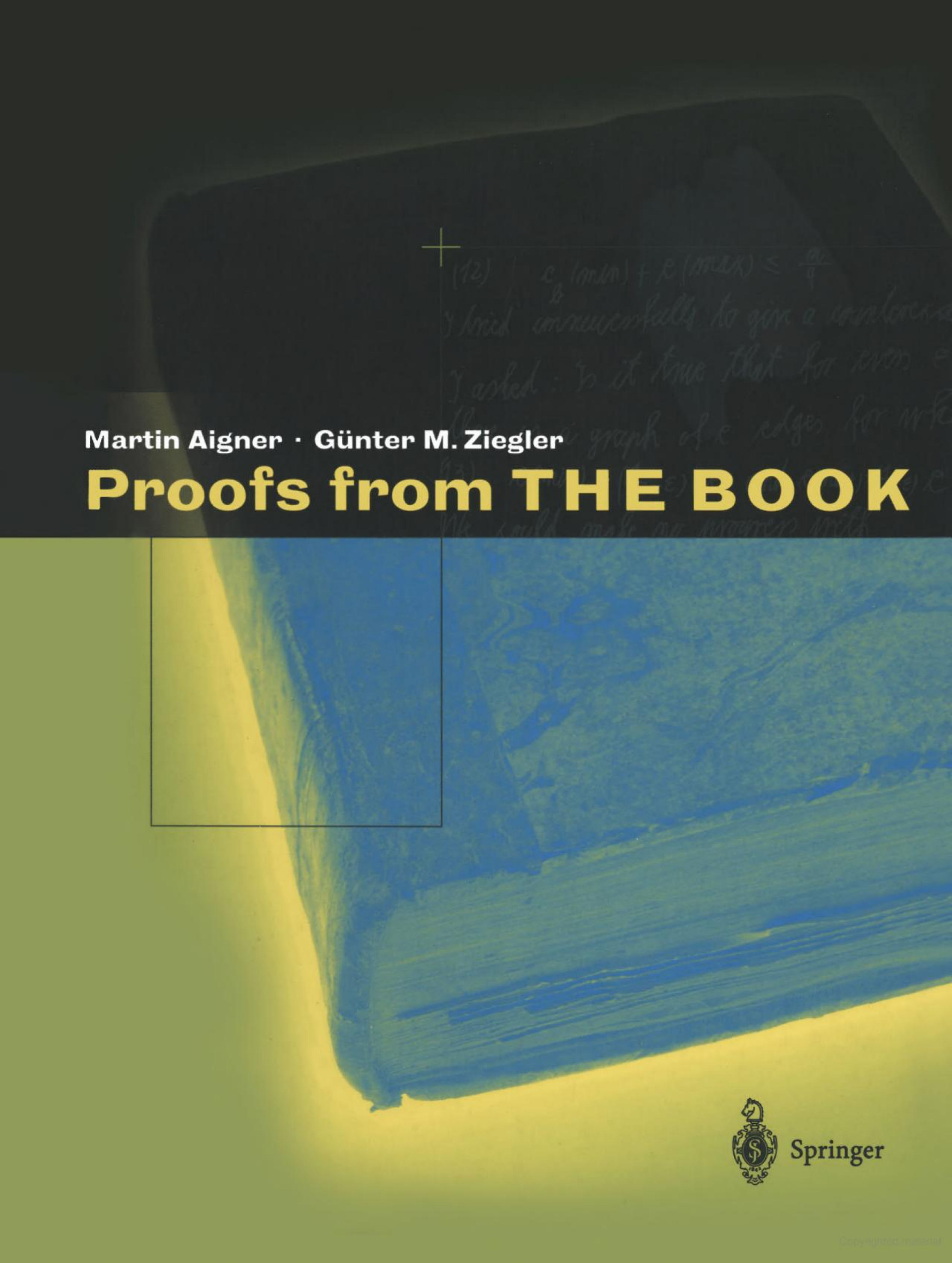


Martin Aigner · Günter M. Ziegler

Proofs from THE BOOK

Springer

Martin Aigner
Günter M. Ziegler

Proofs from THE BOOK

With 220 Figures
Including Illustrations
by Karl H. Hofmann

Springer

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

Günter M. Ziegler
Technische Universität Berlin
Fachbereich Mathematik, MA 7-1
Straße des 17. Juni 136
D-10623 Berlin, Germany
email: ziegler@math.tu-berlin.de

