Introduction

Number theory is the study of the set of integers $0, \pm 1, \pm 2, \ldots$, or some of its subsets or extensions. Denote the set of all natural numbers by $\mathbb{N} = \{1, 2, 3, \ldots\}$ and the set of all integers by $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} = -\mathbb{N} \cup \{0\} \cup \mathbb{N}$.

Many of proofs make use of the following property of integers.

The principle of induction. If Q is a set of integers such that

(1) $1 \in Q$,

(2) $n \in Q$ implies $n + 1 \in Q$,

then all positive integers belong to Q.

The well-ordering principle. If A is a nonempty set of positive integers, then A contains a smallest member.

We assume that the reader is familiar with those principles.

Theorem 0.1. *There is no integer between 0 and 1.*

Proof. If the assertion is false, then there is an $a \in \mathbb{Z}$ with $0 < a < 1$. Multiplying through by the positive integer a gives $a^2 \in \mathbb{Z}$ with $0 < a^2 < a$, and similarly we get a^k for all $k \geq 1$. Then the set $A = \{a^k : k \in \mathbb{N}\} \subset \mathbb{N}$ contains a smallest member, say a^{k_0} for some $k_0 \in \mathbb{N}$. However $a^{k_0+1} \in A$ and $a^{k_0+1} < a^{k_0}$. This is a contradiction. Hence there is no integer between 0 and 1. □

This simple fact is quite useful.

Theorem 0.2. *The real number* $e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots = 2.71828\cdots$ *is irrational.*

Proof. If e is rational, then we can write $e = \frac{a}{b}$ with $a, b \in \mathbb{N}$ and $(a, b) = 1$. For any $n \in \mathbb{N}$, we have

$$n!a = n!be = q_n + r_n.$$

where

$$q_n = \left(n! + \frac{n!}{1!} + \frac{n!}{2!} + \cdots + \frac{n!}{n!}\right) b \quad \text{and} \quad r_n = \left(\frac{n!}{(n+1)!} + \frac{n!}{(n+2)!} + \cdots\right) b.$$

Note that $q_n \in \mathbb{Z}$ and hence we have $r_n = n!a - q_n \in \mathbb{Z}$. However we have

$$\begin{aligned}\frac{b}{n+1} < r_n &< \left(\frac{1}{n+1} + \frac{1}{(n+2)(n+1)} + \frac{1}{(n+3)(n+2)} + \cdots\right) b \\ &= \left(\frac{1}{n+1} + \frac{1}{n+1} - \frac{1}{n+2} + \frac{1}{n+2} - \frac{1}{n+3} + \cdots\right) b = \frac{2b}{n+1}.\end{aligned}$$

Take $n > 2b$. Then we have $0 < r_n < 1$. This is a contradiction. Hence e is irrational. □

Arithmetic functions are functions $f : \mathbb{N} \to \mathbb{C}$ which is one of the fundamental concepts in number theory. In Chapter 2, we introduce some important examples of arithmetic functions and discuss their basic properties. We also define the Dirichlet convolution and multiplicative functions. In Chapter 3, the order and average order of magnitude of some important arithmetic functions were given.

Prime number is one of the basic concepts in number theory. Denote $\mathbb{P} = \{2, 3, 5, 7, 11, \ldots\}$ the set of all positive prime numbers. Euler was the first to use analytic arguments for the purpose of studying properties of integers, specifically by constructing generating power series. Euler made use of the divergence of the zeta function and the corresponding product over primes to give a proof of the infinity of prime numbers. This was the beginning of analytic number theory. It was conjectured by Legendre and Gauss that the number of primes not exceeding x satisfies the asymptotic formula

$$\pi(x) := \sum_{p \leq x} 1 \sim \frac{x}{\log x}.$$

This assertion is called the prime number theorem, and it has been proven much later independently by Hadamard and de la Vallée Poussin (1896), based on the celebrated memoir of Riemann on the zeta function. In Chapter 4, an elementary proof of the prime number theorem will be given.

Dirichlet created the theory of L-functions for characters, resulting in the proof of the infinity of primes in arithmetic progressions, which makes him the true father of analytic number theory. In Chapter 8 we define the Dirichlet characters and prove some basic properties of them. We also introduce the Gauss sums and the Pólya–Vinogradov inequality, which concern sums of characters. In Chapter 9, we will prove

$$\sum_{\substack{p \leq x \\ p \equiv a \bmod q}} \frac{\log p}{p} = \frac{1}{\varphi(q)} \log x + O_q(1),$$

as $x \to \infty$, for $a \in \mathbb{Z}$, $q \in \mathbb{N}$ such that $(a, q) = 1$.

