SOME PROOFS OF THE INFINITUDE OF PRIME NUMBERS

ALESSIO DEL VIGNA

A *prime number* is an integer greater than 1 which is divisible by 1 and itself. We shall denote by $\mathfrak{P} = \{p_n : n \geq 1\}$ the set of prime numbers, so that

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \quad \dots$$

that is, p_n is the n-th prime number. The main character of this note is the following well known result.

Theorem 1. *There are infinitely many prime numbers.*

This property was proved by Euclid in his *Elements* (Book IX, Proposition 20) and it is known by nearly every mathematics student. Many proofs of Euclid's theorem are currently known and our aim for this note is to present some of them.

1. Euclid's proof

Here we present the proof given by Euclid, of course with a modern language, and a variation of it given by Kummer [3] in 1878.

Proof (Euclid). Suppose by contradiction that there are finitely many prime numbers, say $p_1 < p_2 < \cdots < p_k$. Define

$$N = p_1 p_2 \cdots p_k + 1,$$

which cannot be prime because $N > p_k$. But N is not divisible by any of the p_i's, which gives us a contradiction. □

Kummer's proof is very similar to Euclid's one in spirit.

Proof (Kummer). Suppose by contradiction that there are finitely many prime numbers, say $p_1 < p_2 < \cdots < p_k$, with $k \geq 2$. Define

$$N = p_1 p_2 \cdots p_k.$$

The number $N - 1$ is greater than 1, thus it has a prime divisor among the primes $p_1, \dots, p_k$. Let p_j be this prime divisor. But p_j is also a divisor of N by construction, thus $p_j \mid N - (N-1) = 1$, which is a contradiction. □

2. A modern proof

After the classical proof by Euclid we now take a leap forward of more than two millennia and present a recent proof by Saidak [4]. This proof dates back to 2005, showing that original proofs of Euclid's theorem can be found even nowadays.

Proof (Saidak). Let n be a positive integer greater than 1. Since n and $n+1$ are consecutive integers, they must be relatively prime. It follows that the number $n(n+1)$ has at least two distinct prime factors. Similarly, $n(n+1)$ and $n(n+1)+1$ are relatively prime, thus the number $n(n+1)\cdot(n(n+1)+1)$ has at least three prime factors. This process can be continued indefinitely, showing that the number of primes is infinite. □

3. Fermat and Mersenne numbers

We recall that a *Fermat number* is an integer of the form

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

for $n \geq 0$. Arguing inductively, one can prove that for every $n \geq 1$ it holds

$$F_n = F_0 \cdots F_{n-1} + 2,$$

from which it easily follows that distinct Fermat numbers are relatively prime. From this fact we get another proof of the infinitude of primes.

Proof. For each Fermat number we can choose one of its prime factors, for instance the smallest one. Since distinct Fermat numbers do not share any common factor, this correspondence is injective, proving that there are infinitely many prime numbers. □

A *Mersenne number* is an integer of the form

$$M_n = 2^n - 1$$

for $n \geq 2$. It is easy to prove that if n is composite then M_n must be composite, so the only possibility for M_n to be prime is that n is prime. A *Mersenne prime* is thus a prime number of the form $2^p - 1$, with p being a prime number.

Proof. Suppose that there are finitely many prime numbers and let p the greatest one. Consider the Mersenne number $M_p = 2^p - 1$ and let q a prime factor of M_p, that is $2^p \equiv 1 \pmod{q}$. Thus the multiplicative order of 2 in $(\mathbb{Z}/q\mathbb{Z})^*$ divides p and hence is exactly p. In a group the order of an elements divides the order of the group, thus $p \mid q-1$. But then $p < q$, which contradicts the maximality of p. □

4. The proof of Euler

Euler is certainly one of the greatest and most prolific mathematicians of all time. His proof of the infinitude of prime numbers, besides being elegant, uses ideas which will later turn out to be useful in many fields of mathematics.