CIP data applied for

Die Deutsche Bibliothek – CIP-Einheitsaufnahme
Aigner, Martin: Proofs from the book / Martin Aigner; Günter M. Ziegler. Incl. ill. by Karl H. Hofmann. – Berlin; Heidelberg; New York; Barcelona; Budapest; Hong Kong; London; Milan; Paris; Singapore; Tokyo: Springer, 1998
ISBN 978-3-662-22345-1

Mathematics Subject Classification (1991): 00-01 (General)

ISBN 978-3-662-22345-1 ISBN 978-3-662-22343-7 (eBook)
DOI 10.1007/978-3-662-22343-7

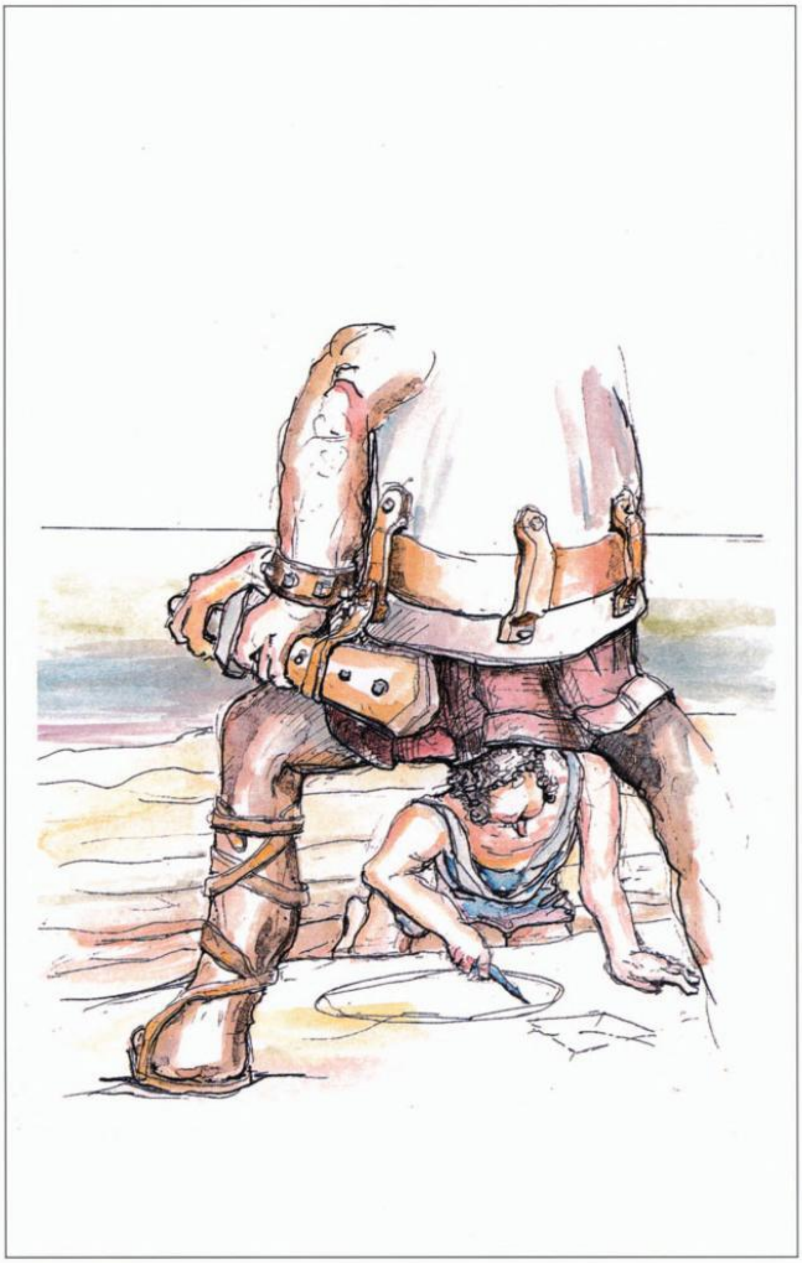
Originally published by Springer-Verlag Berlin Heidelberg New York in 1998
Softcover reprint of the hardcover 1st edition 1998

Typeset in LaTeX by the authors
Computer-to-plate processing by Mercedes-Druck GmbH, Berlin
Cover design: de'blik, Berlin

SPIN 10655190 46/3143 – 5 4 3 2 1 0 – Printed on acid-free paper

Table of Contents

Number Theory



"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. It shows that the sequence of primes does not end.

