Prime Numbers

A prime number is an integer that is greater than 1 and has no positive divisors other than 1 and itself.

$$2, \quad 3, \quad 5, \quad 7, \quad 11, \quad \ldots$$

An integer that is greater than 1 but is not prime is called composite.

$$4, \quad 15, \quad 77, \quad 120, \quad \ldots$$

We call 1 neither a prime nor a composite number. Including it among primes would make the statement of the Fundamental Theorem of Arithmetic inconvenient. Therefore, we call 1 a unit. The primes can be used to build the entire system of positive integers. The first two lemmas will show that every positive integer can be written as a product of primes. Later, we will prove the uniqueness of the representation.

Lemma : (2.1)

Every integer $n > 1$ is divisible by a prime number.

Proof. The set of divisors of n that are greater than 1 and less than n is either empty or non-empty.

If it is empty, then n is a prime number and thus has a prime divisor.

If it is nonempty, then the least integer principle says that it has a smallest element, call it d. If d had a divisor greater than 1 and less than d, then so would n. But this is impossible because d was the smallest such divisor. (Suppose $c \mid d$ and $1 < c < d$. $c \mid d$ and $d \mid n$, so $c \mid n$, but $c < d$).

Therefore, d is prime, and n has a prime divisor, namely d. In both cases, n is divisible by a prime number. □

Lemma : (2.2)

Every integer $n > 1$ can be written as a product of primes.

Proof. From Lemma 2.1, we know that there is a prime p_1 such that $p_1 \mid n$. By the definition of divides, we get that $n = p_1 n_1$, where $1 \leq n_1 < n$.

If $n_1 = 1$, then $n = p_1$ is an expression as a product of primes.

If $n > 1$, then from Lemma 2.1, there is a prime that divides n_1. By applying Lemma 2.1 repeatedly, we will find some n_i equal to 1 because the sequence of n_i is strictly decreasing but larger than 1. $n > n_1 > n_2 > \cdots \geq 1$. For some k, we will have $n_k = 1$, in which case, $n = p_1 p_2 \ldots p_k$ is an expression of n as a product of primes. □

Example

Write the prime decompositions for 60 and 960.

$$\begin{aligned} 60 &= 30 \cdot 2 \\ &= 15 \cdot 2 \cdot 2 \\ &= 5 \cdot 3 \cdot 2 \cdot 2 \end{aligned}$$

$$\begin{aligned} 960 &= 480 \cdot 2 \\ &= 240 \cdot 2 \cdot 2 \\ &= 120 \cdot 2 \cdot 2 \cdot 2 \\ &= 60 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \\ &= 5 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \end{aligned}$$

Theorem

There are infinitely many primes.

Proof. Suppose there are finitely many primes. Denote them by:

$$p_1, p_2, \ldots, p_r$$

Consider the integer

$$n = p_1 p_2 \ldots p_r + 1$$

From Lemma 2.1, we have that n is divisible by a prime, and since there are only finitely many primes, it must be one of $p_1, p_2, \ldots, p_r$. Suppose that it is p_k. Then, since $p_k \mid n$ and $p_k \mid p_1 p_2 \ldots p_r$, we get that $p_k \mid 1$, a contradiction. □

Lemma : (2.5)

If $p \mid (ab)$, then $p \mid a$ or $p \mid b$.

Proof. Since p is prime, either $(p, a) = p$ or $(p, a) = 1$. In the first case, $p \mid a$ and we are done. In the second case, by Corollary 1.1, $p \mid b$, and we are done. □

Lemma : (2.6)

If $p \mid (a_1 a_2 \ldots a_k)$, then $p \mid a_i$ for some i, $i = 1, 2, \ldots, k$.

Proof. If $k = 1$, then Lemma 2.6 is true by inspection. If $k = 2$, then Lemma 2.5 shows that Lemma 2.6 is true.

Suppose that Lemma 2.6 is true for $k = r$. Suppose that $p \mid (a_1 a_2 \ldots a_{r+1})$, that is, $p \mid (a_1 a_2 \ldots a_r)\, a_{r+1}$. Then, Lemma 2.5 gives us that $p \mid a_{r+1}$ or $p \mid (a_1 a_2 \ldots a_r)$.

In the first case, $p \mid a_{r+1}$. In the second case, by the induction step, $p \mid a_i$ for some $1 \leq i \leq r$. In either case, $p \mid a_i$ for some i, $i = 1, 2, \ldots, r + 1$.

Therefore, if $p \mid (a_1 a_2 \ldots a_k)$, then $p \mid a_i$ for some i, $i = 1, 2, \ldots, k$. □

Lemma : (2.7)

If $q_1, q_2, \ldots, q_n$ are primes, and $p \mid (q_1 q_2 \ldots q_k)$, then $p = q_k$ for some k.

Proof. From Lemma 2.7, we know that $p \mid q_k$ for some k. However, the only divisors of q_k are q_k and 1. Also, p is not 1 since p is a prime. Therefore, we have that $p = q_k$. $\square$

Theorem : Fundamental Theorem of Arithmetic

Any positive integer can be written as a product of primes in one and only one way.

Proof. From Lemma 2.2, any integer $n > 1$ can be written as a product of primes. Suppose that there are two representations

$$n = p_1 p_2 \ldots p_m \quad \text{and} \quad n = q_1 q_2 \ldots q_r$$

We must show that the same primes appear in each product and that they appear the same number of times. Since $p_1 \mid n$, we have that $p_1 \mid (q_1 q_2 \ldots q_r)$. From Lemma 2.7, it follows that $p_1 = q_i$ for some i. If we divide by the common factor we have that

$$p_2 p_3 \ldots p_m = q_1 q_2 \ldots q_{t-1} q_{t+1} \ldots q_r$$

Applying Lemma 2.7 repeatedly, we find that each p is a q. Similarly, by interchanging p and q, we find that each q is a p.

Therefore, $p_1, p_2, \ldots, p_m$ are a rearrangement of $q_1, q_2, \ldots, q_r$, and the two factorizations differ only in the order of the factors. $\square$