CHAPTER 1

Divisibility theory

1.1. Divisibility of integers

Definition 1.1. For $d, n \in \mathbb{Z}$, we say d **divides** n and we write $d \mid n$ if $n = cd$ for some $c \in \mathbb{Z}$. We also say that n is a **multiple** of d, that d is a **divisor** (or **factor**) of n. If d does not divide n then we write $d \nmid n$.

Theorem 1.2 (The division theorem). *If a is positive and b is any integer, there is exactly on pair of integers q and r such that we have*

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

*Here q is called the **quotient** and r the **remainder** when b is divided by a.*

Theorem 1.3. *Let $S \subset \mathbb{Z}$ be any non-empty subset of all integers. Assume that S is closed under subtraction, that is, for any $x, y \in S$ we have $x - y \in S$. Then there exists a unique non-negative integer d such that $S = d\mathbb{Z} = \{0, \pm d, \pm 2d, \ldots\}$.*

This shows that $(\mathbb{Z}, +, \cdot)$ is a principal ideal domain.

1.2. The prime numbers

Definition 1.4. We say ± 1 are the **units**. The **prime numbers** are those integers n for which the conditions

$$n = ab, \quad a, b \in \mathbb{Z}, \quad a, b \text{ not units},$$

cannot be satisfied simultaneously. Numbers that are not unit or prime are called **composite**. Denote the set of all positive prime numbers by $\mathbb{P}$.

Theorem 1.5 (Euclid). *There are infinitely many prime numbers.*

Theorem 1.6 (Fundamental lemma of arithmetic). *Let $p \in \mathbb{P}$ and $a, b \in \mathbb{Z}$. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

1.3. The Fundamental theorem of arithmetic

Theorem 1.7. *Every positive integer $n > 1$ can be represented as a product of prime factors in only one way, apart from the order of the factors.*

By Theorem 1.7 we have the prime-power decomposition of $n > 1$,

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

where the p_i are now distinct primes and the a_i are positive integers. The factor p^a corresponding to a particular prime p in this decomposition is called the p-component of n. Thus $p^a \mid n$, but $p^{a+1} \nmid n$, denoted by $p^a \parallel n$.

Corollary 1.8. *If $n = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ is the prime-power decomposition, then the set of positive divisors of n is the set of numbers of the form $\prod_{i=1}^r p_i^{c_i}$, where $0 \le c_i \le a_i$ for $1 \le i \le r$.*

1.4. The greatest common divisor and the least common multiple

Definition 1.9. Let $m, n \in \mathbb{Z}$, not both zero. The **greatest common divisor** (GCD) of m and n, denoted by (m, n), is the largest integer d such that $d \mid m$ and $d \mid n$.

Theorem 1.10. *Let $m, n \in \mathbb{Z}$, not both zero. Assume $m = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ and $n = p_1^{b_1}p_2^{b_2}\cdots p_r^{b_r}$ with $a_i, b_i \in \mathbb{Z}_{\ge 0}$. Then any common divisor d_1 of m and n, i.e., $d_1 \mid a$ and $d_1 \mid b$, has the following form*

$$d_1 = up_1^{c_1}p_2^{c_2}\cdots p_r^{c_r}, \quad u = \pm 1,\ c_i \in \mathbb{Z}_{\ge 0},\ c_i \le \min(a_i, b_i).$$

In particular, we have $(m, n) = \prod_{1 \le i \le r} p_i^{\min(a_i,b_i)}$.

Corollary 1.11. *Let $m, n \in \mathbb{Z}$, not both zero. Let $d = (m, n)$ and d_1 a common divisor of m and n. Then $d_1 \mid d$.*

Definition 1.12. Let $m, n \in \mathbb{Z} \setminus \{0\}$. The **least common multiple** (LCM) of m and n, denoted by $[m, n]$, is the smallest positive integer ℓ such that $m \mid \ell$ and $n \mid \ell$. If $m = 0$ or $n = 0$, we define their least common multiple $[m, n] = 0$.

Theorem 1.13. *Let $m, n \in \mathbb{Z} \setminus \{0\}$. Then we have*

$$[m, n] = \frac{|mn|}{(m, n)}.$$

1.5. The functions $[x]$ and $\{x\}$

An important function in number theory is the function $[x]$ which represent the largest integer not exceeding x. In other word, for each $x \in \mathbb{R}$, $[x]$ is the unique integer such that $x - 1 < [x] \le x < [x] + 1$. Let $\{x\} = x - [x]$ denote the fractional part of x. We have the following basic properties:

a) $x = [x] + \{x\}$, where $0 \le \{x\} < 1$.

b) $[x + n] = [x] + n$, if $n \in \mathbb{Z}$.

c) $[x] + [-x] = \begin{cases} 0, & \text{if } x \text{ is an integer,} \\ -1, & \text{otherwise.} \end{cases}$

d) $[x] + [y] \le [x + y]$.

