Primes: the indivisible and the indispensable (4)

Philomathes • 5 Feb 2025

Infinitude of Primes and Euclid’s Proof

Earlier, we acquired an age-old but reliable weapon: proof by contradiction. However, this single weapon alone is not enough to prove the infinitude of prime numbers. Proof by contradiction is like a final weapon, a bomb that demolishes enemy strongholds. Relying solely on it and charging forward recklessly might lead to unexpected pitfalls. When proving that natural numbers are infinite, the simple principle that "if x is a natural number, then x+1 is also a natural number" sufficed. But to prove the infinitude of primes, we need a more refined and sophisticated tool.

Let’s first establish a few mathematical terms. An integer is a number that falls into the sequence ..., -3, -2, -1, 0, 1, 2, 3, ... without any decimal points. Consider any two integers. For example, taking 5 and 7, their sum is 12, their difference is -2, and their product is 35, all of which remain integers. This holds true for any pair of integers—their sum, difference, and product are always integers. We express this property by saying that "integers are closed under addition, subtraction, and multiplication." However, integers are not closed under division; for instance, dividing 5 by 7 gives 5/7, which is not an integer.[1]

When defining prime numbers, we often use the concept of "divisibility." We naturally say things like "4 is divisible by 2," "5 is not divisible by 2," and "since 5 is prime, it is only divisible by 1 and 5." However, someone might ask, "Why isn’t 5 divisible by 2? After all, 5/2 = 2.5." Even such an obvious and familiar concept as "divisibility" requires a precise definition!

Definition. *Let a be a non-zero itneger and b be an integer. We say ”a divides b” if there exists an integer x such that $b = ax$. (This is denoted as $a \mid b$.)*

From this definition, we derive the following facts:

- 3 divides 6 because there exists an integer x such that $6 = 3x$ (in this case, $x = 2$).
- 3 does not divide 5 because there is no integer x such that $5 = 3x$.

- 3 divides 0 because there exists an integer x such that $0 = 3x$ (in this case, $x = 0$).
- 3 divides -3 because there exists an integer x such that $-3 = 3x$ (in this case, $x = -1$).

As a side note, any integer x that is divisible by 2 (i.e., $2 \mid x$) is called an even number. This definition includes -2 and 0 as even numbers.

In science, important verified facts are called laws. In mathematics, they are called theorems. The difference lies in the methodology: science verifies laws through experiments and observations, whereas mathematics proves theorems using definitions and logic. Great theorems do not appear out of thin air. Just as magnificent castles require solid foundations, proving elegant theorems requires small yet essential preliminary facts. These facts are called lemmas. To prove the infinitude of primes, we first need the following lemma.

Lemma. *Let a be a non-zero integer a and b and c be integers. Suppose a divides both b and c. Then a also divides $b - c$.*

Let's build intuition by looking at examples. For instance, 3 divides both 15 and 21, since there exist integers x and y such that $15 = 3x$ and $21 = 3y$ (specifically, $x = 5$ and $y = 7$). The difference $15 - 21$ is -6, and indeed, there exists an integer z such that $-6 = 3z$ (in this case, $z = -2$). Our intuition suggests that this lemma should be true. However, in the rigorous world of mathematics, examples merely illustrate special cases. To establish this property for all integers, we must prove it.

Proof. Since a divides both b and c, by definition, there exist integers x and y such that $b = ax$ and $c = ay$. Thus, $b - c = ax - ay = a(x - y)$.

Since x and y are integers and integers are closed under subtraction, $x - y$ is also an integer. Hence, there exists an integer z such that $b - c = az$, where $z = x - y$. Therefore, a divides $b - c$. □

Thus, the proof is complete.[2]

Now, we are ready to prove that there are infinitely many prime numbers. We will use proof by contradiction, so we begin by assuming the opposite of our claim.

