Number Theory

Ikhan Choi

July 22, 2022

Contents

Part I

Quadratic reciprocity

Chapter 1

Quadratic residue

1.1 Legendre symbol

1.1.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad (p \neq 2).$$

$$\left(\frac{2}{p}\right) = 1 \text{ if and only if } p \equiv \pm 1 \pmod 8 \quad (p \neq 2).$$

$$\left(\frac{3}{p}\right) = 1 \text{ if and only if } p \equiv \pm 1 \pmod{12} \quad (p \neq 2).$$

$$\left(\frac{5}{p}\right) = 1 \text{ if and only if } p \equiv \pm 1 \pmod 5 \quad (p \neq 2).$$

1.2.

$$x^2 \equiv 0, 1 \pmod{3, 4}$$

$$x^2 \equiv 0, 1, 4 \pmod{5, 8}$$

$$x^2 \equiv 0, 1, 3, 4 \pmod 6$$

$$x^2 \equiv 0, 1, 2, 4 \pmod 7$$

$$x^2 \equiv 0, 1, 4, 7 \pmod 9$$

$$x^2 \equiv 0, 1, 4, 9 \pmod{12}$$

1.2 Gauss sum

Higher order sides: At least a prime divisor of f with a congruence (e.g. $4k+3$) Quantratic sides: Every prime divisor of f must satisfy a congruence (e.g. $4k+1$)

Exercises

1.3 (Dirichlet theorems by quadratic reciprocity). (a) For $f(x) \in \mathbb{Z}[x]$, there exist infinitely many primes p such that $p \mid f(x)$ for some x.

(b) There are infinitely many primes p such that $p \equiv 1 \pmod 4$.

Problems

1. Show that if $\frac{x^2+y^2+z^2}{xy+yz+zx}$ is an integer, then it is not divided by three.
2. 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

3.1 (Heegner number). There are only nine numbers

$$-1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Exercises

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

3.3 (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 $\mathbb{F}_p$