■ **Euclid's Proof.** For any finite set $\{p_1, \dots, p_r\}$ 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 $n - p_1 p_2 \dots p_r = 1$, which is impossible. So a finite set $\{p_1, \dots, p_r\}$ cannot be the collection of *all* prime numbers. □

Before we continue let us fix some notation. $\mathbb{N} = \{1, 2, 3, \dots\}$ is the set of natural numbers, $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ the set of integers, and $\mathbb{P} = \{2, 3, 5, 7, \dots\}$ 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 $p \mid q - 1$, and hence $p < q$. □

■ **Third Proof.** Next let us look at the *Fermat numbers* $F_n = 2^{2^n} + 1$ for $n = 0, 1, 2, \dots$. 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

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

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 $\{a, a^2, \dots, a^m\}$ 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.

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

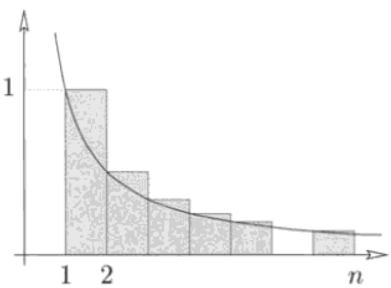
The first few Fermat numbers

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

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

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. $\square$

■ **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

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

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

"Pitching flat rocks, infinitely"

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

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

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). □

■ **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

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

Let N_b be the number of positive integers $n \le N$ which are divisible by at least one big prime, and N_s the number of positive integers $n \le N$ 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 $n \le N$ which are multiples of p_i. Hence by (1) we obtain

$$N_b \ \le \ \sum_{i \ge k+1} \left\lfloor \frac{N}{p_i} \right\rfloor \ < \ \frac{N}{2}. \qquad (2)$$

Let us now look at N_s. We write every $n \le N$ 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 $b_n \le \sqrt{n} \le \sqrt{N}$, we find that there are at most $\sqrt{N}$ different square parts, and so

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

Since (2) holds for *any* N, it remains to find a number N with $2^k \sqrt{N} \le \frac{N}{2}$ or $2^{k+1} \le \sqrt{N}$, 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.

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 $N := 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p$ 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 $n < p \leq 2n$.

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]) 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.

■ **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.

(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 is not from Erdős' original paper, but it is also due to Erdős, 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 $q = 2m + 1$. For these 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

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

are two (equal!) summands that appear in

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

> **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 $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ 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. □

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

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

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.

(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

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

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 $n < 4000$. □

One can extract even more from this proof: from (2) the same type of estimates that we just used proves that

$$\prod_{n<p\le 2n} p \ge 2^{\frac{1}{30}n} \quad \text{for} \quad n \ge 4000,$$

and thus that there are at least

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

primes in the range between n and $2n$.

This is not that bad an estimate: the "true" number of primes in this range is roughly $n/\log n$. This follows from the famous "prime number theorem," which says that the limit

$$\lim_{n\to\infty} \frac{\#\{p \le n : p \text{ is prime}\}}{n/\log n}$$

exists, and equals 1. This was first proved by Hadamard and de la Vallée-Poussin in 1896; Selberg and Erdős found an elementary proof (without complex analysis tools, but still long and involved) in 1948.

On the prime number theorem itself the final word, it seems, is still not in: for example a proof of the Riemann hypothesis (see page 33), one of the major unsolved open problems in mathematics, would also give a substantial improvement for the estimates of the prime number theorem. But also for Bertrand's postulate, one could expect dramatic improvements. In fact, the following is an unsolved problem [3, p. 19]:

Is there always a prime between n^2 and $(n+1)^2$?

