Proofs of the infinitude of primes

Tomohiro Yamada

Abstract

In this document, I would like to give several proofs that there exist infinitely many primes.

0 Introduction

It is well known that the number of primes is infinite.

In this document, I would like to give several proofs of this theorem. Many of these proofs give poor estimates for the number of primes below a given number. Let $\pi(x)$ denote the number of primes below a given number x. Then many proofs give estimates such that $\pi(x) > c \log x$ for some constant $c > 0$.

The proofs in Sections 1, 2, 3, 4, 5, 6, 10, 11, 12 are given in [6]. The proofs in Sections 1, 3, 6, 13, 11 are introduced in [3]. Eudős' proof and Chebysheff's proof can be found in the book of Hardy-Wright [4]. Other proofs are given by [1], [2], [5] and [7]. There literatures can be found by the search result of MathSciNet by "infinitude of prime*".

Of course, there are more proofs of the infinitude of primes. I would like to add such proofs later.

1 Euclid's proof

Suppose that $2 = p_1 < p_2 < \cdots < p_r$ are all of the primes. Let $P = p_1 p_2 \cdots p_r + 1$ and p be a prime dividing P. Since none of $p_1, p_2, \ldots, p_r$ divides $P = p_1 p_2 \cdots p_r + 1$, p must be another prime. Therefore $p_1, p_2, \ldots, p_r$ cannot be all of the primes. □

Euclid's proof will be the most popular proof of the infinitude of primes.

It is very simple. Moreover, Euclid's proof can be modified so that it gives an information on the distribution of primes; there exists a prime p with $R < p \leq R^R + 1$ for any $R \geq 2$.

Suppose that $2 = p_1 < p_2 < \cdots < p_r$ are all of the primes below R. Let $P = p_1 p_2 \cdots p_r + 1$ and p be a prime dividing P. Since none of $p_1, p_2, \ldots, p_r$ divides $P = p_1 p_2 \cdots p_r + 1$, p must be another prime. We clearly have $p \leq R^r + 1 \leq R^R + 1$. Since $p_1, p_2, \ldots, p_r$ are all of the primes below R, we see that $p > R$.

We can see that $R^R + 1$ can be replaced by $R^{R/2+1} + 1$, finding that the number of primes below R cannot exceed $R/2 + 1$ since 1 and all even integers other than 2 cannot be prime.

Of course, it is very poor result.

We note that a number of the form $p_1 p_2 \cdots p_r + 1$ is not necessarily itself prime. Indeed, we see that $2 \times 3 \times 11 \times 13 + 1 = 59 \times 509$.

Euclid's proof has many variants.

2 Kummer's proof

Suppose that $2 = p_1 < p_2 < \cdots < p_r$ are all of the primes. Let $N = p_1 p_2 \cdots p_r > 2$. The integer $N - 1 > p_r$, being a product of primes, must have a prime divisor p_i. So p_i divides $N - (N - 1) = 1$, which is impossible. □

Kummer's proof is essentially the same as Euclid's one. Kummer's uses $p_1 p_2 \cdots p_r - 1$ while Euclid's uses $p_1 p_2 \cdots p_r + 1$. Similar to Euclid's proof, Kummer's proof can be modified to show that there exists a prime p with $R < p \leq R^{R/2+1} - 1$ for any $R \geq 2$.

3 Stieltjes' proof

Assume that $p_1, p_2, \ldots, p_r$ are the only primes. Let $N = p_1 p_2 \cdots p_r$ and let $N = mn$ be any factorization of N with $m, n \geq 1$. Since each prime p_i divides exactly one of m and n, none of p_i's divides $m + n$. This means $m + n$ is divisible by none of the existing primes, which is impossible since $m + n > 1$. □

4 Goldbach's proof

We begin by showing that the Fermat numbers $F_n = 2^{2^n} + 1 (n \geq 0)$ are pairwise coprime. Indeed, we see that $F_m - 2 = 2^{2^n} - 1 = (2^{2^n-1}+1)(2^{2^n-1} - 1) = F_0 F_1 \cdots F_{m-1}$. Therefore any prime dividing both F_m and $F_n (m > n)$ must divide $2 = F_m - (F_m - 2)$. However, there can be no such prime since F_n is odd for any n.