Lemma 1.14. *Let $x \in \mathbb{R}^+$ and $a \in \mathbb{N}$. Then the number of positive integers not exceeding x which are divisible by a is $[\frac{x}{a}]$.*

Proof. The positive integers which are divisible by a is

$$\{a, 2a, 3a, \ldots\}$$

Those integers which is less than x are $\{a, 2a, \ldots, [\frac{x}{a}]a\}$. This completes the proof. □

Let $n \in \mathbb{N}$. The factorial of n, denoted by $n!$, is the product of all positive integers less than or equal to n:

$$n! = n(n-1)(n-2)\cdots 2 \cdot 1.$$

We have the following prime-power decomposition of $n!$.

THEOREM 1.15. *Let $n \in \mathbb{N}$. Denote $n! = \prod_{p \le n} p^{h(p,n)}$, then we have*

$$h(p,n) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right].$$

PROOF. Given prime p and positive integer n. Denote $p^r \parallel n$ if $p^r \mid n$ and $p^{r+1} \nmid n$. Hence we have

$$h(p,n) = \sum_{k=1}^{\infty} \sum_{\substack{1 \le m \le n \\ p^k \parallel m}} k = \sum_{1 \le m \le n} \sum_{\substack{k=1 \\ p^k \parallel m}}^{\infty} k = \sum_{1 \le m \le n} \sum_{\substack{k=1 \\ p^k \mid m}}^{\infty} 1 = \sum_{k=1}^{\infty} \sum_{\substack{1 \le m \le n \\ p^k \mid m}} 1.$$

By Lemma 1.14, we have

$$h(p,n) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right],$$

as claimed. □

THEOREM 1.16. *Let $a \in \mathbb{Z}$ and $k \in \mathbb{N}$. Then we have*

$$\frac{(a+1)(a+2)\cdots(a+k)}{k!} \in \mathbb{Z}.$$

PROOF. If $a \in [-k, -1]$, then $\frac{(a+1)(a+2)\cdots(a+k)}{k!} = 0 \in \mathbb{Z}$. If $a = 0$, then $\frac{(a+1)(a+2)\cdots(a+k)}{k!} = 1 \in \mathbb{Z}$. If $a \ge 1$, then by Theorem 1.15, we have

$$\frac{(a+1)(a+2)\cdots(a+k)}{k!} = \frac{(a+k)!}{a!k!} = \prod_{p \le (a+k)} p^{h(p,a+k)-h(p,a)-h(p,k)}.$$

Note that

$$h(p,a+k) - h(p,a) - h(p,k) = \sum_{j=1}^{\infty} \left(\left[\frac{a+k}{p^j} \right] - \left[\frac{a}{p^j} \right] - \left[\frac{k}{p^j} \right] \right) \in \mathbb{Z}_{\ge 0}.$$

Hence $\frac{(a+1)(a+2)\cdots(a+k)}{k!} \in \mathbb{Z}$. If $a < -k$, then $\frac{(a+1)(a+2)\cdots(a+k)}{k!} = \frac{(-1)^k(-a-1)(-a-2)\cdots(-a-k)}{k!} \in \mathbb{Z}$. This completes the proof. □

THEOREM 1.17. *Let $p \in \mathbb{P}$. Then for any $a \in \mathbb{Z}$, we have $p \mid (a^p - a)$.*

PROOF. If $p \mid (a-b)$, then $p \mid ((a^p - a) - (b^p - b))$. Indeed, we have $(a^p - a) - (b^p - b) = (a-b)(a^{p-1} + a^{p-2}b + \cdots + b^{p-1} + 1)$. So we only need to prove $p \mid (a^p - a)$ for $0 \le a \le p-1$.

If $a = 0$ then $a^p - a = 0$ and $p \mid 0$. Now assume $p \mid (a^p - a)$. Note that we have

$$(a+1)^p - (a+1) = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k + 1 - a - 1 = (a^p - a) + \sum_{k=1}^{p-1} \binom{p}{k} a^k,$$

and $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ and hence $p \mid \binom{p}{k}$ for $1 \le k \le p-1$. So we have $p \mid (a+1)^p - (a+1)$. By induction, we complete the proof. □