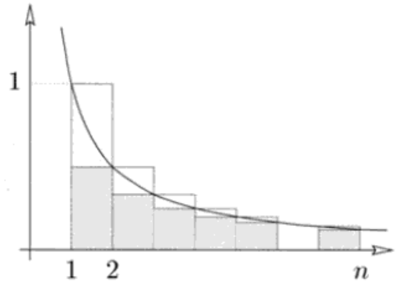
Appendix: Some estimates

Estimating via integrals

There is a very simple-but-effective method of estimating sums by integrals (as already encountered on page 4). For estimating the *harmonic numbers*

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

we draw the figure in the margin and derive from it



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

by comparing the area below the graph of $f(t) = \frac{1}{t}$ $(1 \le t \le n)$ with the area of the dark shaded rectangles, and

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

by comparing with the area of the large rectangles (including the lightly shaded parts). Taken together, this yields

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

In particular, $\lim_{n\to\infty} H_n \to \infty$, and the order of growth of H_n is given by $\lim_{n\to\infty} \frac{H_n}{\log n} = 1$. But much better estimates are known (see [2]), such as

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

Here $O\left(\frac{1}{n^6}\right)$ denotes a function $f(n)$ such that $f(n) \le c\frac{1}{n^6}$ holds for some constant c.

where $\gamma \approx 0.5772$ is "Euler's constant."

Estimating factorials — Stirling's formula

The same method applied to

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

yields

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

where the integral is easily computed:

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

Thus we get a lower estimate on $n!$

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

and at the same time an upper estimate

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

Here a more careful analysis is needed to get the asymptotics of $n!$, as given by *Stirling's formula*

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

Here $f(n) \sim g(n)$ means that $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$.

And again there are more precise versions available, such as

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

Estimating binomial coefficients

Just from the definition of the binomial coefficients $\binom{n}{k}$ as the number of k-subsets of an n-set, we know that the sequence $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$ of binomial coefficients

- sums to $\sum_{k=0}^{n} \binom{n}{k} = 2^n$
- is symmetric: $\binom{n}{k} = \binom{n}{n-k}$.

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

Pascal's triangle

From the functional equation $\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}$ one easily finds that for every n the binomial coefficients $\binom{n}{k}$ form a sequence that is symmetric and *unimodal*: it increases towards the middle, so that the middle binomial coefficients are the largest ones in the sequence:

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

Here $\lfloor x \rfloor$ resp. $\lceil x \rceil$ denotes the number x rounded down resp. rounded up to the nearest integer.

From the asymptotic formulas for the factorials mentioned above one can obtain very precise estimates for the sizes of binomial coefficients. However, we will only need very weak and simple estimates in this book, such as the following: $\binom{n}{k} \le 2^n$ for all k, while for $n \ge 2$ we have

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

with equality only for $n = 2$. In particular, for $n \ge 1$,

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

This holds since $\binom{n}{\lfloor n/2 \rfloor}$, a middle binomial coefficient, is the largest entry in the sequence $\binom{n}{0} + \binom{n}{n}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}$, whose sum is 2^n, and whose average is thus $\frac{2^n}{n}$.

On the other hand, we note the upper bound for binomial coefficients

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

which is a reasonably good estimate for the "small" binomial coefficients at the tails of the sequence, when n is large (compared to k).

References

[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.

So for each i the number of multiples of p^i among $n, \dots, n-k+1$, and hence among the a_j's, is bounded by $\lfloor \frac{k}{p^i} \rfloor + 1$. This implies that the exponent of p in $a_0 a_1 \cdots a_{k-1}$ is at most

$$\sum_{i=1}^{\ell-1} \Big(\Big\lfloor \frac{k}{p^i} \Big\rfloor + 1 \Big),$$

with the reasoning that we used for Legendre's theorem in Chapter 2. The only difference is that this time the sum stops at $i = \ell - 1$, since the a_j's contain no ℓ-th powers.

Taking both counts together, we find that the exponent of p in v^ℓ is at most

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

and we have our desired contradiction, since v^ℓ is an ℓ-th power.

This suffices already to settle the case $\ell = 2$. Indeed, since $k \geq 4$ one of the a_i's must be equal to 4, but the a_i's contain no squares. So let us now assume that $\ell \geq 3$.

We see that our analysis so far agrees with $\binom{50}{3} = 140^2$, as

$$50 = 2 \cdot 5^2$$
$$49 = 1 \cdot 7^2$$
$$48 = 3 \cdot 4^2$$

and $5 \cdot 7 \cdot 4 = 140$.

