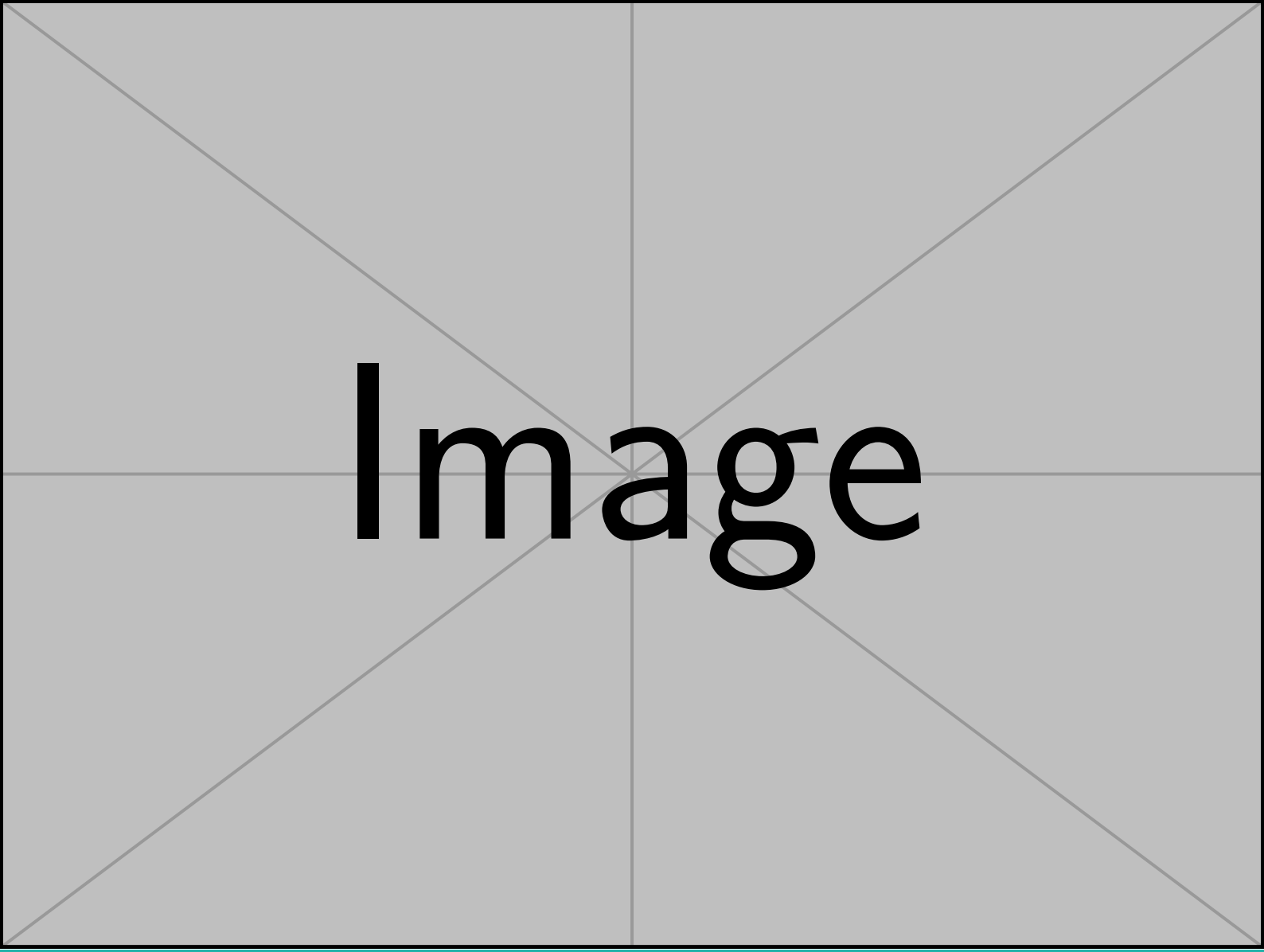


# Théorie des Nombres

**Author:** CatMono

**Date:** February, 2026

**Version:** 0.1

# Contents

**Preface** ii

**Chapter 1 Integers** 1

1.1 Divisibility . . . 1

1.2 Carry System . . . 2

1.3 Greatest Common Divisor and Least Common Multiple . . . 4

1.4 Prime Numbers . . . 5

1.5 Fundamental Theorem of Arithmetic . . . 6

**Chapter 2 Congruences** 7

**Chapter 3 Quadratic Residues** 8

**Chapter 4 Number Theoretic Functions** 9

**Chapter 5 Prime Numbers** 10

**Chapter 6 Asymptotic Methods and Continued Fractions** 11

**Chapter 7 Diophantine Equations** 12

# Preface

Version notes are in the table below.

