is taken over all *prime* numbers $p \le x$. The proof that we present for this fact uses induction on the number of these primes. It is not from Erdős' original paper, but it is also due to Erdős (see the margin), and it is a true Book Proof. First we note that if q is the largest prime with $q \le x$, then

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

Thus it suffices to check (1) for the case where $x = q$ is a prime number. For $q = 2$ we get "$2 \le 4$," so we proceed to consider odd primes $q = 2m+1$. (Here we may assume, by induction, that (1) is valid for all integers x in the set $\{2, 3, \ldots, 2m\}$.) For $q = 2m+1$ we split the product and compute

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

All the pieces of this "one-line computation" are easy to see. In fact,

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

holds by induction. The inequality

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

follows from the observation that $\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}$ is an integer, where the primes that we consider all are factors of the numerator $(2m+1)!$, but not of the denominator $m!(m+1)!$. Finally

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

holds since

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

are two (equal!) summands that appear in

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

(3) From Legendre's theorem (see the box) we get that $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ contains the prime factor p exactly

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

Legendre's theorem

The number $n!$ contains the prime factor p exactly

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

times.

■ **Proof.** Exactly $\lfloor \frac{n}{p} \rfloor$ of the factors of $n! = 1 \cdot 2 \cdot 3 \cdots n$ are divisible by p, which accounts for $\lfloor \frac{n}{p} \rfloor$ p-factors. Next, $\lfloor \frac{n}{p^2} \rfloor$ of the factors of $n!$ are even divisible by p^2, which accounts for the next $\lfloor \frac{n}{p^2} \rfloor$ prime factors p of $n!$, etc. □

times. Here each summand is at most 1, since it satisfies

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

and it is an integer. Furthermore the summands vanish whenever $p^k > 2n$. Thus $\binom{2n}{n}$ contains p exactly

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

times. Hence the largest power of p that divides $\binom{2n}{n}$ is not larger than $2n$. In particular, primes $p > \sqrt{2n}$ appear at most once in $\binom{2n}{n}$.

Furthermore — and this, according to Erdős, is the key fact for his proof — primes p that satisfy $\frac{2}{3}n < p \leq n$ do not divide $\binom{2n}{n}$ at all! Indeed, $3p > 2n$ implies (for $n \geq 3$, and hence $p \geq 3$) that p and $2p$ are the only multiples of p that appear as factors in the numerator of $\frac{(2n)!}{n!n!}$, while we get two p-factors in the denominator.

Examples such as
$\binom{26}{13} = 2^3 \cdot 5^2 \cdot 7 \cdot 17 \cdot 19 \cdot 23$
$\binom{28}{14} = 2^3 \cdot 3^3 \cdot 5^2 \cdot 17 \cdot 19 \cdot 23$
$\binom{30}{15} = 2^4 \cdot 3^2 \cdot 5 \cdot 17 \cdot 19 \cdot 23 \cdot 29$
illustrate that "very small" prime factors $p < \sqrt{2n}$ can appear as higher powers in $\binom{2n}{n}$, "small" primes with $\sqrt{2n} < p \leq \frac{2}{3}n$ appear at most once, while factors in the gap with $\frac{2}{3}n < p \leq n$ don't appear at all.

(4) Now we are ready to estimate $\binom{2n}{n}$. For $n \geq 3$, using an estimate from page 12 for the lower bound, we get

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

and thus, since there are not more than $\sqrt{2n}$ primes $p \leq \sqrt{2n}$,

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

(5) Assume now that there is no prime p with $n < p \leq 2n$, so the second product in (2) is 1. Substituting (1) into (2) we get

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

or

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

which is false for n large enough! In fact, using $a + 1 < 2^a$ (which holds for all $a \geq 2$, by induction) we get

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

and thus for $n \geq 50$ (and hence $18 < 2\sqrt{2n}$) we obtain from (3) and (4)

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

This implies $(2n)^{1/3} < 20$, and thus $n < 4000$. □