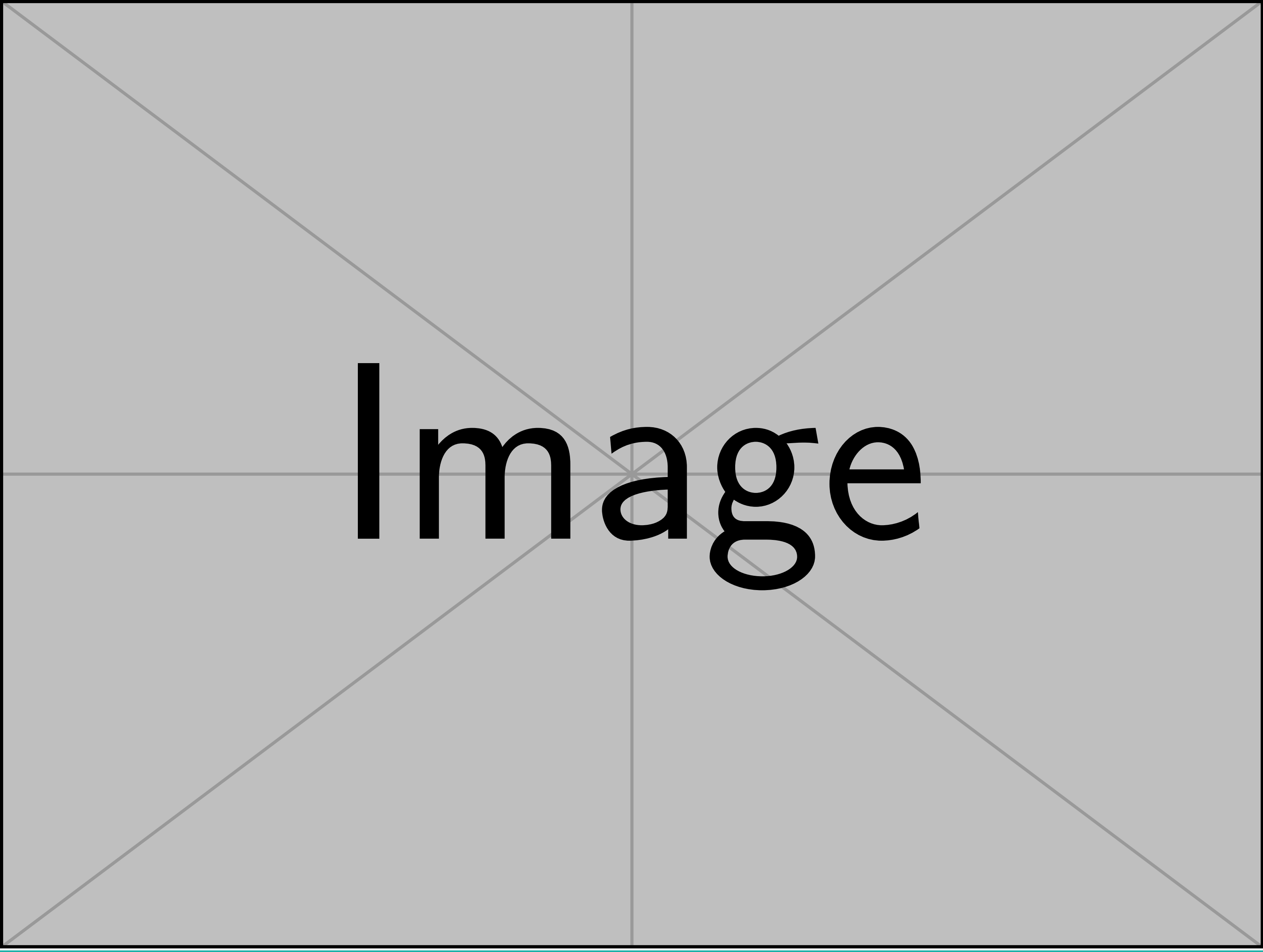

Théorie des Nombres

Author: CatMono

Date: February, 2026

Version: 0.1

Contents

Preface

Version notes are in the table below.

Version	Date	Description
0.1	February, 2026	Initial version

Chapter 1 Integers

1.1 Divisibility and Prime Numbers

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:

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

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

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

♣

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 Algorithm)

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

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

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 $b \ne a, b \ne 1$, then b is called a proper divisor of a.

♡

Property *If $b \ne 0, c \ne 0$, 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.*

1.2 Carry System

Carry system (or positional numeral system) is a method of representing numbers using a radix (or base) r ($r \ge 2$). 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 $0 \le a_i < r$ and $a_k \ne 0$.

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

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:

$$\begin{aligned} 45 \div 2 &= 22 \text{ remainder } 1 \\ 22 \div 2 &= 11 \text{ remainder } 0 \\ 11 \div 2 &= 5 \text{ remainder } 1 \\ 5 \div 2 &= 2 \text{ remainder } 1 \\ 2 \div 2 &= 1 \text{ remainder } 0 \\ 1 \div 2 &= 0 \text{ remainder } 1 \end{aligned}$$

   Reading remainders from bottom to top gives 101101.
   For fractional part 0.625:

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

   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:

$$
\begin{aligned}
&64 \div 3 = 21 \text{ remainder } 1 \\
&21 \div 3 = 7 \text{ remainder } 0 \\
&7 \div 3 = 2 \text{ remainder } 1 \\
&2 \div 3 = 0 \text{ remainder } 2 \quad (\text{replace } 2 \text{ with } Z, \text{ increment quotient to } 1) \\
&1 \div 3 = 0 \text{ remainder } 1
\end{aligned}
$$

   Reading remainders from bottom to top gives $1Z0Z1$. Thus, $64_{10} = (1Z0Z1)_{3b}$.

2. Since $1 \times 3^4 + (-1) \times 3^3 + 0 \times 3^2 + (-1) \times 3^1 + 1 \times 3^0 = 81 - 27 + 0 - 3 + 1 = 52$; thus, $(1Z0Z1)_{3b} = 52_{10}$.

□

1.3 Greatest Common Divisor and Least Common Multiple

1.4 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.