

# Proof of the Fundamental Theorem of Arithmetic

Fundamental Theorem of Arithmetic:

Let  $p_1, p_2, p_3, \dots$  be the primes in ascending order.

For all natural numbers  $n$ , 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.

---

Key facts:

Lemma:  $\forall n \in \mathbb{N} \setminus \{1\} \exists p \in \mathcal{P} (p|n)$  (i.e. every natural number greater than 1 is divisible by some prime number)

Lemma (prime property):  $\forall p \in \mathcal{P} \forall x, y \in \mathbb{Z} (p|xy \rightarrow p|x \vee p|y)$

# Proof of the Fundamental Theorem of Arithmetic

We'll prove the Fundamental Theorem of Arithmetic by induction.

Base case:  $n=1$ .  $c_1=0, c_2=0, c_3=0, \dots$  is the unique sequence of non-negative integers such that  $1 = \prod_{j=1}^{\infty} p_j^{c_j}$ .

Inductive step: Assume the theorem is true for all  $n \leq m$  for some  $m \in \mathbb{N}$  and consider  $n=m+1$ .

Existence of  $c_1, c_2, c_3, \dots$ :

$\exists k \in \mathbb{N} (p_k | n)$ .  $\exists q \in \mathbb{N} (n = qp_k)$ . By the inductive hypothesis,  $q$  has a prime factorization  $q = \prod_{j=1}^{\infty} p_j^{a_j}$ .  $n = qp_k = \left( \prod_{j=1}^{k-1} p_j^{a_j} \right) p_k^{a_k+1} \left( \prod_{j=k+1}^{\infty} p_j^{a_j} \right)$

Uniqueness of  $c_1, c_2, c_3, \dots$ :

Assume  $n = \prod_{j=1}^{\infty} p_j^{c_j}$  and  $n = \prod_{j=1}^{\infty} p_j^{c'_j}$  where  $\forall j \in \mathbb{N} (c_j, c'_j \in \mathbb{N} \cup \{0\})$

$\exists k \in \mathbb{N} (p_k | n)$ . By the prime property,  $c_k \geq 1$  as otherwise  $p_k \nmid \prod_{j=1}^{\infty} p_j^{c_j}$  but  $p_k$  does not divide any term in this product.

Similarly,  $c'_k \geq 1$ .  $\frac{n}{p_k} = \left( \prod_{j=1}^{k-1} p_j^{c_j} \right) p_k^{c_k-1} \left( \prod_{j=k+1}^{\infty} p_j^{c_j} \right) = \left( \prod_{j=1}^{k-1} p_j^{c'_j} \right) p_k^{c'_k-1} \left( \prod_{j=k+1}^{\infty} p_j^{c'_j} \right)$ . By the inductive hypothesis,  $\frac{n}{p_k}$  has a unique prime factorization so  $\forall j \in \mathbb{N} (c'_j = c_j)$