Five proofs of the infinitude of primes

David Kohel
Institut de Mathématiques de Marseille

Marseille
January 2020

The infinitude of primes

In this talk we give a selection of the most elegant proofs of the infinitude of primes. Precisely, we proof the following theorem.

Theorem

The set of primes in $\mathbb{N}$ is infinite.

The earliest known proof is due to Euclid (*Elements*, ca. 300 B.C.).

We permit ourselves to use more modern notions in mathematics: arithmetic of $\mathbb{Z}/n\mathbb{Z}$ and basic results from analysis and topology.

Primes

Definition

Let $\mathscr{P}$ denote the set of primes in $\mathbb{N}$. For a real number $x \in \mathbb{R}$, we denote by $\mathscr{P}_x$ the subset of primes bounded by x. The cardinality of this set is denoted by

$$\pi(x) = |\mathscr{P}_x| = |\{p \in \mathscr{P} \; : \; p \leq x\}|.$$

Finally we denote $\mathscr{P}(n) \subset \mathscr{P}$ to be the set of prime divisors of n.

The infinitude of primes can be expressed equivalently by:

1. $\mathscr{P}$ is not finite.
2. $\mathscr{P}_x \neq \mathscr{P}$ for any $x \in \mathbb{R}$.
3. $\mathscr{P}(n) \neq \mathscr{P}$ for any $n \in \mathbb{N}$.
4. The function $\pi : \mathbb{R} \to \mathbb{N}$ is not bounded.

The earliest proofs assumed that $\mathscr{P}$ was finite and derived a contradiction.

Euclid's proof

Proof [Euclid].

Suppose that $\mathscr{P}$ is finite, set

$$n = \prod_{p \in \mathscr{P}} p,$$

and let q be a prime divisor of $n+1$. By construction, q is a prime divisor of both n and and $n+1$, hence of $\gcd(n, n+1) = 1$, a contradiction. □

Remark. Expressed differently, this argument can be viewed as a construction of a new prime q outside of any finite subset $S \subseteq \mathscr{P}$.

Proof by Fermat numbers

The next proof constructs an infinite family of subsets $S_n \subseteq \mathscr{P}$ which are nonempty and pairwise disjoint. In particular, if (a_n) is a sequence such that

$$a_n > 1, \text{ and } \gcd(a_m, a_n) = 1 \text{ for all } m \neq n,$$

then $(S_n) = (\mathscr{P}(a_n))$ is such a family. The infinitude of $\mathscr{P}$ follows.

Proof [Fermat numbers].

Let $(F_n) = (3, 5, 17, \dots)$ the sequence of Fermat numbers, defined by

$$F_n = 2^{2^n} + 1.$$

Clearly $F_n > 1$ for all n. It remains to show that $\gcd(F_m, F_n) = 1$ (we say that F_m and F_n are coprime).

A recursion for Fermat numbers

Interlude. In order to show that Fermat numbers are coprime, we prove the following recursion for Fermat numbers.

Lemma

For all $n > 1$ the following recursion $\prod_{m=0}^{n-1} F_m = F_n - 2$ holds.

Proof by induction.

For $n = 1$ the equality $F_0 = F_1 - 2 = 3$ is verified. Assuming the recursion holds for n, then

$$\prod_{m=0}^{n} F_m = (F_n - 2)F_n = (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2,$$

and the recursion follows by induction. □

Coprimality of Fermat numbers

Proof by Fermat numbers continued.

Let $r = \gcd(F_m, F_n)$, for $m < n$. To complete the proof, we show that $r = 1$. By the lemma, F_m divides $F_n - 2$. Thus $r = 1$ or 2, and since F_n is odd, $r = 1$.