| Version | Date | Description |
|---|---|---|
| 0.1 | February, 2026 | Initial version |

# Chapter 1 Integers

## 1.1 Divisibility

Let[1]

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}, \quad \mathbb{N}_+ = \{1, 2, 3, \ldots\}, \quad \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

*Definition 1.1 (Gauß Symbols)*

For a real number $x$, the floor function (greatest integer function) is defined as:

$$\lfloor x \rfloor = \max\{n \in \mathbb{Z} \mid n \leq x\}.$$

Similarly, the ceiling function (least integer function) is defined as:

$$\lceil x \rceil = \min\{n \in \mathbb{Z} \mid n \geq x\}.$$

♣

**Property**

1. *For any $m \in \mathbb{N}_+$, there is **Hermite's identity**:*

$$\lfloor mx \rfloor = \lfloor x \rfloor + \left\lfloor x + \frac{1}{m} \right\rfloor + \cdots + \left\lfloor x + \frac{m-1}{m} \right\rfloor.$$

$$\lceil mx \rceil = \lceil x \rceil + \left\lceil x - \frac{1}{m} \right\rceil + \cdots + \left\lceil x - \frac{m-1}{m} \right\rceil.$$

2.

*Theorem 1.1 (Euclidean Division (Division with Remainder))*

For any integers $a$ and $b$ with $b > 0$, there exist unique integers $q$ and $r$ such that

$$a = bq + r, \quad 0 \leq r < b.$$

$r$ is called the remainder of $a$ divided by $b$, denoted as $r = a \bmod b$.

If $r = 0$, then $b$ divides $a$, denoted as $b \mid a$; otherwise, $b$ does not divide $a$, denoted as $b \nmid a$. In other words, $b \mid a$ if and only if there exists an integer $k$ such that $a = bk$.

If $a = kb$ and $b \neq a, b \neq 1$, then $b$ is called a proper divisor of $a$.

♡

**Property** *If $b \neq 0, c \neq 0$, then*

1. *If $b \mid a, c \mid b$, then $c \mid a$.*
2. *If $b \mid a$, then $bc \mid ac$.*
3. *If $c \mid d, c \mid e$, then $c \mid (md + ne)$, for any integers $m, n$.*

*Definition 1.2 (Modular Arithmetic and Modular Inverse)*

For any integers $a, b$, and positive integer $m$, if $m \mid (a - b)$, then $a$ is congruent to $b$ modulo $m$, denoted as

$$a \equiv b \pmod{m}.$$

If there exists an integer $x$ such that

$$ax \equiv 1 \pmod{m},$$

then $x$ is called the modular inverse of $a$ modulo $m$, also denoted as $a^{-1} \equiv x \pmod{m}$.

♣

[1] Sometimes, natural numbers refer to the set of positive integers excluding zero, i.e., $\mathbb{N}_+ = \{1, 2, 3, \ldots\}$.

## 1.2 Carry System

Carry system (or positional numeral system) is a method of representing numbers using a radix (or base) $r$ ($r \geq 2$). In base $r$, any non-negative integer $N$ can be expressed as:

$$N = a_k r^k + a_{k-1} r^{k-1} + \cdots + a_1 r + a_0 = \sum_{i=0}^{k} a_i r^i =: (a_k a_{k-1} \cdots a_1 a_0)_r,$$

where $a_i$ are the digits satisfying $0 \leq a_i < r$ and $a_k \neq 0$.

This can be extended to decimal fractions as:

$$N = a_k r^k + a_{k-1} r^{k-1} + \cdots + a_1 r + a_0 + a_{-1} r^{-1} + a_{-2} r^{-2} + \cdots = \sum_{i=-m}^{k} a_i r^i =: (a_k a_{k-1} \cdots a_1 a_0 . a_{-1} a_{-2} \cdots a_{-m})_r,$$

where $m$ is a positive integer.

