

Elementary Number Theory

Apiros3

January 25, 2025

1 Introduction

Number theory is the study of integers and their properties. It is one of the oldest branches of mathematics and has applications in cryptography, computer science, and physics.

2 Divisibility

2.1 Basic Properties

For integers a , b , and c :

- If $a \mid b$ and $b \mid c$, then $a \mid c$
- If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$
- If $a \mid b$, then $a \mid bc$ for any integer c

2.2 Greatest Common Divisor

The **greatest common divisor** of two integers a and b , denoted $\gcd(a, b)$, is the largest positive integer that divides both a and b .

3 Prime Numbers

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

3.1 Fundamental Theorem of Arithmetic

Every positive integer greater than 1 can be written uniquely as a product of primes, up to the order of the factors.

4 Congruences

We say that a is **congruent** to b modulo m , written $a \equiv b \pmod{m}$, if $m \mid (a - b)$.

4.1 Properties of Congruences

For integers a , b , c , and d :

- $a \equiv a \pmod{m}$ (reflexive)
- If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$ (symmetric)
- If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$ (transitive)