

Fundamental Theorem of Arithmetic

Fundamental Theorem of Arithmetic:

For all natural numbers $n > 1$, there is a unique **prime factorization** of n . More precisely, there is a unique $k \in \mathbb{N}$, primes $p_1 < p_2 < \dots < p_k$, and natural numbers c_1, \dots, c_k such that $n = \prod_{j=1}^k p_j^{c_j}$.

Examples: $5 = 5^1$, $36 = 2^2 \cdot 3^2$, $80 = 2^4 \cdot 5^1$

Alternate statement:

Letting p_1, p_2, p_3, \dots be the primes in ascending order, for all $n \in \mathbb{N}$, there is a unique sequence c_1, c_2, c_3, \dots such that:

1) $\forall j \in \mathbb{N} (c_j \in \mathbb{N} \cup \{0\})$

2) $n = \prod_{j=1}^{\infty} p_j^{c_j}$

3) Only finitely many c_j are nonzero.

Examples: $5 = 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^0 \dots$

$36 = 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^0 \dots$, $80 = 2^4 \cdot 3^0 \cdot 5^1 \cdot 7^0 \dots$

Fundamental Theorem of Arithmetic

Lemma: For all natural numbers n ,
if $n = \prod_{j=1}^{\infty} p_j^{c_j}$ is the prime factorization of n

then $\text{Div}(n) \cap \mathbb{N} = \left\{ \prod_{j=1}^{\infty} p_j^{a_j} : \forall j \in \mathbb{N}, a_j \in \mathbb{Z} \wedge 0 \leq a_j \leq c_j \right\}$

Example: $12 = 2^2 \cdot 3^1$ so $\text{Div}(12) \cap \mathbb{N} = \{ 2^{a_1} \cdot 3^{a_2} : a_1 \in \{0, 1, 2\} \wedge a_2 \in \{0, 1\} \}$

Proof: $= \{ 1, 2, 4, 3, 6, 12 \}$

If $d = \prod_{j=1}^{\infty} p_j^{a_j}$ where $\forall j \in \mathbb{N} (0 \leq a_j \leq c_j)$ then take

$q = \prod_{j=1}^{\infty} p_j^{b_j}$ where $\forall j \in \mathbb{N} (b_j = c_j - a_j)$. Now $q \cdot d = \prod_{j=1}^{\infty} p_j^{(a_j + b_j)} = \prod_{j=1}^{\infty} p_j^{c_j} = n$

If $d = \prod_{j=1}^{\infty} p_j^{a_j}$ where $\exists j \in \mathbb{N} (a_j > c_j)$, assume $\exists q \in \mathbb{N} (n = q \cdot d)$.

Let $q = \prod_{j=1}^{\infty} p_j^{b_j}$ be the prime factorization of q . $n = q \cdot d = \prod_{j=1}^{\infty} p_j^{(a_j + b_j)}$

Since the prime factorization of n is unique, $\forall j \in \mathbb{N} (c_j = a_j + b_j)$.
This is impossible as $\exists j \in \mathbb{N} (a_j > c_j)$. Since $b_j \geq 0$, $a_j + b_j > c_j$. Contradiction.