Prime factorization

Definition 2.2.1

A *prime number** is a positive integer having no divisors other than 1 and itself. If a positive integer is not 1 and is not a prime number, then it is called a *composite number*.

In the Hasse diagram of divisibility of positive integers, the above notions can be interpreted as follows:

- 1 is the root/origin;
- prime numbers are nodes adjacent to 1;
- composite number are other nodes.

*There is no standard notation for the set of prime numbers. But many use $\mathbb{P}$.

Theorem 2.2.2 (Primarity, fundamental property of primes)

Let p be a prime number. Then for any integers a, b, if $p \mid ab$, then either $p \mid a$ or $p \mid b$.

$6 \nmid 4$ or 9 $\qquad$ $6 \mid 4 \times 9$

Theorem 2.2.2 (Primarity, fundamental property of primes)

Let p be a prime number. Then for any integers a, b, if $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Proof. We may assume $p \nmid a$. Then since there is no other divisor of p than 1 and p, we must have $\gcd(p, a) = 1$.

By *Bézout's identity*, there are integers x_0, y_0 such that $px_0 + ay_0 = 1$. Lets multiple both sides by b, we get

$$pbx_0 + aby_0 = b.$$

Since $p \mid ab$, by *2-out-of-3 principle*, we must have $p \mid b$. □

Theorem 2.2.3 (Fundamental Theorem of Arithmetic)

Let n be any positive integer.

1. *(existence) n admits a prime factorization, i.e. there exist natural numbers e_p for each prime p such that**

$$n = 2^{e_2} \cdot 3^{e_3} \cdots p^{e_p} \cdots$$

2. *(uniqueness) Suppose n admits another prime factorization, say*

$$n = 2^{f_2} \cdot 3^{f_3} \cdots p^{f_p} \cdots .$$

Then, for every prime p, we have $e_p = f_p$.

*Note that this is a finite product.

Proof of uniqueness

We first prove the uniqueness.

Suppose we have two distinct prime factorizations of n, say

$$n = 2^{e_2} \cdot 3^{e_3} \cdots p^{e_p} \cdots ,$$
$$n = 2^{f_2} \cdot 3^{f_3} \cdots p^{f_p} \cdots .$$

Then there is a prime p such that $e_p \neq f_p$, say $e_p > f_p$.

We first prove the uniqueness.

Suppose we have two distinct prime factorizations of n, say

$$n = 2^{e_2} \cdot 3^{e_3} \cdots p^{e_p} \cdots ,$$
$$n = 2^{f_2} \cdot 3^{f_3} \cdots p^{f_p} \cdots .$$

Then there is a prime p such that $e_p \neq f_p$, say $e_p > f_p$.

Consider $a = \frac{n}{p^{f_p}}$. By the first factorization, we have $p \mid a$. By the second factorization and theorem 2.2.2, $p \nmid a$ (indeed, 2.2.2 implies: if each factor of a product is not a multiple of p, then the product is not a multiple of p). This gives a contradiction. Therefore, we must have $e_p = f_p$ for all prime p.

Proof of existence

Now we prove the existence.

For each prime p. Consider the sequence

$$1 = p^0, p^1, p^2, \cdots$$

Among them, there is a largest one, say p^{e_p}, such that $p^{e_p} \mid n$.

Now we prove the existence.

For each prime p. Consider the sequence

$$1 = p^0, p^1, p^2, \cdots$$

Among them, there is a largest one, say p^{e_p}, such that $p^{e_p} \mid n$.

We will show that, from $p^{e_p} \mid n$ for all prime p, we can conclude that

$$2^{e_2} \cdot 3^{e_3} \cdots p^{e_p} \cdots \mid n.$$

Let's say $n = d \cdot 2^{e_2} \cdot 3^{e_3} \cdots p^{e_p} \cdots$. Then if $d \neq 1$, there must be a prime divisor p_0 of d (e.g. the smallest divisor of d other than 1). Then we have $p_0^{e_{p_0}+1} \mid n$, which contradicts with the maximality of e_{p_0}.