UNIVERSITY OF CALGARY

Numerical Tests of Two Conjectures in Fake Real Quadratic Orders

by

Hongyan Wang

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF MASTER OF SCIENCE

GRADUATE PROGRAM IN MATHEMATICS AND STATISTICS

CALGARY, ALBERTA

January, 2017

Abstract

A fake real quadratic order is defined based on an imaginary quadratic field and a prime p but behaves similarly to real quadratic orders. Two conjectures regarding fake real quadratic orders are discussed in the thesis. The first one is the Cohen-Lenstra heuristic. Our computation showed that for fixed p, the proportion of fake real quadratic orders for which the odd part of the class number is one converges to $C = 0.754458...$, which equals exactly the proportion of real quadratic fields for which the odd part of the class number is one. The second one is the Ankeny-Artin-Chowla conjecture, which states that $D \nmid b$ where b is the second coefficient of the fundamental unit in the real quadratic field $\mathbb{Q}(\sqrt{D})$. No counterexamples have been found in real quadratic fields but we found numerous counterexamples in fake real quadratic orders and this is evidence that the conjecture is false for real quadratic fields.

Acknowledgements

I would like to show a deep appreciation to my supervisors, Dr. Renate Scheidler and Dr. Michael J. Jacobson, Jr. Without their encouragement and help, I would not have been able to start, not to mention completing this. Thanks Dr. Cunningham and Dr. Greenberg for their comments on my thesis.

Thanks to Anton, who shared his data and codes with me and helped me debug my program. Without his generous help, I would not have finished this on time.

Thanks Dmitri Rozmanov, Paul Wellings, Christopher Mag-Ata, especially Doug Phillips, who spent countless hours helping me test my programs on different systems.

Thanks to the Department of Mathematics and Statistics of the University of Calgary, who made it possible to accomplish this thesis.

Many thanks to Henri Cohen, who provided his unpublished manuscript on fake real quadratic orders. He just made everything much easier. Thanks to Monireh and Majid, who gave me insight into how to solve difficult problems. Thanks to Mark, who shared his perfect thesis Latex template with me.

Thanks to my friends, Jialin, Yuan, Kunlin, Jixian, Ruike, for their support throughout my years in graduate studies. They made my life more fun.

Finally, many thanks to my parents and my dear brother. Without their understanding, my life would be more difficult.

Table of Contents

List of Figures and Illustrations

List of Tables

List of Symbols, Abbreviations and Nomenclature

Symbol or abbreviation	Definition
AAC	Ankeny-Artin-Chowla
CL	Cohen-Lenstra

Chapter 1

Overview

The quadratic field is a classical mathematical object that has been studied for two centuries [Mil14, p. 7]. A quadratic field is a number field K of degree two over $\mathbb{Q}$. It is normally denoted as $K = \mathbb{Q}(\sqrt{D})$, and any number in K can be written as $a + b\sqrt{D}$ where a and b are rational numbers. If $D > 0$, K is called a real quadratic field and when $D < 0$, K is called an imaginary quadratic field. There are already numerous nice results about quadratic fields regarding the unit group, prime factorizations, ideals, class numbers etc. Real and imaginary quadratic fields behave quite differently. The unit group of an imaginary quadratic field is finite while the unit group of a real quadratic field is infinite. A real quadratic field has a group-like structure called infrastructure while imaginary quadratic fields have no such property. A lot is also unknown about quadratic fields. Some conjectures like the Gauss conjecture and the Cohen-Lenstra heuristic regarding class numbers are still open problems [CL84]. The search for counterexamples to the Ankeny-Artin-Chowla conjecture has never stopped [vdPtRW01].

The idea of fake real quadratic orders was proposed by Henri Cohen in his unpublished manuscript [Coh13]. He suggested that if a prime p splits in the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field, it might be interesting to study the structure of $\mathcal{O}_K[\mathfrak{p}^{-1}]$ where $\mathfrak{p}$ is a prime ideal above p. Cohen called the ring $\mathcal{O}_K[\mathfrak{p}^{-1}]$ a fake real quadratic order, and let

$\mathcal{O}_{K,p}$ be the shorthand for it [Coh13]. Though the definition is based on imaginary quadratic fields, Cohen observed that the class group and unit group structures are similar to those of real quadratic orders. Cohen gave analogues to some open questions and found similarities and differences between real quadratic orders and fake real quadratic orders.

This chapter is organized as follows. In Section 1.1, we describe the motivation of the study of fake real quadratic orders, followed by previous work that has been done in this field. In Section 1.2, our contributions to this field are described. Section 1.3 outlines the organization of the thesis.

1.1 Motivation and Previous Work

The idea of fake real quadratic orders is fairly new and there are still a lot of unknown things to discover. The concept of fake real quadratic orders was proposed by Cohen in his manuscript [Coh13] and to date has been only studied by Richard Oh in his PhD thesis [Oh14]. Cohen gave the definition and basic theorems concerning fake real quadratic orders. In his thesis, Oh gave detailed proofs of all the theorems. Many proofs can be found regarding generalizations of fake real quadratic orders in [Coh00, Ch.7].

The similarity with real quadratic orders gives us a perspective to study fake real quadratic orders. Let $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field and $\mathcal{O}_K$ be its ring of integers. Cohen described the unit group structure of $\mathcal{O}_{K,p}$ and found that there exists a bijection between integral ideals of $\mathcal{O}_{K,p}$ and integral ideals of $\mathcal{O}_K$ that are coprime to $\mathfrak{p}$. Since the class number formula is known for imaginary quadratic fields, this relation gives us the class number formula for $\mathcal{O}_{K,p}$ as well as determines the class group structure of $\mathcal{O}_{K,p}$.

How to compute the fundamental unit of $\mathcal{O}_{K,p}$ is another interesting problem. Oh proved that the fundamental unit is a generator of $\mathfrak{p}^n$ where n is the order of the ideal class of $\mathfrak{p} \subset \mathcal{O}_K$ [Oh14, Proposition 1.2]. So we can find the fundamental unit by looking for a generator of $\mathfrak{p}^n$. Alternatively, the fundamental unit has the form $x + y\sqrt{D}$ where $x, y \in (\frac{1}{2})\mathbb{Z}$. So it

can be computed by solving the Diophantine Equation $x^2 + Dy^2 = p^n$. In a real quadratic field, the infrastructure gives us an easier way to find the fundamental unit. Since fake real quadratic orders behave similarly to real quadratic orders, Oh expected the existence of infrastructures in $\mathcal{O}_{K,p}$ [Oh14], though he did not give a description of such group-like structures.

In his manuscript [Coh13], Cohen gave analogues to the Cohen-Lenstra heuristics for fake real quadratic orders. Let p-Cohen-Lenstra heuristics be the shorthand for the heuristic in fake real quadratic orders. Cohen and Lenstra hypothesized that the proportion of real quadratic fields for which the odd part of the class number [1] is one should exist and be equal to a constant number $C = 0.7544...$ [CL84]. For fake real quadratic orders, Cohen suggested that for a fixed p, the proportion of $\mathcal{O}_{K,p}$ for which the odd part of the class number is one should also exist and be equal to $C = 0.7544....$ He performed computations for $|D|$ up to 2^{28}, $p < 30$ and the proportion did converge to C for each p. The convergence is quite slow and even the proportion nearest to C is greater than 0.76. Cohen gave two functions to describe the proportion convergence rate, $0.754458 + \frac{80}{\log(x)^3}$ and $0.754458 + \frac{0.49}{x^{1/5}}$, where x is an upper bound on $|D|$. However, it is difficult to compare these two functions when the upper bound on $|D|$ is small.

One more motivation for investigating fake real quadratic orders is the Ankeny-Artin-Chowla conjecture, which states that $D \nmid b$ where b is the second coefficient of the fundamental unit in the real quadratic field $\mathbb{Q}(\sqrt{D})$. Let p-Ankeny-Artin-Chowla conjecture be the shorthand notation for the conjecture in fake real quadratic orders. Many people believe that the Ankeny-Artin-Chowla conjecture is true since no counterexamples have been found. But counterexamples were found for fake real quadratic orders. Cohen performed experiments for $p < 1000$ and $|D| < 1072000$ and found several counterexamples. Since the upper bound on $|D|$ in Cohen's experiments is quite small, it might be reasonable to hypothesize that the p-Ankeny-Artin-Chowla conjecture holds for large $|D|$. If the conjecture does not hold for

[1] The odd part of a class number is the largest odd divisor of the class number.

any D, it will be interesting to investigate the number of counterexamples for each D.

Based on the studies that have been done in fake real quadratic orders, we can summarize similarities between fake real quadratic orders and real quadratic orders as follows: The first similarity lies in the structures of their unit groups. We know that every unit is a power of the fundamental unit up to sign in a real quadratic order. In a fake real quadratic order $\mathcal{O}_{K,p}$, if we look at the units modulo the units in $\mathcal{O}_K$, each unit can also be written as a power of the fundamental unit. The existence of infrastructures in both real and fake real quadratic orders implies one more similarity. These two similarities are discussed in Chapter 3. In addition, the mean numbers of three-torsion elements in both real and fake real quadratic orders are the same [Oh14, p. 26]. Another similarity lies in the statistical behaviours regarding the Cohen-Lenstra heuristics, which is discussed in more detail in Chapter 4.

There are also a few subtle differences between real quadratic orders and fake real quadratic orders. Based on the definitions of regulators, the regulator in a real quadratic order is a real number while the regulator in a fake real quadratic order is an integer. Moreover, the fundamental unit in a fake real quadratic order can be found by computing a generator of $\mathfrak{p}^{o(\mathfrak{p})}$, but there is no such prime ideal $\mathfrak{p}$ in a real quadratic order. These are discussed in detail in Chapter 3.

1.2 Contributions

In this thesis, we give a description of infrastructures in fake real quadratic orders. According to our study, the infrastructure in $\mathcal{O}_{K,p}$ does not provides us with a faster algorithm to find the fundamental unit than reducing $\mathfrak{p}^n$.

For the p-Cohen-Lenstra heuristics, Cohen performed experiments to show that the conjecture seems to be true. Though he only did computation for all the prime discriminants less than 2^{28}, the result still looks convincing. In this thesis, the author did experiments for all the discriminants less than 2^{40} with $p = 2, 3, 5, 7, 11, 101, 1009$, which strongly support

the p-Cohen-Lenstra conjecture. With such a large data set, we also investigated the convergence rate by studying those two functions given by Cohen. It seems like the function with powers of $\log(x)$ is slightly better than the other one.

Since a fake real quadratic order is defined based on two parameters, D and p, another perspective to look at the p-Cohen-Lenstra heuristic is to fix D and find the proportion of $\mathcal{O}_{K,p}$ for which the odd part of the class number is one for p up to an arbitrarily large number. Certainly, it is reasonable to believe that the proportion does not converge to $C = 0.7544....$ In fact, our computations showed that the proportion is determined by the class group structure of $\mathcal{O}_K$.

For the p-Ankeny-Artin-Chowla conjecture, Cohen found a few counterexamples when checking all the prime discriminants less than 1072000 and all the primes less than 1000. The author did computations for all discriminants less than 2^{40} with primes $p = 2, 3, 5, 7, 11, 101,$ 1009 and only one counterexample was found. An experiment was also performed for the discriminants less than $10 \cdot 2^{28}$ with all primes less than 30000. In this case, thousands of counterexamples were found. A few counterexamples with large discriminants were also found, which implies that the p-Ankeny-Artin-Chowla conjecture might not hold for any discriminant, even for extremely large ones. The author also found that for a fixed D, the proportion of counterexamples converges to $1/|D|$, which agrees with the expected proportion if the b coefficients of fundamental units were randomly distributed in the integers. Since fake real quadratic orders behave similarly to real quadratic orders, those counterexamples may be an evidence to support that the Ankeny-Artin-Chowla conjecture does not hold for real quadratic fields.

1.3 Organization of the Thesis

The thesis is organized as follows. Chapter 2 contains the fundamental background of real and imaginary quadratic fields. The unit group, the ideal class and the infrastructure are

discussed. In Chapter 3, we present the definition of and basic theorems about fake real quadratic orders. Most of the results are from the unpublished manuscript [Coh13] while the proofs of most theorems are credited to Oh [Oh14]. In Section 3.4, we give an analogue to the infrastructure in fake real quadratic orders. At the end of Chapter 3, the p-Cohen-Lenstra heuristics and the p-Ankeny-Artin-Chowla conjecture are discussed. Implementation and all the numerical results are described in Chapter 4. Chapter 5 concludes the thesis and gives an overview of future work.

Chapter 2

Background on Quadratic Fields

Before looking at fake real quadratic orders, we first present some fundamental facts about quadratic fields. Fake real quadratic orders are defined based on imaginary quadratic fields and behave similarly to real quadratic orders. The introduction in this chapter helps us understand the results in the next chapter.

2.1 Definitions

Definition 2.1. [JW09, p. 77] A quadratic number field is an extension K of $\mathbb{Q}$ of degree 2. K can be written as $K = \mathbb{Q}(\sqrt{D})$ where D is not a square of another rational number. The elements of K are of the form $a + b\sqrt{D}$ with $a, b \in \mathbb{Q}$

For $\alpha = a + b\sqrt{D} \in K$, the conjugate of α is defined as $\overline{\alpha} = a - b\sqrt{D}$ and the norm of α is $N(\alpha) = \alpha\overline{\alpha}$.

In this thesis, we exclusively discuss quadratic fields and fake real quadratic orders when D is a fundamental discriminant. So $D \equiv 1 \pmod 4$ or $D \equiv 8, 12 \pmod{16}$ and D is not divisible by the square of any odd prime number. Suppose that $D = f^2 D_0$ where D_0 is square-free. Then we have $f = 1, 2$ and

$$D_0 = \begin{cases} \frac{D}{4} & : \quad D \not\equiv 1 \pmod 4 \\ D & : \quad D \equiv 1 \pmod 4 \end{cases}$$

Put

$$r = \begin{cases} 1 & : \quad D \not\equiv 1 \pmod 4 \\ 2 & : \quad D \equiv 1 \pmod 4 \end{cases} \tag{2.1}$$

and define $\omega_0 = (r - 1 + \sqrt{D_0})/r$.

That is

$$\omega_0 = \begin{cases} \frac{\sqrt{D}}{2} & : \quad D \not\equiv 1 \pmod 4 \\ \frac{1+\sqrt{D}}{2} & : \quad D \equiv 1 \pmod 4 \end{cases}$$

Definition 2.2. [JW09, p. 76] The ring of integers, $\mathcal{O}_K$, of K is the set of all elements of K which are roots of a monic polynomial in $\mathbb{Z}[x]$.

It has been proved that $\mathcal{O}_K$ is finitely generated as a $\mathbb{Z}$-module by 1 and ω_0; that is, $\mathcal{O}_K = [1, \omega_0]$. So any element in $\mathcal{O}_K$ has the form $x + y\sqrt{D}$ where $x, y \in (\frac{1}{2})\mathbb{Z}$. $\mathcal{O}_K$ is also known as the maximal order of K. In this thesis, we just write ω for ω_0.

The first concern to us will be the units in $\mathcal{O}_K$. For $\alpha, \beta \in \mathcal{O}_K$ with α non-zero, we write $\alpha \mid \beta$ if α is a divisor of β in $\mathcal{O}_K$.

Definition 2.3. [JW09, p. 77] η is said to be a unit of $\mathcal{O}_K$ if $\eta|1$ in $\mathcal{O}_K$.

Clearly, units are the elements in $\mathcal{O}_K$ with norm ± 1. Denote the set of all units in $\mathcal{O}_K$ by $\mathcal{O}_K^*$. It has been proved [JW09, p. 78] that if $D < 0$, then

$$\mathcal{O}_K^* = \begin{cases} \{1, -1, \zeta, \zeta^2, -\zeta, -\zeta^2 : \zeta^2 + \zeta + 1 = 0\} & : \quad D = -3 \\ \{1, -1, i, -i : i^2 + 1 = 0\} & : \quad D = -4 \\ \{1, -1\} & : \quad D < -4 \end{cases}$$

where $\zeta \in K$. That is

$$| \mathcal{O}_K^* | = \begin{cases} 6 & : \quad D = -3 \\ 4 & : \quad D = -4 \\ 2 & : \quad D < -4 \end{cases}$$

If $D > 0$, any unit can be written as $\eta = \pm\epsilon_D^n$ where ϵ_D is a fundamental unit of $\mathcal{O}_K$. For example, in $K = \mathbb{Q}(\sqrt{5})$, $\epsilon = \frac{1+\sqrt{5}}{2}$ is a fundamental unit. Then all the units η are given by $\pm(\frac{1+\sqrt{5}}{2})^n$. It is clear that a real quadratic field has infinitely many units while an imaginary quadratic field has a finite number of units.

2.2 Ideals of $\mathcal{O}_K$

This section contains a brief introduction to ideals of $\mathcal{O}_K$. An important type of ideal, called reduced ideal, will be discussed in detail. We describe ideal multiplication and ideal reduction algorithms at the end of this section.

Definition 2.4. [JW09, p. 84] An (integral) ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is an additive subgroup of $\mathcal{O}_K$ such that $\xi\mathfrak{a} \subseteq \mathfrak{a}$ for any $\xi \in \mathcal{O}_K$.

Assume $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of $\mathcal{O}_K$, then ideal multiplication can be defined as follows,

$$\mathfrak{ab} = \{a_1b_1 + a_2b_2 + ... + a_nb_n : a_i \in \mathfrak{a} \text{ and } b_i \in \mathfrak{b}, i = 1, 2, ..., n; \text{ for } n = 1, 2, ...\}$$

From now on, we assume all the ideals are non-zero. Given an ideal, we are interested in how to represent this ideal. In fact, every ideal $\mathfrak{a}$ is a $\mathbb{Z}$-module of rank 2, and we write $\mathfrak{a} = [\alpha, \beta]$ if $\{\alpha, \beta\}$ is a $\mathbb{Z}$-basis of $\mathfrak{a}$. We have the following theorem.

Theorem 2.5. [JW09, p. 86] $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ if and only if $\mathfrak{a}$ can be represented as $[a, b + c\omega]$ where $a, b, c \in \mathbb{Z}$, $a > 0$, $c > 0$, $0 \leq b < a$, $c \mid a$, $c \mid b$ and $ac \mid N(b + c\omega)$.

The proof of Theorem 2.5 can be found in [JW09, p. 86]. The ideal $\overline{\mathfrak{a}}$ is defined as the conjugate of ideal $\mathfrak{a}$, where $\overline{\mathfrak{a}} = \left[\overline{\alpha}, \overline{\beta}\right]$ if $\mathfrak{a} = [\alpha, \beta]$ [JW09,p. 90]. If an ideal only has one $\mathcal{O}_K$-generator, say $\mathfrak{a} = (\theta) = \theta\mathcal{O}_K$ with $\theta \in \mathcal{O}_K$, then $\mathfrak{a}$ is said to be a principal ideal. In particular, $\mathcal{O}_K = (1)\mathcal{O}_K$ is a principal ideal. There is also a definition of the norm of an ideal.

Definition 2.6. [JW09, p. 90] The norm $N(\mathfrak{a})$ of an $\mathcal{O}_K$-ideal $\mathfrak{a}$ is defined to be the index $|\mathcal{O}_K/\mathfrak{a}|$.

It is clear that $N(\mathfrak{a}) = ac$ for $\mathfrak{a} = [a, b + c\omega]$.

We now look at the representation of the ideal $\mathfrak{p}$ where p is a rational prime with $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ in $\mathcal{O}_K$, i.e., [1] $(\frac{D}{p}) = 1$. This result is required when we discuss the form of elements in fake real quadratic orders. Suppose that $D \equiv s^2 \pmod{p}$ with $s \in \mathbb{Z}$ and $0 < s < p$, i.e., $s^2 - D \equiv (s + \sqrt{D})(s - \sqrt{D}) \equiv 0 \pmod{p}$. By Theorem 2.5, we can write $\mathfrak{p}$ as $\mathfrak{p} = [a, b + c\omega]$ with $a > 0$, $c > 0$, $0 < b < a$, $ac = N(\mathfrak{p})$, $c \mid a$ and $ac \mid N(b + c\omega)$, where $\omega = \frac{\sqrt{D}}{2}$ if $D \not\equiv 1 \pmod{4}$ and $\omega = \frac{1+\sqrt{D}}{2}$ otherwise. Since $N(\mathfrak{p}) = p$, then $a = p$ and $c = 1$. So $\mathfrak{p} = [p, b + \omega]$. First, suppose that $\omega = \frac{\sqrt{D}}{2}$, then $p \mid N(b + \frac{\sqrt{D}}{2}) = (b + \frac{\sqrt{D}}{2})(b - \frac{\sqrt{D}}{2})$. That is, $(2b + \sqrt{D})(2b - \sqrt{D}) \equiv 0 \pmod{p}$. Thus, $b = \frac{\pm s + kp}{2}$ where $k \in \mathbb{Z}$. So $\mathfrak{p} = [p, b + \frac{\sqrt{D}}{2}] = [p, \frac{\pm s + kp}{2} + \frac{\sqrt{D}}{2}] = [p, \frac{\pm s + \sqrt{D}}{2}]$. Without loss of generality, we set $\mathfrak{p} = [p, \frac{s+\sqrt{D}}{2}]$ and $\overline{\mathfrak{p}} = [p, \frac{s-\sqrt{D}}{2}]$.