We first recall the definition of the arithmetic function π, which counts the prime numbers. To be more precise, for $x \in \mathbb{R}$ we set

$$\pi(x) \coloneqq \#\{p \leq x \,:\, p \in \mathfrak{P}\} = \sum_{p \leq x} 1.$$

Proof (Euler). If $n < x \leq n+1$ then

$$\log x = \int_1^x \frac{1}{t}\,dt \leq 1 + \frac{1}{2} + \cdots + \frac{1}{n} \leq \sum_{m \in \Lambda_x} \frac{1}{m},$$

where Λ_x is the set of positive integers with prime divisors not greater than x. The brilliant idea of Euler is to convert the above sum into a product over the prime numbers. Indeed from the fundamental theorem of arithmetic we have

$$\sum_{m\in\Lambda_x}\frac{1}{m}=\prod_{p\leq x}\sum_{k=0}^{\infty}\frac{1}{p^k},$$

hence

$$\log x\leq\prod_{p\leq x}\sum_{k=0}^{\infty}\frac{1}{p^k}=\prod_{p\leq x}\frac{1}{1-\frac{1}{p}}=\prod_{r=1}^{\pi(x)}\frac{1}{1-\frac{1}{p_r}}.$$

Since $p_r\geq r+1$ for every $r\geq 1$ we have

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

Since $\log x$ diverges as $x\to\infty$, we have that also $\pi(x)$ diverges, which implies that $\mathfrak{P}$ is infinite. □

The following is not a proof given by Euler, but exploits the same idea.

Proof. Consider the product

$$\prod_p\frac{1}{1-\frac{1}{p^2}}$$

and write its general term as a geometric series. Limiting the product to the primes not exceeding a certain $N>1$, we have

$$\prod_{p\leq N}\frac{1}{1-\frac{1}{p^2}}=\prod_{p\leq N}\sum_{k=0}^{\infty}\left(\frac{1}{p^2}\right)^k=\sum_{n\in\Lambda_N}\frac{1}{n^2},\tag{1}$$

where Λ_N is the set of numbers whose prime divisors do not exceed N. Taking the limit for $N\to\infty$ we get

$$\prod_p\frac{1}{1-\frac{1}{p^2}}=\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6}.$$

If $\mathfrak{P}$ were a finite set then the left hand side would be rational, being it a finite product of rational numbers. But the right hand side is not rational because $\pi^2\notin\mathbb{Q}$, which gives us a contradiction. □

Remark 2. The fact that $\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6}$ is not trivial. Three different and clever proofs can be found in the beautiful book [1].

Remark 3. When we used that π^2 is not rational we implicitely assumed that π is not only irrational, but also transcendental. In 1794 Legendre proved that π is irrational and later, in 1882, Lindemann proved that π is transcendental. Both facts were not known to Euler, though he had supposed that they were true.

5. Erdös and the series of the recicprocals of the primes

In this section we prove that the series

$$\sum_p \frac{1}{p}$$

diverges, which implies that the set $\mathfrak{P}$ is infinite. We follow the brilliant proof given by Erdös, also presented in [1].

Proof (Erdös). Suppose by contradiction that the series $\sum_p \frac{1}{p}$ is convergent. Then there exists k such that

$$\sum_{j\geq k+1} \frac{1}{p_j} < \frac{1}{2}.$$

We shall call *small primes* the prime numbers $p_1, \ldots, p_k$ and *big primes* the prime numbers in $\mathfrak{P} \setminus \{p_1, \ldots, p_k\}$. Given a non-negative integer N we set

$$\mathcal{N}_b = \{n \in \mathbb{N} \,:\, 0 < n \leq N \text{ and } n \text{ has at least a big prime factor}\}$$

and

$$\mathcal{N}_s = \{n \in \mathbb{N} \,:\, 0 < n \leq N \text{ and } n \text{ has only small prime factors}\}.$$

Note that $1 \in \mathcal{N}_s$, being it the empty product. Let

$$N_b = \#\mathcal{N}_b \quad \text{and} \quad N_s = \#\mathcal{N}_s.$$

Of course $N = N_b + N_s$ and now we show that by assuming that $\sum_p \frac{1}{p}$ converges we obtain the contradiction $N \neq N_b + N_s$.

