Modern Number Theory

Qiū Cáiyóng

Number theory is the study of integers. Modern number theory uses modern mathematics tools to study integers.

邱才[illegible].

Contents

Chapter 1

Unique Factorization Domains

Arithmetics can be done in an abstract setting:

Definition 1.0.1 (Ring, domain and fields)**.** A **ring** is a set R, together with two operations $+ : R \times R \to R$ and $\times : \times R \to R$. But instead of writing $+(a, b)$ and $\times(a, b)$, we write $a + b$ and ab. These two operations has to satisfy the following axioms:

Associativity	$(a + b) + c = a + (b + c), (ab)c = a(bc)$ for all $a, b, c \in R$
Commutativity	$a + b = b + a, ab = ba$ for all $a, b \in R$
Identity	There are two elements $0_R, 1_R \in R$ such that $0_R + a = a, 1_R a = a$ for all $a \in R$
Inverse	For all $a \in R$, there is an element $-a \in R$ such that $a + (-a) = 0_R$.
Distributivity	$a(b + c) = ab + ac$ for all $a, b, c \in R$.

If $a, b \in R$ are both nonzero implies that ab is nonzero, we say that the ring R is a **domain** or an **integral domain**.

If $0 \neq a \in R$ is nonzero and there is an element $a^{-1} \in R$ such that $aa^{-1} = 1_R$ then we say that a is a **unit** in R. If every nonzero element is a unit, then we say the ring R is a **field**.

$a0_R = 0_R$ is true for any $a \in R$ and any ring R. In a ring, it is allowed that $1_R = 0_R$, although we will then have a boring ring: there is only one element $1_R = 0_R$ since $a = a1_R = a0_R = 0_R$.

Strictly speaking, what we've defined are the so-called commutative rings. If we don't require that $ab = ba$, then we have the notion of a general ring. But we will always assume that all rings are commutative. (Sometimes mathematicians do not even require the existence of 1_R! Things get weird when R does not have an identity.)

Example 1.0.1. $\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ are rings. $\mathbf{N}, \mathbf{N}_+$ are not rings. $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ are fields.

Example 1.0.2. If R is a ring, we define the **polynomial ring with coefficients in** R by

$$R[x] := \{\sum_{i=0}^{n} a_i x^i : n \in \mathbf{N}, a_i \in R\}$$

Addition and multiplication is defined by

$$\left(\sum_{i=0}^{n} a_i x^i\right) + \left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i=0}^{n} (a_i + b_i) x^i$$

$$\left(\sum_{i=0}^{n} a_i x^i\right) \left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i \in \mathbf{N}} \sum_{\alpha+\beta=i} a_\alpha b_\beta x^i$$

The $R[x]$ is again a ring. For example, when $R = \mathbf{R}$ we get the ring of polynomials with real coefficients; when $R = \mathbf{C}$ we get the ring of polynomials with complex coefficients; when $R = \mathbf{Z}$ we get the ring of polynomials with integer coefficients.

By induction, $(R[x])[y]$ is also a ring, just have two variables. We also write $(R[x])[y]$ simply by $R[x, y]$.

In this chapter, we studies four rings: $\mathbf{Z}, k[x], \mathbf{Z}[i], \mathbf{Z}[\omega]$. They can be treated uniformly, since all of them are of a special class of rings: UFD (Unique Factorization Domain).

(Actually, Fields are EDs (Euclidean domain), EDs are PIDs (Principal Ideal Domain), PIDs are UFDs, UFDs are domains. $\mathbf{Z}, k[x], \mathbf{Z}[i], \mathbf{Z}[\omega]$ are all Euclidean domains.)

Lemma 1.0.1 (Gauss)**.** If R is a UFD, then so do $R[x]$.

1.1 Unique factorization in Z

We say that a number a divides a number b is there is a number c such that $b = ac$. If a divides b, we use the notation $a|b$. For example, $2|8, 3|15$, but $6 \not| 21$. We say that a number p is a prime if its only divisors are 1 and p. The first prime numbers are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, \ldots$. Let $\pi(x)$ be the number of primes between 1 and x. What can be said about the function $\pi(x)$? The prime number theorem, we proved by J.Hadamard and independently Ch.J. de la Vallé Poussin says that

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$$

The theorem of unique factorization is sometimes referred to as the fundamental theorem of arithmetic. As an illustration consider the number 180. We have

$180 = 2^2 \times 3^2 \times 5$. Uniqueness in this case means that the only primes dividing 180 are $2, 3, 5$ and that the exponents $2, 2, 1$ are uniquely determined by 180.

Z will denote the ring of integers, i.e., the set $0 \pm 1, \pm 2, \pm 3, \ldots,$ together with the usual definition of sum and product. It will be more convenient to work with **Z** rather than restricting ourselves to the positive integers. The notion of divisibility carries over with no difficulty to **Z**. We shall not consider 1 or -1 as primes, this is simply a useful convention. Note that 1 and -1 divide everything and that they are the only integers with this property. They are called the units of **Z**. Notice also that every nonzero integer divides zero.

1.2 Unique factorization in $k[x]$

1.3 Unique factorization in a PID

1.4 Unique factorization in Gauss integers

1.5 Unique factorization in Eisenstein integers

Chapter 2

Applications of Unique Factorization

2.1 Infinitely many primes in $\mathbf{Z}$

2.2 Arithmetic functions

2.3 Divergence of $\sum \frac{1}{p}$

Chapter 3

Congruence

3.1 Congruence in $\mathbb{Z}$

3.2 Congruence equations

3.3 The Chinese remainder theorem

Chapter 4

Primitive Roots

4.1 Primitive roots

4.2 nth power residues

Chapter 5

Quadratic Reciprocity

5.1 Quadratic residues

5.2 Law of quadratic reciprocity

5.3 Proof of the law of quadratic reciprocity

Chapter 6

Gauss and Jacobi Sums

6.1 Algebraic numbers and algebraic integers

6.2 The quadratic character of 2

6.3 Quadratic Gauss sums

6.4 The sign of the quadratic Gauss sum

6.5 Multiplicative characters

6.6 Gauss sums

6.7 Jacobi sums

6.8 Applications

Chapter 7

Cubic Reciprocity

7.1 Residue class rings

7.2 Cubic residue character

7.3 Proofs of the low of cubic reciprocity

7.4 The cubic character of 2

Chapter 8

Biquadratic Reciprocity

8.1 Preliminaries

8.2 The quartic residue symbol

8.3 Law of biquadratic reciprocity

8.4 Rational biquadratic reciprocity

Chapter 9

Bonus Chapter: Constructibility of Regular Polygons