# Euclid's proof of the Infinitude of Primes

A prime number (or prime, for short) is a natural number greater than 1 that has no positive divisors other than itself and 1. After this definition we want to start with the theorem that gives this chapter its name:

**Theorem 1 (Euclid).** ***There are infinitely many primes.***

*Proof.* (modern modification of Euclid's proof,
taken from [Oswald, Steuding, 2015]):
Let $p_1 = 2, p_2, ..., p_n$ be a set of primes[1]. Now we define a natural number $q$ by $q := p_1 \cdot p_2 \cdot ... \cdot p_n + 1$. This number $q$ is larger than 1 and with the Fundamental theorem of arithmetic[2] it follows that $q$ has a prime factor $p$, i.e. $p$ divides $q$. It could happen that $p = q$ but that is not relevant here. If $p$ would now be among the prime numbers $p_1, p_2, ..., p_n$ then it would follow that $p$ divides the product of these primes and therefore it would divide $q - 1$ because $p_1 \cdot p_2 \cdot ... \cdot p_n = q - 1$. So, $p$ would divide $q$ and $q - 1$, and thus it would have to divide 1 since it would also divide the linear combination of $q$ and $q - 1$, i.e. $q - (q - 1) = 1$, a contradiction because we assumed p to be prime (so it cannot be 1, check the definition). Because of that $p$ is not contained in our given set $p_1, p_2, ..., p_n$, and with that we have found an 'additional' prime. That's why the set of all primes is infinite. □

In fact, there are innumerably many proofs of this theorem, and still nowadays people find different proofs. For example, another proof deals with the infinitude of Fermat numbers (see [Oswald, Steuding, 2015, p. 89f.]).
If we go back in time, we will notice that this theorem, which is named after him, was not what Euclid originally stated nor what he actually proved.
Euclid was a Greek mathematician who lived around the third century. He wrote his famous *Elements*, a series of textbooks that were still used throughout medieval times and even for a long time after that. In book IX, in his proposition 20 he claimed:

**Theorem 2 (Original statement of Euclid).** ***"Prime numbers are more than any assigned multitude of prime numbers"*** *([Dawson, 2015, p. 51]).*

[1] $p_1 = 2$ is needed. Otherwise it could happen that we argue over an empty set of primes.

[2] **Fundamental theorem of arithmetic**: *every integer greater than 1 either is prime itself or is the product of prime numbers. This product is unique, up to the order of the factors.*

Here, one can already see the small difference from our modern statement of the theorem: Euclid did not state that there are infinitely many primes but that if he had an arbitrary set of primes, then he could always find another prime that was not already contained in the given set (for this argument, see also the proof of Theorem 1). In ancient and medieval times, people were not sure about the concept of infinitude and mistrusted it. That is why Euclid's original statement did not really concern the infinity aspect.
Next, we want to have a closer look at the original proof given by Euclid. The following is an English translation of Euclid's *Elements* that can be found in [Dawson, 2015] on page 51:

*Proof.* Let A, B, C be the assigned prime numbers. I say that there are more prime numbers than A, B, C. For let the least number measured by them be taken and let it be [represented by the line segment] DE, [then] let the unit [segment] DF be added to DE. Then EF is either prime or not. First, let it be prime. Then A, B, C, EF have been found which are more than A, B, C. Next, let EF not be prime; therefore [by proposition VII,31][3] it is measured by some prime number. Let it be measured by the prime number G. I say that G is not the same as any of the numbers A, B, C. For, if possible, let it be so. Now A, B, C measure DE; therefore, G will also measure DE. But it also measures EF. Therefore G, being a number, will measure the remainder, the unit DF, which is absurd. Therefore G is not the same as any of the numbers A, B, C. And by hypothesis it is prime. Therefore the prime numbers A, B, C, G have been found, which are more than the assigned multitude of A, B, C. □

The following picture helps to illustrate the proof:

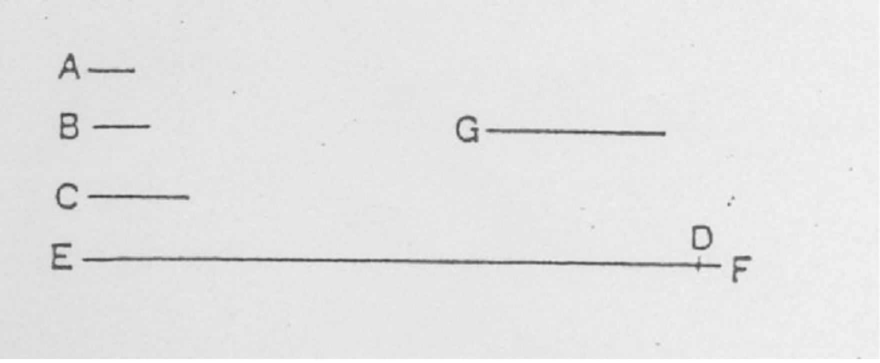

Figure 1: Illustration of Euclid's original proof, [Siegmund-Schultze, 2014, p. 90].

[3] This is a theorem from the 7th book of the *Elements* and it states that: ”Any product of numbers (none of them the unit) is divisible by a prime number”, cf. [Siegmund-Schultze, 2014, p. 90].

Surely, there are some differences from our modern proof. Euclid did not start with an arbitrary set of primes but with only three primes (i.e. A, B and C). This was usually done in Ancient Greek times, and such methods can also be found in the works of many mathematicians who came later, see for example the chapter *Pascal's Triangle*. Nevertheless, "it is clear from the statement of the proposition that that is merely by way of example, and it does not affect the validity of the argument", cf. [Dawson, 2015, p. 51]. In addition, the geometrical approach of Euclid, with the line segments, is also typical for Ancient Greece and maybe a bit strange to our modern approach.
However, the overall strategy for tackling the claim is the same as in our modern proof. Furthermore, the proof is very beautiful as it is very simple and constructive. It gives a method of finding a new prime different from a given set of primes. Hence, if one takes a closer look at Euclid's original proof, one finds that it "is **not indirect**[4], as is often claimed", cf. [Dawson, 2015, p. 52].

# References

[Dawson, 2015] John W. Dawson, Jr., Why Prove it Again? Alternative Proofs in Mathematical Practice, Springer International Publishing, Switzerland 2015

[Oswald, Steuding, 2015] Nicola Oswald, Jörn Steuding, Elementare Zahlentheorie. Ein sanfter Einstieg in die höhere Mathematik, Springer-Verlag, Berlin Heidelberg, 2015

[Siegmund-Schultze, 2014] Reinhard Siegmund-Schultze, Euclids proof of the infinitude of primes: distorted, clarified, made obsolete, and confirmed in Modern Mathematics, The Mathematical Intelligencer, December 2014, Volume 36, Issue 4, pp 8797

[4] In the proof, Euclid does **not** assume that the set A, B, C is the set of all possible primes and then gets a contradiction. "At one point Euclid assumes, by reductio, that G is equal to one of A, B, or C. But that reductio can easily be eliminated" [Dawson, 2015, p. 52].