

Number Theory

Ikhan Choi

May 27, 2022

Contents

I	Quadratic reciprocity	2
1	Quadratic residue	3
1.1	Legendre symbol	3
1.2	Gauss sum	3
2	Binary quadratic forms	4
2.1	Representation problems	4
3	Class groups	5
II	Multiplicative number theory	6
4	Arithmetic functions	7
5	Dirichlet's theorem	8
6	Prime number theorem	9
III	Quadratic Diophantine equations	10
7	Pell's equation	11
7.1	Continued fraction	11
8	p -adic numbers	12
8.1	Hensel lemma	12
9	Local-global principle	13
9.1	Hasse-Minkowski theorem	13
IV	Elliptic curves	14
10	Elliptic curves over \mathbb{C}	15
11	Elliptic curves over \mathbb{Q}	16
11.1	Finitely generatedness	16
11.2	Integral solutions	16
12	Elliptic curves over \mathbb{F}_p	17

Part I

Quadratic reciprocity

Chapter 1

Quadratic residue

1.1 Legendre symbol

1.2 Gauss sum

Exercises

- 1.1. There is no integral solution of the equation $x^7 + 7 = y^2$.
- 1.2. If $\frac{x^2+y^2+z^2}{xy+yz+zx}$ is an integer, then it is not divided by 3.
- 1.3. There is no non-trivial integral solution of $x^4 - y^4 = z^2$.

Chapter 2

Binary quadratic forms

2.1 Representation problems

Chapter 3

Class groups

Exercises

3.1 (Mordell equation with no solutions). (a) $y^2 = x^3 + 7$ has no integral solutions.

3.2 (Mordell equation with solutions). (a) $y^2 = x^3 - 2$ has only two solutions.

Part II

Multiplicative number theory

Chapter 4

Arithmetic functions

Chapter 5

Dirichlet's theorem

Chapter 6

Prime number theorem

Part III

Quadratic Diophantine equations

Chapter 7

Pell's equation

7.1 Continued fraction

Diophantine approximation, Thue theorem

Chapter 8

p -adic numbers

8.1 Hensel lemma

Chapter 9

Local-global principle

9.1 Hasse-Minkowski theorem

Part IV

Elliptic curves

Chapter 10

Elliptic curves over \mathbb{C}

Chapter 11

Elliptic curves over \mathbb{Q}

11.1 Finitely generatedness

Mordell-Weil, Mazur torsion

11.2 Integral solutions

Nagell-Lutz, Siegel, Baker's bound

Chapter 12

Elliptic curves over \mathbb{F}_p