Theorem: Fundamental Theorem of Arithmetic

Theorem: Fundamental Theorem of Arithmetic

Every natural number greater than 1 can be represented uniquely as a product of Prime Number numbers, up to the order of factors.

Statement

For every natural number $n > 1$, there exist unique prime numbers $p_1 < p_2 < \cdots < p_k$ and positive integers $a_1, a_2, \ldots, a_k$ such that:

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$$

This representation is called the **prime factorization** of n.

Two Parts

The theorem consists of two claims:

1. **Existence**: Every $n > 1$ has at least one prime factorization
2. **Uniqueness**: The prime factorization is unique (up to ordering)

Proof Outline

Existence (by strong induction): - Base case: $n = 2$ is prime, so $n = 2^1$ - Inductive step: If n is prime, we're done. Otherwise, $n = ab$ where $1 < a, b < n$ - By induction hypothesis, both a and b have prime factorizations - Combining these gives a prime factorization of n

Uniqueness (by contradiction): - Suppose n has two different prime factorizations - Using the prime property (if $p \mid ab$, then $p \mid a$ or $p \mid b$) - Show that every prime in one factorization must appear in the other - The exponents must also match

Examples

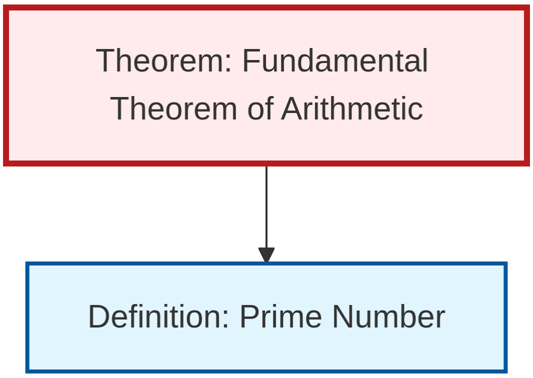
- $12 = 2^2 \cdot 3^1$
- $30 = 2^1 \cdot 3^1 \cdot 5^1$
- $100 = 2^2 \cdot 5^2$
- $17 = 17^1$ (prime numbers have trivial factorization)

Applications

The fundamental theorem enables: - Greatest common divisor (GCD) calculations - Least common multiple (LCM) calculations - Rational number arithmetic - Many results in algebraic number theory

This theorem justifies calling primes the "building blocks" of the natural numbers.

Dependency Graph



Local dependency graph