Now suppose that $\omega = \frac{1+\sqrt{D}}{2}$, then $\mathfrak{p} = [p, \frac{2b+1}{2} + \frac{\sqrt{D}}{2}]$. So $p \mid N(b + c\omega)$ implies $4p \mid (2b + 1 + \sqrt{D})(2b + 1 - \sqrt{D})$. That is, $(2b + 1 + \sqrt{D})(2b + 1 - \sqrt{D}) \equiv 0 \pmod{p}$. So $b = \frac{\pm s - 1}{2} + \frac{kp}{2}$ where $k \in \mathbb{Z}$. Then $\mathfrak{p} = [p, \frac{2b+1}{2} + \frac{\sqrt{D}}{2}] = [p, \frac{\pm s + kp}{2} + \frac{\sqrt{D}}{2}] = [p, \frac{\pm s + \sqrt{D}}{2}]$. Without loss of generality, we set $\mathfrak{p} = [p, \frac{s+\sqrt{D}}{2}]$ and $\overline{\mathfrak{p}} = [p, \frac{s-\sqrt{D}}{2}]$.

Thus, $\mathfrak{p}$ can always be represented by

$$\mathfrak{p} = [p, \frac{s + \sqrt{D}}{2}] \text{ where } D \equiv s^2 \pmod{p}. \tag{2.2}$$

[1] $(\frac{D}{p})$ is the Legendre symbol of D modulo p.

Definition 2.7. [JW09, p. 88] An $\mathcal{O}_K$-ideal $\mathfrak{a}$ is invertible if there exists another $\mathcal{O}_K$-ideal $\mathfrak{b}$ such that

$$\mathfrak{a}\mathfrak{b} \in [\mathcal{O}_K]\,.$$

So an $\mathcal{O}_K$-ideal $\mathfrak{a}$ is invertible if and only if there exists an ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b}$ is a principal ideal. Specifically, all nonzero $\mathcal{O}_K$-ideals are invertible [JW09, p. 153].

Furthermore, for any invertible ideal $\mathfrak{a}$, $\mathfrak{a}\overline{\mathfrak{a}} = (N(\mathfrak{a}))$ [JW09, p. 90]. Another important result is given in the following theorem.

Theorem 2.8. [JW09, p. 92] If $\mathfrak{a}$ and $\mathfrak{b}$ are both invertible $\mathcal{O}_K$-ideals, then $\mathfrak{a}\mathfrak{b}$ is invertible and $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.

Clearly, two elements are enough to represent an ideal of $\mathcal{O}_K$ as a $\mathbb{Z}-$module. If both $\mathfrak{a} = (\alpha)$ and $\mathfrak{b} = (\beta)$ are principal ideals, then $\alpha = \beta$ implies $\mathfrak{a} = \mathfrak{b}$. Suppose that $\mathfrak{a} = \mathfrak{b}$, i.e., $\alpha\mathcal{O}_K = \beta\mathcal{O}_K$. So

$$\alpha \in \alpha\mathcal{O}_K = \beta\mathcal{O}_K$$

and

$$\beta \in \beta\mathcal{O}_K = \alpha\mathcal{O}_K.$$

Then both α/β and β/α are in $\mathcal{O}_K$. Thus, they must be units of $\mathcal{O}_K$. So $\mathfrak{a} = \mathfrak{b}$ implies $\alpha = \beta\eta$ for some unit η of $\mathcal{O}_K$.

For ideals that are not principal, we can also define such a relation as follows.

Definition 2.9. [JW09, p. 88] Two $\mathcal{O}_K$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent if there exist $\alpha, \beta \in \mathcal{O}_K$ such that $\alpha\beta \neq 0$ and

$$(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}.$$

We write this as $\mathfrak{a} \sim \mathfrak{b}$.

Proposition 2.10. [JW09, p. 88] Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals of $\mathcal{O}_K$. Then $\mathfrak{a} \sim \mathfrak{b}$ if and only if $\mathfrak{b} = \kappa\mathfrak{a}$ for some $\kappa \in K$ and $\kappa \neq 0$.

Definition 2.11. [JJSW06, p. 86] Let $\mathfrak{a}$ and $\mathfrak{b}$ be equivalent ideals. The term relative generator refers to an element $\psi \in K$ generating a principal fractional ideal [2] such that $(\psi)\mathfrak{a} = \mathfrak{b}$.

The equivalence of Definition 2.9 establishes an equivalence relation on all ideals of $\mathcal{O}_K$. If $\mathfrak{a}$ is an $\mathcal{O}_K$-ideal, the set of all $\mathcal{O}_K$-ideals that are equivalent to $\mathfrak{a}$ is denoted by $[\mathfrak{a}]$, which is called an ideal class of $\mathcal{O}_K$. Note that $[\mathcal{O}_K]$ is the set of all principal ideals of $\mathcal{O}_K$.

We next discuss the ideal class group by collecting all the ideal classes together.

Definition 2.12. [JW09, p. 153] The set of equivalence classes of invertible $\mathcal{O}_K$-ideals of a quadratic order is a finite abelian group called the ideal class group, denoted by Cl_K.

The group operation, written multiplicatively, is given by $[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}]$. It is well-defined and closure, associativity and commutativity follow easily from the definition of ideal multiplication. Clearly, the identity element of the class group is the principal ideal class $[\mathcal{O}_K]$ while the inverse of an ideal class $[\mathfrak{a}]$ is $[\overline{\mathfrak{a}}]$.

Definition 2.13. [JW09, p. 153] The class number of $\mathcal{O}_K$ is defined as the order of Cl_K and is denoted by h_K.

Class number formulas will be given in Chapter 3, along with the class number formula for fake real quadratic orders. Gauss hypothesized that there is a finite number of imaginary quadratic fields but infinitely many real quadratic fields with class number one. This is still

[2] A fractional ideal of $\mathcal{O}_K$ is a subset $\mathfrak{a}$ of $\mathbb{Q}(\sqrt{D})$ such that $d\mathfrak{a}$ is an integral $\mathcal{O}_K$-ideal for some $d \in \mathbb{Z}, d > 0$. [JW09, p. 154 Definition 7.3]

an open problem for $D > 0$. Number theorists have found the complete list of imaginary quadratic fields with class number up to 100 [Wat04]. Another famous problem regarding class numbers is the Cohen-Lenstra Heuristics, which is discussed in Chapter 3.

We now discuss primitive ideals and reduced ideals of $\mathcal{O}_K$. Note that for $\mathfrak{a} = [a, b + c\omega]$, $c|a$ and $c|b$. So $\mathfrak{a}$ can be written as $\mathfrak{a} = c\left[\frac{a}{c}, \frac{b}{c} + \omega\right]$, which implies that $\mathfrak{a} \sim \left[\frac{a}{c}, \frac{b}{c} + \omega\right]$. Hence, $\mathfrak{a}$ and $\left[\frac{a}{c}, \frac{b}{c} + \omega\right]$ are in the same ideal class. Since we are more interested in the ideal class group instead of a specific ideal, we restrict our discussion to a particular type of ideal, called primitive ideal of $\mathcal{O}_K$.

Definition 2.14. [JW09, p. 97] An ideal $\mathfrak{a}$ is primitive if it cannot be written as

$$\mathfrak{a} = m\mathfrak{b}$$

where $\mathfrak{b}$ is an ideal of $\mathcal{O}_K$ and $m \in \mathbb{Z}$, $|m| > 1$.

It is clear that we can always represent a primitive ideal $\mathfrak{b}$ by

$$\mathfrak{b} = [s, t + \omega],$$

where $s, t \in \mathbb{Z}$, $N(\mathfrak{b}) = |s|$ and $N(\mathfrak{b}) \mid N(t + \omega)$.

We now focus our discussion on reduced ideals of $\mathcal{O}_K$, which are special cases of primitive ideals. Recall that when we perform arithmetic on $\mathbb{Z}$, it is helpful to simplify the calculation by reducing the results modulo some integer m. For ideal arithmetic, it is also useful to reduce the ideal before or after the calculation. The ideal reduction algorithm is a way to accomplish that. We now discuss some basic facts about reduced ideals.

Definition 2.15. [JW09, p. 98] If $\mathfrak{a}$ is an $\mathcal{O}_K$-ideal, then $\mathfrak{a}$ is said to be a reduced ideal if $\mathfrak{a}$ is primitive and there does not exist a non-zero $\alpha \in \mathfrak{a}$ such that both $|\alpha| < N(\mathfrak{a})$ and

$|\overline{\alpha}| < N(\mathfrak{a})$ hold.

We can prove that the basic elements s, t of a reduced ideal $\mathfrak{a} = [s, t + \omega]$ are bounded by $\sqrt{|D|}$ [JW09, p. 99]. When we multiply two ideals, the parameters of the product grow fast and could become unmanageable. Since parameters of reduced ideals are bounded and we care more about the ideal class instead of a particular ideal, we can reduce ideals before multiplication. That will simplify the computation. After multiplication, we can also reduce the product to get a smaller result.

Since parameters of reduced ideas are bounded, it is clear that there is always a finite number of reduced ideals in $\mathcal{O}_K$. Given an ideal class, we may want to represent the class by a reduced ideal in that class. The question is whether or not such a reduced ideal exists and is unique. The following theorems investigate this problem.

Theorem 2.16. [JW09, p. 108] Let $D < 0$. If $\mathfrak{a}$ and $\mathfrak{b}$ are reduced $\mathcal{O}_K$-ideals such that $\mathfrak{a} \sim \mathfrak{b}$, then $\mathfrak{a} = \mathfrak{b}$.

Actually, $\mathfrak{a} \sim \mathfrak{b}$ implies that $\mathfrak{a} = \mathfrak{b}$ or $\mathfrak{a} = \overline{\mathfrak{b}}$. For convenience, we canonically pick the ideal among $\mathfrak{b}$ and $\overline{\mathfrak{b}}$ with smaller t, where t is the second coefficient in the ideal representation $[s, t + \omega]$, to make the reduced ideal in any ideal class unique. For any ideal $\mathfrak{a}$ of $\mathcal{O}_K$, we denote by red($\mathfrak{a}$) the reduced ideal in the class $[\mathfrak{a}]$.

Theorem 2.16 shows the uniqueness of the reduced ideal in any given ideal class of an imaginary quadratic field. For a real quadratic field, this is not the case.

Theorem 2.17. [JW09, p. 115] Let $\mathfrak{a}(= \mathfrak{a}_1)$ be any reduced ideal of $\mathcal{O}_K$. If we have k reduced ideals $\mathfrak{b}_1, \mathfrak{b}_2, ..., \mathfrak{b}_k$ in $[\mathfrak{a}]$ such that

$$N(\mathfrak{b}_i) \neq N(\mathfrak{b}_j) \text{ for } i \neq j$$

and

$$N(\mathfrak{b}_i) \nmid 2D/r \text{ for } i = 1, 2, ..., k$$

then there are at least $2k + 1$ distinct reduced ideals in $[\mathfrak{a}]$.

In a real quadratic order $\mathcal{O}_K$, $\log(\epsilon)$ provides an estimate of the number of reduced ideals in an equivalent class, where ϵ is the fundamental unit of $\mathcal{O}_K$ [JS14]. It is konwn that $h_K \log(\epsilon) \approx \sqrt{D}$. So if h_K is small, the number of reduced ideals in an equivalent class can be as large as $O(\sqrt{D})$.

It is clear that for imaginary quadratic fields, there is only one reduced ideal in each ideal class $[\mathfrak{a}]$. But there are multiple reduced ideals in any ideal class $[\mathfrak{a}]$ in real quadratic fields. The problem is how to find such reduced ideals. Before the description of reduction algorithms, we first introduce two alternative representations of an ideal.

As we mentioned earlier, any $\mathcal{O}_K$-ideal can be represented by $\mathfrak{a} = [a, b + c\omega]$ where $a, b, c \in \mathbb{Z}$, $a > 0$, $c > 0$, $0 \leq b < a$, $c \mid a$, $c \mid b$ and $ac \mid N(b + c\omega)$. If we put $S = c$, $Q = ra/c$ and $P = (rb/c) + r - 1$ with r as defined by (2.1), then we can represent $\mathfrak{a}$ by

$$\mathfrak{a} = S\left[\frac{Q}{r}, \frac{P + \sqrt{D}}{r}\right], \tag{2.3}$$

where $S, Q, P \in \mathbb{Z}$, $r \mid Q$ and $rQ \mid D - P^2$ [JW09, p. 102]. For primitive ideals, we can just take $S = 1$.

Let $\mathfrak{a} = [a, b + \omega]$ be a primitive $\mathcal{O}_K$-ideal where the equivalent representation of $\mathfrak{a}$ is given by

$$\mathfrak{a} = \left[\frac{Q}{r}, \frac{P + \sqrt{D}}{r}\right].$$

Define an operation ρ on $\mathfrak{a}$ such that $\mathfrak{a}' = \rho(\mathfrak{a}) = \left[\frac{Q_1}{r}, \frac{P_1+\sqrt{D}}{r}\right]$ as follows: [3]

$$q = \begin{cases} \lfloor \frac{P}{Q} \rceil & : \quad D < 0 \\ \lfloor \frac{P+\sqrt{D}}{Q} \rfloor & : \quad D > 0 \end{cases}$$

$$P_1 = qQ - P$$

$$Q_1 = \frac{D - {P_1}^2}{Q}$$

We can prove that $\rho(\mathfrak{a}) \sim \mathfrak{a}$ [JW09, p. 99]. If $\mathfrak{a} = [a, b+\omega]$ is a primitive ideal and $D < 0$, then $\mathfrak{a}$ is reduced if and only if $N(\rho(\mathfrak{a})) \geq N(\mathfrak{a})$ [JW09, p. 100]. When $D > 0$ and $a > 0$, $\mathfrak{a}$ is reduced implies that $\rho(\mathfrak{a})$ is also reduced [JW09, p. 106]. So for $D < 0$, if we start with a primitive $\mathcal{O}_K$-ideal $\mathfrak{a}$ and define $\rho^n(\mathfrak{a})$ recursively by $\rho^n(\mathfrak{a}) = \rho(\rho^{n-1}\mathfrak{a})$, then the sequence of positive integers

$$N(\mathfrak{a}), N(\rho(\mathfrak{a})), N(\rho^2(\mathfrak{a}))...$$

cannot be strictly decreasing infinitely. Thus, at some point, we must have

$$N(\rho^{i+1}(\mathfrak{a})) \geq N(\rho^i(\mathfrak{a}))$$

for some $i \geq 0$. It follows that $\rho^i(\mathfrak{a})$ is a reduced ideal equivalent to $\mathfrak{a}$.

In our program, for efficiency, we store c as $c = \frac{b^2-D}{4a}$ for each ideal $\mathfrak{a} = [a, b + c\omega]$. This representation is essentially that of a binary quadratic form [JJSW06]. An ideal is reduced when $-a < b \leq a < c$ or $0 \leq b \leq a = c$. Readers please refer [Say13] to find more detailed information.

We now describe important algorithms that we used in our program. They include several algorithms implemented by Sayles [Say13], including an ideal reduction algorithm, an ideal composition algorithm, NUCOMP, and an algorithm implemented by the author [Wan16] which is used for relative generator computations.

[3] $\lfloor x \rceil$ is the integer nearest to x. $\lfloor x \rfloor$ is the integer nearest to x that is smaller than x.

Algorithm 1 is used to compute relative generators in ideal reduction processes. This algorithm was used when testing the p-Ankeny-Artin-Chowla conjecture, which will be discussed in Chapter 3. Steps 2, 10, 15, 16 are not required when we only need to reduce an ideal without computing relative generators.

Algorithm 1 Relative Generator in an Ideal Reduction Process

Input: An ideal $\mathfrak{a} = (a_1, b_1, c_1)$ in $\mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{D})$, $D < 0$

Output: A reduced ideal $\mathfrak{r} = (a, b, c)$ that is equivalent to $\mathfrak{a}$, a relative generator β such that $\beta\mathfrak{r} = \mathfrak{a}$

1: $a \leftarrow a_1$, $b \leftarrow b_1$, $c \leftarrow c_1$

2: $A \leftarrow 1$, $B \leftarrow 0$, $s \leftarrow \gcd(\frac{b_1+b_2}{2}, \gcd(a_1, a_2))$

3: **while** $a > c$ **do**

4: $\quad n_a \leftarrow c$, $a_2 \leftarrow 2n_a$

5: $\quad q \leftarrow \lfloor -b/a_2 \rfloor$, $n_b \leftarrow -b \pmod{a_2}$

6: $\quad$ **if** $n_b > n_a$ **then**

7: $\quad\quad n_b \leftarrow n_b - a_2$, $q \leftarrow q + 1$

8: $\quad$ **end if**

9: $\quad c \leftarrow a - q(n_b - b)/2$, $b \leftarrow n_b$, $a \leftarrow n_a$

10: $\quad \text{temp} \leftarrow qA + B$, $B \leftarrow A$, $A \leftarrow -\text{temp}$

11: **end while**

12: **if** $a = c$ and $b < 0$ **then**

13: $\quad b \leftarrow -b$

14: **end if**

15: $\beta_x = 2Aa - Bb$

16: $\beta = \frac{\beta_x - B\sqrt{D}}{2a_1} s$

Algorithm 2 Ideal Composition Algorithm

Input: Ideals $\mathfrak{a}_1 = (a_1, b_1, c_1)$ and $\mathfrak{a}_2 = (a_2, b_2, c_2)$ in $\mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{D})$, $D < 0$

(Suppose $N(\mathfrak{a}_1) \geq N(\mathfrak{a}_2)$ and neither $\mathfrak{a}_1$ nor $\mathfrak{a}_2$ is $\mathcal{O}_K$)

Output: A reduced ideal $\mathfrak{r} = (a, b, c)$ that is equivalent to $\mathfrak{a}_1\mathfrak{a}_2$

1: $g \leftarrow \gcd(a_1, a_2)$ where $g = xa_2 + x_1a_1$

2: $p_{12} \leftarrow \frac{b_1+b_2}{2}$, $m_{12} \leftarrow p_{12} - b_2$

3: $u \leftarrow xm_{12} \pmod{a_1}$, $s \leftarrow 1$

4: **if** $g \neq 1$ **then**

5: $\quad s \leftarrow \gcd(p_{12}, g)$ where $s = yp_{12} + zg$

6: $\quad$ **if** $s \neq 1$ **then**

7: $\quad\quad a_1 \leftarrow \frac{a_1}{s}$, $a_2 \leftarrow \frac{a_2}{s}$

8: $\quad$ **end if**

9: $\quad u \leftarrow (uz) \pmod{a_1}$

10: $\quad t \leftarrow [y(c_2 \pmod{a_1})] \pmod{a_1}$

11: $\quad u \leftarrow (u - t) \pmod{a_1}$

12: **end if**

13: **if** $u < 0$ **then**

14: $\quad u \leftarrow u + a_1$

15: **end if**

// Normal Composition

16: $a \leftarrow a_1a_2$, $b \leftarrow 2a_2u + b_2 \pmod{2a}$, $c \leftarrow \frac{b^2-D}{4a}$

17: Use Algorithm 1 to reduce (a, b, c)

The square of an ideal is a special case of ideal multiplication; we will not describe that algorithm in this thesis. More information can be found at [Say13, libqform]. After we find the product of $\mathfrak{a}_1$ and $\mathfrak{a}_2$, we can perform the reduction algorithm to find a reduced ideal equivalent to $\mathfrak{a}_1\mathfrak{a}_2$.

Shanks discovered a more efficient way to find a reduced ideal equivalent to $\mathfrak{a}_1\mathfrak{a}_2$ than

first multiplying $\mathfrak{a}_1$ by $\mathfrak{a}_2$ and then using a reduction algorithm on the product. He keeps the numbers involved in the calculation as small as possible, roughly of order $\sqrt{D}$. This new technique is called NUCOMP, standing for "New COMPosition".

In NUCOMP, most of the numbers are no more than $|D|^{1/4}$. Even in the worst case, the numerators of two parameters are about $|D|^{3/4}$ and the denominator about $|D|^{1/2}$.

Before we describe the NUCOMP algorithm, we need to introduce the sequences of C_i and R_i, which are used in Algorithm 3. Suppose that $\mathfrak{a}_1 = \left[\frac{Q_1}{r}, \frac{P_1+\sqrt{D}}{r}\right]$ and $\mathfrak{a}_2 = \left[\frac{Q_2}{r}, \frac{P_2+\sqrt{D}}{r}\right]$ are two primitive ideals in $\mathcal{O}_K$. Given R_{-2} and R_{-1}, we can find $\{C_i\}, \{R_i\}$ as follows,

$$
\begin{aligned}
B_{-2} &= 1, B_{-1} = 0, \\
q_j &= \lfloor R_{j-2}/R_{j-1} \rfloor, \\
R_{j-2} &= q_j R_{j-1} + R_j, \\
B_j &= q_j B_{j-1} + B_{j-2}, \\
C_j &= (-1)^{j-1} B_j
\end{aligned}
$$

where $j = 0, 1, 2, \ldots$. Then there exists i such that

$$
R_i < \sqrt{r|Q_1/Q_2|}|D|^{1/4} < R_{i-1}. \tag{2.4}
$$

In Algorithm 3, Step 17, xgcd$(r_1, r_0, C_1, C_0, \text{bound})$ is a function looking for $R_i, R_{i-1}, C_i, C_{i-1}$ such that $R_i < \sqrt{r|Q_1/Q_2|}|D|^{1/4} < R_{i-1}$ using the procedure described above. To find detailed descriptions of this algorithm, readers please refer to [JW09, Section 5.4].

Note that the NUCOMP algorithm was only used when computing the order of $[\mathfrak{p}]$ in Cl_K. The computation of relative generators when reducing the product of two ideals requires normal ideal compositions in our program.