Note that $\left[\frac{N}{p_j}\right]$ counts how many integers $\leq N$ are divisible by p_j, thus we have

$$N_b \leq \sum_{j\geq k+1} \left[\frac{N}{p_j}\right] \leq \sum_{j\geq k+1} \frac{N}{p_j} < \frac{N}{2}.$$

We now estimate N_s. Let $n \in \mathcal{N}_s$ and note that it can be uniquely written as

$$n = a_n^2 b_n,$$

with b_n being a square-free integer. Since $n \in \mathcal{N}_s$ the factor b_n must be a product of distinct small primes, hence it can be chosen in 2^k ways. Furthermore, since $a_n \leq \sqrt{n} \leq \sqrt{N}$ we have at most $\sqrt{N}$ possibilities for a_n. As a consequence

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

By choosing $N = 2^{2k+2}$ we obtain the estimate $N_s \leq \frac{N}{2}$, which implies $N = N_b + N_s < N$, a contradiction. □

6. A topological proof

In 1955, Furstenberg gave his famous topological proof of the infinitude of the primes in the paper [2].

Proof (Furstenberg). In the first part of the proof we define a topology on the set $\mathbb{Z}$. For $a, b \in \mathbb{Z}$ with $b > 0$ we set

$$N_{a,b} = \{a + nb \,:\, n \in \mathbb{Z}\}$$

and we say that $\mathcal{O} \subseteq \mathbb{Z}$ is an open set if $\mathcal{O}$ is empty or if for all $a \in \mathcal{O}$ there exists $b > 0$ with $N_{a,b} \subseteq \mathcal{O}$. We observe that each set $N_{a,b}$ is open. Proving that we actually defined a topology is an easy task.

(i) The empty set is open by definition and $\mathbb{Z} = N_{0,1}$, thus it is open.

(ii) It is clear that the union of open sets is open.

(iii) If $\mathcal{O}_1$ and $\mathcal{O}_2$ are open sets and $a \in \mathcal{O}_1 \cap \mathcal{O}_2$ then there exist $b_1 > 0$ and $b_2 > 0$ such that $N_{a,b_1} \subseteq \mathcal{O}_1$ and $N_{a,b_2} \subseteq \mathcal{O}_2$. Then $a \in N_{a,b_1 b_2} \subseteq \mathcal{O}_1 \cap \mathcal{O}_2$, from which it follows that the intersection of a finite number of open sets is open.

We have two properties of this topology:

(P1) every non-empty open set is infinite;

(P2) every open set $N_{a,b}$ is also closed because it can be written as $N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}$, which is the complement of a finite union of open sets.

Every integer $n \in \mathbb{Z} \setminus \{-1, 1\}$ is either zero or has a prime factor p, thus it is contained in $N_{0,p}$. Hence

$$\mathbb{Z} \setminus \{-1, 1\} = \bigcup_p N_{0,p}.$$

If the set $\mathfrak{P}$ were finite, then $\bigcup_p N_{0,p}$ woudl be closed since it is a finite union of closed sets by the property (P2) . From this it follows that $\{-1, 1\}$ would be an open set, which contradicts property (P1) . □

References

[1] M. Aigner and G. M. Ziegler, *Proofs from THE BOOK*, 4th, Springer Publishing Company, Incorporated, 2009

[2] H. Furstenberg, *On the Infinitude of Primes*, The American Mathematical Monthly **62**(5): 353–353, 1955

[3] E. Kummer, *Neuer elementarer Beweis des Satzes, daß die Anzahl aller Primzahlen eine unendliche ist*, Monatsber. Preuss. Akad. Wiss., 1878

[4] F. Saidak, *A New Proof of Euclid's Theorem*, The American Mathematical Monthly **113**(10): 937–938, 2006

Dipartimento di Matematica, Università di Pisa
Email address: `alessio.delvigna@dm.unipi.it`