Proofs from THE BOOK

Martin Aigner Günter M. Ziegler
with illustrations by Karl H. Hofmann

Springer-Verlag Heidelberg/Berlin
to appear August 1998

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 1997, he is not listed as a co-author. Instead this book is dedicated to his memory.

Paul Erdős

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.

"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, 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*

Table of Contents

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. 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 $n - p_1 p_2 \ldots p_r = 1$, 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 three proofs are folklore, the fifth proof was proposed by Harry Fürstenberg, while the last proof is due to Paul Erdős.

The second and the third proof use special well-known number sequences.

■ **Second 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 $p \,|\, q - 1$, and hence $p < q$. □

■ **Third Proof.** Next let us 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

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

Lagrange's Theorem

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

■ **Proof.** Consider the binary relation

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

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.

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

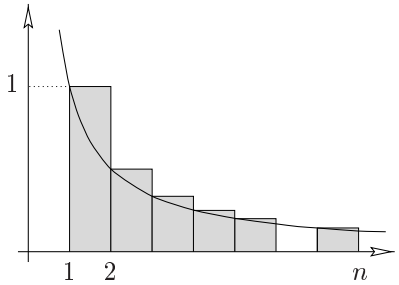
The first few Fermat numbers

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.

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

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

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



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

■ **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 $\mathbb{P} = \{p_1, p_2, p_3, \dots\}$ 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

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

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

[2] L. EULER: *Introductio in Analysin Infinitorum*, Tomus Primus, Lausanne 1748; Opera Omnia, Ser. 1, Vol. 90.

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