

**Definition:**

$p$  is a **prime**  $\Leftrightarrow p \in \mathbb{N}, p \geq 2, \forall n \in \mathbb{N} \ n | p \rightarrow n \in \{1, p\}$ .

Iff  $n \in \mathbb{N}, n > 1$  and is not a prime, then  $n$  is called **composite**.

**Facts:**

1.  $\forall n \in \mathbb{N}, n > 1 \exists p \ni p$  is a prime and  $p | n$ .

*Proof:* by contradiction, using the Well-Ordering Principle (p.115).

2. The number of all primes is infinite.

*Proof:* Suppose the opposite is true: suppose that  $\{p_1, \dots, p_m\}$  is the finite set of all primes. Consider the number  $n = p_1 \dots p_m + 1$ . This  $n$  is not equal to any of  $p$ 's, therefore, by assumption,  $n$  is not a prime but a composite, therefore (by definition of a composite),  $n$  has a divisor – label it  $q_1$  – that is greater than 1 and less than  $n$ . Now we shall see that  $n$  must have a prime divisor. If  $q_1$  is a prime, then  $n$  has a prime divisor. If  $q_1$  is not a prime, then we take its divisor  $q_2, 1 < q_2 < q_1$ , which therefore is also a divisor of  $n$ . If  $q_2$  is a prime, then  $n$  has a prime divisor. If  $q_2$  is not a prime, then we take its divisor  $q_3, 1 < q_3 < q_2$ , which therefore is also a divisor of  $n$ . Given any finite  $n$ , we can continue this process until we reach a prime divisor  $q$  in a finite number of steps. The number of steps is finite, because there is only a finite set of numbers between 1 and  $n$ . Therefore, we have a prime  $q$  that is a divisor of  $n$ . By assumption,  $q$  is already in the set  $\{p_1, \dots, p_m\}$ . Therefore,  $n$  can be written as

$$n = qN + 1, \quad (*)$$

where  $N$  is the product of all  $p$ 's except one. By the Theorem 4.1.3, given  $n$  and  $q$ , there is only one decomposition  $n = qb + r$  with  $0 \leq r < q$ . Therefore, we have  $r = 1$  (\*), and therefore  $q$  is not a divisor of  $n$ . This conclusion contradicts our assumption that  $n$  has a divisor other than 1 and  $n$ . Therefore,  $n$  must be a prime, which contradicts the assumption that  $\{p_1, \dots, p_m\}$  is the finite set of all primes. Therefore, the number of primes is infinite.

3.  $\forall n \in \mathbb{N}$ ,  $n$  is composite  $\Leftrightarrow \exists$  a prime  $p \leq \sqrt{n} \ni p \mid n$ .

*Proof:* It is sufficient to prove the left-to-right implication. Since  $n$  is not a prime, we can write  $n=ab$  with some  $a, b \in \mathbb{N}$ ,  $1 < a < n$ ,  $1 < b < n$ . Without any loss of generality, assume that  $a \leq b$ . Suppose that  $a > \sqrt{n}$ , then also  $b > \sqrt{n}$ , which implies  $ab > n$ , in contradiction with  $ab=n$ . Therefore,  $a \leq \sqrt{n}$ . By Fact 1,  $a$  has a prime divisor  $p \leq a$  (which inevitably is also a divisor of  $n$ ). Therefore,  $n$  has a prime divisor  $p \leq \sqrt{n}$ .

***Algorithm (The sieve of Eratosthenes):***

To find all prime numbers less or equal to  $n$ , list all natural numbers less or equal to  $n$  and exclude multiples of all primes  $p$ ,  $1 < p \leq \sqrt{n}$ . *Proof* by Fact 3.

***The Fundamental Theorem of Arithmetic (prime decomposition):***

$\forall n \in \mathbb{N} \exists!$  infinite sequence

$$(\alpha_1, \alpha_2, \dots), \alpha_i \in \{0, 1, 2, \dots\} \ni n = \prod_{i=1}^{\infty} p_i^{\alpha_i},$$

where  $\{p_i \mid i \in \mathbb{N}\}$  is the ordered set of all primes. The  $p$ 's with nonzero  $\alpha$ 's are called ***prime factors***, or ***prime divisors*** of  $n$ .

Equivalently,  $\forall n \in \mathbb{N}, n > 1 \exists!$  finite nondecreasing sequence of primes  $(p_1, p_2, \dots, p_m) \ni n = p_1 p_2 \dots p_m$ . (repetitions are allowed).

*Proof:* Suppose there are two different prime decompositions of a natural number  $n > 1$ :

$$n = p_1 p_2 \dots p_m = q_1 q_2 \dots q_k,$$

where not all  $p$ 's are equal to (or have) corresponding  $q$ 's. Divide both sides of the right equation by those primes that appear in both decompositions. Then you get an equation

$$p_1 p_2 \dots p_m = q_1 q_2 \dots q_k$$

in which all  $p$ 's are different from all  $q$ 's. Now we have a contradiction. Indeed, if any side of the equation is equal to one (no  $p$ 's and/or no  $q$ 's are left), then the contradiction is obvious; therefore, consider the case when both sides are greater than one. Consider  $p_1$ , which is a prime divisor of the l.h.s. If it is also a divisor of the r.h.s., then the r.h.s. has a unique decomposition  $p_1 M$  with some integer quotient  $M$  and the zero remainder. By construction,  $p_1$  is not divisible by any  $q$ 's, therefore, all  $q$ 's must divide  $M$ , which leads to a contradiction: after dividing r.h.s. by  $q$ 's there is  $p_1$  left instead of 1. Therefore, the assumption was wrong: there are no two different decompositions of a number  $n$ .