Fundamental Theorem of Arithmetic

1. FTA: ① Every natural number greater than 1 can be written as a product of primes, and ② the expression of a number as a product of primes is unique except for the order of factors.

proof: 2.2.4 has shown ①. I'll prove uniqueness.

Assume for contradiction $S:\{n\in\mathbb{N}: n$ does not have unique prime factorization$\}$.

Assume $S\neq\emptyset$.

Since $S\neq\emptyset$ and $S\subseteq\mathbb{N}$, by WOP, there exist smallest element $N_0\in S$.

$\Rightarrow N_0 = p_1\cdot p_2\cdots p_r$ or $N_0 = q_1\cdot q_2\cdots q_s$. where $r,s\in\mathbb{N}$. and p_i, q_j are prime $\forall i\in\{1,\dots,r\}$. $\forall j\in\{1,\dots,s\}$.

WTS: $p_i\neq q_j$, $\forall i,j$.

Prove by contradiction, suppose $p_{i^*} = q_{j^*}$ for some $i^*\in\{1,\dots,r\}$ and $j^*\in\{1,\dots,s\}$.

Since $p_1\cdots p_i\cdots p_r = N_0 = q_1\cdots q_{j^*}\cdots q_s$; by cancellation, gives,

$\Rightarrow p_1\cdots p_{i-1}\cdot p_{i+1}\cdots p_r = q_1\cdots q_{j-1}\cdot q_{j+1}\cdots q_s$.

$\Rightarrow \frac{N_0}{p_{i^*}} = \frac{N_0}{q_{j^*}}\in\mathbb{N}$, and $\frac{N_0}{p_{i^*}} < N_0$ and $\frac{N_0}{q_{j^*}} < N_0$.

Since both $\frac{N_0}{p_{i^*}}$ and $\frac{N_0}{q_{j^*}}$ have two diff. factorization, they're in S.

However they're less than N_0 contradicts to N_0 is the smallest element in S.

I've shown $p_i\neq q_j$ $\forall i,j$.

Since $\forall i,j.\ p_i\neq q_j$, gives $p_1\neq q_1$. which $p_1<q_1$ or $p_1>q_1$

Assume. with WLOG. $p_1<q_1$

Define $M = N_0 - (p_1\cdot q_2\cdots q_s) < N_0$.

$\Rightarrow M = (p_1\cdot p_2\cdots p_r) - (p_1\cdot q_2\cdots q_s)$

$\Rightarrow M = p_1(p_2 \cdots p_r - q_2 \cdots q_s)$.

$\Rightarrow p_1 \mid M$

Since p_1 is a prime, $M \geq 1$. gives. $1 < M < N_0$.

Since N_0 is the smallest number in set. $M \notin S$.

M has unique prime factorization.

Also. $M = N_0 - (p_1 \cdot q_2 \cdots q_s)$

$= (q_1 \cdot q_2 \cdots q_s) - (p_1 \cdot q_2 \cdots q_s)$

$= (q_1 - p_1)(q_2 \cdots q_s)$.

Since $p_1 \mid M \wedge M \notin S$ (M has a unique factorization).

Since $p_1 \neq q_j$. $\forall j$. gives. $p_1 \mid (q_1 - p_1) \Rightarrow p_1 \mid q_1$.

However, q_1 is prime $\wedge\ q_1 \neq p_1 \Rightarrow p_1 \mid q_1$ is impossible

Thus, $S = \phi$. ■

2. Canonical Factorization (prime factorization): Every natural number N greater than 1 has a canonical factorization into primes; that is, each natural number N greater than 1 has a unique representation of the form $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, where each p_i is a prime, p_i is less than p_{i+1} for i, and each α_i is a natural number.

↑ 消除了其 order 问题

3. Euclid's Lemma: If p is a prime number and a and b are natural numbers such that p divides ab, then p divides at least one of a and b. (If a prime divides a product, then it divides at least one of the factors.)

1). modulo: p is prime $\wedge\ ab \equiv 0 \pmod p$

$\Rightarrow a \equiv 0 \pmod p \vee b \equiv 0 \pmod p$.

2). Generalized: p is a prime $\wedge\ p \mid (a_1 \cdots a_n)$ where $a_i \in \mathbb{N}$.

$\Rightarrow p \mid a_i$ for some $j \in \{1, \ldots, n\}$.

3). Proof: (PMI). $\forall p \in \mathbb{N}$. p is a prime

WTS: $\forall n \in \mathbb{N}$, $n \geq 2$, $p \mid (a_1 \cdots a_n) \Rightarrow p \mid a_j$.

B.C. $n=2$.

when $n=2$. $p \mid a_1 \cdot a_2$.

By E.L. $p \mid a_1$ or $p \mid a_2$.

I.S. Let $n \in \mathbb{N}$. $n \geq 2$.

I.H. Assume $p \mid (a_1 \cdots a_n) \Rightarrow p \mid a_j$ for some $j \in \{1, \ldots, n\}$.

Assume $p \mid (a_1 \cdots a_n \cdot a_{n+1})$. WTS. $p \mid a_k$ for some $k \in \{1, \ldots, n, n+1\}$.

Since $p \mid (a_1 \cdots a_n \cdot a_{n+1})$. gives.

$\Rightarrow p \mid (a_1 \cdots a_n) \cdot a_{n+1}$.

By B.C. $p \mid (a_1 \cdots a_n)$ or $p \mid a_{n+1}$.

By I.H. $p \mid (a_1 \cdots a_n) \Rightarrow p \mid a_j$ for some $j \in \{1, \ldots, n\}$.

Overall, $p \mid a_k$ for some $k \in \{1, \ldots, n+1\}$.

■

5). Proof. (F.L).

Let p be prime number. Let $a, b \in \mathbb{N}$. $p \mid ab$.

WTS. $p \mid a$ or $p \mid b$.

Since $p \mid ab$. $\exists d \in \mathbb{N}$. s.t. $d \cdot p = a \cdot b$, gives the unique factorization of ab into primes contain prime p and all the primes that divides d.

Also, a and b each have unique factorizations into primes.

From the canonical factorization gives, $a = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_m^{\alpha_m}$. and.

$b = r_1^{\beta_1} \cdot r_2^{\beta_2} \cdots r_k^{\beta_k}$. gives.

$$a \cdot b = (q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_m^{\alpha_m}) \cdot (r_1^{\beta_1} \cdot r_2^{\beta_2} \cdots r_k^{\beta_k}).$$

Since the factorization of ab into primes is unique. -----

■

6). Proof (Z. L. — gcd)

Let p be prime number. Let $a, b \in \mathbb{N}$. $p \mid ab$.

WTS. $p \mid a$ or $p \mid b$.

Case 1: Assume $p \mid a$ → Done.

Case 2: Assume $p \nmid a$

Since p is prime. $p \mid p \wedge 1 \mid p$.

Since $p \nmid a$. gives $\gcd(a, p) = 1$.

By Lemma 0, $\exists x, y \in \mathbb{Z}$ s.t. $ax + py = 1$.

$\Rightarrow axb + pyb = b$.

$\Rightarrow abx + bpy = b$.

Since $p \mid ab$, $\exists k_1 \in \mathbb{Z}$ s.t. $k_1 p = ab$.

$\Rightarrow k_1 p \cdot x + bpy = b$.

$\Rightarrow p(k_1 x + by) = b$.

Since $p \mid p(k_1 x + by)$, gives $p \mid b$.