Algorithm 3 Ideal Composition Algorithm Using NUCOMP

Input: Ideals $\mathfrak{a}_1 = (a_1, b_1, c_1)$ and $\mathfrak{a}_2 = (a_2, b_2, c_2)$ in $\mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{D})$, $D < 0$ (Suppose $N(\mathfrak{a}_1) \geq N(\mathfrak{a}_2)$ and neither $\mathfrak{a}_1$ nor $\mathfrak{a}_2$ is $\mathcal{O}_K$)

Output: A reduced ideal $\mathfrak{r} = (a, b, c)$ that is equivalent to $\mathfrak{a}_1\mathfrak{a}_2$

$g \leftarrow \gcd(a_1, a_2)$ where $g = xa_2 + x_1a_1$

$p_{12} \leftarrow \frac{b_1+b_2}{2}$, $m_{12} \leftarrow p_{12} - b_2$

$u \leftarrow xm_{12} \pmod{a_1}$, $s \leftarrow 1$

if $g \neq 1$ **then**

    $s \leftarrow \gcd(p_{12}, g)$ where $s = yp_{12} + zg$

    if $s \neq 1$ **then**

        $a_1 \leftarrow \frac{a_1}{s}$, $a_2 \leftarrow \frac{a_2}{s}$

    end if

    $u \leftarrow (uz) \pmod{a_1}$

    $t \leftarrow [y(c_2 \pmod{a_1})] \pmod{a_1}$

    $u \leftarrow (u - t) \pmod{a_1}$

end if

if $u < 0$ **then**

    $u \leftarrow u + a_1$

end if

// NUCOMP

$r_1 \leftarrow a_1$, $r_0 \leftarrow u$

// Give that $R_{-2} = a_1$, $R_{-1} = u$, compute $r_1 = R_{i-1}$, $r_0 = R_i$, $'C_1' = C_{i-1}$, $'C_0' = C_i$ which satisfies (2.5)

$\text{xgcd}(r_1, r_0, C_1, C_0, \text{bound})$

$m_1 \leftarrow (a_2r_0 + m_{12}C_0)/a_1$, $m_2 \leftarrow (p_{12}r_0 - sC_0c_2)/a_1$

$a \leftarrow r_0m_1 - C_0m_2$, $b \leftarrow [2(a_2r_0 - a|C_1|)/C_0 - b_2] \pmod{2a}$, $c \leftarrow \frac{b^2-D}{4a}$

Use Algorithm 1 to reduce (a, b, c)

2.3 The Infrastructure of Real Quadratic Fields

In this section, we describe infrastructures of real quadratic fields. For more details on this topic, readers are recommended to consult Jacobson and Scheidler's [JS14].

In real quadratic fields, each ideal class contains a finite set of reduced ideals. We may represent an ideal class by a reduced ideal. The main problem is how to test whether two ideal classes are equal. Although the number of reduced ideals is finite, it can be as large as $O(\sqrt{D})$, which is too large do perform an exhaustive comparison. Shanks first noticed that the set of reduced ideals of any ideal class has a group-like structure, which he termed the infrastructure [4]. This discovery makes it possible to improve the methods for computing the fundamental unit, testing equality of two ideal classes and computing class groups.

In a real quadratic field, let $\mathfrak{a} = [a, b+\omega]$ be a reduced $\mathcal{O}_K$-ideal. It has been proved that there exists a minimal integer l for which $\mathfrak{a} = \rho^l(\mathfrak{a})$ [JW09, p. 113]. Also, the l ideals in the set

$$\{\mathfrak{a}, \rho(\mathfrak{a}), \rho^2(\mathfrak{a}), ..., \rho^{l-1}(\mathfrak{a})\}$$

are distinct and make up the complete collection of the reduced ideals equivalent to $\mathfrak{a}$. Assume $a > 0$, then

$$\mathcal{C} = \{\mathfrak{a}_1 = \mathfrak{a}, \mathfrak{a}_2 = \rho(\mathfrak{a}), \mathfrak{a}_3 = \rho^2(\mathfrak{a}), ..., \mathfrak{a}_l = \rho^{l-1}(\mathfrak{a})\},$$

is a cycle of reduced ideals. We call $\mathcal{C}$ the infrastructure of ideal class $[\mathfrak{a}]$.

Recall that $\rho(\mathfrak{a}) \sim \mathfrak{a}$, in fact, we have

$$\mathfrak{a}_{i+1} = (\psi_i)\mathfrak{a}_i$$

[4] This group-like structure does not satisfy the asscociativity condition. [JS14]

where $\psi_i = \frac{P_i+\sqrt{D}}{Q_{i-1}}$. We can also obtain θ_i where $\mathfrak{a}_i = (\theta_i)\mathfrak{a}_1$ by

$$\theta_i = \prod_{k=1}^{i-1} \psi_k.$$

and define $\theta_1 = 1$.

For any two ideals $\mathfrak{a}_m$ and $\mathfrak{a}_n$, $m < n$, Shanks defined the distance from $\mathfrak{a}_m$ to $\mathfrak{a}_n$,

$$\delta(\mathfrak{a}_m, \mathfrak{a}_n) = \log(\theta_n/\theta_m).$$

Specifically, $\delta(\mathfrak{a}_m, \mathfrak{a}_1) = \log(\theta_m)$ and $\delta(\mathfrak{a}_m, \mathfrak{a}_{m-1}) = \log(\psi_{m-1})$.

If we confine the discussion to the class of principal ideals, then

$$\mathcal{C} = \{\mathfrak{a}_1 = (1), \mathfrak{a}_2 = (\theta_2), ..., \mathfrak{a}_l = (\theta_l)\}$$

is the infrastructure of $\mathcal{O}_K$.

For any infrastructure $\mathcal{C} = \{\mathfrak{a}_1, \mathfrak{a}_2, ..., \mathfrak{a}_l\}$, we have $\mathfrak{a}_{l+1} = (\theta_{l+1})\mathfrak{a} = \rho^l(\mathfrak{a}) = \mathfrak{a}$. It is clear to see that $\delta(\mathfrak{a}_{l+1}, \mathfrak{a}) = \log(\theta_{l+1})$ where θ_{l+1} is the fundamental unit of $K = \mathbb{Q}(\sqrt{D})$. We define $R_D = \log(\theta_{l+1})$ as the regulator of $\mathbb{Q}(\sqrt{D})$. The regulator measures the distance around the entire cycle of reduced principal ideals. It has been shown that $\delta(\mathfrak{a}_i) \approx i$ [JS14]. So the regulator, $R_D \approx \log(l+1)$, provides an estimate of the number of reduced ideals in an equivalent class.

Shanks' goal in developing the infrastructure was to apply his baby-step giant-step method for computing the order of an element in a finite abelian group to the problem of computing the regulator. Consider a multiplicative cyclic group $G = \langle g \rangle$ with order l. To generate the group, we begin with the identity element 1 and then successively multiply by g until we get $g^l = 1$. In an infrastructure, we begin with a reduced ideal $\mathfrak{a}$, then perform the recurrence on $\mathfrak{a}$ until we obtain $\mathfrak{a}$ again after l steps. The elements of $\mathcal{C}$ form a cycle and are ordered in terms of distance. Walking through the entire cycle using baby steps yields

the regulator, which is analouguous to the order of g.

The giant-steps allow one to move t steps through the cycle in a single operation. In the case of $\langle g \rangle$, multiplication by g^t acts as such a giant step, as $g^s g^t = g^{s+t}$. The element g^{s+t} is precisely t steps further along in the cycle from g^s. To apply giant-steps on the infrastructure, the only problem is to compute a reduced ideal $\mathfrak{a}_k$ equivalent to $\mathfrak{a}_s\mathfrak{a}_t$. This step can be done using ideal multiplication followed by reduction or using only NUCOMP. It was found that $\delta(\mathfrak{a}_k)$ is close to $\delta(\mathfrak{a}_s) + \delta(\mathfrak{a}_t)$ but not equal, so the infrastructure is not a group, but baby-steps and giant-steps are possible.

Let $\mathfrak{a}_s$ and $\mathfrak{a}_t$ be reduced principal ideals in $\mathcal{C}$ and consider the product of $\mathfrak{a}_s\mathfrak{a}_t$. We know that the product can be written as

$$(S)\mathfrak{c} = \mathfrak{a}_s\mathfrak{a}_t,$$

where $\mathfrak{c} = S[Q_m/r, (P_m + \sqrt{D})/r]$. After that, we can compute a reduced ideal $\mathfrak{c}'$ that is equivalent to $\mathfrak{c}$. Suppose $\mathfrak{c}' = [Q'_m/r, (P'_m + \sqrt{D})/r]$. Let k be the index with $\mathfrak{a}_k = \mathfrak{c}'$. By [JW09, p. 103 (5.10)], $\mathfrak{c}' = (\theta'_m)\mathfrak{c}$. So

$$\mathfrak{a}_k = (\theta'_m/S)\mathfrak{a}_s\mathfrak{a}_t.$$

Thus, we have

$$\theta_k = \theta_s\theta_t\frac{|\theta'_m|}{S}.$$

If we set $\kappa = \log(|\theta'_m|/S)$, we obtain

$$\delta(\mathfrak{a}_k) = \delta(\mathfrak{a}_s) + \delta(\mathfrak{a}_t) + \kappa. \tag{2.5}$$

By [JW09, p. 118 (5.38)], we know that $-\log(D) < \kappa < \log(2)$, so $\delta(\mathfrak{a}_k) \approx \delta(\mathfrak{a}_s) + \delta(\mathfrak{a}_t)$, as required. NUCOMP yields a similar result [JW09, p. 175].

We can depict this group-like structure on a circle. Notice that the distances between two consecutive ideals are not necessarily equal.

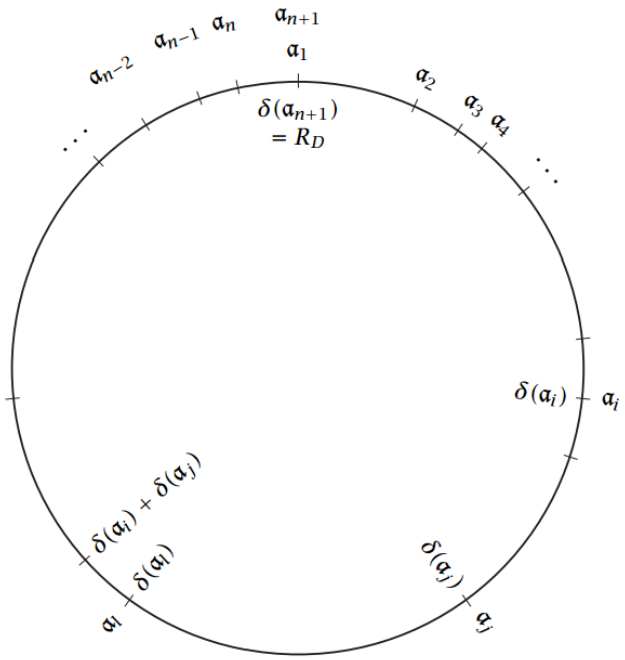

Figure 2.1: The Infrastructure of the principal class of $\mathbb{Q}(\sqrt{D})$ [JW09, p. 175].

The infrastructure is a powerful tool to compute the regulator and therefore the fundamental unit of $\mathbb{Q}(\sqrt{D})$. Shanks' baby-step giant-step algorithm computes the regulator in time $O(D^{1/4+\epsilon})$ [JW09, p. 179]. Lenstra improved the baby-step giant-step algorithm to an $O(D^{1/5+\epsilon})$ algorithm [Len82].

Chapter 3

Fake Real Quadratic Orders

Cohen defined a fake real quadratic order by inverting an ideal above a split prime p followed by adjoining the inverse of this ideal to $\mathcal{O}_K$, where K is an imaginary quadratic field [Coh13]. A fake real quadratic order is a Dedekind domain [Oh14, Prop 1.1] with a similar structure as a real quadratic order. In this chapter, we investigate further aspects of fake real quadratic orders, such as the class group, the unit group and the infrastructure.

3.1 Definition of Fake Real Quadratic Orders

Definition 3.1. [Coh13] Let p be a fixed prime number. Take any fundamental discriminant $D < 0$ such that $(\frac{D}{p}) = 1$. We put $K = \mathbb{Q}(\sqrt{D})$ and let $\mathcal{O}_K$ denote its ring of integers. We write $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ and define the ring $\mathcal{O}_K[\mathfrak{p}^{-1}]$ as a fake real quadratic order. Let $\mathcal{O}_{K,p}$ be the shorthand notation for it.

Note that $\mathcal{O}_K[\mathfrak{p}^{-1}]$ is canonically isomorphic to $\mathcal{O}_K[\overline{\mathfrak{p}}^{-1}]$ via sending α to its conjugate $\overline{\alpha}$. This is why we simply write $\mathcal{O}_{K,p}$. By definition, it is clear that for a factorization of any integral ideal I in $\mathcal{O}_{K,p}$

$$I = \mathfrak{p}^n \mathfrak{p}_1^{n_1} \mathfrak{p}_2^{n_2} ... \mathfrak{p}_k^{n_k},$$

all the exponents have to be positive except the exponent of $\mathfrak{p}$, which can be a negative number. In other words, $\mathcal{O}_{K,p}$ is the smallest ring containing $\mathcal{O}_K$ and $\mathfrak{p}^{-1}$. Since

$$\mathcal{O}_K \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{p}^{-2} \subseteq ... \subseteq \mathcal{O}_{K,p} \subseteq K,$$

we can write $\mathcal{O}_{K,p}$ as

$$\mathcal{O}_{K,p} = \bigcup_{k\geq 0} \mathfrak{p}^{-k}.$$

Proposition 3.2. $\mathfrak{p}\mathcal{O}_{K,p} = \mathcal{O}_{K,p}$.

Proof. Since $\mathcal{O}_{K,p} = \bigcup_{k\geq 0} \mathfrak{p}^{-k}$, we have

$$\mathfrak{p}\mathcal{O}_{K,p} = \bigcup_{k\geq -1} \mathfrak{p}^{-k}.$$

$\mathfrak{p} \subseteq \mathcal{O}_K = \mathfrak{p}^0$ implies that

$$\bigcup_{k\geq -1} \mathfrak{p}^{-k} = (\bigcup_{k\geq 0} \mathfrak{p}^{-k}) \bigcup \mathfrak{p} = \bigcup_{k\geq 0} \mathfrak{p}^{-k}.$$

Hence, $\mathfrak{p}\mathcal{O}_{K,p} = \mathcal{O}_{K,p}$. □

3.2 Elements in Fake Real Quadratic Orders

We are interested in the form of elements in $\mathcal{O}_{K,p}$. The following lemma and proposition give us representations of these elements. Since $(\frac{D}{p}) = 1$, there exists $s \in \mathbb{Z}$, $0 < s < p$ such that $D \equiv s^2 \pmod{p}$. By the discussion in Section 2.2, we may choose the sign of the square root such that

$$\mathfrak{p} = [p, \frac{s + \sqrt{D}}{2}].$$

Lemma 3.3. [Coh13] Let $\alpha = x + y\sqrt{D} \in \mathcal{O}_K$, with $x, y \in (\frac{1}{2})\mathbb{Z}$ and [1] $\gcd(x, y, p) = 1$. Then for any $k > 0$, we have $\alpha \in \mathfrak{p}^k$ if and only if $p^k \mid x^2 - Dy^2$ and $x \equiv sy \pmod{p}$ where $D \equiv s^2 \pmod{p}$.

[1] For $x = \frac{x_0}{2}, y = \frac{y_0}{2} \in \frac{1}{2}\mathbb{Z}$, and $p \in \mathbb{Z}$, $\gcd(x, y, p)$ is defined as $\gcd(x_0, y_0, p)$.

Proof. To see sufficiency, let $\alpha \in \mathfrak{p}^k$. Then $N(\mathfrak{p}^k) \mid N(\alpha)$. Since $\alpha = x + y\sqrt{D}$, we have $N(\alpha) = x^2 - Dy^2$, and $N(\mathfrak{p}^k) = p^k$. Therefore,

$$p^k \mid x^2 - Dy^2.$$

For $k > 0$, $\alpha \in \mathfrak{p}^k \subseteq \mathfrak{p}$, so $\alpha \in \mathfrak{p}$. Since $\mathfrak{p} = [p, \frac{s+\sqrt{D}}{2}]$, we have

$$\alpha = pu + \frac{s+\sqrt{D}}{2}v = (pu + \frac{sv}{2}) + \frac{v}{2}\sqrt{D}, \text{ for some } u, v \in \mathbb{Z}.$$

So $x = pu + \frac{sv}{2}$ and $y = \frac{v}{2}$. Thus,

$$x = pu + \frac{sv}{2} \equiv \frac{sv}{2} = sy \pmod{p}.$$

For necessity, assume that $p^k \mid x^2 - Dy^2$ and $x \equiv sy \pmod{p}$. Since $k > 0$, we have $p \mid N(\alpha)$. Then either $\alpha \in \mathfrak{p}$ or $\alpha \in \overline{\mathfrak{p}}$. If

$$\alpha \in \overline{\mathfrak{p}} = p\mathbb{Z} + \frac{s-\sqrt{D}}{2}\mathbb{Z},$$

then

$$\alpha = pu + \frac{s-\sqrt{D}}{2}v, \text{ for some } u, v \in \mathbb{Z}.$$

This gives us $x = pu + \frac{sv}{2}$ and $y = -\frac{v}{2}$. So

$$x = pu + \frac{sv}{2} \equiv \frac{sv}{2} = -sy \pmod{p}.$$

Since $x \equiv sy \pmod{p}$, we have $2x \equiv 0 \pmod{p}$, i.e., $p \mid 2x$. When $p = 2$, we have $s = 1$ and $x \equiv y \pmod{p}$. Thus, $\gcd(x, y, p) = \gcd(2x, 2y, p) = 2$, which contradicts the assumption that $\gcd(x, y, p) = 1$. When $p \neq 2$, we know that $p \mid x$. Using the fact that $(\frac{D}{p}) = 1$ and $p \mid (x^2 - Dy^2)$, we have $p \mid y$. Thus, $\gcd(x, y, p) = p$, which also contradicts the

assumption that $\gcd(x, y, p) = 1$.

Therefore, $\alpha \notin \overline{\mathfrak{p}}$ i.e., $\overline{\mathfrak{p}} \nmid (\alpha)$. So $\overline{\mathfrak{p}}^k \nmid (\alpha)$ i.e., $\mathfrak{p}^k \nmid (\overline{\alpha})$ for $k > 0$. $p^k \mid x^2 - Dy^2$ implies that

$$\mathfrak{p}^k \overline{\mathfrak{p}}^k \mid (\alpha)(\overline{\alpha}).$$

Since $\mathfrak{p}^k \nmid (\overline{\alpha})$, we have

$$\mathfrak{p}^k \mid (\alpha).$$

Thus, $\alpha \in \mathfrak{p}^k$. □

The main idea of the proof of Lemma 3.3 is credited to Oh [Oh14, Lemma 1.4]. The author added the proof for the case when $p = 2$. This lemma provides necessary and sufficient conditions on the coefficients of $\alpha \in \mathcal{O}_K$ to guarantee that $\alpha \in \mathfrak{p}^k$ for $k > 0$. It also gives us insight into what the elements in $\mathcal{O}_{K,p}$ look like. That is explained in the following corollary.

Corollary 3.4. [Coh13] Any element $\alpha \in \mathcal{O}_{K,p}$ can be written in a unique way as

$$\alpha = \frac{x + y\sqrt{D}}{p^k},$$

where $k \in \mathbb{Z}$, $x, y \in (\frac{1}{2})\mathbb{Z}$, $\gcd(x, y, p) = 1$, and either $k \leq 0$ (i.e. $\alpha \in \mathcal{O}_K$) or $k > 0$, which means that $\mathfrak{p}^k \mid x^2 - Dy^2$ and $x \equiv -sy \pmod{p}$ where $D \equiv s^2 \pmod{p}$.

Proof. For any $\alpha \in \mathcal{O}_{K,p}$, there exists $k \in \mathbb{Z}$ such that $\mathfrak{p}^k(\alpha) \subseteq \mathcal{O}_K$. Then we have $p^k\alpha \in \mathcal{O}_K$. Therefore,

$$\alpha = \frac{x + y\sqrt{D}}{p^k} \text{ for some } x, y \in (\frac{1}{2})\mathbb{Z}.$$

Since we could divide out the largest power of p from $\gcd(2x, 2y)$, we can further assume that $\gcd(x, y, p) = 1$. Therefore, it is easy to show that this representation is unique as follows.

Suppose $\alpha = \frac{x_1+y_1\sqrt{D}}{p^{k_1}} = \frac{x_2+y_2\sqrt{D}}{p^{k_2}}$. Then $k_1 = k_2$ implies $x_1 = x_2, y_1 = y_2$. If $k_1 \neq k_2$, assume $k_1 < k_2$. Then $p^{k_2-k_1}(x_1 + y_1\sqrt{D}) = x_2 + y_2\sqrt{D}$. So $\gcd(x_2, y_2, p)$ is a multiple of p, which contradicts the fact that $\gcd(x_2, y_2, p) = 1$.

If $k \leq 0$, then $\alpha \in \mathcal{O}_K \subseteq \mathcal{O}_{K,p}$. If $k > 0$, since $\alpha \in \mathcal{O}_{K,p}$ and $\overline{\mathfrak{p}} \neq \mathfrak{p}$, then

$$v_{\overline{\mathfrak{p}}}(\alpha) \geq 0,$$

where $v_{\overline{\mathfrak{p}}}(\alpha)$ is the power of $\overline{\mathfrak{p}}$ in the prime ideal factorization of α. Therefore,

$$v_{\overline{\mathfrak{p}}}(x + y\sqrt{D}) = v_{\overline{\mathfrak{p}}}(\alpha) + v_{\overline{\mathfrak{p}}}(p^k) \geq v_{\overline{\mathfrak{p}}}(p^k) = k.$$

Thus, $x + y\sqrt{D} \in \overline{\mathfrak{p}}^k$. Apply Lemma 3.3 to $\overline{\mathfrak{p}}$, then we have $\mathfrak{p}^k \mid x^2 - Dy^2$ and $x \equiv -sy \pmod{p}$. □

The main idea of this proof comes from Oh [Oh14, Corollary 1.5]. The author added more details in the second part of the proof.

