How many primes are there?

Fermat's Christmas Theorem series

2025-12-08

ENG ITA

Introduction

In the previous post we asked some questions about prime numbers such as:

- Which numbers could be written as the product of primes?
- How many primes are there?

The goal of this post is to give a precise answer to these two questions.

The first person to rigorously answer these questions was the Greek mathematician Euclid, and we will roughly follow his reasoning.

What a prime is?

Let's start with a short recap. In school we learned that a positive integer is prime if its only divisors are 1 and itself (1 is not considered prime). So we have that $2, 3, 5, \ldots$ are the first few primes.

Consider the prime 2. Note that every time 2 divides a product of two integers $a \cdot b$, it divides one of the two factors (i.e. either 2 divides a or 2 divides b). Try a few examples to convince yourself. For instance, 2 divides the product $4 \cdot 5 = 20$ and indeed 2 divides 4. You can try any product and the property will hold. There is nothing special about 2; indeed, every prime number satisfies this (i.e. if a prime number p divides a product $a \cdot b$ then either p divides a or p divides b). Note that this property characterises primes. For example, observe that 6 (which isn't prime) divides the product $3 \cdot 4 = 12$, but 6 divides neither 3 nor 4.

Since this property is important, we define prime numbers as follows:

Definition: An integer p is *prime* if whenever p divides a product $a \cdot b$, then p divides a or p divides b.

We will instead use the term *irreducible* for the other definition we know:

Definition: An integer q is *irreducible* if its only divisors are itself, 1, -1, and $-q$.

We include -1 and $-q$ because we allow negative integers; for instance -3 is irreducible since its only divisors are -1, 1, -3, and 3.

For integers, a number is irreducible if and only if it is prime, so the two definitions agree. This is why we often use the irreducible definition for primes.

Back to school: the Euclidean division

We know how division of integers works. For example, to divide 7 by 2 we count how many times 2 can be added without exceeding 7. We see that $2 + 2 + 2 = 6$, so the quotient is 3 and the remainder is 1. We write in symbols

$$7 = 2 \cdot 3 + 1$$

Another example: dividing 17 by 15 yields quotient 1 and remainder 2, i.e.

$$17 = 15 \cdot 1 + 2$$

As a final example, suppose we want to divide 3 by 12. Since 12 is too big, the quotient is 0 and the remainder is 3, i.e.

$$3 = 12 \cdot 0 + 3$$

We learned that we can always perform division with remainder: for positive integers n, m we can write

$$n = m \cdot q + r$$

where q is the quotient and r is the remainder. We are ready to state this as a theorem:

Theorem 0.1 (Euclidean division.)**.** *For every two integers $n \geq 0$ and $m > 0$ (we cannot divide by 0), there exist integers $q, r \geq 0$ such that*

$$n = m \cdot q + r$$

where $r < m$. Moreover q and r are uniquely determined.

Okay, pause for a moment: this theorem seems more complicated than it should be. First, it should be clear that we can write our n as

$$n = m \cdot q + r$$

for some q and r. Why must r be strictly less than m? Because if it were not, we could divide further. For example suppose we write

$$15 = 4 \cdot 2 + 6$$

This is not admissible, since $6 = 4 + 2$; we can still divide by 4 to get

$$15 = 4 \cdot 3 + 2$$

Now, since 2 is smaller than 4, we cannot divide it again, so we are done and what we get is the division.

The other question is: what does it mean that q and r are uniquely determined? It means there is only one way to write n as $m \cdot q + r$, with $r < m$. Take a pen and paper and try to convince yourself that this writing is unique by doing some example.

The fundamental theorem of arithmetic

Now we want to answer the question of which numbers could be written as a product of primes. The following theorem gives us the answer.

Theorem 0.1 (Fundamental theorem of arithmetic.)**.** *Every integer n strictly bigger than one (i.e. $n > 1$) can be written* uniquely *as the product of prime numbers.*

This helps us understand why primes are so important. In this sense they are the basic building blocks of the integers. We can always decompose an integer as the product of primes and this is done uniquely.

Let's give some examples to clarify the theorem. Consider 15. Its prime divisors are 3 and 5 so $15 = 3 \cdot 5$. Another example could be 4; it is divided only by 2, so $4 = 2^2$.

