

Introduction to Elementary Number Theory

Selim Kaan Ozsoy, Middle East Technical University

Elementary number theory is the branch of mathematics concerned with the study of the integers and their fundamental properties.

Unlike many areas of mathematics that rely heavily on continuous structures, number theory focuses on discrete objects and exact relationships. Its questions are often simple to state, yet surprisingly deep, and many have shaped the development of modern mathematics.

At its core, number theory seeks to understand the structure of the integers: how numbers divide one another, how primes are distributed, and how arithmetic behaves under various constraints.

Despite its elementary appearance, number theory plays a central role in areas ranging from algebra and analysis to cryptography and computer science.

It is highly recommended for students who major in computer engineering or physics to study elementary number theory, as it helps in understanding the patterns and behaviors.

Preliminaries

Elementary facts:

- (1) There is "addition on \mathbb{Z} ", denoted by "+" such that for any $a, b \in \mathbb{Z}$, $a + b$ is uniquely determined.
- (2) For any $a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$.
- (3) There exists an integer, namely 0, such that $a + 0 = a = 0 + a$ for all $a \in \mathbb{Z}$.
- (4) For any $a, b \in \mathbb{Z}$, $a + b = b + a$.

(5) There is "multiplication on \mathbb{Z} ", denoted by " \cdot " such that for any $a, b \in \mathbb{Z}$, $a \cdot b$ is uniquely determined.

(6) For any $a, b, c \in \mathbb{Z}$,

$$a \cdot (b + c) = ab + ac \quad \text{and} \quad (a + b) \cdot c = ac + bc.$$

(7) $1 \cdot a = a = a \cdot 1$.

(8) For any $a, b \in \mathbb{Z}$, $a \cdot b = b \cdot a$.

(9) For any $a, b, c \in \mathbb{Z}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(10) For all $a \in \mathbb{Z}$, $a \cdot 0 = 0 \cdot a = 0$.

Remark. The definition of standard number sets may vary depending on the context. For instance, in some areas of mathematics, the set of natural numbers is defined as

$$\mathbb{N} = \{0, 1, 2, 3, \dots\},$$

whereas in number theory it is common to define

$$\mathbb{N} = \{1, 2, 3, 4, \dots\} = \mathbb{Z}^+.$$

Throughout these notes, we adopt the latter convention, that is, \mathbb{N} denotes the set of positive integers.

Remark.

For any $a \in \mathbb{Z}$, one and only one of the following holds:

- (i) $a \in \mathbb{Z}^+$
- (ii) $a = 0$
- (iii) $a \in \mathbb{Z}^-$.

Definition. **Axiom** is a statement assumed to be true without any proof.

We construct our mathematical structures and theorems using axioms.