In quadratic fields, a fundamental unit is a unit ϵ such that any unit can be written as a power of ϵ up to sign. There is a finite number of units in imaginary quadratic fields while there are infinitely many units in real quadratic fields. For fake real quadratic orders, we are also interested in the unit group and the fundamental unit.

Proposition 3.5. [Coh13] Let $U_{K,p}$ denote the unit group of $\mathcal{O}_{K,p}$. Then $U_{K,p} = \mu_K \times \epsilon^{\mathbb{Z}}$, where μ_K is the group of roots of unity in $\mathcal{O}_K$, and the fundamental unit ϵ is a generator of the principal ideal $\mathfrak{p}^{o(\mathfrak{p})}$, where $o(\mathfrak{p})$ is the order of the class of $\mathfrak{p}$ in the ideal class group Cl_K.

Proof. For any $\alpha \in U_{K,p}$, $1/\alpha \in U_{K,p}$. So $1/\alpha \in \mathcal{O}_{K,p}$. Then by the definition, $\alpha \in U_{K,p}$ if and only if $v_{\mathfrak{q}}(\alpha) \geq 0$ and $v_{\mathfrak{q}}(1/\alpha) \geq 0$ for all prime ideals $\mathfrak{q} \neq \mathfrak{p}$. Therefore, $\alpha \in U_{K,p}$ if and only if $v_{\mathfrak{q}}(\alpha) = 0$ for all prime ideals $\mathfrak{q} \neq \mathfrak{p}$. Thus, $\alpha\mathcal{O}_K = \mathfrak{p}^k$ for some $k \in \mathbb{Z}$. Since $o(\mathfrak{p})$ is defined as the order of the ideal class of $\mathfrak{p}$ in Cl_K, we have $o(\mathfrak{p})|k$.

Let ϵ be a generator of the principal ideal $\mathfrak{p}^{o(\mathfrak{p})}$, then

$$\alpha\mathcal{O}_K = (\epsilon\mathcal{O}_K)^{k/o(\mathfrak{p})}.$$

Thus, $\alpha = \eta\epsilon^{k/o(\mathfrak{p})}$ for some unit η in $\mathcal{O}_K$. Since the group of units in $\mathcal{O}_K$ is μ_K, the roots of unity, we have $\alpha \in U_{K,p}$ if and only if $\alpha = \eta\epsilon^{k/o(\mathfrak{p})}$ with $\eta \in \mu_K$. Therefore, $U_{K,p} = \mu_K \times \epsilon^{\mathbb{Z}}$. $\square$

The proof of Proposition 3.5 is credited to Oh [Oh14, Proposition 1.2]. As we can see, like real quadratic fields, there are also infinitely many units in fake real quadratic orders. In quadratic fields, all the units can be found by taking a power of the fundamental unit. Similarly, in a fake real quadratic order $\mathcal{O}_{K,p}$, the fundamental unit is a generator of $U_{K,p}$ modulo the roots of unity in $\mathcal{O}_K$. To find the fundamental unit, it is crucial to know its form.

It is obvious that the fundamental unit ϵ of $\mathcal{O}_{K,p}$ is in $\mathcal{O}_K$. Since ϵ generates $\mathfrak{p}^{o(\mathfrak{p})}$, $\epsilon \in \mathfrak{p}^{o(\mathfrak{p})} \subseteq \mathcal{O}_K$, i.e., $\epsilon \in \mathcal{O}_K$. Thus, we have $\epsilon = x + y\sqrt{D}$ where $x, y \in (\frac{1}{2})\mathbb{Z}$. Since ϵ is a generator of the principal ideal $\mathfrak{p}^{o(\mathfrak{p})}$, we know that

$$N(\epsilon) = N(\mathfrak{p}^{o(\mathfrak{p})}).$$

It follows that

$$x^2 + y^2|D| = p^{o(\mathfrak{p})}.$$

So the fundamental unit of $\mathcal{O}_{K,p}$ can be found by solving this norm equation. Thus, it is crucial to find $o(\mathfrak{p})$, the order of the ideal class of $\mathfrak{p}$. Algorithms to find the fundamental unit of a fake real quadratic order are described in Section 3.5.

3.3 Class Groups of Fake Real Quadratic Orders

We just introduced the elements and the unit group of fake real quadratic orders. We now look at ideals of $\mathcal{O}_{K,p}$. Moreover, we want to study the class group structure and compute the class number of $\mathcal{O}_{K,p}$. These problems are discussed in this section.

Proposition 3.6 Define a map ϕ from the set of integral ideals of $\mathcal{O}_{K,p}$ to the set of integral

ideals of $\mathcal{O}_K$ coprime to $\mathfrak{p}$, such that

$$\phi(I) = I \cap \mathcal{O}_K.$$

Then ϕ is a bijection preserving prime and maximal ideals. The inverse of ϕ is given by $\phi^{-1}(\mathfrak{a}) = \mathfrak{a}\mathcal{O}_{K,p}$ for any integral ideal $\mathfrak{a}$ of $\mathcal{O}_K$.

Proof. Clearly, $I \cap \mathcal{O}_K$ is an ideal of $\mathcal{O}_K$. If I, J are two integral ideals of $\mathcal{O}_{K,p}$ such that $\phi(I) = \phi(J)$, then $I \cap \mathcal{O}_K = J \cap \mathcal{O}_K$. To show $I = J$, it is sufficient to show that

$$(I \cap \mathcal{O}_K)\mathcal{O}_{K,p} = I \text{ and } (J \cap \mathcal{O}_K)\mathcal{O}_{K,p} = J$$

First, we know that

$$(I \cap \mathcal{O}_K)\mathcal{O}_{K,p} \subseteq I\mathcal{O}_{K,p} = I.$$

For any $x \in I$, there exists $k > 0$ such that $x \in \mathfrak{p}^{-k}$. Thus, $x\mathfrak{p}^k \subseteq \mathcal{O}_K$. Since I is an ideal of $\mathcal{O}_{K,p}$, we have $x\mathfrak{p}^k \subseteq I$. Therefore,

$$x\mathfrak{p}^k \subseteq I \cap \mathcal{O}_K.$$

That is

$$x \in (I \cap \mathcal{O}_K)\mathfrak{p}^{-k} \subseteq (I \cap \mathcal{O}_K)\mathcal{O}_{K,p}.$$

So $I \subseteq (I \cap \mathcal{O}_K)\mathcal{O}_{K,p}$, which implies that $I = (I \cap \mathcal{O}_K)\mathcal{O}_{K,p}$.

Similarly, we have $J = (J \cap \mathcal{O}_K)\mathcal{O}_{K,p}$. Since $I \cap \mathcal{O}_K = J \cap \mathcal{O}_K$, then

$$I = (I \cap \mathcal{O}_K)\mathcal{O}_{K,p} = (J \cap \mathcal{O}_K)\mathcal{O}_{K,p} = J.$$

Thus, $I = J$, showing that ϕ is injective.

To show ϕ is surjective, let $\mathfrak{a}$ be an integral ideal of $\mathcal{O}_K$. Set $I = \mathfrak{a}\mathcal{O}_{K,p}$. Clearly, I is an

ideal of $\mathcal{O}_{K,p}$ and $\phi(I) = \mathfrak{a}\mathcal{O}_{K,p} \cap \mathcal{O}_K \supseteq \mathfrak{a}\mathcal{O}_K \cap \mathcal{O}_K = \mathfrak{a}$. That is

$$(\mathfrak{a}\mathcal{O}_{K,p} \cap \mathcal{O}_K)\mathcal{O}_{K,p} \supseteq \mathfrak{a}\mathcal{O}_{K,p}.$$

Therefore, $v_{\mathfrak{q}}(\mathfrak{a}\mathcal{O}_{K,p} \cap \mathcal{O}_K) \leq v_{\mathfrak{q}}(\mathfrak{a})$ for all prime ideals $\mathfrak{q} \neq \mathfrak{p}$.

On the other hand,

$$(\mathfrak{a}\mathcal{O}_{K,p} \cap \mathcal{O}_K)\mathcal{O}_{K,p} \subseteq (\mathfrak{a}\mathcal{O}_{K,p})\mathcal{O}_{K,p} = \mathfrak{a}\mathcal{O}_{K,p}.$$

Thus, $v_{\mathfrak{q}}(\mathfrak{a}\mathcal{O}_{K,p} \cap \mathcal{O}_K) \geq v_{\mathfrak{q}}(\mathfrak{a})$ for all prime ideals $\mathfrak{q} \neq \mathfrak{p}$. So we have $v_{\mathfrak{q}}(\mathfrak{a}\mathcal{O}_{K,p} \cap \mathcal{O}_K) = v_{\mathfrak{q}}(\mathfrak{a})$. Since $\mathfrak{a}$ is coprime to $\mathfrak{p}$, then $\mathfrak{a}\mathcal{O}_{K,p} \cap \mathcal{O}_K$ is also coprime to $\mathfrak{p}$. Therefore, $\mathfrak{a}\mathcal{O}_{K,p} \cap \mathcal{O}_K = \mathfrak{a}$ i.e., $\phi(\mathfrak{a}\mathcal{O}_{K,p}) = \mathfrak{a}$.

So ϕ is surjective and therefore bijective, and $\phi^{-1}(\mathfrak{a}) = \mathfrak{a}\mathcal{O}_{K,p}$

Suppose I is a prime ideal of $\mathcal{O}_{K,p}$ and $I \cap \mathcal{O}_K = \mathfrak{a}$. Assume $\mathfrak{a}$ is not a prime ideal of $\mathcal{O}_K$, i.e., $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$ where $\mathfrak{a}_1, \mathfrak{a}_2$ are proper ideals[2] of $\mathcal{O}_K$. Then

$$I = \mathfrak{a}\mathcal{O}_{K,p} = \mathfrak{a}_1\mathfrak{a}_2\mathcal{O}_{K,p} = \mathfrak{a}_1\mathcal{O}_{K,p}\mathfrak{a}_2\mathcal{O}_{K,p} = I_1I_2,$$

where I_1 and I_2 are ideals of $\mathcal{O}_{K,p}$. Since $\mathfrak{a}_1, \mathfrak{a}_2$ are proper ideals of $\mathcal{O}_K$, then I_1, I_2 are proper ideals of $\mathcal{O}_{K,p}$. So it contradicts the fact that I is a prime ideal of $\mathcal{O}_{K,p}$. Thus, $\mathfrak{a}$ is a prime ideal of $\mathcal{O}_K$, i.e., ϕ preserves prime ideals.

Suppose I is a maximal ideal of $\mathcal{O}_{K,p}$ and $I \cap \mathcal{O}_K = \mathfrak{a}$. If $\mathfrak{a}$ is not a maximal ideal of $\mathcal{O}_K$, then there exists a proper ideal $\mathfrak{b}$ of $\mathcal{O}_K$ such that $\mathfrak{a} \subset \mathfrak{b}$. Then

$$I = \mathfrak{a}\mathcal{O}_{K,p} \subset \mathfrak{b}\mathcal{O}_{K,p} = J$$

where J is an ideal of $\mathcal{O}_{K,p}$. Since $\mathfrak{b}$ is a proper ideal of $\mathcal{O}_K$, then J is a proper ideal of $\mathcal{O}_{K,p}$. So it contradicts the fact that I is a maximal ideal of $\mathcal{O}_{K,p}$. Thus, ϕ preserves

[2]An ideal I of a ring R is proper if I is a proper subset of R.

maximality. □

This proposition shows a connection between integral ideals of $\mathcal{O}_{K,p}$ and integral ideals of $\mathcal{O}_K$ that are coprime to $\mathfrak{p}$. Based on this relationship, it is easy to find the structure of the class group and a class number formula for fake real quadratic orders.

Proposition 3.7. [Coh13] The class group $Cl_{K,p}$ of $\mathcal{O}_{K,p}$ is canonically isomorphic to $Cl_K/\langle[\mathfrak{p}]\rangle$, where Cl_K is the ideal class group of K and $\langle[\mathfrak{p}]\rangle$ is the cyclic subgroup of Cl_K generated by the class of $\mathfrak{p}$. In particular, we have $h_{K,p} = |Cl_{K,p}| = h_K/o(\mathfrak{p})$.

Proof. Consider the map φ from ideal classes in Cl_K to ideal classes in $Cl_{K,p}$ such that

$$\varphi([\mathfrak{a}]) = \left[\phi^{-1}(\mathfrak{a})\right] = [\mathfrak{a}\mathcal{O}_{K,p}]\,.$$

It is clear to see that φ is a well-defined group homomorphism. By Proposition 3.6, the map $\mathfrak{a} \to \mathfrak{a}\mathcal{O}_{K,p}$ is a bijection for all integral ideals $\mathfrak{a}$ of $\mathcal{O}_K$ coprime to $\mathfrak{p}$. So a principal ideal in $\mathcal{O}_{K,p}$ has the form $x\mathcal{O}_{K,p}$ where $x \in \mathcal{O}_K$. If $\mathfrak{a}\mathcal{O}_{K,p} = x\mathcal{O}_{K,p}$ for some $x \in \mathcal{O}_K$, then $\mathfrak{a} = x\mathfrak{p}^k$ for some $k \in \mathbb{Z}$. Therefore,

$$[\mathfrak{a}] = [x\mathfrak{p}^k] = [(x)\mathfrak{p}^k] = [\mathfrak{p}^k] = [\mathfrak{p}]^k \in \langle[\mathfrak{p}]\rangle\,.$$

Moreover, $[\mathfrak{p}] \in \ker(\varphi)$ as $\mathfrak{p}\mathcal{O}_{K,p} = \mathcal{O}_{K,p}$. Hence, $\ker(\varphi) = \langle[\mathfrak{p}]\rangle$. By the fundamental isomorphism theorem, we have

$$Cl_K/\langle[\mathfrak{p}]\rangle \cong Cl_{K,p}.$$

It follows immediately that $h_{K,p} = |Cl_{K,p}| = h_K/o(\mathfrak{p})$. □

The main idea of the proof of Proposition 3.7 is from Oh's thesis while the author corrected some inaccuracies in his proof. For the comparison, please refer to [Oh14, Proposition 1.3].

By Proposition 3.7, we know that given h_K, we can find $h_{K,p}$ by computing $n = o(\mathfrak{p})$. The following algorithm shows how to find the order of $[\mathfrak{p}]$. A standard group element order algorithm is used to find n. We first set $n = h_K$ and find all distinct prime factors $p_1, p_2, ..., p_k$ of h_K. Clearly, the power $\mathfrak{p}^{h_K}$ is a principal ideal. Since $n \mid h_K$, the prime factors of n are also prime factors of h_K. We divide the order by a prime factor multiple times until the power is not a principal ideal, determining the power of that prime factor in the factorization of n. After we repeat this step for each prime factor, the order n will be found. Then $h_{K,p}$ can be computed by $h_{K,p} = h_K/n$.

Algorithm 4 The order of $[\mathfrak{p}]$ in Cl_K

Input: Discriminant $D < 0$, reduced ideal $\mathfrak{s}$ equivalent to $\mathfrak{p}$, class number h_K of $\mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{D})$, all distinct prime factors $p_1, p_2, ..., p_k$ of h_K

Output: The order of $[\mathfrak{p}]$ in Cl_K

1: $i \leftarrow 1, n \leftarrow h_K$
2: **while** $i < k$ **do**
3: **while** $p_i \mid n$ **do**
4: $n \leftarrow n/p_i$
5: Find the reduced ideal $\mathfrak{r}$ equivalent to $\mathfrak{s}^n$
6: **if** $\mathfrak{r} \neq \mathcal{O}_K$ **then**
7: $n \leftarrow n \cdot p_i$, end the inner loop
8: **end if**
9: **end while**
10: $i \leftarrow i + 1$
11: **end while**
12: Return n

Theorem 3.8. Consider an imaginary quadratic order $\mathcal{O}_K$ and a prime number p where $p = \mathfrak{p}\overline{\mathfrak{p}}$ splits in $\mathcal{O}_K$. Given the class number of $\mathcal{O}_K$, h_K, and all its distinct prime factors $p_1, p_2, ..., p_k$, Algorithm 4 computes the order of $\mathfrak{p}$ in $O(\log(|D|)^{4+\epsilon})$ bit operations.

Proof. Algorithm 4 contains two nested loops. Suppose that $h_K = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$. Then the outer loop iterates k times and the inner loop iterates at most e_i times for each $1 \leq i \leq k$. So the total number of iterations is at most $e_1 + e_2 + ... + e_k = O(\log(h_K)) = O(\log(\sqrt{|D|})) = O(\log(|D|))$. Clearly, Step 5 dominates the runtime for each iteration. The computation and the reduction of $\mathfrak{s}^n$ take $O(\log(n)) = O(\log(h_K)) = O(\log(|D|))$ ideal multiplications and reductions while sizes of all the coefficients are bounded by $O(\log(|D|))$ in each step. We assume that the Schönhage-Strassen integer multiplication methods are used, which multiplies two k-bit integers in $O(k \log(k) \log\log(k))$ bit operations [SS71]. So the cost of each multiplication and reduction step is $O(\log(|D|)^{2+\epsilon})$ [Sch91]. It implies that the asymptotic complexity of Algorithm 4 is $O(\log(|D|) \log(|D|) \log(|D|)^{2+\epsilon}) = O(\log(|D|)^{4+\epsilon})$. □

We now give the class number formula for fake real quadratic orders. Before that, we recall the class number formula for imaginary quadratic fields. Gauss already realized the form of the class number formula for quadratic fields in 1801. After that, Dirichlet published a proof of the class number formula in 1839. The Dirichlet class number formula is a famous example using L-functions to compute the class number of a number field. An L-function $L(s, \chi)$ is of the form $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ where χ is a Dirichlet character [Spi69].

Definition 3.9. [FUW99] χ_D is the Kronecker symbol of K and $\chi_D(a) = (\frac{D}{u}) \prod_{i=1}^{k} (\frac{D}{p_i})^{e_i}$, where $a = u p_1^{e_1} ... p_k^{e_k}$ is the prime factorization of a with $u = \pm 1$.

For odd primes p, $\chi_D(p) = (\frac{D}{p})$ is just the Legendre symbol. In addition, $(\frac{D}{1}) = 1$.

$$\left(\frac{D}{-1}\right) = \begin{cases} 1 & : \quad D \geq 0 \\ -1 & : \quad D < 0. \end{cases}$$

$$\left(\frac{D}{2}\right) = \begin{cases} 0 & : \quad D \text{ is even} \\ 1 & : \quad D \equiv \pm 1 \pmod 8 \\ -1 & : \quad D \equiv \pm 3 \pmod 8. \end{cases}$$

For an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$,

$$h(D) = \frac{|\mathcal{O}_K^*| \cdot \sqrt{|D|} L(1, \chi_D)}{2\pi},$$

where $|\mathcal{O}_K^*|$ denotes the number of roots of unity in $\mathbb{Q}(\sqrt{D})$.

By observing the relationship between the class number of imaginary quadratic fields and the class number of fake real quadratic orders, Oh gave a class number formula for fake real quadratic orders and the corresponding proof.

Theorem 3.10. [Oh14, Theorem 1.9] The class number formula for fake real quadratic orders $\mathcal{O}_{K,p}$ is given by

$$h_{K,p} = \frac{|\mathcal{O}_K^*| \sqrt{|D|} L(1, \chi_D)}{2\pi \log_p N(\epsilon_{D,p})},$$

where $\epsilon_{D,p}$ is the fundamental unit of $\mathcal{O}_{K,p}$.

Proof. The class number formula for an imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$ is given by

$$h_K = \frac{|\mathcal{O}_K^*| \sqrt{|D|} L(1, \chi_D)}{2\pi}.$$

By Proposition 3.8, we know that $h_{K,p} = h_K / o(\mathfrak{p})$. Therefore,

$$h_{K,p} = \frac{|\mathcal{O}_K^*| \sqrt{|D|} L(1, \chi_D)}{2\pi o(\mathfrak{p})}.$$

Since the fundamental unit $\epsilon_{D,p}$ is the generator of the principal ideal $\mathfrak{p}^{o(\mathfrak{p})}$, we have $N(\epsilon_{D,p}) =$

$N(\mathfrak{p}^{o(\mathfrak{p})})$. Thus,

$$N(\epsilon_{D,p}) = p^{o(\mathfrak{p})}.$$

Hence,

$$o(\mathfrak{p}) = \log_p N(\epsilon_{D,p}).$$

Then $h_{K,p} = \frac{|\mathcal{O}_K^*|\sqrt{|D|}L(1,\chi_D)}{2\pi \log_p N(\epsilon_{D,p})}$. □

3.4 The Infrastructure of Fake Real Quadratic Orders

In Chapter 2, we described the infrastructure in real quadratic fields. Since fake real quadratic orders and real quadratic orders behave similarly, it is reasonable to expect the existence of such a group-like structure in fake real quadratic orders. We also want to investigate whether the fundamental unit can be easily found by using the infrastructure.

We will see later that the infrastructure of each ideal class in $\mathcal{O}_{K,p}$ is a collection of equivalent reduced ideals. The infrastructure in $\mathcal{O}_{K,p}$ is also a group-like structure in which we can give analogues to the regulator and the distance between two ideals . However, unlike in real quadratic orders, the infrastructure in a fake real quadratic order does not provide a more efficient way to determine the fundamental unit.

Before we define infrastructures in fake real quadratic orders, we first give the definition of reduced ideals in $\mathcal{O}_{K,p}$.

Definition 3.11. An $\mathcal{O}_{K,p}$-ideal $\mathfrak{a}$ is reduced if $\mathfrak{a} \cap \mathcal{O}_K$ is a reduced $\mathcal{O}_K$-ideal.

By Definition 3.11, we know that the map we defined in Proposition 3.6 also preserves reducedness.