(4) Since $k \geq 4$, we must have $a_{i_1} = 1, a_{i_2} = 2, a_{i_3} = 4$ for some i_1, i_2, i_3, that is,

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

We claim that $(n - i_2)^2 \neq (n - i_1)(n - i_3)$. If not, put $b = n - i_2$ and $n - i_1 = b - x$, $n - i_3 = b + y$, where $0 < |x|, |y| < k$. Hence

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

where $x = y$ is plainly impossible. Now we have by part **(1)**

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

which is absurd.

So we have $m_2^2 \neq m_1 m_3$, where we assume $m_2^2 > m_1 m_3$ (the other case being analogous), and proceed to our last chains of inequalities. We obtain

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

Since $\ell \geq 3$ and $n > k^\ell \geq k^3 > 6k$, this yields

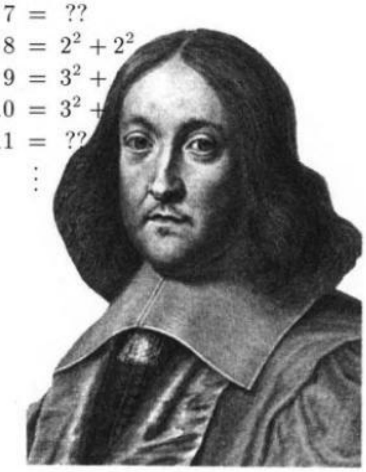
$$\begin{aligned} 2(k-1)n m_1 m_3 \;&>\; 4\ell m_1^\ell m_3^\ell \;=\; \ell(n - i_1)(n - i_3) \\ &>\; \ell(n - k + 1)^2 \;>\; 3(n - \frac{n}{6})^2 \;>\; 2n^2. \end{aligned}$$

Representing numbers as sums of two squares

Chapter 4

Which numbers can be written as sums of two squares?

$1 = 1^2 + 0^2$
$2 = 1^2 + 1^2$
$3 = \, ??$
$4 = 2^2 + 0^2$
$5 = 2^2 + 1^2$
$6 = \, ??$
$7 = \, ??$
$8 = 2^2 + 2^2$
$9 = 3^2 +$
$10 = 3^2 +$
$11 = \, ??$
$\vdots$



Pierre de Fermat

This question is as old as number theory, and its solution is a classic in the field. The "hard" part of the solution is to see that every prime number of the form $4m + 1$ is a sum of two squares. G. H. Hardy writes that this *two square theorem* of Fermat "is ranked, very justly, as one of the finest in arithmetic." Nevertheless, our Book Proof below is recent and dates from 1990.

Let's start with some "warm-ups." First, we need to distinguish between the prime $p = 2$, the primes of the form $p = 4m + 1$, and the primes of the form $p = 4m + 3$. Every prime number belongs to exactly one of these three classes. At this point we may note (using a method "à la Euclid") that there are infinitely many primes of the form $4m + 3$. In fact, if there were only finitely many, then we could take p_k to be the largest prime of this form. Setting

$$N_k \; := \; 2^2 \cdot 3 \cdot 5 \cdots p_k - 1$$

(where $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$ denotes the sequence of all primes), we find that N_k is congruent to $3 \pmod 4$, so it must have a prime factor of the form $4m + 3$, and this prime factor is larger than p_k — contradiction. At the end of this chapter we will also derive that there are infinitely many primes of the other kind, $p = 4m + 1$.

Our first lemma is a special case of the famous "law of reciprocity": it characterizes the primes for which -1 is a square in the field $\mathbb{Z}_p$ (which is reviewed in the box on the next page).

Lemma 1. *The equation $x^2 \equiv -1 \pmod p$ has a solution for $p = 2$ and for the primes of the form $p = 4m + 1$, but not for the primes $p = 4m + 3$.*

■ **Proof.** For $p = 2$ take $x = 1$. For odd p, we construct the equivalence relation on $\{1, 2, \ldots, p-1\}$ that is generated by identifying every element with its additive inverse and with its multiplicative inverse in $\mathbb{Z}_p$. Thus the "general" equivalence classes will contain four elements

$$\{x, -x, \overline{x}, -\overline{x}\}$$

since such a 4-element set contains both inverses for all its elements. However, there are smaller equivalence classes if some of the four numbers are not distinct:

image
not
available

image
not
available

Index