¶ **Radix Conversion**

Here are *methods for converting between decimal and base $r$*:

- Decimal to base $r$:
  1. For the integer part, repeatedly divide by $r$ and record the remainders.
  2. For the fractional part, repeatedly multiply by $r$ and record the integer parts.
  3. Combine the results to form the base $r$ representation.
- Base $r$ to decimal:
  1. For the integer part, multiply each digit by $r$ raised to its position power and sum them.
  2. For the fractional part, multiply each digit by $r$ raised to its negative position power and sum them.
  3. Combine both sums to get the decimal representation.

**Example 1.1**

1. Convert decimal $45.625$ to binary.
2. Convert binary $(1101.101)_2$ to decimal.

*Solution*

1. For integer part $45$:

$$45 \div 2 = 22 \text{ remainder } 1$$
$$22 \div 2 = 11 \text{ remainder } 0$$
$$11 \div 2 = 5 \text{ remainder } 1$$
$$5 \div 2 = 2 \text{ remainder } 1$$
$$2 \div 2 = 1 \text{ remainder } 0$$
$$1 \div 2 = 0 \text{ remainder } 1$$

Reading remainders from bottom to top gives $101101$.

For fractional part $0.625$:

$$0.625 \times 2 = 1.25 \quad \text{(integer part 1)}$$
$$0.25 \times 2 = 0.5 \quad \text{(integer part 0)}$$
$$0.5 \times 2 = 1.0 \quad \text{(integer part 1)}$$

Reading integer parts gives $101$.

Combining both parts, we get $45.625_{10} = (101101.101)_2$.

2. Since $1\times2^3+1\times2^2+0\times2^1+1\times2^0+1\times2^{-1}+0\times2^{-2}+1\times2^{-3}=8+4+0+1+0.5+0+0.125=13.625$; thus, $(1101.101)_2=13.625_{10}$.

□

¶ Generalized Carry System

¶ Balanced Ternary

**Balanced ternary** (symmetric ternary) is a non-standard positional numeral system that uses three digits: $-1$, $0$, and $1$. Since $-1$ is not a standard digit, it is often represented by the symbol $Z$ or $\bar{1}$. The weight calculation is the same as standard ternary, with the weight of the $i$-th digit being $3^i$.

*Theorem 1.2 (Uniqueness of Balanced Ternary Representation)*

Every integer can be uniquely represented in balanced ternary. ♡

*Proposition 1.1*

For negative numbers, simply negate each digit of the corresponding positive integer's balanced ternary representation. ♠

Here are *methods for converting between decimal and balanced ternary*:

- Decimal to balanced ternary:
  1. Repeatedly divide the number by 3, recording the remainders.
  2. If a remainder is 2, replace it with $-1$ (or $Z$) and increment the quotient by 1.
  3. Continue until the quotient is 0.
  4. Read the remainders from bottom to top to form the balanced ternary representation.
- Balanced ternary to decimal:
  1. Multiply each digit by 3 raised to its position power and sum them.
  2. For digits equal to $-1$ (or $Z$), treat them as $-1$ in the calculation.

**Example 1.2**

1. Convert decimal 64 to balanced ternary.
2. Convert balanced ternary $1Z0Z1$ to decimal.

*Solution*

1. For integer part 64:

$$\begin{aligned}
&64\div3=21 \text{ remainder } 1\\
&21\div3=7 \text{ remainder } 0\\
&7\div3=2 \text{ remainder } 1\\
&2\div3=0 \text{ remainder } 2 \quad (\text{replace } 2 \text{ with } Z,\ \text{increment quotient to } 1)\\
&1\div3=0 \text{ remainder } 1
\end{aligned}$$

   Reading remainders from bottom to top gives $1Z0Z1$. Thus, $64_{10}=(1Z0Z1)_{3b}$.
2. Since $1\times3^4+(-1)\times3^3+0\times3^2+(-1)\times3^1+1\times3^0=81-27+0-3+1=52$; thus, $(1Z0Z1)_{3b}=52_{10}$.