To conclude, we recall that we have $F_n > 1$ for all $n \in \mathbb{N}$, which implies that the set $\mathscr{P}(F_n)$ of prime divisors of F_n is nonempty. Moreover $\gcd(F_m, F_n) = 1$ implies that $\mathscr{P}(F_m) \cap \mathscr{P}(F_n) = \emptyset$, and consequently

$$\bigcup_{n=0}^{\infty} \mathscr{P}(F_n)$$

is an infinite subset of $\mathscr{P}$. □

Proof by Mersenne numbers

Proof by Mersenne numbers.

Suppose that $\mathscr{P}$ is finite and $p = \max(\mathscr{P})$. Let $2^p - 1$ be the p-th Mersenne number, and suppose that q is a prime divisor.

Then $2^p \equiv 1 \mod q$ and since p is prime (and $2 \not\equiv 1 \mod q$), the element 2 has order p in $\mathbb{F}_q^*$ (by Lagrange).

In particular p divdes $q - 1$, and so $p < q$, a contradiction. □

Remark. The proof is constructive: for any given finite set of primes $S \subset \mathscr{P}$ one can construct a new prime outside of S.

An analytic lower bound

Proof by analysis.

We show that the function $\pi(x) = |\mathscr{P}_x|$ is bounded below by $\log(x)$. We observe that

$$\log(x) = \int_1^x \frac{1}{t}dt \leq 1 + \frac{1}{2} + \cdots \frac{1}{n},$$

for all $n \leq x < n+1$. If $S(x)$ is the set of positive integers whose prime divisors are in $\mathscr{P}_x$, then

$$\log(x) \leq \sum_{m \in S(x)} \frac{1}{m} = \prod_{p \in \mathscr{P}_x} \left(\sum_{i=0}^{\infty} \frac{1}{p^i} \right).$$

An analytic lower bound continued

Proof continued.

This gives the inequality

$$\log(x) \leq \prod_{p \in \mathscr{P}_x} \left(\sum_{i=0}^{\infty} \frac{1}{p^i} \right) = \prod_{p \in \mathscr{P}_x} \frac{1}{1 - 1/p} = \prod_{p \in \mathscr{P}_x} \frac{p}{p-1}.$$

If we denote $\mathscr{P}_x = \{p_1, p_2, \dots, p_{\pi(x)}\}$ such that $p_k < p_{k+1}$, and observe that $p_k \geq k+1$, then

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

Thus $\log(x) - 1 \leq \pi(x)$. Since $\log(x)$ is unbounded so is $\pi(x)$. □

Remark. This proof is remarkable for giving not only a proof of infinitude, but also an explicit lower bound on $\pi(x)$.

Fursternberg's exotic topology

Furstenberg's proof uses an exotic topology on $\mathbb{Z}$ in order to give an elegant but nonconstructive proof of the infinitude of primes. The idea is to declare the arithmetic sequences

$$S(a, b) = a + b\mathbb{Z} = \{a + bn \ : \ n \in \mathbb{Z}\},$$

to be open. The topology generated by the basis

$$\mathscr{B} = \{S(a, b) \ : \ a, b \in \mathbb{Z}\},$$

is called the *evenly spaced topology* on $\mathbb{Z}$.

We remark that $U \subset \mathbb{Z}$ is an open in this topology if and only for each $x \in U$, there exists $b \in \mathbb{Z}$ such that $S(x, b) \subseteq U$.

Fursternberg's topological proof

The evenly spaced topology of Furstenberg satisfies the following propoerties.

1. If U is open then either $U = \emptyset$ or U is not finite.
2. The sets $S(a, b)$ are both open and closed, since $\mathbb{Z}$ is the disjoint union: $\mathbb{Z} = S(0, b) \cup S(1, b) \cup \cdots \cup S(b-1, b)$.
3. $\mathbb{Z}\backslash\{\pm 1\} = \bigcup_{p \in \mathscr{P}} S(0, p)$.

These properties give the following simple proof.

Furstenberg's proof.

If $\mathscr{P}$ were finite, then $\mathbb{Z}\backslash\{\pm 1\}$ would be closed by **2**, hence $\{\pm 1\}$ would be open, contradicting **1**. □