We now describe the infrastructure of $\mathcal{O}_{K,p}$. Set

$$\mathcal{C} = \{\mathcal{O}_K, \mathfrak{p}, \mathfrak{p}^2, ..., \mathfrak{p}^{n-1}\} \text{ where } n = o(\mathfrak{p}).$$

By Proposition 3.2, we know that $\mathfrak{p}^k\mathcal{O}_{K,p} = \mathcal{O}_{K,p}$. Let $\mathfrak{r}_k$ be the reduced ideal equivalent to $\mathfrak{p}^k$ in $\mathcal{O}_K$ where $\mathfrak{r}_k = (\theta_k)\mathfrak{p}^k$ for some $\theta_k \in K$. Then we have $\{\mathfrak{r}_k\mathcal{O}_{K,p} \mid 0 \leq k < n\}$ are equivalent in $\mathcal{O}_{K,p}$. Each $\mathfrak{r}_k$ can be obtained by reducing $\mathfrak{r}_{k-1}\mathfrak{p}$ while the corresponding relative generator is denoted as β_k. Then

$$\mathfrak{r}_0 = \mathcal{O}_K = (1)\mathcal{O}_K,\ \theta_0 = 1,$$

$$\mathfrak{r}_1 = (\theta_1)\mathfrak{p} = \mathrm{red}(\mathfrak{p}),$$

$$\mathfrak{r}_2 = (\theta_2)\mathfrak{p}^2 = \mathrm{red}(\mathfrak{r}_1\mathfrak{p}) = \mathrm{red}(\theta_1\mathfrak{p}^2) = (\beta_2\theta_1)\mathfrak{p}^2,$$

$$\mathfrak{r}_3 = (\theta_3)\mathfrak{p}^3 = \mathrm{red}(\mathfrak{r}_2\mathfrak{p}) = \mathrm{red}(\theta_2\mathfrak{p}^3) = (\beta_3\theta_2)\mathfrak{p}^2,$$

$$\ldots$$

$$\mathfrak{r}_k = (\theta_k)\mathfrak{p}^k = \mathrm{red}(\mathfrak{r}_{k-1}\mathfrak{p}) = \mathrm{red}(\theta_{k-1}\mathfrak{p}^k) = (\beta_k\theta_{k-1})\mathfrak{p}^k,$$

$$\ldots$$

$$\mathfrak{r}_{n-1} = (\theta_{n-1})\mathfrak{p}^{n-1} = \mathrm{red}(\mathfrak{r}_{n-2}\mathfrak{p}) = \mathrm{red}(\theta_{n-2}\mathfrak{p}^{n-1}) = (\beta_{n-1}\theta_{n-2})\mathfrak{p}^{n-1},$$

If we continue this procedure, we have

$$\mathfrak{r}_n = (\theta_n)\mathfrak{p}^n = (\theta_n\epsilon)\mathcal{O}_K = (1)\mathcal{O}_K = \mathfrak{r}_0,$$

where ϵ is the fundamental unit of $\mathcal{O}_{K,p}$. Therefore, $\epsilon = \frac{1}{\theta_n}$.

Clearly, $\mathcal{C}' = \{\mathfrak{r}_0\mathcal{O}_{K,p}, \mathfrak{r}_1\mathcal{O}_{K,p}, ..., \mathfrak{r}_{n-1}\mathcal{O}_{K,p}\}$ is a finite set of equivalent reduced ideals of $\mathcal{O}_{K,p}$. We define $\mathcal{C}'$ as the infrastructure of the principal ideal class $[\mathcal{O}_{K,p}]$.

In Section 2.3, when we discussed the infrastructure in real quadratic orders, the distance was defined as

$$\delta(\mathfrak{a}_s, \mathfrak{a}_t) = \log(\theta_t/\theta_s) = \log(\theta_t) - \log(\theta_s)$$

and the regulator is $R_D = \log(\theta_l)$ where l is the number of reduced ideals in the cycle $\mathcal{C}$.

Now we draw an analogue for fake real quadratic orders. Define the distance between $\mathfrak{r}_s$ and $\mathfrak{r}_t$ as

$$\delta(\mathfrak{r}_s, \mathfrak{r}_t) = \log_p(N(\theta_s/\theta_t)) = \log_p(N(\theta_s)) - \log_p(N(\theta_t)).$$

In particular, the distance between $\mathfrak{r}_0$ and $\mathfrak{r}_n$ is

$$\delta(\mathfrak{r}_0, \mathfrak{r}_n) = \log_p(N(\theta_0/\theta_n)) = \log_p(N(1/\theta_n)) = \log_p(N(\epsilon)) = n$$

and we define $R_{D,p} = \log_p(N(\epsilon)) = n$ as the regulator of $\mathcal{O}_{K,p}$.

As we can see, given $\mathfrak{r}_m = (\theta_m)\mathfrak{p}^m$, we can obtain $\mathfrak{r}_{m+1}$ by performing a baby-step, which is a multiplication of $\mathfrak{r}_m$ by $\mathfrak{p}$ followed by a reduction algorithm. Given $\mathfrak{r}_s$ and $\mathfrak{r}_t$, the giant-step requires us to find $\mathfrak{r}_{s+t}$. Since $\mathfrak{r}_s = (\theta_s)\mathfrak{p}^s$ and $\mathfrak{r}_t = (\theta_t)\mathfrak{p}^t$, $\mathfrak{r}_{s+t}$ can be easily found by reducing $\mathfrak{r}_s\mathfrak{r}_t$. This is analogous to the giant step defined in the infrastructure of real quadratic fields.

Suppose that $\mathfrak{r}_k = \mathrm{red}(\mathfrak{p}^k) = (\theta_k)\mathfrak{p}^k$ where $k = s + t$. We give analogues to (2.5) for fake real quadratic orders. Recall that in real quadratic fields, $\mathfrak{r}_k$ is a reduced ideal equivalent to $\mathfrak{r}_s\mathfrak{r}_t$. The relationship between $\delta(\mathfrak{r}_k)$ and $\delta(\mathfrak{r}_s) + \delta(\mathfrak{r}_t)$ is given by

$$\delta(\mathfrak{r}_k) = \delta(\mathfrak{r}_s) + \delta(\mathfrak{r}_t) + \kappa$$

where $-\log(D) < \kappa < \log(2)$, which implies that $\delta(\mathfrak{r}_k) \approx \delta(\mathfrak{r}_s) + \delta(\mathfrak{r}_t)$. For fake real quadratic orders, we also want to find such κ and give upper and lower bounds on it.

Since $\mathfrak{r}_k = (\theta_{s+t})\mathfrak{p}^{s+t}$ is the reduced ideal equivalent to $\mathfrak{p}^{s+t}$, then $\mathfrak{r}_k$ is also the reduced ideal equivalent to $\mathfrak{r}_s\mathfrak{r}_t = (\theta_s\theta_t)\mathfrak{p}^{s+t}$. Suppose that $\mathfrak{r}_k = (\theta)\mathfrak{r}_s\mathfrak{r}_t$ for some $\theta \in K$. Then

$$(\theta_{s+t})\mathfrak{p}^{s+t} = (\theta\theta_s\theta_t)\mathfrak{p}^{s+t}.$$

Thus,

$$\theta_{s+t} = \eta\theta\theta_s\theta_t$$

for some η in the unit group of $\mathcal{O}_K$, i.e., $N(\eta) = 1$. Then we have

$$\delta(\mathfrak{r}_k) = -\log_p(N(\eta)) - \log_p(N(\theta)) + \delta(\mathfrak{r}_s) + \delta(\mathfrak{r}_t) = -\log_p(N(\theta)) + \delta(\mathfrak{r}_s) + \delta(\mathfrak{r}_t).$$

Let $\kappa = \log_p(N(\theta))$. By [JW09, p. 99 Cor.5.5.1], we have $N(\mathfrak{r}_s), N(\mathfrak{r}_t) \leq \sqrt{|D|/3}$. So

$$N(\theta) = N(\mathfrak{r}_k)/(N(\mathfrak{r}_s)N(\mathfrak{r}_t)) \geq 1/(\sqrt{|D|/3}\sqrt{|D|/3}) \geq 1/(|D|/3) = 3/|D|.$$

Thus,

$$\kappa = \log_p(N(\theta)) \geq \log_p(3/|D|) = -\log_p(|D|/3).$$

To find an upper bound on κ, suppose that the reduction of $\mathfrak{r}_s\mathfrak{r}_t$ takes m steps and let

$$\mathfrak{b}_0 = \mathfrak{r}_s\mathfrak{r}_t$$

$$\mathfrak{b}_1 = \rho(\mathfrak{b}_0) = (\gamma_1)\mathfrak{b}_0$$

$$\cdots$$

$$\mathfrak{b}_i = \rho(\mathfrak{b}_{i-1}) = (\gamma_i)\mathfrak{b}_{i-1}$$

$$\cdots$$

$$\mathfrak{b}_m = \rho(\mathfrak{b}_{m-1}) = (\gamma_m)\mathfrak{b}_{m-1}$$

where $\mathfrak{b}_m$ is a reduced ideal equivalent to $\mathfrak{r}_s\mathfrak{r}_t$ and γ_i is the relative generator of $\mathfrak{b}_i$ with respect to $\mathfrak{b}_{i-1}$. Since $\mathfrak{r}_k$ is also the reduced ideal equivalent to $\mathfrak{r}_s\mathfrak{r}_t$, then we have $\mathfrak{b}_m = \mathfrak{r}_k$ by Theorem 2.16. Thus, $N(\theta) = N(\gamma_1)N(\gamma_2)...N(\gamma_m)$. Since $\mathfrak{b}_i$ is not reduced for $0 \leq i \leq m-1$, by [JW09, p. 100 Thm 5.7], we know that $N(\mathfrak{b}_{i+1}) = N(\gamma_{i+1})N(\mathfrak{b}_i) < N(\mathfrak{b}_i)$ for $0 \leq i \leq m-1$.

So $N(\gamma_i) < 1$ for $1 \leq i \leq m$. Then we have $N(\theta) = N(\gamma_1)N(\gamma_2)...N(\gamma_m) < 1$. Thus,

$$\kappa = \log_p(N(\theta)) < \log_p(1) = 0.$$

It follows that $-\log_p(|D|/3) \leq \kappa < 0$.

To find the fundamental unit using the infrastructure, we need to find θ_n. The best method we know to compute θ_n using the infrastructure would be to use baby-steps and giant-steps, where baby-steps are multiplications by $\mathfrak{p}$. This is the same thing as computing the order of $[\mathfrak{p}]$ and a generator of $\mathfrak{p}^n$. Thus, the infrastructure does not provide an easier way to determine the regulator or the fundamental unit than computing the generator of $\mathfrak{p}^n$.

We confined our discussion of infrastructures to the cycle of principal ideals in $\mathcal{O}_{K,p}$. However, like real quadratic fields, each ideal class in $\mathcal{O}_{K,p}$ has its own infrastructure. For any ideal $\mathfrak{a}$ of $\mathcal{O}_K$, set

$$\mathcal{C} = \{\mathfrak{a}\mathfrak{p}^0, \mathfrak{a}\mathfrak{p}^1, \mathfrak{a}\mathfrak{p}^2, ..., \mathfrak{a}\mathfrak{p}^{n-1}\}, \text{ where } n = o(\mathfrak{p}),$$

then the infrastructure of ideal class of $\mathfrak{a}\mathcal{O}_{K,p}$ is defined as

$$\mathcal{C}' = \{\mathfrak{r}_0\mathcal{O}_{K,p}, \mathfrak{r}_1\mathcal{O}_{K,p}, ..., \mathfrak{r}_{n-1}\mathcal{O}_{K,p}\},$$

where $\mathfrak{r}_k$ is the reduced ideal equivalent to $\mathfrak{a}\mathfrak{p}^k$. Clearly, the number of infrastructures in $\mathcal{O}_{K,p}$ is equal to $h_{K,p}$.

3.5 Open Conjectures

In this section, we discuss two open conjectures, the Cohen-Lenstra heuristics and the Ankeny-Artin-Chowla conjecture. Cohen and Lenstra described several heuristics about class groups in real and imaginary quadratic fields [CL84]. In this thesis, we only discuss the

one which conjectures the proportion of real quadratic fields whose class number has odd part one. Cohen found numerical evidence which shows that this conjecture also holds for fake real quadratic orders [Coh13]. As for the Ankeny-Artin-Chowla conjecture, unlike real quadratic fields, counterexamples have been found in fake real quadratic orders [Coh13]. Our goal is to perform computations based on a large data set to support the Cohen-Lenstra heuristics and investigate the existence of counterexamples to the Ankeny-Artin-Chowla conjecture in fake real quadratic orders.

3.5.1 The Cohen-Lenstra Heuristic

The Cohen-Lenstra heuristic under consideration herein relates to the class number problems of quadratic fields, which is one of the most prominent problems in the history of algebraic number theory. The first well-known open problem regarding class numbers of quadratic fields was proposed by Gauss in his book [Gau66] published in 1801.

Gauss Class Number Problem. For a given n, determine the complete list of imaginary quadratic fields with class number n.

Baker and Stark gave independent solutions to this problem for $n = 1$ [Bak67][Sta67] and $n = 2$ [Bak71][Sta75]. After that, Oesterlé solved the case $n = 3$ in 1985 [Oes85] and Arno solved the case $n = 4$ in 1992 [Arn92]. In 1996, Wagner solved the cases $n = 5, 6$ and 7 [Wag96]. Arno et al. solved the problem for odd n satisfying $5 \leq n \leq 23$ in 1993 [ARW98]. Then in 2004, Watkins solved this problem for all class numbers up to 100 [Wat04].

Imaginary quadratic fields are much easier to study than real quadratic fields since the unit group is finite. For any given $n \in \mathbb{Z}$, there are finitely many imaginary quadratic fields with class number n. However, for real quadratic fields, it is conjecturally not the case.

Gauss Conjecture. There are infinitely many real quadratic fields with class number one.

This conjecture is still an open problem but it is believed to be true. Cohen and Lenstra assert that the probability that the odd part of the class number of a real quadratic field is one should exist and converge to a constant number. That is the first of the well-known Cohen-Lenstra heuristics. It came from a number of experimental observations about the class number of real quadratic fields [CL84]. They conjectured that the proportion of real quadratic fields whose class number has odd part one tends to be a fixed number (close to 0.75).

Cohen-Lenstra Heuristic. The proportion of real quadratic fields whose class number has odd part one should exist and be equal to [3]

$$C = 1/\prod_{k\geq 2}(1-2^{-k})\zeta(k) = 0.754458173....$$

Cohen and Lenstra make an extra assumption that real quadratic fields with prime discriminant behave identical to arbitrary real quadratic fields regarding the odd part of the class group. Then C is the probability that $h = 1$ for all prime discriminants.

We now look at fake real quadratic orders. Considering the similarity between fake real quadratic orders and real quadratic orders, it is reasonable to give an analogue to the Cohen-Lenstra Heuristics for fake real quadratic orders. The following conjecture was given in Cohen's unpublished manuscript [Coh13].

Cohen Heuristic. Let p be a prime number and $K = \mathbb{Q}(\sqrt{D})$ an imaginary quadratic field. Then the proportion of prime discriminants $D \equiv 1 \pmod 4$ such that $(\frac{D}{p}) = 1$ satisfying $h_{K,p} = 1$ exists and is equal to the constant $C = 0.754458173....$

Cohen tested the conjecture for all the prime discriminant $D < 2^{28}$ and prime numbers $p < 30$. His data showed that, for a fixed prime p, the proportion did converge to C.

[3] $\zeta(s) = \sum_{n\geq 1}\frac{1}{n^s}$.

However, the convergence rate was slow and it was difficult to determine the pattern of the convergence rate on such a small data set. Cohen suggested that the proportion could be $0.754458 + \frac{80}{\log(x)^3}$ or $0.754458 + \frac{0.49}{x^{1/5}}$, where x is an upper bound on $|D|$. Howeverm, it is difficult to distinguish between a big power of $\log(x)$ and a small power of x when x is small.

Cohen restricts the conjecture to prime discriminants D with $D \equiv 1 \pmod 4$ since the class number h_K is odd in this case. Since we have access to all the fundamental discriminants up to 2^{40} and their class numbers [Mos15], we simply give the following conjecture:

p-Cohen-Lenstra Heuristic. Let p be a prime number. Then the proportion of fake real quadratic orders whose class number has odd part one should exist and be equal to the constant $C = 0.754458173....$

The discussion on the p-Cohen-Lenstra heuristic is based on a fixed prime number p. The author then wondered what the proportion would look like if we fix the discriminant D. In this case, the proportion is determined by the class group structure of $\mathcal{O}_K$.

Heuristic 3.12. Consider a fundamental discriminant $D < 0$. Let Cl_K be the ideal class group of $\mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{D})$. If the odd part of Cl_K is not cyclic, then the probability of $\mathcal{O}_{K,p}$ for which the odd part of $h_{K,p}$ equals one is 0. If the odd part of Cl_K is cyclic, the probability is equal to $\frac{H_1-1}{H_1}\frac{H_2-1}{H_2}...\frac{H_m-1}{H_m}$, where $H_1, H_2, ..., H_m$ are all distinct prime factors of the odd part of h_K.

Proof. Let $h_K = 2^r H$ be the class number of $\mathcal{O}_K$, $h_{K,p}$ be the class number of $\mathcal{O}_{K,p}$, and $n = 2^s N$ be the order of $[\mathfrak{p}]$, where H and N are odd. Then $h_{K,p} = 2^{r-s}\frac{H}{N}$. So the odd part of $h_{K,p}$ is $\frac{H}{N}$. Let $\mathfrak{q} = \mathfrak{p}^{2^s}$, then $[\mathfrak{q}]$ has the order N. So $H = N$ if and only if the odd part of Cl_K is generated by $\mathfrak{q}$.

We first suppose that the odd part of Cl_K is not cyclic, then the subgroup generated by $\mathfrak{q}$ is never equal to the odd part of Cl_K. So N is always a proper divisor of H. In this case,

the odd part of $h_{K,p}$ is never equal to 1. So the probability of $\mathcal{O}_{K,p}$ for which the odd part of the class number equals one is 0.

We now suppose that the odd part of Cl_K is cyclic. In this case, there are H elements in Cl_K and the number of generators is given by $\phi(H)$, where ϕ is Euler's phi function. For convenience of our discussion, we just assume that $\mathfrak{q}$ is randomly distributed among ideals whose classes have odd orders. Then the probability that $\mathfrak{q}$ generates the odd part of Cl_K is $\frac{\phi(H)}{H} = \prod_{t|H}(1-\frac{1}{t})$. So if the odd part of Cl_K is cyclic and $H = H_1^{r_1}H_2^{r_2}...H_m^{r_m}$ is the prime factorization of H, then the probability of $\mathcal{O}_{K,p}$ for which the odd part of $h_{K,p}$ equals one is $\frac{H_1-1}{H_1}\frac{H_2-1}{H_2}...\frac{H_m-1}{H_m}$. □

According to the Cohen-Lenstra heuristics [CL84], for imaginary quadratic fields, the odd part of Cl_K is cyclic more than 97% of the time. So the first case only happens heuristically less than 3% of the time.

When the odd part of Cl_K is cyclic, if H has few prime factors, the probability will be quite large. If H has a lot of prime factors, the probability will be very small. Since the probability that a prime number t divides H is about $1/t + 1/t^2$ [CL84], then H will have few prime factors in most of the time. So for most of the discriminants, the probability will be large.

Specially, if $h_K = 1$ or $h_K = 2^k$ for some $k \in \mathbb{Z}$, the odd part of $h_{K,p}$ is always equal to one. In this case, the probability of $\mathcal{O}_{K,p}$ for which the odd part of the class number equals one is 1. The author did tests for several discriminants and the results support our discussion. Numerical data and examples are described in Chapter 4.

3.5.2 The Ankeny-Artin-Chowla Conjecture

The Ankeny-Artin-Chowla conjecture was published in 1953 by N. C. Ankeny, E. Artin and S. Chowla [AAC52]. It concerns the fundamental unit and the discriminant of certain real quadratic fields. Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic field where D is a prime discriminant

such that $D \equiv 1 \pmod 4$. The fundamental unit of K has the form

$$\epsilon = \frac{a + b\sqrt{D}}{2} \text{ with } a, b \in \mathbb{Z},$$

and the Ankeny-Artin-Chowla conjecture asserts that $D \nmid b$.

The first test of the conjecture was given by Ankeny, Artin and Chowla in 1952 [AAC52]. They verified all prime discriminants less than 2000 with $p \equiv 5 \pmod 8$. After that, the verification for larger primes was continuously provided. In 2000, van der Poorten, Te Riele and Williams gave the verification for all prime discriminants less than $2 \cdot 10^{11}$ [vdPtRW01].

Table 3.1: Verification of the Ankeny-Artin-Chowla conjecture for $D < X$ [Oh14]

X	Investigator(s)	Date
2000	Ankeny, Artin, Chowla, $p \equiv 5$ mod 8 [AAC52]	1952
100000	Goldberg [Mor60]	1954
6279714	Beach, Williams, Zarnke [BWZ71]	1971
100028010	Soleng [Sol86]	1986
1000000000	Stephens, Williams [SW88]	1988
200000000000	van der Poorten, te Riele, Williams [vdPtRW01]	2000

Many mathematicians believe that the Ankeny-Artin-Chowla conjecture holds for real quadratic fields since no counterexamples have been found for D up to $2 \cdot 10^{11}$. However, others think the other way. To state the argument, we assume that for any real quadratic field $K = \mathbb{Q}(\sqrt{D})$ with fundamental $\epsilon = \frac{a+b\sqrt{D}}{2}$, the integer b behaves randomly with respect to divisibility by D. So the probability that we could find a counterexample to the Ankeny-Artin-Chowla conjecture is $\frac{1}{D}$. This number is extremely small for large discriminants like

$D \approx 2 \cdot 10^{11}$. For D up to X, the number of counterexamples we expect to find is given by

$$\sum_{\substack{D<X \\ D\equiv 1 \pmod 4 \\ D \text{ is prime}}} \frac{1}{D},$$

which is of order of $\frac{1}{2}\log\log X$. So even for $X = 2 \cdot 10^{11}$, this number is no more than 1.4. Thus, it is reasonable that no counterexamples have been found for D up to $2 \cdot 10^{11}$. As long as we perform enough experiments, there is a chance to find counterexamples.

