There are infinitely many prime numbers

Mathematics Explained and Clarified

The definition and the main theorem statement

Definition

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.

The definition and the main theorem statement

Definition

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.

Theorem

There are infinitely many prime numbers.

The lemma about the existence of a prime divisor

Lemma

Any natural number has a prime divisor.

The lemma about the existence of a prime divisor

Lemma

Any natural number has a prime divisor.

Remark

The lemma 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 the lemma.

The lemma about the existence of a prime divisor

Lemma

Any natural number has a prime divisor.

Remark

The lemma 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 viewers to skip it.

The proof of the lemma

Lemma

Any natural number has a prime divisor.

The proof of the lemma

Lemma

Any natural number has a prime divisor.

Take n.

The proof of the lemma

Lemma

Any natural number has a prime divisor.

Take n. 2 cases:

- n is prime.
- n is not prime.

The proof of the lemma

Lemma

Any natural number has a prime divisor.

Take n. 2 cases:

- n is prime. $\implies$ n is itself its own prime divisor.
- n is not prime.

The proof of the lemma

Lemma

Any natural number has a prime divisor.

Take n. 2 cases:

- n is prime. $\implies$ n is itself its own prime divisor.
- n is not prime. $\implies$ n has a divisor d_1, $d_1 \neq 1$, $d_1 \neq n$.

The proof of the lemma

Lemma

Any natural number has a prime divisor.

Take n. 2 cases:

- n is prime. $\implies$ n is itself its own prime divisor.
- n is not prime. $\implies$ n has a divisor d_1, $d_1 \neq 1$, $d_1 \neq n$.

Repeat the same argument with d_1

The proof of the lemma

Lemma

Any natural number has a prime divisor.

Take n. 2 cases:

- n is prime. $\implies$ n is itself its own prime divisor.
- n is not prime. $\implies$ n has a divisor d_1, $d_1 \neq 1$, $d_1 \neq n$.

Repeat the same argument with d_1: either d_1 prime, or it has a divisor d_2, $d_2 \neq 1$, $d_2 \neq d_1$.

The proof of the lemma

Lemma

Any natural number has a prime divisor.

Take n. 2 cases:

- n is prime. $\implies$ n is itself its own prime divisor.
- n is not prime. $\implies$ n has a divisor d_1, $d_1 \neq 1$, $d_1 \neq n$.

Repeat the same argument with d_1: either d_1 prime, or it has a divisor d_2, $d_2 \neq 1$, $d_2 \neq d_1$.
And so on.

The proof of the lemma

Lemma

Any natural number has a prime divisor.

Take n. 2 cases:

- n is prime. $\implies$ n is itself its own prime divisor.
- n is not prime. $\implies$ n has a divisor d_1, $d_1 \neq 1$, $d_1 \neq n$.

Repeat the same argument with d_1: either d_1 prime, or it has a divisor d_2, $d_2 \neq 1$, $d_2 \neq d_1$.
And so on.
Repeat the same argument with d_k

The proof of the lemma

Lemma

Any natural number has a prime divisor.

Take n. 2 cases:

- n is prime. $\implies$ n is itself its own prime divisor.
- n is not prime. $\implies$ n has a divisor d_1, $d_1 \neq 1$, $d_1 \neq n$.

Repeat the same argument with d_1: either d_1 prime, or it has a divisor d_2, $d_2 \neq 1$, $d_2 \neq d_1$.
And so on.
Repeat the same argument with d_k: either d_k prime, or it has a divisor d_{k+1}, $d_{k+1} \neq 1$, $d_{k+1} \neq d_k$.

The proof of the lemma

Lemma

Any natural number has a prime divisor.

Take n. 2 cases:

- n is prime. $\implies$ n is itself its own prime divisor.
- n is not prime. $\implies$ n has a divisor d_1, $d_1 \neq 1$, $d_1 \neq n$.

Repeat the same argument with d_1: either d_1 prime, or it has a divisor d_2, $d_2 \neq 1$, $d_2 \neq d_1$.
And so on.
Repeat the same argument with d_k: either d_k prime, or it has a divisor d_{k+1}, $d_{k+1} \neq 1$, $d_{k+1} \neq d_k$.
Divisibility is a transitive relationship

The proof of the lemma

Lemma

Any natural number has a prime divisor.

