Number Theory

Ikhan Choi

June 8, 2023

Contents

Part I

Quadratic reciprocity

Chapter 1

Congruence

1.1

1.1 (Computation with binomial theorem).

Chapter 2

Quadratic residue

2.1 Legendre symbol

2.1 (Supplental cases of Legendre symbol)**.** Let p be an odd prime.

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

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

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

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

2.2.

$$
\begin{aligned}
x^2 &\equiv 0,1 \pmod{3,4} \\
x^2 &\equiv 0,1,4 \pmod{5,8} \\
x^2 &\equiv 0,1,3,4 \pmod 6 \\
x^2 &\equiv 0,1,2,4 \pmod 7 \\
x^2 &\equiv 0,1,4,7 \pmod 9 \\
x^2 &\equiv 0,1,4,9 \pmod{12}
\end{aligned}
$$

2.2 Quadratic reciprocity

2.3. Let q be a prime relatively prime to p.

(a) There is a unique non-trivial group homomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$.

(b) $\left(\frac{q}{p}\right) = 1$ if and only if q belongs to the kernel of $(\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$.

2.4 (Quadratic Gauss sum)**.** Let p be an odd prime and a an integer. The *quadratic Gauss sum* is

$$g(a;p) := \sum_{n=0}^{p-1} \zeta_p^{an^2},$$

where $\zeta_p := e^{2\pi i/p}$ is a primitive pth root of unity. Define $p^* := (-1)^{\frac{p-1}{2}} p$.

(a) $g(1,p) = \sqrt{p^*}$. (Eisenstein's proof?)

(b) $\mathbb{Q}(\sqrt{p^*}) < \mathbb{Q}(\zeta_p)$.

2.5 (Splitting of primes in quadratic extension)**.** Let q be a prime relatively prime to p.

(a) q splits in $\mathbb{Q}(\sqrt{p^*})$

Exercises

2.6 (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 $p \equiv 1 \pmod 4$.

2.7. $y^2 = f(x)$

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. $4k+1$)

2.8 (Primes of the form $x^2 - ny^2$). (It is a very important problem in listing primes in $\mathcal{O}_K$) (Want to describe the surjective homomorphism $\operatorname{Spec}\mathbb{Z}[i] \to \operatorname{Spec}\mathbb{Z}$)

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 3

Binary quadratic forms

3.1 Reduced forms

3.2 Indefinite forms

3.3 Ideal class group

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 $\mathbb{F}_p$