The Fundamental Theorem of Arithmetic

0xHaru

April 11, 2026

Remark 1. 1 is not a prime number.

Lemma 1 (Euclid's Lemma)**.** *If a prime p divides the product $a \cdot b$ of two integers a and b, then p must divide at least one of those integers a or b.*

Theorem 1 (Fundamental Theorem of Arithmetic)**.** *Every natural number greater than 1 is either a prime number or can be expressed as a product of prime numbers. This representation is unique, except for the order in which the factors appear.*

Proof of Existence. We proceed by induction on n.

Base case ($n = 2$). Since 2 is a prime number, the statement holds.

Induction hypothesis. Assume that every integer between 2 and n is either prime or a product of primes.

Induction step. Let $m = n + 1$. We show that m also satisfies the statement. There are two cases.

1. *m is a prime number.* The statement holds immediately.
2. *Otherwise,* there are integers a and b where $m = a \cdot b$ and $1 < a \leq b < m$. By the induction hypothesis, $a = p_1 \cdot p_2 \cdot \ldots \cdot p_j$ and $b = q_1 \cdot q_2 \cdot \ldots \cdot q_k$ are products of primes. But then
$$m \;=\; a \cdot b \;=\; p_1 \cdot p_2 \cdot \ldots \cdot p_j \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_k$$
is also a product of primes, completing the induction. □

Proof of Uniqueness. Suppose, for the sake of contradiction, that there exists an integer that has two distinct prime factorizations. Let n be the least such integer, and write
$$n \;=\; p_1 \cdot p_2 \cdot \ldots \cdot p_j \;=\; q_1 \cdot q_2 \cdot \ldots \cdot q_k,$$
where each p_i and each q_i is prime.

We see that p_1 divides $q_1 \cdot q_2 \cdot \ldots \cdot q_k$, so p_1 divides some q_i by Euclid's Lemma. Without loss of generality, say p_1 divides q_1. Since p_1 and q_1 are both prime, it follows that $p_1 = q_1$.

Returning to our factorizations of n, we may cancel these two factors to conclude that
$$p_2 \cdot \ldots \cdot p_j \;=\; q_2 \cdot \ldots \cdot q_k.$$
We now have two distinct prime factorizations of some integer strictly smaller than n, which contradicts the minimality of n. □