There are infinitely many prime numbers

Mathematics Explained and Clarified

Definition 1. A *prime number* is a natural number greater than 1 that is divisible only by 1 and by itself, and does not have any other divisors.

Lemma 1. *Any natural number has a prime divisor.*

Remark 1. Lemma 1 immediately follows from the fundamental theorem of arithmetic, which states that any natural number can be expressed as a product of prime numbers, and that this expression is unique up to the order of the prime divisors. However, we need here only the weaker statement of Lemma 1.

Remark 2. Lemma 1 is more or less obvious. The rough idea of the proof is to divide the number while we can, and when we can no longer divide it further, that would be the required prime divisor of the original number. The proof below is a more detailed formalization of that idea. In my view, it is a technicality, and I actually encourage readers to skip it.

Proof of Lemma 1. Take a natural number, and denote it by n. If it is prime, then it is itself its own prime divisor. Otherwise, it is not prime, and hence has a divisor d_1 other than 1 and itself. By repeating the same argument with this number d_1, we conclude that it is either prime, or it has a divisor d_2 other than 1 and itself. And so on. By repeating the same argument with the number d_k, we conclude that it is either prime, or it has a divisor d_{k+1} other than 1 and itself.

Notice that divisibility is a transitive relationship. This implies that on each step, the number d_{k+1} is not only a divisor of the immediately preceding number d_k, but also of all previous numbers in the sequence $d_1, \ldots, d_k$, and also of the original number n.

Also notice that the sequence $d_1, d_2, d_3, \ldots$ is strictly decreasing: $d_1 > d_2 > \ldots > d_k > \ldots$. Therefore, this process can not continue forever, and it will finish after a finite number of steps. That is, there exists f such that d_f is prime. And d_f is the required prime divisor of the original number n. □

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

Proof. Suppose that the statement is not true, and there is a finite number of prime numbers, and enumerate all of them as $p_1, \ldots, p_n$.

Consider the number $q = p_1 \cdot \ldots \cdot p_n + 1$. Notice that q has the remainder 1 when divided by p_i for any i. In particular, q is not divisible by any of $p_1, \ldots, p_n$. That is, it is not divisible by any of the prime numbers.

On the other hand, by Lemma 1, q must have a prime divisor. A contradiction. □