Proofs of the Infinitude of Primes

Timo Chang
timo65537@protonmail.com

Last edited: June 5, 2025

Abstract

This essay aims to collect various simple proofs of the infinitude of primes.

1 Proofs of the Infinitude of Primes

1.1 Euclid's Original Proof

Theorem 1.1 (Euclid)**.** *Let S be a finite collection of prime numbers. Then there exists a prime that is not in S.*

Proof. Suppose $S = \{p_1, \dots, p_n\}$ and set $P = p_1 \cdots p_n + 1$. If P itself is a prime, then we are done because P is not equal to any of $p_1, \dots, p_n$. So suppose P is composite, then it has a prime factor, say q.

We claim that this q is not in S. Otherwise, we have $q = p_i$ for some $i = 1, \dots, n$. This implies q divides $p_1 \cdots p_n$. And since q also divides P, we have q divides $P - p_1 \cdots p_n = 1$, which is absurd. Hence, q is not in S. □

We mention that Euclid's proof of the "infinitude" of primes did not start with assuming that there are only finitely many. Instead, Theorem 1.1 says that any finite set of primes (not only the first n primes) can be extended to a larger prime set. We illustrate this by the following example.

Example 1.2. Let's say $S := \{2, 17, 43\}$. Then $P = 2 \cdot 17 \cdot 43 + 1$, which is divisible by 7. Thus, we have a new prime 7.

Let's adjoin 7 to our prime list and put $S' := \{2, 7, 17, 43\}$. Then $P' = 2 \cdot 7 \cdot 17 \cdot 43 + 1$, which is divisible by 5. Thus, we have a new prime 5.

Continuing this process, we obtain an infinite sequence of distinct primes. (It would be interesting to ask whether all primes appear in this way.)

Remark 1.3. It is a common mistake (due to the false belief mentioned earlier) to think the product of the first n primes plus 1 is a prime. As an example,

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 59 \cdot 509$$

is not a prime.

1.2 The Limit of the Prime Counting Function

Definition 1.4. The *prime counting function* $\pi : \mathbb{R} \to \mathbb{Z}_{\geq 0}$ is a function which counts the number of primes less than or equal to x. Precisely,

$$\pi(x) := \#\{p \leq x \mid p \text{ is a prime}\}.$$

Proposition 1.5. $\lim_{x \to \infty} \pi(x) = \infty$.

As an immediate corollary, this implies that there are infinitely many prime numbers.

Proof. Our strategy is to find a function which is bounded above by $\pi(x)$, but goes to infinity when $x \to \infty$. Then by comparison theorem we will obtain the result.

Let us fix an x and assume that $n \leq x < n + 1$ for some $n \in \mathbb{N}$. We consider the graph of the function $1/t$ as in Figure 1. Note that the area under the curve $1/t$ from 1 to x is smaller than the area of those rectangles. From basic Calculus, they are simply Riemann integral and the upper Riemann sum, respectively. So we see that

$$\int_1^x \frac{1}{t} dt = \ln x \leq 1 + \frac{1}{2} + \cdots + \frac{1}{n}. \tag{1}$$

Let $p_1 < p_2 < \cdots < p_s$ be all primes $\leq x$. We observe that

$$1 + \frac{1}{2} + \cdots + \frac{1}{n} \leq \sum_{\substack{m = p_1^{\alpha_1} \cdots p_s^{\alpha_s} \\ \alpha_i \in \mathbb{N}}} \frac{1}{m}. \tag{2}$$

This is because every positive integer $\leq n$ (which is now $\leq x$) can be factored uniquely as the product of $p_1, \ldots, p_s$. But the sum on the right runs over all the possible powers, so it contains more terms than the left-hand side.

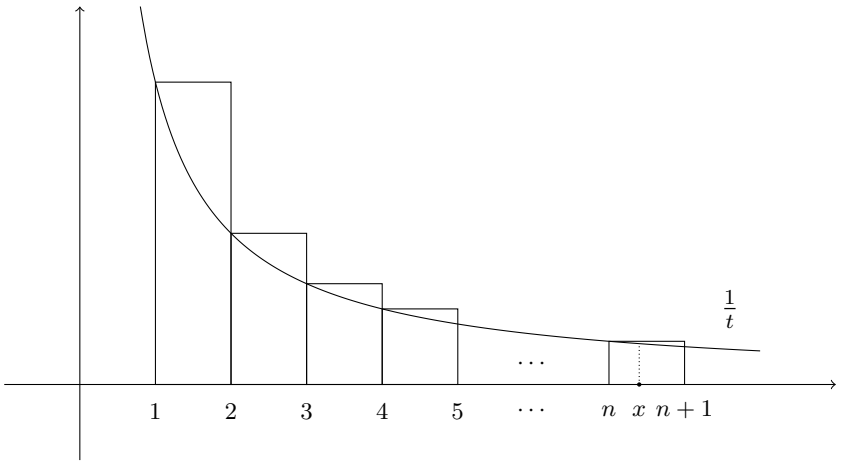

Figure 1

On the other hand, by the distributive law, we see that the sum

$$\sum_{\substack{m=p_1^{\alpha_1}\cdots p_s^{\alpha_s}\\ \alpha_i\in\mathbb{N}}} \frac{1}{m} = \left(1+\frac{1}{p_1}+\frac{1}{p_1^2}+\cdots\right)\cdots\left(1+\frac{1}{p_s}+\frac{1}{p_s^2}+\cdots\right)$$

$$= \prod_{i=1}^{s} \frac{1}{1-\frac{1}{p_i}} = \prod_{i=1}^{s}\left(\frac{p_i}{p_i-1}\right) = \prod_{i=1}^{s}\left(1+\frac{1}{p_i-1}\right).$$