So, if q_1 is a prime dividing F_1, q_2 is a prime dividing F_2, $\ldots$, then $q_1, q_2, \ldots$ is an infinite sequence of primes. □

Part 8, Problem 94 of the book of Pólya and Szegö indicates this proof. However, they are not the first to have this idea. It is written in p. 4 of Ribenboim's book:

> Nobody seems to be the first to have a good idea – especially if it is simple. I thought it was due to Pólya and Szegö (see their book, 1924). E. Specker called my attentino to the fact that Pólya used an exercise by Hurwitz (1891). But, W. Narkiewirz just told me that in a letter to Euler (July 20/31, 1730), Goldbach wrote the proof given below using Fermat numbers – this may well be the only written proof of Goldbach.

Explicitly, the first Fermat numbers are $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$, each of which is itself prime. However, $F_5 = 4294967297 = 641$ is composite.

5 Schorn's proof

Assume that there exist only m primes and let $n = m + 1$. We note the n integers $(n!)i + 1 (i = 1, 2, \ldots, n)$ are pairwise coprime. Indeed, if $1 \leq i < j \leq n$ and $j = i + d$, then $((n!)i + 1, (n!)j + 1) = ((n!)i + 1, (n!)d) = 1$. Let p_i be a prime dividing $(n!)i + 1$ for each $i = 1, 2, \ldots, n$. Then $p_1, p_2, \ldots, p_n$ must be distinct primes. Therefore there exist at least n prime numbers, which is absurd. □

Schorn's proof shows that there exist at least n primes below $(n!)n + 1$ for any integer n.

6 Euler's proof

Euler's proof uses a rather analytic idea while many proofs of the infinitude of primes are elementary. However, Euler's method leads to important developments on the distribution of primes.

Suppost that $p_1, p_2, \ldots, p_n$ are all of the primes. Since each $p_i > 1$, the sum of the geometric series $\sum_{k=0}^{\infty} 1/p_i^k$ is $1/(1-1/p_i)$.

Hence $\prod_{i=1}^{n} 1/(1-1/p_i) = \prod_{i=1}^{n} \sum_{k=0}^{\infty} 1/p_i^k$. The right-hand side is the sum of all positive integers, each counted at least once, since $p_1, p_2, \ldots, p_n$ are all of the primes. Therefore $\sum_{n=1}^{\infty} 1/n \leq \prod_{i=1}^{n} 1/(1-1/p_i)$ must be finite. However, it is well known that $\sum_{n=1}^{\infty} 1/n$ is divergent (we can see this by $\sum_{n=1}^{\infty} 1/n \geq 1 + 1/2 + (1/4+1/4) + (1/8+1/8+1/8+1/8) + \cdots$) This is a contradiction. □

Indeed, Euler obtains the well-known formula that $\sum_{n=1}^{\infty} 1/n^s = \prod_{i=1}^{n} 1/(1-1/p_i^s)$ using the fundamental theorem of arithmetic.

An interesting point of Euler's method lies on indicating the link between the zeta function $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$ and the prime numbers. This is one of the most important basis of analytic number theory.

Euler further shows that the reciprocals of the prime is divergent.

We see that $\sum_{n=1}^{N} 1/n \leq \prod_{p \leq N} 1/(1-1/p)$ for any integer N since any integer $\leq N$ must have a prime divisor $\leq N$. Now $\log \prod_{p \leq N} 1/(1-1/p) = -\sum_{p \leq N} \log(1-1/p)$, and for each prime p we have $\log(1-1/p) = \sum_{m=1}^{\infty} 1/(mp^m) \leq \sum_{m=1}^{\infty} 1/(p^m) = 1/p + 1/p(p-1) < 1/p + 1/(p-1)^2$. Hence, $\log \sum_{n=1}^{N} 1/n \leq \sum_{p \leq N} 1/p + 1/(p-1)^2 \leq \sum_{p \leq N} 1/p + \sum_{n} 1/n^2$.

This shows that $\sum_{p \leq N} 1/p \geq \log \sum_{n=1}^{N} 1/n - c \geq \log\log N - C$ for some constants c and C.

7 Erdős' proof

Erdős gave an elementary proof of divergence of the sum of reciprocals of primes.