Since we believe that fake real quadratic orders behave the same as real quadratic orders, it is reasonable to hypothesize that $D \nmid b$ where $\epsilon = \frac{a+b\sqrt{D}}{2}$ is the fundamental unit of $\mathcal{O}_{K,p}$. We use p-Ankeny-Artin-Chowla conjecture to denote the conjecture in fake real quadratic orders.

However, things are different for the p-Ankeny-Artin-Chowla conjecture. Counterexamples have in fact been found for many pairs of D and p. For example, when $D = -7$ and $p = 347$, the fundamental unit (up to sign) is $\epsilon = 2 + 7\sqrt{-7}$.

Cohen searched for counterexamples with $|D|$ up to 1072000 and p up to 1000. Although a few counterexamples were found, he noticed that there are much fewer counterexamples for larger discriminants. It is possible that no counterexample exists for extremely large discriminants. The other possibility is that counterexamples exist for any prime discriminant. If b behaves randomly with respect to divisibility by D, the chance of finding a counterexample for large discriminants is very small. In fact, our computation showed that the behaviour of b with respect to divisibility by D seems to be close to random. We now describe the algorithm that we used to find counterexamples as follows.

For the p-Ankeny-Artin-Chowla conjecture, prime discriminants are required. Since the fundamental unit $\epsilon = x + y\sqrt{D}$, where $x, y \in (\frac{1}{2})\mathbb{Z}$, is a generator of the principal ideal $\mathfrak{p}^{o(\mathfrak{p})}$, then the order of the ideal class $[\mathfrak{p}]$ is also required. This can be obtained using Algorithm 4, so we just begin our computation by calling Algorithm 4. The main issue is to find a generator of $\mathfrak{p}^{o(\mathfrak{p})}$. The procedure requires ideal reduction algorithms, ideal composition

algorithms, and algorithms to find relative generators, which are described in Section 2.2.

So for the ideal $\mathfrak{p}$, we perform the binary exponentiation algorithm to find $\mathfrak{p}^{o(\mathfrak{p})}$. In each square or composition step, we record the corresponding relative generator. In the end, the multiplication of the proper power of these relative generators modulo D gives us the fundamental unit of $\mathcal{O}_{K,p}$ modulo D. A counterexample is found if the second coefficient of the fundamental unit modulo $|D|$ is equal to zero.

Algorithm 5 Test of the p-AAC Conjecture for $\mathcal{O}_{K,p}$

Input: Prime discriminant D, prime number p, $n = o(\mathfrak{p})$

Output: D and p if $\mathcal{O}_{K,p}$ violates the AAC conjecture

1: Find the prime ideal $\mathfrak{p}$ using the formula (2.2)
2: Write n in binary form as $b_1 b_2 ... b_l$ where b_1 is the lowest bit
3: $\mathfrak{r} \leftarrow \mathfrak{p}$, $i \leftarrow 1$
4: **if** $l = 1$ **then**
5: Reduce $\mathfrak{r}$ and record the relative generator g_1
6: Compute $\epsilon = g_1 \pmod{D}$
7: **end if**
8: **while** $i < l$ **do**
9: $\mathfrak{r} \leftarrow \mathfrak{r}^2$ using normal ideal square algorithm
10: Reduce $\mathfrak{r}$ and record the relative generator g_i
11: **if** $b_i = 1$ **then**
12: $\mathfrak{r} \leftarrow \mathfrak{r} \cdot \mathfrak{p}$ using normal ideal composition algorithm
13: Reduce $\mathfrak{r}$ and record the relative generator g
14: $g_i \leftarrow g_i \cdot g$
15: **end if**
16: $i \leftarrow i + 1$
17: **end while**
18: $\epsilon \leftarrow 1$, $N_\epsilon \leftarrow 1$, $i \leftarrow 1$

Algorithm 5 Test of the p-AAC Conjecture for $\mathcal{O}_{K,p}$ (continued)

19: **while** $i < l$ **do**

20: $\epsilon \leftarrow \epsilon^2 g_i \pmod{|D|}$, $N_\epsilon \leftarrow N_\epsilon^2 N(g_i)$,

21: $i \leftarrow i + 1$

22: **end while**

23: **if** $p^n! = N_\epsilon$ **then**

24: Output error message for D, p and stop

25: **end if**

26: **if** the second coefficient of ϵ equals 0 **then**

27: Return D, p

28: **end if**

Theorem 3.13. Consider a fake real quadratic order $\mathcal{O}_{K,p}$ where $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ and n is the order of $[\mathfrak{p}]$ in Cl_K. Algorithm 5 tests the p-Ankeny-Artin-Chowla conjecture for $\mathcal{O}_{K,p}$ in $O(\sqrt{|D|}^{1+\epsilon}\log(p)^{2+\epsilon})$ bit operations.

Proof. Algorithm 5 contains 4 loops, the loop that computes the binary representation of n (step 2), the loop that computes all relative generators (steps 8-17), the loop that computes $\epsilon \pmod{|D|}$ and $N(\epsilon)$ (steps 19-22), and the loop that computes p^n (step 23). The first loop iterates $l-1$ times and each step does arithmetic with numbers of size $O(\log(n)) = O(\log(h_K)) = O(\log(\sqrt{|D|})) = O(\log(|D|))$. Since $l-1 = O(\log(n)) = \log(|D|)$, the complexity for the first loop is $O(\log(|D|)^{2+\epsilon})$.

The second loop also iterates $l - 1 = O(\log(|D|))$ times. The runtime is dominated by steps 9-10 and steps 12-13. The sizes of coefficients of $\mathfrak{r}$ are bounded by $\log(|D|)$, so steps 9-10 have complexity $\log(|D|)^{2+\epsilon}$. Since $\mathfrak{p}$ has coefficients with sizes $O(\log(p))$, then steps 12-13 has complexity $O(\max\{\log(|D|), \log(p)\}^{2+\epsilon})$. Thus, the second loop has complexity $O(\log(|D|)\max\{\log(|D|), \log(p)\}^{2+\epsilon})$.

The third loop iterates $l - 1 = O(\log(|D|))$ times and the runtime is dominated by

step 20. For the computation $\epsilon^2 g_i \pmod{|D|}$, all the coefficients are bounded by $\log(|D|)$, which implies that the computation of $\epsilon^2 g_i \pmod{|D|}$ has complexity $O(\log(|D|)^{1+\epsilon})$. For the norm computation $N_\epsilon^2 N(g_i)$, the size of N_ϵ is bounded by $O(\log(N(\epsilon))) = O(\log(p^n)) = O(\sqrt{|D|}\log(p))$ while the size of $N(g_i)$ is bounded by $O(\log(|D|)) = O(\sqrt{|D|}\log(p))$. So computing $N_\epsilon^2 N(g_i)$ has complexity $O(\sqrt{|D|}^{1+\epsilon}\log(p)^{1+\epsilon})$. Thus, the complexity of the third loop is

$$O(\log(|D|)(\log(|D|)^{1+\epsilon} + \sqrt{|D|}^{1+\epsilon}\log(p)^{1+\epsilon})) = O(\sqrt{|D|}^{1+\epsilon}\log(p)^{1+\epsilon}).$$

The last loop iterates $\log(n) = \log(|D|)$ times with each step does arithmetic with numbers of size $\log(p)$. So the complexity for the last loop is $O(\log(|D|)\log(p)^{1+\epsilon})$.

Thus, the complexity of Algorithm 5, which is dominated by the second and the third loops, is equal to

$$O(\log(|D|)\max\{\log(|D|), \log(p)\}^{2+\epsilon} + \sqrt{|D|}^{1+\epsilon}\log(p)^{1+\epsilon}) = O(\sqrt{|D|}^{1+\epsilon}\log(p)^{2+\epsilon})$$

□

Before using this fast algorithm, the author tried to find the fundamental unit with Cornacchia's Algorithm [Cor08]. This algorithm is used for solving the Diophantine equation $x^2 + dy^2 = m$. In our context, we need to solve the equation $x^2 - Dy^2 = 4p^n$ to find the coefficients of the fundamental unit $\epsilon = \frac{x}{2} + \frac{y\sqrt{D}}{2}$ where n is the order of $[\mathfrak{p}]$ and $x, y \in \mathbb{Z}$. This algorithm is presented in Algorithm 6.

The time complexity for solving the equation $x^2 + dy^2 = 4N$ is known as $O(\log(N)^{2+\epsilon})$ in bit operations assuming $d < 4N$ [FS16]. In the equation $x^2 - Dy^2 = 4p^n$, we know that $4p^n = O(p^{\sqrt{|D|}})$ and $|D| = O(p^{\sqrt{|D|}})$ is always true. Hence, we can just assume $|D| < 4p^n$ for our asymptotic analysis. So our computation has complexity $O(\log(p^n)^{2+\epsilon}) = O(n^{2+\epsilon}\log(p)^{2+\epsilon}) = O(h_K^{2+\epsilon}\log(p)^{2+\epsilon}) = O(\sqrt{|D|}^{2+\epsilon}\log(p)^{2+\epsilon}) = O(|D|^{1+\epsilon}\log(p)^{2+\epsilon})$. The

author implemented the algorithm and found that this algorithm was much slower than the ideal reduction algorithm, as expected. For example, the author randomly picked a large discriminant $D = -1073741824003$ and $p = 107, 109$. For both cases, it took around 2 hours to find the fundamental unit using Cornacchia's algorithm but only 1 second using the ideal reduction algorithm.

Algorithm 6 Fundamental Unit of $\mathcal{O}_{K,p}$ using the Cornacchia's Algorithm

Input: Prime discriminant D, prime number p, $n = o(\mathfrak{p})$

Output: Fundamental unit $\epsilon = \frac{x}{2} + \frac{y\sqrt{D}}{2}$ of $\mathcal{O}_{K,p}$

1: Find $r_0 \in \mathbb{Z}$ with $r_0 < 2p^n$ such that $r_0^2 \equiv D \pmod{4p^n}$ using Hensel's Lifting Lemma [BW00, §138]

2: Use the Euclidean algorithm to find $r_1 \equiv 4p^n \pmod{r_0}$, $r_2 \equiv r_0 \pmod{r_1}$, $r_3 \equiv r_1 \pmod{r_2}$... until $r_k < 2\sqrt{p^n}$

3: $x \leftarrow r_k$, $y \leftarrow \sqrt{\frac{4p^n - x^2}{-D}}$

Chapter 4

Implementation and Numerical Results

In this chapter, we present numerical results of our program, which was designed to test the p-Cohen-Lenstra heuristics and the p-Ankeny-Artin-Chowla conjecture in fake real quadratic orders. By collecting the results, we then verified the p-Cohen-Lenstra heuristics and found counterexamples for the p-Ankeny-Artin-Chowla conjecture. In Section 4.1, we introduce the computer systems that we used to run the programs. Then we discuss the implementation and performance of the program. In Sections 4.2 and 4.3, we desribe more results on the p-Cohen-Lenstra Heuristics and the p-Ankeny-Artin-Chowla conjecture, respectively.

4.1 Implementation

We used the C language for programming. Our computation relies on Sayles' C libraries *optarith* and *qform* [Say13], which contain a fast implementation of binary quadratic form arithmetic. The GNU MP Bignum library was also used when computing the fundamental unit modulo D of a fake real quadratic order. Before the introduction of the implementation, we first describe the resources we have access to.

1. Mosunov has tabulated the class group decompositions and class numbers for all the

fundamental discriminants $|D| < 2^{40}$ [Mos15]. All the data (2.1Tb) is stored on the penguin1 server in the Department of Computer Science at the University of Calgary. The data are stored in four folders according to the congruence class of $|D|$ modulo 8 or 16. These four folders are cl3mod8, cl7mod8, cl4mod16 and cl8mod16. Each folder contains 4096 compressed files with indices $0, 1, 2, ..., 4095$. The file with index l contains data for $l \cdot 2^{28} < |D| < (l+1) \cdot 2^{28}$. For example, the file cl7mod8.45.gz contains data for $45 \cdot 2^{28} < |D| < 46 \cdot 2^{28}$ with $|D| \equiv 7 \bmod 8$. For file cl$A$mod$M.I$.gz, where $(A, M) = (3, 8), (7, 8), (4, 16)$ or $(8, 16)$ and $I = 0, 1, ..., 4095$, after we decompress the file, it has the following format:

- There is one line for each discriminant
- Discriminants are listed in ascending order (in absolute value)
- Line i for i^{th} discriminant D_i has the form $a\ b\ c_1c_2...c_t$
- $|D_i| = |D_{i-1}| + aM$, $h(\mathbb{Q}(D_i)) = b$, invariant factors for the class group are $[c_1, c_2, ..., c_t]$ and $b = c_1c_2...c_t$
- $|D_1|$ is given by $|D_1| = I \cdot 2^{28} + a_1$ where a_1 is the first number in line 1

2. To find the order of $[\mathfrak{p}]$, we need to perform ideal algorithms in Cl_K. This part is credited to Maxwell Sayles, who implemented almost all the ideal algorithms we needed [Say13]. By using his C libraries *liboptarith* and *libqform*, we can easily find the prime ideal $\mathfrak{p}$ above p. The multiplication, exponentiation and reduction algorithms are also included in his program [Say13]. The only thing we need to add is the relative generator computation.

Our computations were performed on four different systems.

- **Storm**: A server located at the University of Calgary. 700 cores with 10TB storage space for all users.
- **Breezy**: A WestGrid system located at the University of Calgary. 384 cores with 320TB storage space shared with Parallel and Lattice WestGrid systems.

- **Grex**: A WestGrid system located at the University of Manitoba. 3792 cores with 110TB disk space for local users.

- **Orcinus**: A WestGrid system located at the University of British Columbia. 9600 cores with 430TB storage space for all users.

Since the computation for the p-Cohen-Lenstra Heuristics and the p-Ankeny-Artin-Chowla conjecture both require the order of $[\mathfrak{p}]$ and the same dataset, the author combined these computations. Considering the limit of the resources and the unpredictable performance of each system, the computation was performed stage by stage. Stage k was for index between $(k-1)\cdot 1024$ and $k\cdot 1024$. To compare the speed of each system, the author did tests for all discriminants with index=0 and primes $p = 2, 3, 5, 7, 11$. We present the runtime for each system.

Table 4.1: Runtime for the p-CL Heuristic and the p-AAC Conjecture, index=0

Systems	Timing(seconds)
Storm	9124
Breezy	7882
Orcinus	5991
Grex	5601

How to distribute the jobs depends on the speed of each system. Since Storm is the slowest one, we ran our program with smaller indices on it. Since Grex and Orcinus are faster, programs with larger indices were run on these two systems. What is more, Storm is not as busy as the other systems. There were around 300 processors available to the author. However, the number of available processors of each WestGrid system is unknown and variable. Adjustments were made while we performed the computation. At first, the author did computations for $p = 2, 3, 5, 7, 11$. The jobs distributions can be found in Table

4.2.

Table 4.2: Index distribution for the p-CL Heuristic and the p-AAC Conjecture, $p = 2, 3, 5, 7, 11$

Systems	Stage 1	Stage 2	Stage 3	Stage 4
Storm	0-399	1024-1499/2000-2047	2048-2599	3900-4095
Breezy	400-767	1500-1799	2600-2999	N/A
Grex	768-1023	1800-1999	N/A	N/A
Orcinus	N/A	N/A	3000-3071	3072-3899

The computation was finished within 15 days. Not surprisingly, the runtime was longer for larger indices. For example, the runtime for index=0 was 9124 seconds (Storm), 117983 seconds for index=1023 (Grex), 171595 seconds for index=2047 (Storm), 204225 seconds for index=3071 (Orcinus) and 252120 seconds for index=4095(Storm). After that, computations were done for $p = 101, 1009$ to check if the conjectures also hold for bigger primes. Job distributions for these computations are listed in Table 4.3.

Table 4.3: Index distribution for the p-CL Heuristic and the p-AAC Conjecture, $p = 101, 1009$

Systems	Stage 1	Stage 2	Stage 3	Stage 4
Storm	0-1023	1024-2047	2048-2999	N/A
Orcinus	N/A	N/A	3000-3071	3072-4095

The computation was finished within 20 days. It took more time than the computation with the five smallest primes. The runtime for index=0 was 5222 seconds (Storm), 162514 seconds for index=1023 (Storm), 240387 seconds for index=2047 (Storm), 303048 seconds for index=3071 (Storm) and 359257 seconds for index=4095(Orcinus).

We list the runtimes for indices equal to $X-1$, where $X=2^k$ for $k=0,1,2,...12$, i.e., $|D|$ is between $(2^k-1)\cdot 2^{28}$ and $2^k\cdot 2^{28}$.

Table 4.4: Runtimes for the p-CL Heuristic and the p-AAC Conjecture, $p=2,3,5,7,11$

X	Timing (Seconds)	X	Timing (Seconds)
1	9125	128	41673
2	10938	256	57934
4	12871	512	72178
8	15538	1024	117984
16	18711	2048	171595
32	23591	4096	252121
64	30765		

Table 4.5: Runtimes for the p-CL Heuristic and the p-AAC Conjecture, $p=101,1009$

X	Timing (Seconds)	X	Timing (Seconds)
1	5222	128	51535
2	6988	256	74777
4	9094	512	110002
8	12212	1024	162514
16	16870	2048	240387
32	24032	4096	359257
64	34880		

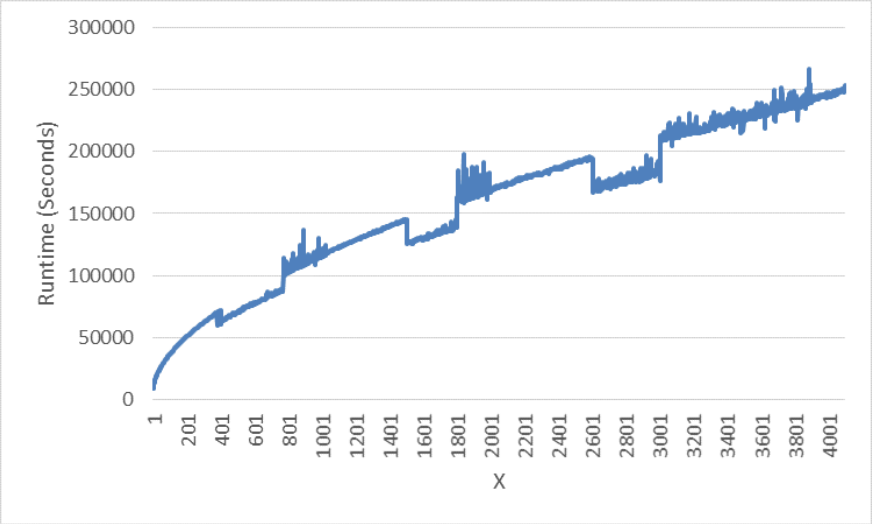

Figure 4.1: Runtimes for the p-CL Heuristic and the p-AAC Conjecture, $p = 2, 3, 5, 7, 11$

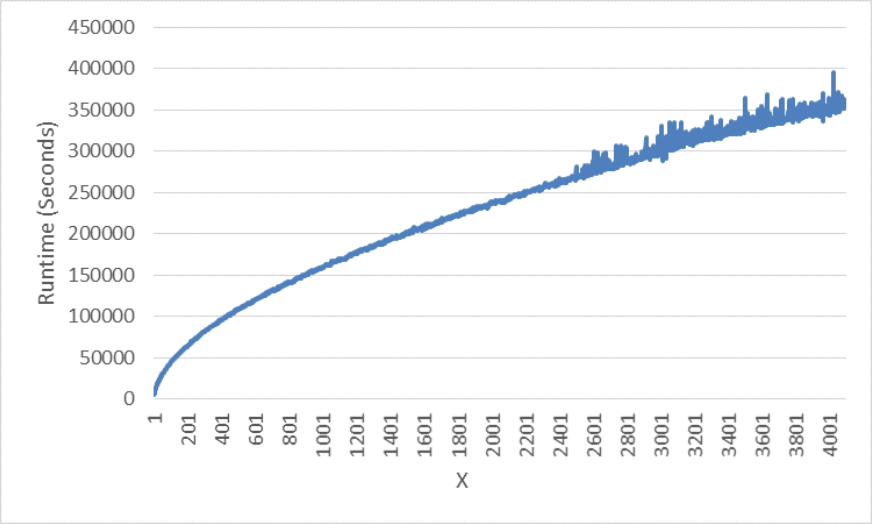

Figure 4.2: Runtimes for the p-CL Heuristic and the p-AAC Conjecture, $p = 101, 1009$

We now look at the runtimes of our program in detail. Clearly, the most important components of our program are the data reading (to obtain D and h_K), the factorization of h_K, the computation of $h_{K,p}$ (or computation of the order of $[\mathfrak{p}]$), the primality test on D, and the test of the p-Ankeny-Artin-Chowla conjecture. The runtime increases as the index increases. We are interested in the part of the computation that increases most significantly and takes most of the runtime. If we can improve that part, the program will run much faster.

The author ran the program for the p-Cohen-Lenstra heuristic and the p-Ankeny-Artin-Chowla conjecture with $p = 2, 3, 5, 7, 11$ and indices $2^k - 1$ where $k = 0, 1, ..., 12$. Table 4.6 shows the timing (in seconds) for each part of the computation and the total runtime. Note that $X = 2^k$ for $k = 0, 1, ..., 12$, so the upper bound on $|D|$ is given by $X \cdot 2^{28}$. The test was done on Storm, and the total runtimes might be slightly different from those in Table 4.4.

