

2.7 Theorem. (Fundamental Theory of Arithmetic - Existence Part) Every natural number greater than 1 is either a prime number or it can be expressed as a finite product of prime numbers. That is, for every natural number greater than 1, there exist distinct primes p_1, p_2, \dots, p_m and natural numbers r_1, r_2, \dots, r_m such that

$$n = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}.$$

Proof. Let $n > 1$ for all natural numbers be given. There exists distinct primes p_1, p_2, \dots, p_m and natural numbers r_1, r_2, \dots, r_m such that

$$n = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}.$$

We will prove by contradiction. That is, suppose there exists a natural number n with $n > 1$ such that n cannot be written as a product of distinct primes for all prime numbers. Consider the set of natural numbers greater than 1 that cannot be written as a product of primes. A prime could not exist in this set because a prime can be written as itself times any prime raised to the zeroth power. Suppose there is a composite number that cannot be expressed as a product of primes such that the set is non-empty. By WOANN there exists a smallest number a . Since a is composite, $a = pk$ for some $p, k \in \mathbb{N}$ and $p, k < a$. Since a is minimal, p, k must be primes. Since we know primes can be written as a product of primes, let $f_1^{h_1} f_2^{h_2} \dots f_u^{h_u}$ be the prime factorization of p and $g_1^{s_1} g_2^{s_2} \dots g_t^{s_t}$ be the prime factorization of k . Since $a = pk$,

$$\begin{aligned} a &= (f_1^{h_1} f_2^{h_2} \dots f_u^{h_u})(g_1^{s_1} g_2^{s_2} \dots g_t^{s_t}) \\ &= f_1^{h_1} g_1^{s_1} f_2^{h_2} g_2^{s_2} \dots f_u^{h_u} g_t^{s_t}. \end{aligned}$$

Let $h_i \leq r_i$ and $s_i \leq r_i$ such that $r_i = h_i + s_i$. Combining common factors,

$$a = p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}.$$

We find that a is a product of distinct primes which contradicts our assumption. Thus, every natural number greater than 1 can be written as the product of distinct primes. \square