Let $p_1 = 2, p_2 = 3, \ldots, p_j$ be all primes below x. Let $n = n_1^2 m$ with m squarefree. Then $m = 2^{b_1} 3^{b_2} \cdots p_j^{b_j}$ with every b_i either 0 or 1. There exists at most 2^j such integers. For each fixed m, the number of possibility of n_1

is at most $x^{1/2}$ since $n_1^2 \leq n \leq x$. Thus we have $x \leq 2^j x^{1/2}$, or, equivalently, $j \leq (\log x)/(2\log 2)$. So that there exist at least $(\log x)/(2\log 2)$ prime numbers below x. □

Using Erdős' argument, we can also prove that the reciprocals of the prime is divergent.

Assume that there exists a number M such that $\sum_{p>M} 1/p < 1/2$. Then we have $\sum_{p>M} N/p < N/2$ for any integer N.

Now divide the positive integers below N into two sets. Let N_1 be the number of positive integer below N which can be divisible by some prime $> M$ and N_2 be the number of remaining integers below N.

Then we have $N_1 \leq \sum_{p>M} N/p < N/2$. Moreover, we have $N_2 < 2^M N^{1/2}$ by repeating the argument given above. So that $N = N_1 + N_2 < N/2 + 2^M N^{1/2} < N$ if we take N sufficiently large. This is absurd. □

8 Chebysheff's proof

Chebysheff used the arithmetic property of the factorials to prove his celebrated theorem that there always exists a prime p with $x < p < 2x$ for $x > 1$. Erdős gave a simple proof.

Chebysheff's argument can be used to give a simple proof of the infinitude of primes.

Let $a(p, N)$ be the exponent of prime p dividing the factorial $N!$.

Then we have $a(p, N) = \lfloor N/p \rfloor + \lfloor N/p^2 \rfloor + \cdots < N/(p-1)$ for any prime p and $a(p, N) = 0$ for $p > N$.

So that $\sum_{p \leq N} (\log p)/(p-1) > \sum_p a(p, N)(\log p)/N = (1/N)\log(N!) > (\log N) - 1$. Therefore the sum $\sum_{p \leq N} (\log p)/(p-1)$ tends to infinity together with N. This clearly implies the infinitude of primes. □

9 Srinivasan's proof

As mentioned above, any infinite sequence of pairwise coprime integers shows the infinite of primes.

If the sequence x_i satisfies $x_i \mid x_{i+1}$ and $\gcd(x_i, x_{i+1}/x_i)$, then we immediately see that the sequence x_{i+1}/x_i contains no two integers which has a nontrivial common divisor.

Let $f(x) = x^2+x+1$. Then $f(n^2) = f(n)f(-n)$ and $\gcd(n^2+n+1, n^2-n+1) = 1$. Indeed, n^2+n+1 must be odd and $d \mid \gcd(n^2+n+1, n^2-n+1)$ implies $d \mid 2n, d \mid n$, thus $d = 1$. So that the sequence $f(2^{2^m})$ works.

The sequence $x_m = 2^{p^m} - 1$ also works. We see that $q \mid x_m$ implies $x_{m+1}/x_m = ((x_m+1)^p - 1)/((x_m+1)-1) = 1+(x_m+1)+\cdots+(x_m+1)^{p-1} \equiv p \pmod q$. So that if a prime q divides x_m and x_{m+1}/x_m, then $q = p$, which is impossible since $x_m = (2^m)^p - 1 \equiv 1 \pmod p$ by Fermat's theorem. □

We note that the prime factor $2^{p^m} - 1$ must be $\equiv 1 \pmod{p^m}$. Therefore, this shows that there are infinitely many primes $\equiv 1 \pmod{p^m}$.

Srinivasan also shows that there are infinitely many primes $\equiv 1 \pmod k$ for every integer $k \geq 1$ using the same method. Actually, this is essentially a variant of Lucas' argument showing that there are infinitely many primes $\equiv 1 \pmod k$ for every integer $k \geq 1$.