Proof. Suppose there are only finitely many primes. Then, there must be a largest prime, denoted by P. Define M as the product of all prime numbers: $M = 2 \times 3 \times 5 \times \cdots \times P$. That is, M is divisible by all primes.

Consider the number $M + 1$. By the fundamental theorem of arithmetic, $M + 1$ must be either prime or composite.

If $M + 1$ is prime, then it is greater than P, contradicting the assumption that P is the largest prime.

If $M + 1$ is composite, then it has some prime divisor Q. Since P is the largest prime, Q must be one of $2, 3, 5, \ldots, P$.

Since Q divides M (by definition of M), and Q also divides $M + 1$, our lemma implies that Q must divide $(M + 1) - M = 1$. However, no prime number divides 1! This contradiction proves that our assumption was false. Therefore, there must be infinitely many prime numbers. □

Let's take a closer look at the core of this proof using a familiar example.

Suppose that the only prime numbers in the world are 2 and 3. Then, $M + 1$ would be 7. Since 7 is a prime number greater than 3, our assumption leads to a contradiction.

If we assume that the only prime numbers are 2, 3, and 5, then $M + 1$ would be 31. Since 31 is a prime number greater than 5, this also results in a contradiction.

If we assume that the only prime numbers are 2, 3, 5, and 7, or even 2, 3, 5, 7, and 11, then $M + 1$ becomes 211 and 2311, respectively—both of which are prime numbers. Since they are greater than 7 and 11, respectively, we again reach a contradiction. A hasty reader might mistakenly conclude, "Oh, $M + 1$ is always a prime number!"[3]

Now, suppose that the only prime numbers are 2, 3, 5, 7, 11, and 13. Then, $M + 1$ would be 30,031, which is a composite number. However, none of 2, 3, 5, 7, 11, or 13 divides 30,031. The prime factorization of 30,031 is 59×509, and both of these numbers are prime numbers greater than 13. Thus, we once again arrive at a contradiction. This means that even if $M + 1$ is a composite number, its prime factors must be greater than the "largest prime" we initially assumed.

This proof is an ancient one, appearing in Elements by Euclid around 300 BCE.[4] While mathematics has since provided various proofs of the infinitude of prime numbers, none is as elegant and simple as this one. One might even say that it is the most outstanding proof, and that there will never be a more remarkable one.

By my standards, the next most beautiful proof is Euler's. Euler showed that the sum of the reciprocals of prime numbers diverges to infinity. In other words, he demonstrated the following[5]:

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\cdots=\infty.$$

Each term in this sum—$1/2, 1/3, 1/5$ and so on—is less than 1. If there were only a finite number of primes, then adding up finitely many values, each less than 1, could never result in infinity. Therefore, there must be infinitely many prime numbers. While this proof may appear more concise than Euclid's, it requires first proving that the sum of the reciprocals of primes diverges to infinity.[6]

---

1. Exercise: Under which operations (addition, subtraction, multiplication, division) are natural numbers closed?↩
2. In mathematical etiquette, it is customary to signal the end of a proof. Historically, the phrase Q.E.D. (Quod Erat Demonstrandum), meaning "that which was to be demonstrated," was used. Nowadays, most proofs conclude with either a black square (■) or an empty square (□) instead.↩
3. Some proofs commonly found on the internet conclude with "Since $M+1$ is always a prime number, this leads to a contradiction," but this is an incorrect argument.↩
4. Elements of Euclid, Book 9, Proposition 20.↩
5. Strictly speaking, Euler did not prove this. The concepts of convergence and divergence were not formally established until about 100 years after Euler's time. Euler provided reasons why the sum of the reciprocals of prime numbers must be infinite, but a rigorous proof was completed by Mertens in 1874.↩
6. To fully understand Euler's explanation, one needs at least elementary number theory. To comprehend Mertens' proof, knowledge of analytic number theory is required. While the proof itself is short, proving the necessary preliminary theorems requires a deep mathematical understanding.↩