Note that by the definition, p_i is the ith prime number. This implies that $p_i - 1 \geq i$. Hence, we have

$$\sum_{\substack{m=p_1^{\alpha_1}\cdots p_s^{\alpha_s}\\ \alpha_i\in\mathbb{N}}} \frac{1}{m} = \prod_{i=1}^{s}\left(1+\frac{1}{p_i-1}\right) \leq \prod_{i=1}^{s}\left(1+\frac{1}{i}\right) = \prod_{i=1}^{s}\left(\frac{i+1}{i}\right) = s+1. \tag{3}$$

But recall that s is the number of primes $\leq x$. This means by Definition 1.4,

$$s+1 = \pi(x)+1. \tag{4}$$

Now, we may combine all of the information and see that

$$\ln x \overset{(1)}{\leq} 1+\frac{1}{2}+\cdots+\frac{1}{n} \overset{(2)}{\leq} \sum_{\substack{m=p_1^{\alpha_1}\cdots p_s^{\alpha_s}\\ \alpha_i\in\mathbb{N}}} \frac{1}{m} \overset{(3)}{\leq} s+1 \overset{(4)}{=} \pi(x)+1.$$

Finally, since $\ln x \to \infty$ as $x \to \infty$, we have $\lim_{x\to\infty} \pi(x) = \infty$. This completes the proof. □

1.3 The Sum of Reciprocals of Primes

Proposition 1.6 (Euler, 1744[1]). *Let $\mathcal{P}$ be the set of all primes. Then the series $\sum_{p\in\mathcal{P}} 1/p$ diverges.*

Proof. We give a short proof due to Clarkson [Cla66]. Suppose on the contrary, the series $\sum_{p\in\mathcal{P}} 1/p$ converges. Then there exists $k \in \mathbb{N}$ such that

$$\sum_{\substack{p\in\mathcal{P}\\ p>k}} \frac{1}{p} \leq \frac{1}{2}.$$

In the case where $\mathcal{P}$ is finite, we take k to be the largest prime in $\mathcal{P}$ minus 1, so that the sum is non-empty.

Let Q be the product of primes $\leq k$. Then for each $n \in \mathbb{N}$, we have $p \nmid 1 + nQ$ for all $p \leq k$. Thus, all the prime divisors of $1 + nQ$ are $> k$. This implies for each $N \in \mathbb{N}$, the partial sum

$$\sum_{n=1}^{N} \frac{1}{1+nQ} \leq \sum_{t=1}^{\infty} \left(\sum_{\substack{p\in\mathcal{P}\\ p>k}} \frac{1}{p} \right)^t \leq \sum_{t=1}^{\infty} \left(\frac{1}{2}\right)^t = 1.$$

Thus, the series $\sum_{n=1}^{\infty} 1/(1+nQ)$ converges. But by the limit comparison test, this series should diverge. □

1.4 Furstenberg's Proof Using Topology

Theorem 1.7 ([Fur55]). *There are infinitely many primes.*

Proof. For $a, b \in \mathbb{Z}$ with $b \neq 0$, put

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

We define the topology on $\mathbb{Z}$ by declaring that $U \subseteq \mathbb{Z}$ is open if it is empty or a union of $S(a,b)$. One checks that this is indeed a topology.

- $\varnothing$ is open by the definition. And $\mathbb{Z} = S(0,1)$ is also open.
- Any union of open sets is open by the definition.
- The intersection of two open sets is open. This is because $S(a_1,b_1) \cap S(a_2,b_2)$, if non-empty, is precisely $S(x,b')$ where $x \in S(a_1,b_1) \cap S(a_2,b_2)$ and $b' := \operatorname{lcm}(b_1,b_2)$.

[1] See https://scholarlycommons.pacific.edu/euler-works/72/ Theorem 19

Note also that the basis $S(a,b)$ is closed because

$$S(a,b) = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} S(a+i,b).$$

Now, since every integer other than ± 1 is an integral multiple of some prime, we have

$$\mathbb{Z} \setminus \{1,-1\} = \bigcup_{p\text{: prime}} S(0,p).$$

The left-hand side is not closed because the finite set $\{1,-1\}$ can not be open. On the other hand, the right-hand side is a union of closed sets $S(0,p)$. Thus, the union can not be finite. This shows that there are infinitely many primes. □

1.5 Whang's Proof Using Legendre's Formula

Theorem 1.8 ([Wha10])**.** *There are infinitely many primes.*

Proof. Recall the following formula due to Legendre: For each $n \in \mathbb{N}$,

$$n! = \prod_{p\text{: prime}} p^{e_p(n)} \quad \text{where} \quad e_p(n) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right].$$

Note that

$$e_p(n) \le \sum_{k=1}^{\infty} \frac{n}{p^k} = \frac{n}{p-1} \le n.$$

Thus,

$$n! \le \prod_{p\text{: prime}} p^n \quad \text{for all} \quad n \in \mathbb{N}.$$

This implies there are infinitely many primes because we always have

$$\lim_{n\to\infty} \frac{c^n}{n!} = 0$$

for any constant $c \in \mathbb{R}$. □

References

[Cla66] James A. Clarkson. "Shorter Notes: On the Series of Prime Reciprocals". In: *Proc. Amer. Math. Soc.* 17.2 (1966), p. 541.

[Fur55] Harry Furstenberg. "On the Infinitude of Primes". In: *Amer. Math. Monthly* 62.5 (1955), p. 353.

[Wha10] Junho Peter Whang. "Another Proof of the Infinitude of the Prime Numbers". In: *Amer. Math. Monthly* 117.2 (2010), p. 181.