10 Thue's proof

Let $n, k \geq 1$ be integers satisfying $(1+n)^k < 2^n$ and $p_1 = 2, p_2 = 3, \ldots, p_r$ be all primes $\leq 2^n$. Every integer $m, 1 \leq m \leq 2^n$ can be written in the form $m = 2^{e_1}3^{e_2}\cdots p_r^{e_r}$. It is clear that every $e_i \leq n$ since $m \leq 2^n$. Since the number of such choices of $e_1, e_2, \ldots, e_r$ is at most $(n+1)^r$, we have $(1+n)^k < 2^n \leq (1+n)^r$. So that $r > k$. For every integer $k \geq 1$, we have $(1+2k^2)^k < 2^{2k^2}$ since $1+2k^2 < 2^{2k}$. Thus we can choose $n = 2k^2$ for every integer $k \geq 1$. It follows that there exist at least $k+1$ primes $p < 2^n = 4^{k^2}$. □

11 Perott's proof

First we note that $\sum_{n=1}^{\infty}(1/n^2)$ is convergent with sum smaller than 2. Indeed, it is a well-known result of Euler that the sum is exactly $\pi^2/6$. A simple and elementary argument gives that $\sum_{n=1}^{\infty}(1/n^2) < 7/4$ since

$$\sum_{n=1}^{\infty}(1/n^2) = 1+1/4+\sum_{n=3}^{\infty}(1/n^2) < 5/4+\sum_{n=3}^{\infty}(1/n(n-1)) = 5/4+\sum_{n=3}^{\infty}(\frac{1}{n-1}-\frac{1}{n}) = 5/4+1/2 = 7/4.$$

Let $\delta = 2 - \sum_{n=1}^{\infty}(1/n^2)$. The above estimate gives $\delta > 1/4$. Let $p_1, p_2, \ldots, p_r$ be all primes $\leq N$. The number of integers $m \leq N$ not divisible by a square is therefore at most 2^r. The number of integers $m \leq N$ divisible by d^2 is at most N/d^2, so that the number of integers $m \leq N$ divisible by some square is at most $\sum_{d=2}^{\infty}(N/d^2) = N(\sum_{d=1}^{\infty}(N/d^2) - 1) = N(1-\delta)$. Therefore $N \leq 2^r + N(1-\delta)$. Thus $2^r \geq \delta N \geq N/4$. This gives $r > (\log N/\log 2) - 2$. □

Perott's proof counts that the number of integers $m \leq N$ not divisible by a square by excluding the set of integers $m \leq N$ divisible by each square d^2. This argument is essentially the basis of sieve theory developed to provide estimates for the number of integers satisfying given conditions.

12 Auric's proof

Suppose that $p_1 < p_2 < \cdots < p_r$ are all of the primes. Let $t \geq 1$ be any integer and $N = p_r^t$.

Each positive integer $m \leq N$ is written as $m = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$ with the r-tuple $(f_1, f_2, \ldots, f_r)$ uniquely defined. Letting $E = (\log p_r)/(\log p_1)$, we have $f_i \leq tE$ since $p_1^{f_i} \leq p_i^{f_i} \leq N = p_r^t$ for every i. Thus N is at most the number of r-tuples $(f_1, f_2, \ldots, f_r)$ and therefore $p_t^r = N \leq (tE+1)^r \leq t^r(E+1)^r$, which is clearly impossible for sufficiently large t. □

13 Boije and Gennäs

Let X be an arbitrary real number and $2, 3, \ldots, p_n$ be all primes $\leq X$. Take $P = 2^{e_1}3^{e_2}\cdots p_n^{e_n}$ with each $e_i \geq 1$. Write P as a product of relatively prime factors $\delta, P/\delta$, where $Q = P/\delta - \delta > 1$. Since Q is divisible by no prime $\leq X$, it must be a product of primes $> X$. In particular, there exists a prime $> X$. □

14 Barnes' proof

In 1976, Barnes published a new proof of the infinitude of primes using the theory of periodic continued fractions and the theory of Pellian equations.

Let $p_1 = 2, p_2 = 3, \ldots, p_t$ be all of the primes and $P = \prod_{i=1}^{t} p_i, Q =$

$\prod_{i=2}^{t} p_i$. Consider the continued fraction $x = [p, p, \ldots]$. Then we have $x = (P + \sqrt{P^2+4})/2 = Q + \sqrt{Q^2+1}$.