□

## 1.3 Greatest Common Divisor and Least Common Multiple

*Definition 1.3 (Greatest Common Divisor (GCD))*

For two integers $a$ and $b$, not both zero, the greatest common divisor (GCD) of $a$ and $b$, denoted as $\gcd(a,b)$ (if there is no ambiguity, it can be abbreviated as $(a,b)$), is the largest positive integer that divides both $a$ and $b$. Id est, $\gcd(a,b)=d$ if and only if:

1. $d \mid a$ and $d \mid b$;
2. For any integer $c$ such that $c \mid a$ and $c \mid b$, it follows that $c \mid d$.

♣

*Definition 1.4 (Least Common Multiple (LCM))*

For two integers $a$ and $b$, not both zero, the least common multiple (LCM) of $a$ and $b$, denoted as $\operatorname{lcm}(a,b)$ (if there is no ambiguity, it can be abbreviated as $[a,b]$), is the smallest positive integer that is a multiple of both $a$ and $b$. Id est, $\operatorname{lcm}(a,b)=m$ if and only if:

1. $a \mid m$ and $b \mid m$;
2. For any integer $n$ such that $a \mid n$ and $b \mid n$, it follows that $m \mid n$.

♣

**Remark** Sometimes, $\gcd(a,0)$ is defined as $|a|$.

**Property** *GCD and LCM have the following relationship:*

1. $(a,b)[a,b]=|ab|$;
2. $(ab,bc,ca)[a,b,c]=|abc|$;
3. $\frac{(a,b,c)^2}{(a,b)(b,c)(a,c)}=\frac{[a,b,c]^2}{[a,b][b,c][a,c]}$

*Theorem 1.3 (Euclidean Algorithm)*

For any integers $a$ and $b$ with $b \neq 0$,

$$\gcd(a,b)=\gcd(b,a \bmod b).$$

♡

*Proof* By the definition of GCD, let $d=\gcd(a,b)$. Then $d \mid a$ and $d \mid b$, which implies $d \mid (a-bq)$ for any integer $q$. Choosing $q=\lfloor a/b \rfloor$, we have $d \mid (a \bmod b)$. Thus, $d$ is a common divisor of $b$ and $a \bmod b$.
Conversely, let $d'=\gcd(b,a \bmod b)$. Then $d' \mid b$ and $d' \mid (a \bmod b)$, which implies $d' \mid (bq+(a \bmod b))=a$. Thus, $d'$ is a common divisor of $a$ and $b$.
Since both $d$ and $d'$ are the greatest common divisors of their respective pairs, we conclude that $d=d'$. ■

According to the Euclidean algorithm, we can compute the GCD of two integers efficiently by repeatedly applying the division with remainder until the remainder is zero.

**Example 1.3** Find $\gcd(252,105)$ using the Euclidean algorithm.

*Solution*

$$252=2\times 105+42$$
$$105=2\times 42+21$$
$$42=2\times 21+0$$

Thus, $\gcd(252,105)=21$. □

*Theorem 1.4 (Bézout's Identity)*

For any integers $a$, $b$, and $m$, the linear Diophantine equation (known as the Bézout identity):

$$ax + by = m$$

has integer solutions if and only if $m$ is a multiple of $d$ ($d = \gcd(a, b)$).

When the Bézout identity has solutions, there are infinitely many integer solutions $x$, $y$, each of which is called a Bézout coefficient, and they can be found using the extended Euclidean algorithm. ♡

*Proof* If either $a$ or $b$ is zero, the statement is obviously true.

Without loss of generality, assume both $a$ and $b$ are non-zero.

Let $A = \{xa + yb | x, y \in \mathbb{Z}\}$, next, we will prove that the smallest positive integer in $A$ is $\gcd(a, b)$.

First, $A \cap \mathbb{N}_+$ is non-empty since $a$ and $b$ are non-zero. Since $\mathbb{N}_+$ is well-ordered, $A$ has a smallest positive integer, denoted as $d_0 = x_0a + y_0b$.

Consider any one positive integer $p \in A$, by the division with remainder, there exist integers $q \in \mathbb{N}_+$ and $r \in [0, d_0)$ such that

$$p = qd_0 + r, \quad 0 \leq r < d_0,$$

where $r = p - qd_0 = (p - qx_0a) + (-qy_0b) \in A$.

