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.

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

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

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

The first few Fermat numbers

M. Aigner, G. M. Ziegler, *Proofs from THE BOOK*, https://doi.org/10.1007/978-3-662-57265-8_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

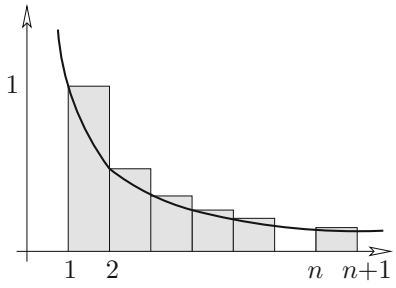
$$a \sim b :\iff ba^{-1} \in U.$$

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 $\{a, a^2, \ldots, a^m\}$ 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. In particular, we have $a^{|G|} = 1$.



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

■ **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 $\pi(x) \coloneqq \#\{p \le x : p \in \mathbb{P}\}$ 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 12 for this method.) Thus for $n \le x < n + 1$ we have

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

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 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.

"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

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

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). □

■ **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. □

Appendix: Infinitely many more proofs

Issai Schur

Our collection of proofs for the infinitude of primes contains several other old and new treasures, but there is one of very recent vintage that is quite different and deserves special mention. Let us try to identify sequences S of integers such that the set of primes $\mathbb{P}_S$ that divide some member of S is infinite. Every such sequence would then provide its own proof for the infinity of primes. The Fermat numbers F_n studied in the second proof form such a sequence, while the powers of 2 don't. Many more examples are provided by a theorem of Issai Schur, who showed in 1912 that for every nonconstant polynomial $p(x)$ with integer coefficients the set of all nonzero values $\{p(n) \neq 0 : n \in \mathbb{N}\}$ is such a sequence. For the polynomial $p(x) = x$, Schur's result gives us Euclid's theorem. As another example, for $p(x) = x^2 + 1$ we get that the "squares plus one" contain infinitely many different prime factors.

The following result due to Christian Elsholtz is a real gem: It generalizes Schur's theorem, the proof is just clever counting, and it is in a certain sense best possible.

Let $S = (s_1, s_2, s_3, \dots)$ be a sequence of integers. We say that

- S is *almost injective* if every value occurs at most c times for some constant c,
- S is *of subexponential growth* if $|s_n| \le 2^{2^{f(n)}}$ for all n, where $f\colon \mathbb{N} \to \mathbb{R}_+$ is a function with $\frac{f(n)}{\log_2 n} \to 0$.

In place of 2 we could take any other base larger than 1; for example, $|s_n| \le e^{e^{f(n)}}$ leads to the same class of sequences.

Theorem. *If the sequence $S = (s_1, s_2, s_3, \dots)$ is almost injective and of subexponential growth, then the set $\mathbb{P}_S$ of primes that divide some member of S is infinite.*

■ **Proof.** We may assume that $f(n)$ is monotonely increasing. Otherwise, replace $f(n)$ by $F(n) = \max_{i \le n} f(i)$; you can easily check that with this $F(n)$ the sequence S again satisfies the subexponential growth condition.

Let us suppose for a contradiction that $\mathbb{P}_S = \{p_1, \dots, p_k\}$ is finite. For $n \in \mathbb{N}$, let

$$s_n = \varepsilon_n p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad \text{with } \varepsilon_n \in \{1, 0, -1\},\ \alpha_i \ge 0,$$

where the $\alpha_i = \alpha_i(n)$ depend on n. (For $s_n = 0$ we can put $\alpha_i = 0$ for all i.) Then

$$2^{\alpha_1 + \cdots + \alpha_k} \le |s_n| \le 2^{2^{f(n)}} \quad \text{for } s_n \ne 0,$$

and thus by taking the binary logarithm

$$0 \le \alpha_i \le \alpha_1 + \cdots + \alpha_k \le 2^{f(n)} \quad \text{for } 1 \le i \le k.$$

Hence there are not more than $2^{f(n)} + 1$ different possible values for each $\alpha_i = \alpha_i(n)$. Since f is monotone, this gives a first estimate

$$\#\{\text{distinct } |s_n| \ne 0 \text{ for } n \le N\} \ \le\ (2^{f(N)} + 1)^k \ \le\ 2^{(f(N)+1)k}.$$

On the other hand, since S is almost injective only c terms in the sequence can be equal to 0, and each nonzero absolute value can occur at most $2c$ times, so we get the lower estimate

$$\#\{\text{distinct } |s_n| \ne 0 \text{ for } n \le N\} \ \ge\ \frac{N - c}{2c}.$$

Altogether, this gives

$$\frac{N - c}{2c} \ \le\ 2^{k(f(N)+1)}.$$

Taking again the logarithm with base 2 on both sides, we obtain

$$\log_2(N - c) - \log_2(2c) \ \le\ k\,(f(N) + 1) \quad \text{for all } N.$$

This, however, is plainly false for large N, as k and c are constants, so $\frac{\log_2(N-c)}{\log_2 N}$ goes to 1 for $N \to \infty$, while $\frac{f(N)}{\log_2 N}$ goes to 0. □

Can one relax the conditions? At least neither of them is superfluous.

That we need the "almost injective" condition can be seen from sequences S like $(2, 2, 2, \dots)$ or $(1, 2, 2, 4, 4, 4, 4, 8, \dots)$, which satisfy the growth condition, while $\mathbb{P}_S = \{2\}$ is finite.

As for the subexponential growth condition, let us remark that it cannot be weakened to a requirement of the form $\frac{f(n)}{\log_2 n} \leq \varepsilon$ for a fixed $\varepsilon > 0$. To see this, one analyzes the sequence of all numbers of the form $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ arranged in increasing order, where $p_1, \dots, p_k$ are fixed primes and k is large. This sequence S grows roughly like $2^{2^{f(n)}}$ with $\frac{f(n)}{\log_2 n} \approx \frac{1}{k}$, while $\mathbb{P}_S$ is finite by construction.

References

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

[2] C. ELSHOLTZ: *Prime divisors of thin sequences,* Amer. Math. Monthly **119** (2012), 331-333.

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

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

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

[6] I. SCHUR: *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen,* Sitzungsberichte der Berliner Math. Gesellschaft **11** (1912), 40-50.