How do we factor a number in practice? Pick an integer, for example 36. We look at the first few primes

$$2, 3, 5, 7, 11, ...$$

and test the divisibility by successive primes:

- Is 36 divisible by 2? Yes: $36 = 2 \cdot 18$.
- Is 18 divisible by 2? Yes: $18 = 2 \cdot 9$.
- Is 9 divisible by 2? No: we move on to the next prime.
- Is 9 divisible by 3? Yes: $9 = 3 \cdot 3$.

So we get

$$36 = 2 \cdot 18 = 2 \cdot (2 \cdot 9) = 2 \cdot (2 \cdot (3 \cdot 3)) = 2^2 \cdot 3^2$$

By this process we can factor any positive integer. For negative integers, include a leading minus sign; e.g. $-36 = -(2^2 \cdot 3^2)$.

Now consider 7. Since it is prime, it can't be factorized further. Therefore, we will say that its factorization is just itself, i.e. given by

$$7 = 7$$

where on the right hand side we are writing the factors (just 7) of the factorization.

We want to convince ourselves that a factorization always exists, so we dive into its proof.

Existence of the prime factorization. Suppose some positive integers could not be factorized. Take the smallest such integer and call it m. The integer m cannot be a prime number, since if it were its factorization would be $m = m$ (as we did in the case of 7). Since m is not prime, there must be some number s other than m and 1 which divides it. We can therefore write $m = s \cdot t$ for some other integer t. But now observe that s and t are both smaller than m. Since m was the smallest such number that could not be factorized, both s and t can be factorized into prime factors. In particular we get that

$$m = s \cdot t = (\text{prime factorization of } s) \cdot (\text{prime factorization of } t)$$

This yields a factorization of m. For example, $144 = 4 \cdot 36$; factoring gives $4 = 2^2$ and $36 = 2^2 \cdot 3^2$, hence

$$144 = 4 \cdot 36 = (2^2) \cdot (2^2 \cdot 3^2) = 2^4 \cdot 3^2$$

Therefore, we proved that the smallest number which couldn't be factorized can actually be factorized. Hence, we get the claim. □

Moreover, the theorem tells us that the factorization is unique: you can't write an integer (> 1) as a product of primes in two different ways. Try some examples to convince yourself.

How many primes are there?

Finally, we are ready to answer this question. You may have guessed the answer, but I really want to give a neat argument that will convince you it is true.

Theorem 0.1. *There exist infinitely many prime numbers.*

Euclid's proof. Suppose there were only finitely many prime numbers, call them $p_1, \dots, p_n$. Define m as the product of all these primes plus 1, i.e.

$$m = p_1 \cdot p_2 \cdots p_n + 1$$

Observe that m is not divisible by any of the primes $p_1, \dots, p_n$. To convince ourselves, take p_1 and write

$$m = p_1 \cdot (p_2 \cdots p_n) + 1$$

Define $q := (p_2 \cdots p_n)$. We are saying

$$m = p_1 \cdot (p_2 \cdots p_n) + 1 = p_1 \cdot q + 1$$

Thus, m has remainder 1 when divided by p_1, so p_1 does not divide m (if it did the remainder would be 0). Nothing is special about p_1: we can repeat the same argument for all the other primes $p_2, \dots, p_n$.

So we are convinced that no prime in the list $p_1, \dots, p_n$ divides m.

But we said (Theorem 0.1) that any integer number can be written as the product of primes. However, since m is not divisible by any prime in the list $p_1, \dots, p_n$, it means that the list does not contain all of the primes.

Hence, whenever we suppose a finite list $p_1, \dots, p_n$ contains all primes, we can construct a prime not in the list; thus any finite list is incomplete.

We conclude that there must be infinitely many primes. □

Conclusion

To prove there are *infinitely many* primes we used a common strategy. We understood that proving the statement as it appears is very difficult. How can you prove there are infinitely many primes? The natural idea is: suppose there were only finitely many, and derive a contradiction. This is what we call a *proof by contradiction* (you prove your claim by proving that its negation is false).

There is another cool idea we used today. When we proved Theorem 0.1 we had the idea of supposing that there were some numbers not satisfying our statement. Then we took the minimum among these numbers and proved that the minimum actually satisfied our claim. This kind of argument is often called *proof by minimal counterexample* (a form of induction), and it is also common.

Think about these two kinds of proofs and how we used them in the arguments. If you'd like to practice, try proving uniqueness of prime factorization (proceed by contradiction and use the two definitions of prime introduced above).

In any case, see you next week!

This article is part of the series *Fermat's Christmas Theorem*.

Previous: Introduction to Fermat's Christmas Theorem

Next: Some basic modular arithmetic