For the factorization of h_K, we have two options. The first one is to create a table with the factorizations of all the integers up to the upper bound on h_K. We consult this table to find the factorization of the class number when we need it. The second method is to factor h_K each time we need it. The first method is space consuming while the second one is time consuming. The author tried both methods and found that for large indices like 2047 or 4095, the first method took at least 30Gb memory, while the memory limit for most of our systems is less than 10Gb. According to Algorithm 4, our program only requires all the distinct prime factors of h_K. Since the upper bound of h_K for $|D|$ up to 2^{40} is less than 10^{10} [Mos15, p. 51], then the number of distinct prime factors of h_K is less than 10. It only takes several bytes to store these prime factors. So we chose to factor h_K in each computation.

Figures 4.3-4.8 plot the total runtime and the runtime for each computation part. Figure 4.9 shows the runtime percentage of each computation part. Each bar height is not exactly equal to 100% as there are some other parts which we did not take into account, like "prime sieve" and data writing.

For the h_K factorization, we need to find all the primes that divide h_K. We use trial division here. There are asymptotically faster factoring algorithms such as the number field sieve. However, it is not worth employing a faster but more complicated factoring method since h_K is relatively small (not much larger than 2^{20}) under consideration. In the worst case, the number of iterations is the number of prime numbers less than h_K, which is approximately $\frac{h_K}{\log(h_K)} = O(\frac{\sqrt{|D|}}{\log(\sqrt{|D|})}) = O(\frac{\sqrt{|D|}}{\log(|D|)})$. The cost of each iteration is $O(\log(|D|)^{1+\epsilon})$. Thus, the complexity of h_K factorization is $O(\frac{\sqrt{|D|}}{\log(|D|)} \log(|D|)^{1+\epsilon}) = O(\sqrt{|D|}^{1+\epsilon})$.

We us trial division for the primality test of D. This requires the division of $|D|$ by all the

prime numbers less than $\sqrt{|D|}$ (the worst case). So the number of iterations is approximately $\frac{\sqrt{|D|}}{\log(\sqrt{|D|})}$. Like the h_K factorization, primality test also has complexity $O(\sqrt{|D|}^{1+\epsilon})$. There are much faster primality tests but the factorization of h_K would then generally still dominate asymptotically over the primality test.

The complexity of the class number computation is the same as Algorithm 4, which is $O(\log(|D|)^{4+\epsilon})$. The test of the p-AAC conjecture, as we described in Theorem 3.13, has complexity $O(\sqrt{|D|}^{1+\epsilon}\log(p)^{2+\epsilon})$. Thus, the whole program has complexity

$$O(\sqrt{|D|}^{1+\epsilon}\log(p)^{2+\epsilon} + \log(|D|)^{4+\epsilon} + 2\sqrt{|D|}^{1+\epsilon}) = O(\sqrt{|D|}^{1+\epsilon}\log(p)^{2+\epsilon}).$$

Table 4.6: Runtime components for the p-CL heuristic and the p-AAC conjecture for $p = 2, 3, 5, 7, 11$

X	Data Reading	h_K Factorization	$h_{K,p}$	$\epsilon \pmod D$	AAC	Total
1	27	308	4897	3009	1050	9513
2	25	433	5351	3719	1660	11406
4	27	564	5690	4604	2299	13415
8	34	725	6001	5826	3099	15958
16	34	916	6282	7700	4098	19307
32	27	1144	6559	10686	5427	24072
64	27	1466	6856	15503	7165	31265
128	29	1879	7197	23159	9516	42014
256	29	2417	7553	35531	12629	58400
512	31	3136	7880	54475	16765	82544
1024	31	4082	8231	83706	22369	118681
2048	33	5319	8600	126951	29834	171021
4096	42	6990	8990	193072	39927	249351

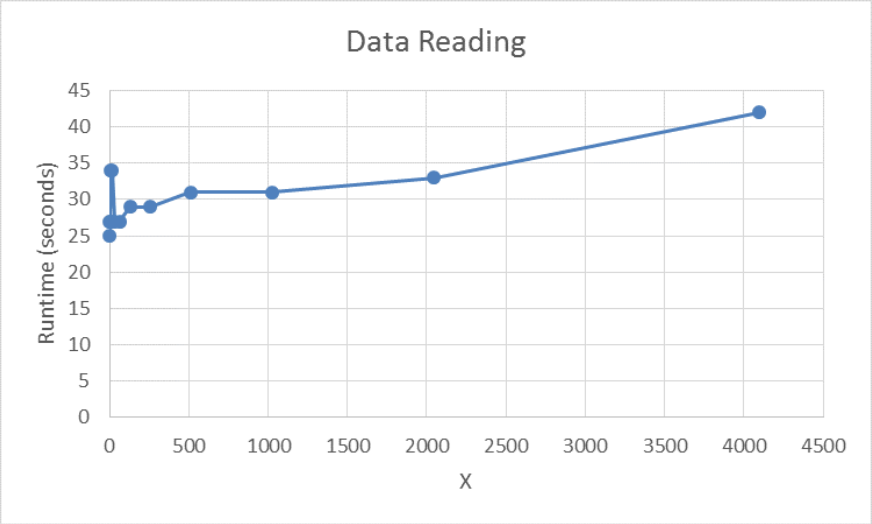

Figure 4.3: Runtime of Data Reading for the p-CL heuristic and the p-AAC conjecture for $p = 2, 3, 5, 7, 11$

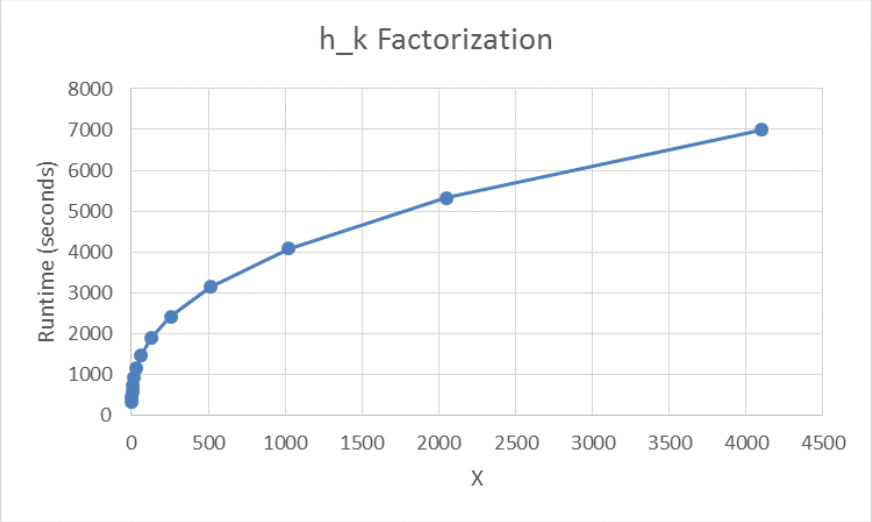

Figure 4.4: Runtime of h_K Factorization for the p-CL heuristic and the p-AAC conjecture for $p = 2, 3, 5, 7, 11$

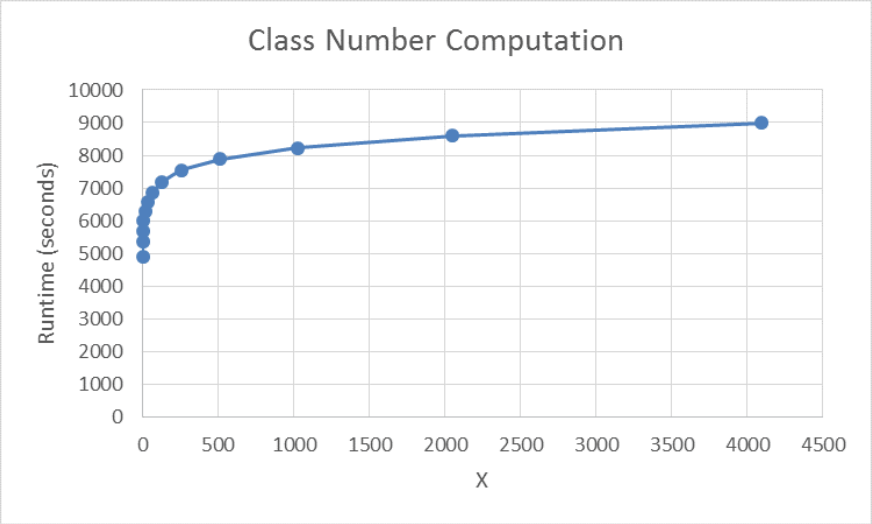

Figure 4.5: Runtime of Class Number Computation for the p-CL heuristic and the p-AAC conjecture for $p = 2, 3, 5, 7, 11$

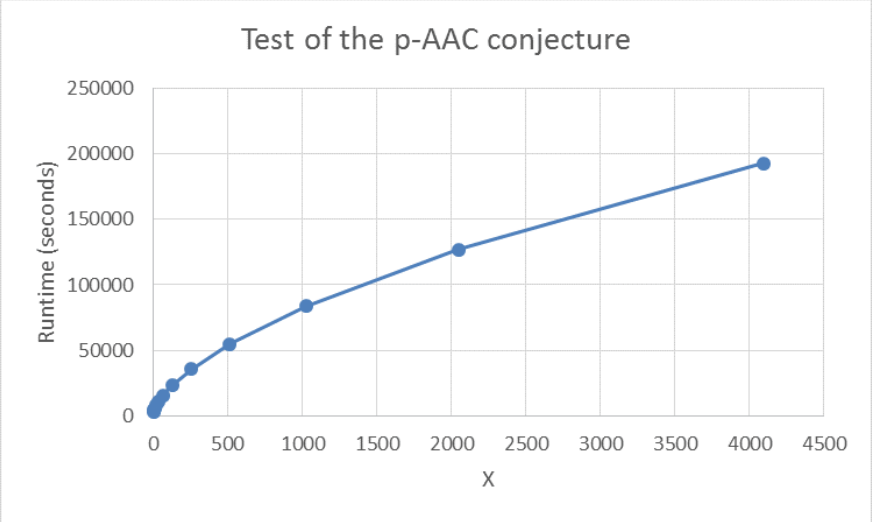

Figure 4.6: Runtime of the Test of the p-AAC conjecture inside the tests for the p-CL heuristic and the p-AAC conjecture for $p = 2, 3, 5, 7, 11$

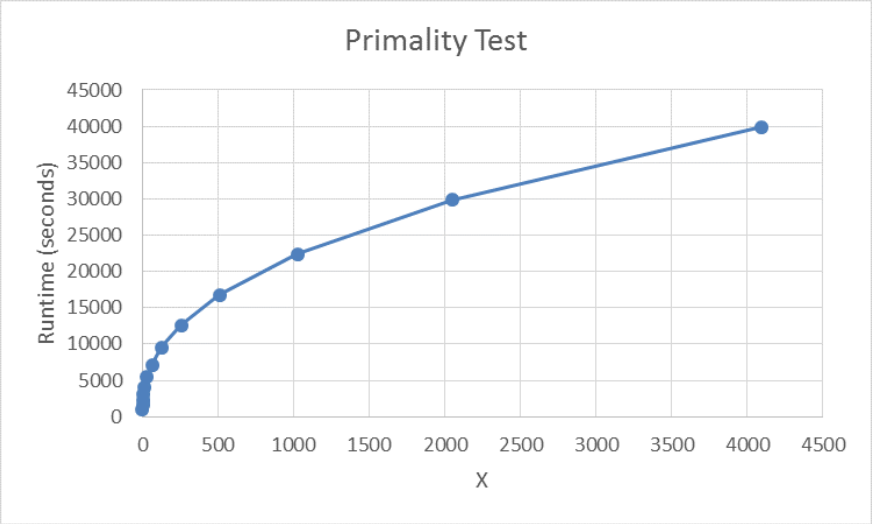

Figure 4.7: Runtime of Primality Test for the p-CL heuristic and the p-AAC conjecture for $p = 2, 3, 5, 7, 11$

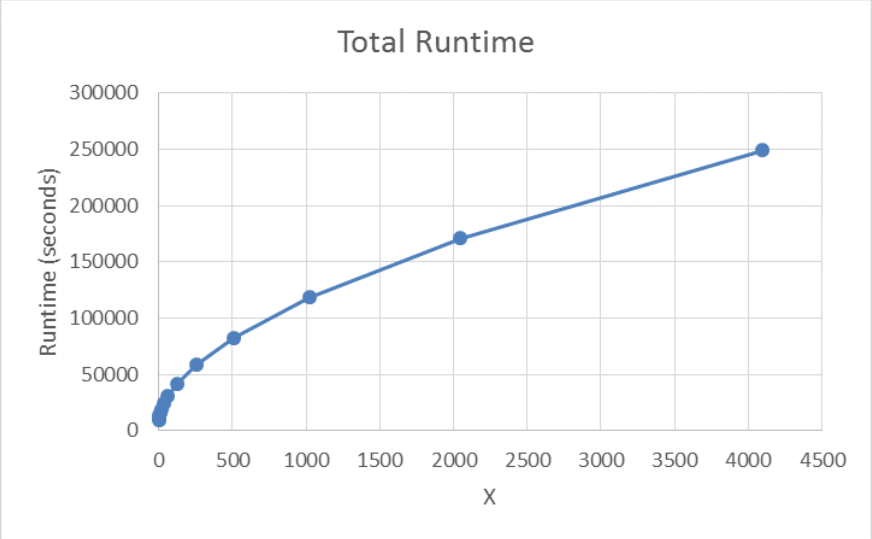

Figure 4.8: Total Runtime for the p-CL heuristic and the p-AAC conjecture for $p = 2, 3, 5, 7, 11$

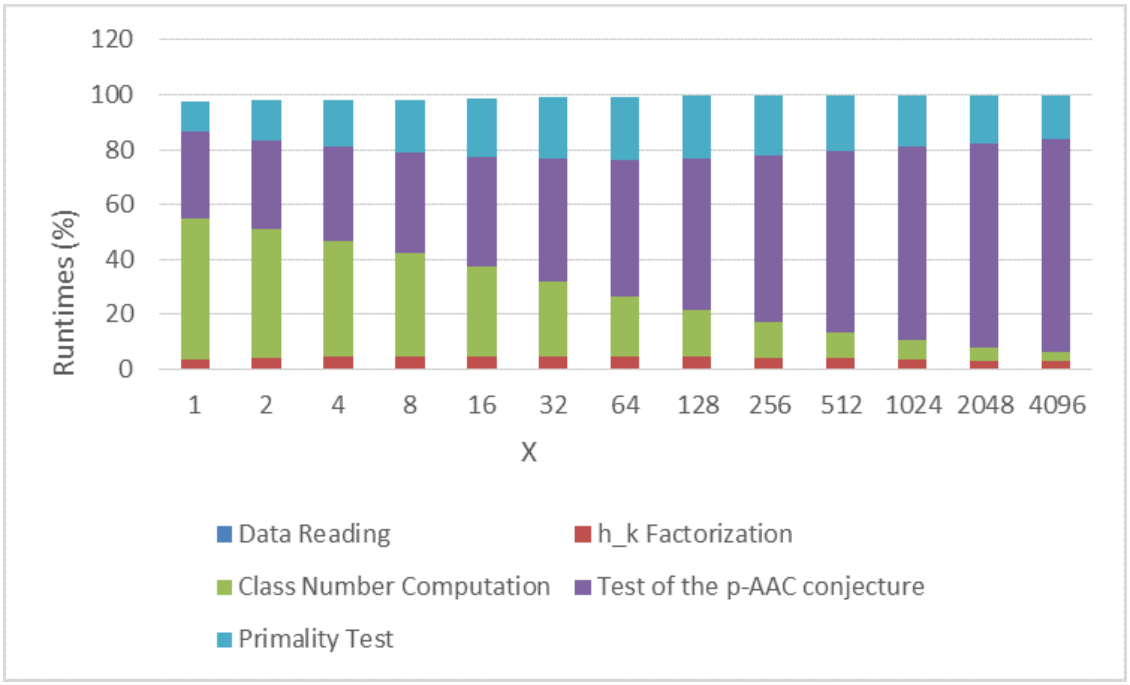

Figure 4.9: Runtime components for the p-CL heuristic and the p-AAC conjecture for $p = 2, 3, 5, 7, 11$

The runtime for each state matches our asymptotic estimate very well. As we can see in Table 4.6 and Figure 4.9, the computing time for the test of the p-AAC conjecture increases most significantly and takes most of the runtime. This is caused by the norm computation in step 20 in Algorithm 5. If we omit the norm test, the run time is then dominated by the loop in steps 8-17, which has complexity $O(\log(|D|)(\max\{\log(|D|), \log(p)\}^{2+\epsilon}) = O(\log(|D|)^{3+\epsilon})$ when p is fixed. In this case, the entire program has complexity $O(\sqrt{|D|}^{1+\epsilon})$.

Figures 4.10-4.11 show the timing for the test of p-AAC conjecture and the total runtime without norm tests. In Figure 4.10, though it is not smooth, we can still see that the graph looks roughly like $O(\log(|D|)^3)$. The total runtime without the norm test again scales like $O(\sqrt{|D|})$. Clearly, without norm tests, the total runtime is dominated by the h_K factorization and the primality test. The asymptotic runtime is the same with and without the norm tests (assuming p is negligible) while the version without the norm tests is in practice much faster. Thus, to feasibly extend the computations to larger parameters, the norm test in Algorithm 5 should be removed and more efficient factoring and primality

testing methods might be employed.

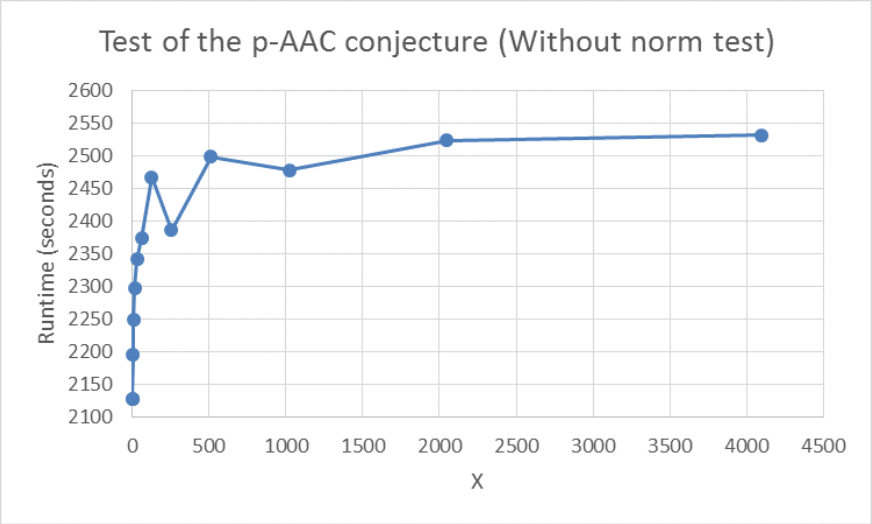

Figure 4.10: Runtime of the Test of the p-AAC conjecture inside the tests for the p-CL heuristic and the p-AAC conjecture for $p = 2, 3, 5, 7, 11$ without norm tests

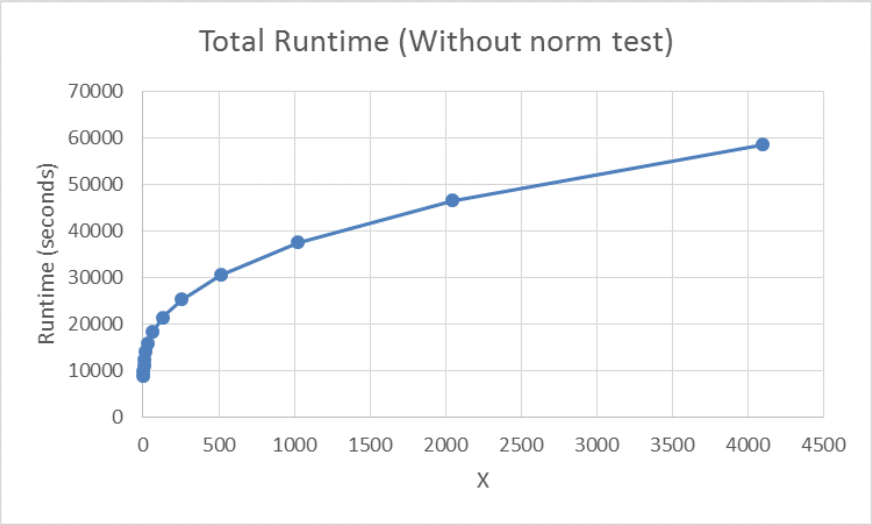

Figure 4.11: Total Runtime for the p-CL heuristic and the p-AAC conjecture for $p = 2, 3, 5, 7, 11$ without norm tests

4.2 The p-Cohen-Lenstra Heuristic

For the heuristic of p-Cohen-Lenstra, we want to find the proportion of D for which the odd part of $h_{K,p}$ equals one. The author did tests for $|D| < 2^{40}$ and primes $p = 2, 3, 5, 7, 11, 101, 1009$.

Table 4.7 shows some of our results. Each entry denotes the proportion of discriminants $|D| < X \cdot 2^{28}$ such that the odd part of class number equals one for some fixed p. We picked $X = 2^k$ where $k = 0, 1, 2, ..., 12$.