Now $Q^2 + 1$ must be a power of two and therefore $Q^2 + 1 = 2^{2l+1}$ or $Q^2 - 2(2^l)^2 = -1$. This means that $Q/2^l$ is an even approximant of $[1, 2, 2, \ldots]$, the continued fraction for $\sqrt{2}$. Denote the dinominator of the approximants by B_m. Thus we have $B_0 = 1, B_1 = 2, B_{m+1} = 2B_m + B_{m-1}$ and B_m must be odd for even m. Thus $l = 0$ and $Q = 1$. This is a contradiction. □

Of course $Q^2 + 1$ cannot be a power of two since $Q^2 + 1 > 2$ and $Q^2 + 1$ cannot be divisible by 4.

15 Braun's proof

Suppose that there exist only t primes $p_1, p_2, \ldots, p_t$ and consider the sum $m/n = \sum_{i=1}^{t} 1/p_i$. Now $1/2 + 1/3 + 1/5 > 1$, so that $m/n > 1$ and therefore $m > n \geq 1$. Thus m must have a prime factor p_i. However, no p_i can divide m since $p_i \mid m$ implies $p_i \mid p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_t$. This is a contradiction. □

16 Harris' proof

Let A_0, A_1, A_2 be positive and pairwise coprime integers, and for $n \geq 3$ set $A_n = A_0 A_1 \cdots A_{n-3} A_{n-1} + A_{n-2}$. Now we can show that $A_0, A_1, \ldots, A_n$ are pairwise coprime by induction; $p \mid \gcd(A_n, A_{n-2})$ implies $p \mid \gcd(A_{n-i}, A_{n-2})$ for some $i \geq 1, i \neq 2$ and $p \mid \gcd(A_n, A_{n-j})$ for some $j \geq 1, j \neq 2$ implies $p \mid \gcd(A_{n-j}, A_{n-2})$. Since $A_n > 1$ at least for $n \geq 3$, we see that $A_0, A_1, \ldots$ contains an infinite set of integers > 1 no two of which has a common prime factor. Therefore the number of primes is infinite. □

We note that taking the sequence $b_i (i \geq 0)$ such that $A_0 = b_0, A_1 = b_0 b_1 + 1, A_2 = b_0 b_1 b_2 + b_0 + b_2$ and $b_n = A_0 A_1 \cdots A_{n-3}$, A_n is the numerator of approximants of the regular infinite continued fraction $[b_0, b_1, b_2, \ldots]$.

17 Chernoff's proof

Chernoff's proof uses only a simple enumerating argument. Suppose that there are only k primes $p_1, p_2, \ldots, p_k$. If N is any positive integer, there are exactly N k-tuples of nonnegative integers $(e_1, e_2, \ldots, e_k)$ satisfying the inequality $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \le N$, or, equivalently, $e_1 \log p_1 + e_2 \log p_2 + \cdots + e_k \log p_k \le \log N$. The number of such k-tuples is $(\log N)^k / (k! \log p_1 \log p_2 \cdots \log p_k)$. Therefore $N \le c(\log N)^k$ for some constant c, which is clearly false. Thus there are infinitely many primes. □

We note that we need not use the uniqueness of prime factorization; the fact suffices that there are at most N k-tuples of nonnegative integers $(e_1, e_2, \ldots, e_k)$ satisfying the above inequality.

Moreover, the argument works even if we suppose that there are only k primes $p_1, p_2, \ldots, p_k$ below N. We can take $c = 1/(k! \log 2)$ and therefore $N \le (\log N)^k / (k! \log 2)$. This gives $k > c'(\log N)$ for some positive constant c'.

References

[1] C. W. Barnes, The infinitude of primes; a proof using continued fractions, *L'Enseignement Math.* (2) **22** (1976), 313–316.

[2] Paul R. Chernoff, A "Lattice Point" Proof of the Infinitude of Primes. *Math. Mag.* **38** (1965), 208.

[3] L. E. Dickson, *History of the Theory of Numbers, Vol. I: Divisibility and Primality*, Carnegie Institution of Washington, 1919 (reprint: Dover Publication, New York, 2005).

[4] G. H. Hardy and E. M. Wright, D. R. Heath-Brown, J. Silverman, A. Wiles, *An Introduction to the Theory of Numbers*, the 6th edition, Oxford University Press, 2008.

[5] V. C. Harris, Another proof of the infinitude of primes, *Amer. Math. Monthly* **63** (1956), 711.

[6] P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, New York, 1996.

[7] S. Srinivasan, on infinitude of primes, *Hardy Ramanujan J.* **7** (1984), 21–26.