Euler's totient function and another way to state that there are infinitely many primes

Euro Vidal Sampaio

March 06 2025

1 Introduction

One of the first mathematical proofs that are introduced to students at school, is one that is attributed to Euclid of Alexandria, a mathematician from Ancient Greece. This is the proof that there are more primes than any finite list of primes can provide. Indeed, considering any such finite list, denote the product of their elements by P. Then we notice that $P+1$ must have some prime divisor, and any such prime cannot be in the original list, or else, it divides the difference $(P+1)-P=1$, which is absurd because all primes exceed one. End of proof. More than 2 thousand years later, we now know stronger results. The progress has been impressive, but lets take a step back and ask ourselves the following: what is a result that is *equivalent* to Euclid's theorem? By this, we mean some proposition, which is a consequence to Euclid's theorem and, conversely, implies Euclid's theorem as a consequence. We want to briefly review some of these stronger results, and then show such an equivalent proposition using what is called Euler's totient function. We will use only elementary tools along the way, including the Pigeonhole principle.

2 What implies Euclid's Theorem?

Christian Elsholtz has shown that Euclid's Theorem is a consequence of Ramsey's Theorem, which deals with sets of vertices and edges called complete graphs, and, given some colouring of the edges of this graph with a finite number of colours, states that some monochromatic structures must appear when the graph is large enough. However, it does not appear to be the case that Euclid's Theorem implies Ramsey's Theorem, meaning that Ramsey's Theorem would be a strictly stronger result.

3 The totient function

The Euler totient function is the map $\varphi : N \to N$, which maps each positive integer n to the cardinality of the following set:

$[k \in \mathrm{N}: 1 \leq k \leq n, mdc(k,n) = 1]$

In other words, the totient of a number counts how many positive integers up to this number are coprime with it. This function is named after Leonhard Euler. But what does this function have to help us relate it to the infinitude of primes? The main ingredient is a product formula for this function, proved by Euler:

$\varphi(n)/n = \prod_{p|n} (1 - 1/p)$,

where the letter p indicates a prime number, so that the product is calculated over all the prime divisors of n. The total number of factors in this product is the number of distinct prime divisors of n.

Do you understand why this formula is true? If you are scratching your head, here is a hint: lets think about what this formula means in terms of probability. The left hand side of this formula gives the probability that, upon randomly choosing some number from the sequence $1, ..., n$, the selected number is coprime with n. Now, the right hand side calculates this probability by considering each prime divisor of n separately. Indeed, for each prime divisor p of n, the event that some randomly picked number is not divisible by this prime, has probability $(p-1)/p = 1-1/p$ because there are p possible remainders upon division by p, and one remainder, namely 0 , has to be avoided. Then, some number is coprime to n if and only if it is not divisible by any the prime factors of n. Now, given that any two different primes are coprime, these events are independent. This means we can calculate the total probability by multiplying all these probabilities $1 - 1/p$, and the result is precisely the right hand side of this formula. We are done for now. In the next section, we use Euler's function and its product formula in order to finally prove a result which is equivalent to the infinitude of primes.

4 The boundless multiplicity of the totient function

We are ready to enunciate the proposition that is logically equivalent to the infinitude of primes.

Proposition) For any positive integer s, there exist $s + 1$ distinct positive integers $x_1, x_2, ...x_{s+1}$, such that they all share the same totient:

$\varphi(x_1) = \varphi(x_2) = ... = \varphi(x_{s+1})$

Proof) Lets now convince ourselves as to why this proposition is logically equivalent to Euclid's theorem. The easier thing to verify, as it turns out, is that this proposition implies Euclid's Theorem. Indeed, assume that it holds, and furthermore assume that there exist only k prime numbers, where k is a natural number. As we know from elementary arithmetic, for each natural number, there exists a finite (possibly empty) subset of the primes which consists of all primes that divide exactly such number. Then, since we only have k primes at our disposal, there exist only 2^k subsets of primes available. Now, according

to our proposition, we can choose the number s to be as large as we wish. We choose $s = 2^k$:

$\varphi(x_1) = \varphi(x_2) = ... = \varphi(x_{s+1})$.

And now note that we have $2^k + 1$ positive integers among the x's, and only 2^k associated sets of prime divisors. Thus, by the Pigeonhole principle, we know that two of these x's must have the same set of prime divisors. Say these two are x_i and x_j. Now remember that in the previous section we stated the product formula for Euler's function, which shows that the ratio $\varphi(n)/n$ depends only on the set of prime divisors of n, and since we know that x_i and x_j have the same set of prime divisors, we know that

$\varphi(x_i)/x_i = \varphi(x_j)/x_j$ and that $\varphi(x_i) = \varphi(x_j)$.

Together, these two equations imply that $x_i = x_j$, which is absurd since we assume that the x's are all distinct. Thus we see that this proposition implies Euclid's theorem.

Now, for the converse, assume Euclid's theorem, and let us show that the proposition holds true as a consequence. This proof is due to Andrzej Schinzel, and we reproduce it here. First, put $x_{s+1} = p_1 p_2 ... p_s$, where p_i denotes the i-th prime. Note that this only makes sense because of Euclid's theorem, else we could not talk about, say, the 1001th prime if there were only 1000 primes. As for the other x's, we define, for each i from one to s, the value of x_i as:

$x_i = p_1 p_2 ... p_{i-1}(p_i - 1)p_{i+1} ... p_s$

We then compute $\varphi(x_i)$, using the product formula for the totient function:

$\varphi(x_i) = \varphi(p_1 p_2 ... p_{i-1}(p_i - 1)).\varphi(p_{i+1} ... p_s) =$
$= (p_i - 1).\varphi(p_1 p_2 ... p_{i-1})..\varphi(p_{i+1} ... p_s) =$
$= \varphi(p_i).\varphi(p_1 p_2 ... p_{i-1})..\varphi(p_{i+1} ... p_s) =$
$= \varphi(x_{s+1})$

We easily verify that $x_1 < x_2 < ... < x_{s+1}$, and therefore all the x's defined in this way are distinct, yet they all share the same value for Euler's totient function. Since s can be any positive integer we please, the proof is complete. We have checked that the proposition and Euclid's theorem imply each other, meaning they are essentially equivalent.

5 Conclusion

Along the way of pursuing our goal of obtaining some number-theoretic result equivalent to Euclid's theorem, we stumbled upon Euler's totient function, and verified that such a proposition does indeed exists, and it can enunciated in terms of the multiplicity of the totient function, namely asserting that such a multiplicity can be arbitrarily large. We briefly saw that Euclid's theorem is a consequence of Ramsey's theorem, but ultimately we had to stick to number-theoretic results in order to prove the equivalence of two propositions. Just as Euclid's theorem is a result in elementary number theory, so too were the arguments we used along the way, namely the product formula for the totient function and the Pigeonhole principle. Near the end, we reproduced a proof from Andrej Schinzel, which shows that Euclid's theorem implies the boundless multiplicity of the totient function. Our contribution here consisted in supplying a proof of the converse. We hope that the reader felt motivated to think about the interesting logical relations between results in number theory, and in mathematics in general, and realized that certain propositions, despite being written differently from one another, may turn out to be equivalent!