Take n. 2 cases:

- n is prime. $\implies$ n is itself its own prime divisor.
- n is not prime. $\implies$ n has a divisor d_1, $d_1 \neq 1$, $d_1 \neq n$.

Repeat the same argument with d_1: either d_1 prime, or it has a divisor d_2, $d_2 \neq 1$, $d_2 \neq d_1$.
And so on.
Repeat the same argument with d_k: either d_k prime, or it has a divisor d_{k+1}, $d_{k+1} \neq 1$, $d_{k+1} \neq d_k$.
Divisibility is a transitive relationship $\implies$ on each step, d_{k+1} is not only a divisor of d_k, but also a divisor of all $d_1, \ldots, d_k$, and of n.

The proof of the lemma

$$d_1 > d_2 > \ldots > d_k > \ldots$$

The proof of the lemma

$d_1 > d_2 > \ldots > d_k > \ldots \implies$ the process will finish after a finite number of steps.

The proof of the lemma

$d_1 > d_2 > \ldots > d_k > \ldots \implies$ the process will finish after a finite number of steps. $\implies$ there exists f such that d_f is prime.

The proof of the lemma

$d_1 > d_2 > \ldots > d_k > \ldots \implies$ the process will finish after a finite number of steps. $\implies$ there exists f such that d_f is prime. $\implies$ d_f is the required prime divisor of n.

The proof of the main theorem

Theorem

There are infinitely many prime numbers.

The proof of the main theorem

Theorem

There are infinitely many prime numbers.

Suppose not true.

The proof of the main theorem

Theorem

There are infinitely many prime numbers.

Suppose not true. $\implies$ There is a finite number of prime numbers

The proof of the main theorem

Theorem

There are infinitely many prime numbers.

Suppose not true. $\Longrightarrow$ There is a finite number of prime numbers: $p_1, \ldots, p_n$.

The proof of the main theorem

Theorem

There are infinitely many prime numbers.

Suppose not true. $\implies$ There is a finite number of prime numbers: $p_1, \ldots, p_n$.
Consider $q = p_1 \cdot \ldots \cdot p_n + 1$.

The proof of the main theorem

Theorem

There are infinitely many prime numbers.

Suppose not true. $\implies$ There is a finite number of prime numbers: $p_1, \ldots, p_n$.
Consider $q = p_1 \cdot \ldots \cdot p_n + 1$.
q has the remainder 1 when divided by p_i $\forall i$.

The proof of the main theorem

Theorem

There are infinitely many prime numbers.

Suppose not true. $\Longrightarrow$ There is a finite number of prime numbers: $p_1, \ldots, p_n$.
Consider $q = p_1 \cdot \ldots \cdot p_n + 1$.
q has the remainder 1 when divided by p_i $\forall i$. $\Longrightarrow$ q is not divisible by any of $p_1, \ldots, p_n$.

The proof of the main theorem

Theorem

There are infinitely many prime numbers.

Suppose not true. $\Longrightarrow$ There is a finite number of prime numbers: $p_1, \ldots, p_n$.
Consider $q = p_1 \cdot \ldots \cdot p_n + 1$.
q has the remainder 1 when divided by p_i $\forall i$. $\Longrightarrow$ q is not divisible by any of $p_1, \ldots, p_n$. $\Longrightarrow$ q is not divisible by any of the prime numbers.

The proof of the main theorem

Theorem

There are infinitely many prime numbers.

Suppose not true. $\implies$ There is a finite number of prime numbers: $p_1, \ldots, p_n$.
Consider $q = p_1 \cdot \ldots \cdot p_n + 1$.
q has the remainder 1 when divided by p_i $\forall i$. $\implies$ q is not divisible by any of $p_1, \ldots, p_n$. $\implies$ q is not divisible by any of the prime numbers.
But by the lemma, q must have a prime divisor.

The proof of the main theorem

Theorem

There are infinitely many prime numbers.

Suppose not true. $\implies$ There is a finite number of prime numbers: $p_1, \ldots, p_n$.
Consider $q = p_1 \cdot \ldots \cdot p_n + 1$.
q has the remainder 1 when divided by p_i $\forall i$. $\implies$ q is not divisible by any of $p_1, \ldots, p_n$. $\implies$ q is not divisible by any of the prime numbers.
But by the lemma, q must have a prime divisor. A contradiction.