Therefore, if $r > 0$, it contradicts the minimality of $d_0$. Hence, $r = 0$, which implies that $d_0 \mid p$ for any $p \in A$.

In particular, $d_0 \mid a$ and $d_0 \mid b$, so $d_0$ is a common divisor of $a$ and $b$.

On the other hand, for any positive common divisor $d$ of $a$ and $b$, let $a = kd, b = ld$, then $d_0 = x_0a + y_0b = x_0kd + y_0ld = (x_0k + y_0l)d$, which implies $d \mid d_0$.

Thus, $d_0 = \gcd(a, b)$.

In the equation $ax + by = m$, if $m = m_0d_0$, then the equation has infinitely many integer solutions obviously,

$$\left\{\left(m_0x_0 + \frac{kb}{d}, m_0y_0 - \frac{ka}{d}\right) \mid k \in \mathbb{Z}\right\}.$$

Conversely, if the equation has integer solutions, then $|m| \in A$. Thus, $d_0 \mid |m|$, i.e., $m$ is a multiple of $d_0$. ■

This proof is essentially the process of the extended Euclidean algorithm. Extended Euclidean algorithm not only computes $\gcd(a, b)$, but also finds integers $x$ and $y$ such that

$$ax + by = \gcd(a, b).$$

Using it, we can compute the modular inverse of $a$ modulo $m$ when $\gcd(a, m) = 1$.

## 1.4 Prime Numbers

*Definition 1.5 (Prime Number)*

A **prime number** is a natural number greater than 1 that has no positive divisors other than 1 and itself. In other words, the set of prime numbers is defined as:

$$\{p = ab | p \in \mathbb{N}_+ \setminus \{1\}, a = 1 \text{ or } b = 1\}.$$

If a natural number greater than 1 is not prime, it is called a **composite number**. ♣

$\mathbb{N}_+$ can be divided into three disjoint subsets: $\{1\}$, the set of prime numbers and the set of composite numbers.

To determine whether a number is prime, we introduce primality tests.

*Theorem 1.5 (Trial Division Primality Test (Sieve of Eratosthenes))*

To determine whether a natural number $n > 1$ is prime, it suffices to check for divisibility by all prime numbers less than or equal to $\sqrt{n}$. If $n$ is not divisible by any of these primes, then $n$ is prime; otherwise, it is composite. ♡

Euler's sieve is an optimized version of the Sieve of Eratosthenes for finding all prime numbers up to a given limit $n$. It works by iteratively marking the multiples of each prime number starting from 2, ensuring that each composite number is marked only once. Its procedure is as follows:

1. Create a list of consecutive integers from 2 to $n$.
2. Start with the first number in the list (which is 2).
3. Mark all multiples of this number (except the number itself) as composite.
4. Move to the next unmarked number in the list and repeat step 3 until you reach $\sqrt{n}$.
5. The remaining unmarked numbers in the list are all prime numbers up to $n$.

```
vector<int> euler_sieve(int n){
    vector<bool> is_prime(n+1, true);
    vector<int> primes;

    is_prime[0] = is_prime[1] = false;

    for (int i = 2; i <= n; ++i) {
        if (is_prime[i]) {
            primes.push_back(i);
        }

        for(int p : primes) {
            if (i*p>n) break;
            is_prime[i*p] = false;
            if (i%p==0) break;
        }
    }
    return primes;
}
```

*Theorem 1.6 (Fermat's Little Theorem)*

If $p$ is a prime number and $a$ is an integer not divisible by $p$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Equivalently, for any integer $a$,

$$a^p \equiv a \pmod{p}.$$

♡

## 1.5 Fundamental Theorem of Arithmetic

# Chapter 2 Congruences

# Chapter 3 Quadratic Residues

# Chapter 4 Number Theoretic Functions

# Chapter 5 Prime Numbers

# Chapter 6 Asymptotic Methods and Continued Fractions

# Chapter 7 Diophantine Equations

# Bibliography

[1] 华罗庚. 华罗庚文集 数论卷 II. 北京: 科学出版社, 2010.

[2] 余红兵. 数论. 上海: 华东师范大学出版社, 2011.