Table 4.7: Proportion of D with $|D| < X \cdot 2^{28}$ for which the odd part of $h_{K,p}$ equals one

X	$p = 2$	$p = 3$	$p = 5$	$p = 7$	$p = 11$	$p = 101$	$p = 1009$
1	0.771884	0.771422	0.770716	0.770444	0.769551	0.766553	0.76447
2	0.769482	0.769101	0.768603	0.768314	0.767633	0.764972	0.763155
4	0.767504	0.767141	0.766719	0.76644	0.765911	0.76362	0.762071
8	0.765775	0.765499	0.765129	0.764904	0.76441	0.762479	0.761145
16	0.764288	0.764081	0.763727	0.763556	0.76316	0.76147	0.760289
32	0.763043	0.762841	0.762554	0.762399	0.762067	0.760606	0.759578
64	0.761955	0.761779	0.761551	0.761405	0.761122	0.759849	0.758957
128	0.761023	0.760879	0.76067	0.760549	0.760309	0.759195	0.758431
256	0.760222	0.760096	0.759916	0.75981	0.7596	0.758625	0.757961
512	0.759524	0.759418	0.759254	0.759169	0.758985	0.758131	0.757545
1024	0.758915	0.758819	0.758683	0.758608	0.758442	0.757702	0.757187
2048	0.758385	0.758299	0.758183	0.758113	0.757973	0.757321	0.756872
4096	0.757922	0.75785	0.757746	0.757684	0.757563	0.756988	0.756593

Figures 4.12-4.19 show proportions of D for which the odd part of $h_{K,p}$ equals one for each fixed p.

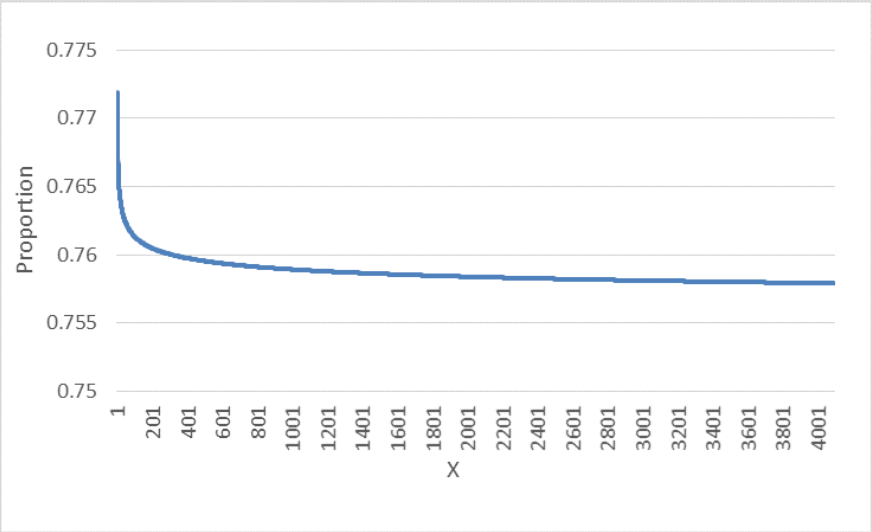

Figure 4.12: p-Cohen-Lenstra Heuristic $p = 2$

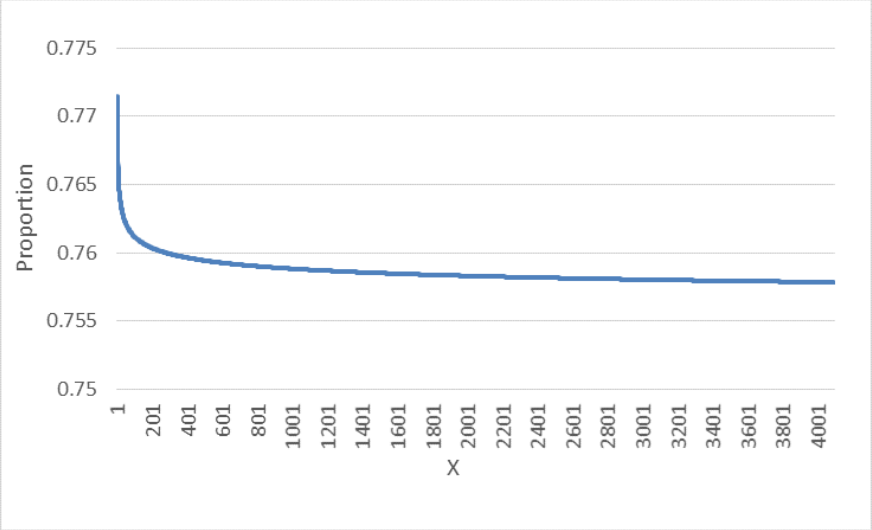

Figure 4.13: p-Cohen-Lenstra Heuristic $p = 3$

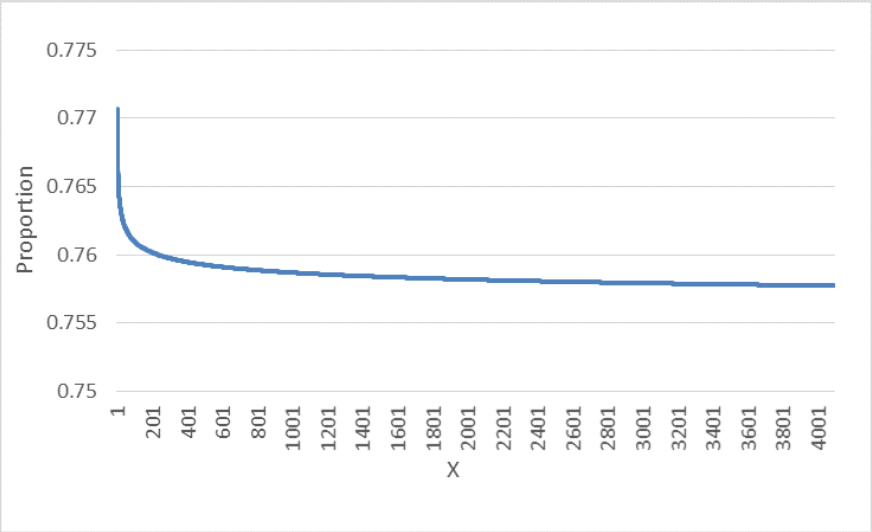

Figure 4.14: p-Cohen-Lenstra Heuristic $p = 5$

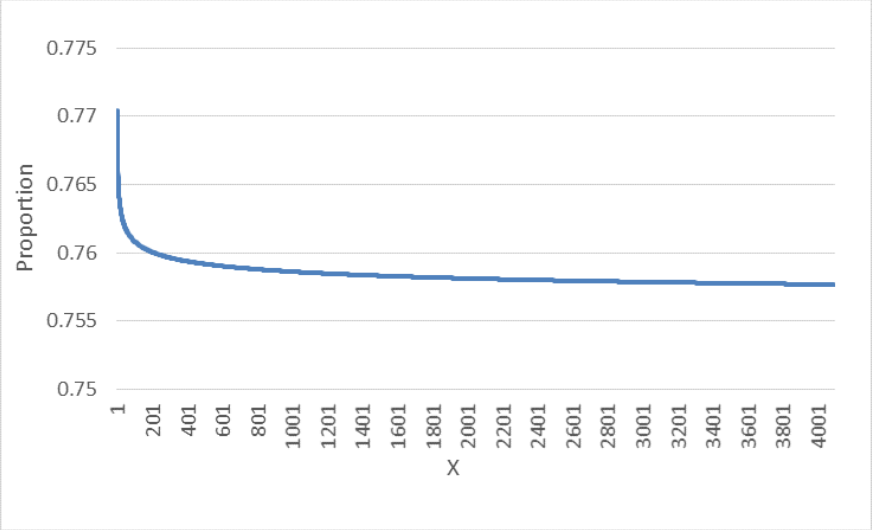

Figure 4.15: p-Cohen-Lenstra Heuristic $p = 7$

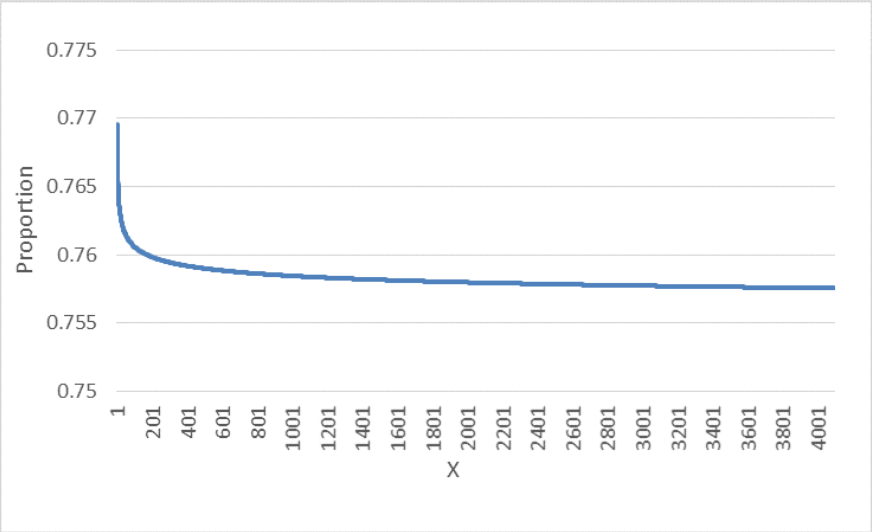

Figure 4.16: p-Cohen-Lenstra Heuristic $p = 11$

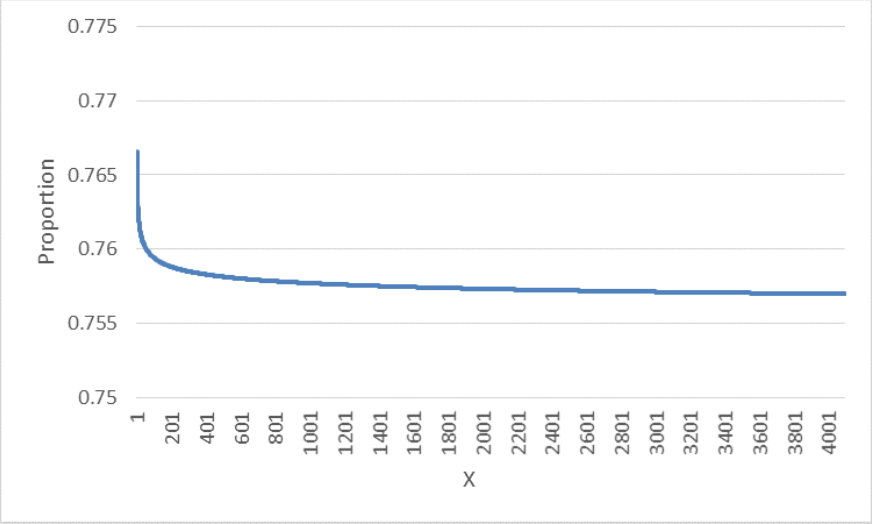

Figure 4.17: p-Cohen-Lenstra Heuristic $p = 101$

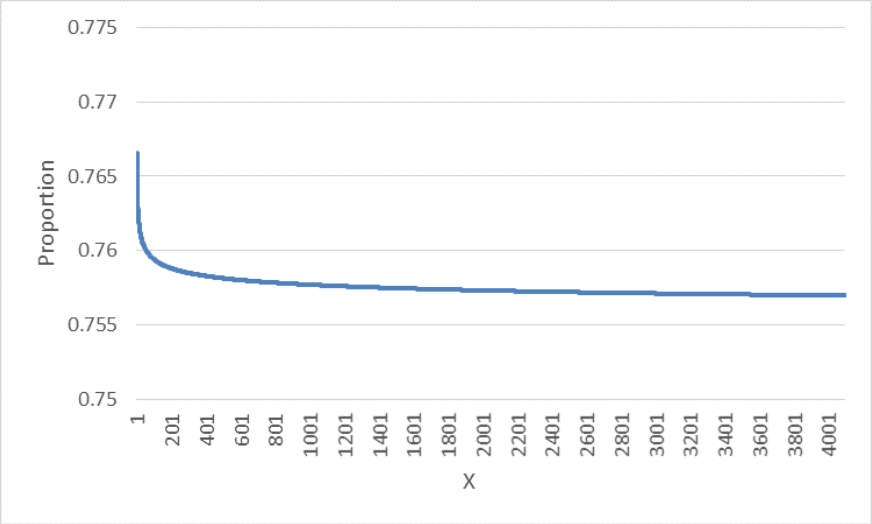

Figure 4.18: p-Cohen-Lenstra Heuristic $p = 1009$

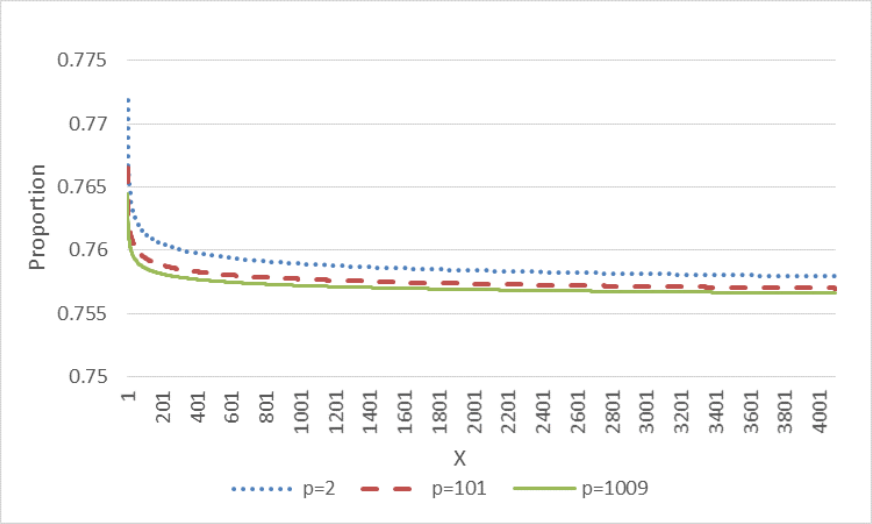

Figure 4.19: p-Cohen-Lenstra Heuristic $p = 2, p = 101, p = 1009$

It is clear that the proportions converge to the expected constant C, but the convergence rate is quite slow especially after X exceeds 600. When $X = 4096$, the proportions for $p = 2, 3, 5, 7, 11, 101, 1009$ are 0.757922, 0.757850, 0.757746, 0.757684, 0.757563, 0.756988 and 0.756593, respectively, which are very close to $C \approx 0.754458$. Moreover, the convergence is slightly faster for larger p since there are more fake real quadratic orders for large p with $|D|$ in the same interval. This is obvious as the number of $\mathcal{O}_{K,p}$ is the number of quadratic residues modulo p, which is half the number of integers in the interval that are not multiples

of p. Since D is much larger than p, there are much more multiples for smaller p, which implies that there are fewer quadratic residues modulo smaller p.

Convergence rate: As mentioned in Section 3.5, according to Cohen, the convergence rate can possibly be described by $0.754458... + 80/\log(x)^3$ or $0.754458... + 0.49/x^{1/5}$, where x is an upper bound on $|D|$. We take $p = 2$ as an example to see whether or not the convergence rate is well described by these functions. In Figures 4.20-4.25, at any point, the upper bound on $|D|$ can be found by $x = X \cdot 2^{28}$.

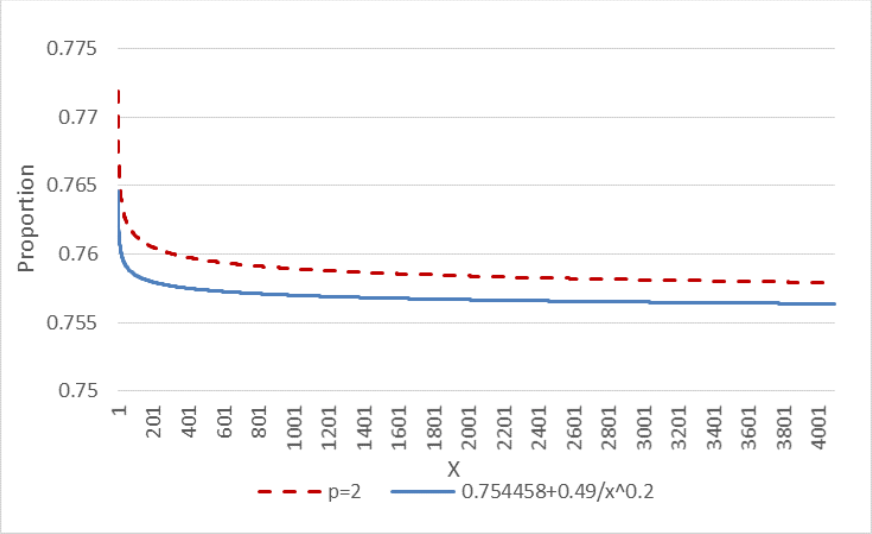

Figure 4.20: Convergence rate for $p = 2$ and $0.754458 + 0.49/\log(x)^{1/5}$

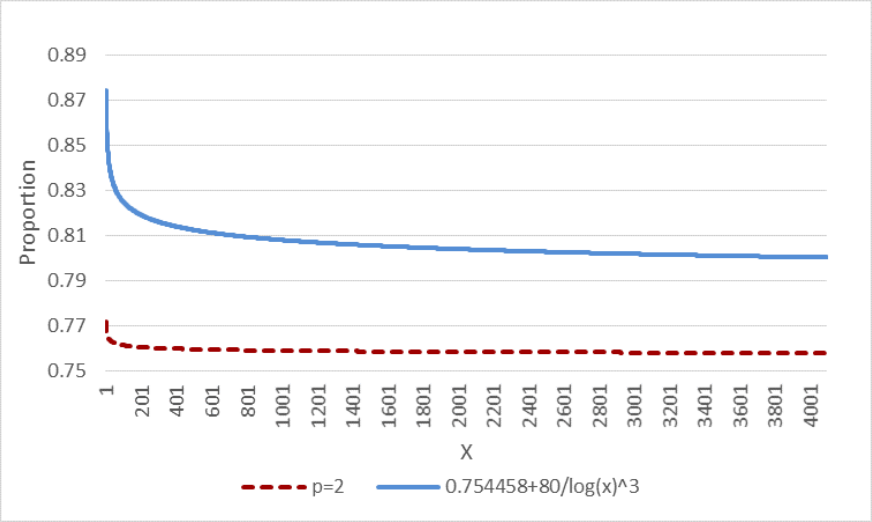

Figure 4.21: Convergence rate for $p = 2$ and $0.754458 + 80/\log(x)^3$

It is clear to see that these two functions are not accurate enough to describe the convergence rate. However, if we adjust the coefficients and powers of $\log(x)$ and x, we can get better agreement. For example, we compare the convergence rate for $p = 2$ with the functions $0.754458 + 0.88/x^{0.2}$ and $0.754458 + 870/\log(x)^5$, respectively.

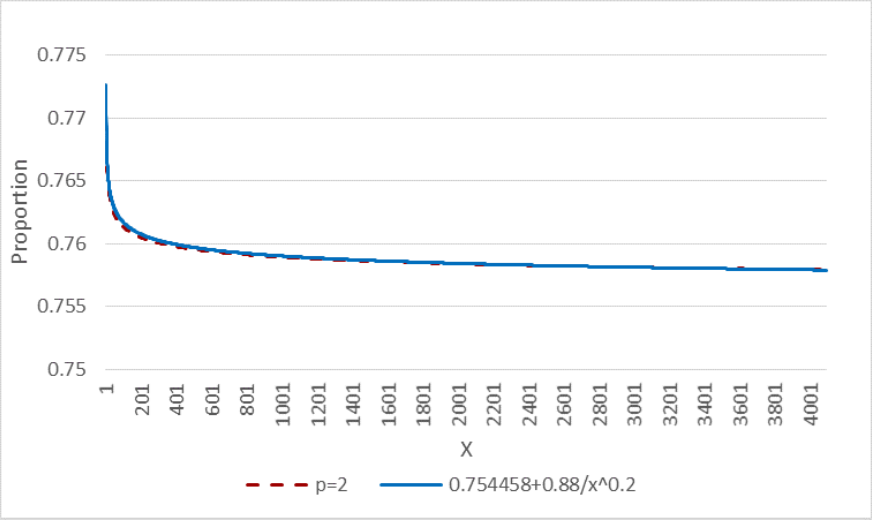

Figure 4.22: Convergence rate for $p = 2$ and $0.754458 + 0.88/x^{0.2}$

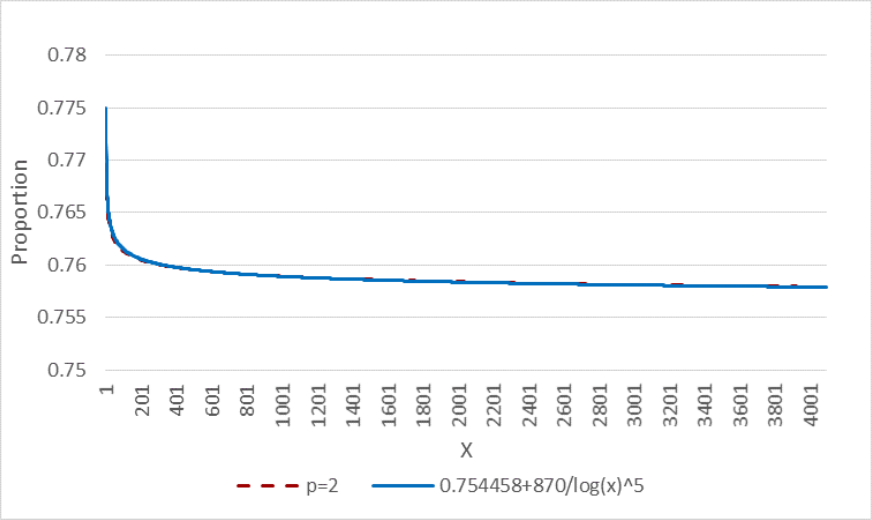

Figure 4.23: Convergence rate for $p = 2$ and $0.754458 + 870/\log(x)^5$

We can see that $0.754458 + 870/\log(x)^5$ is slightly better than $0.754458 + 0.88/x^{0.2}$. Such functions can also be found for other primes. For instance, we look at the convergence rate for $p = 11$, $0.754458 + 790/\log(x)^5$ and $p = 1009$, $0.754458 + 540/\log(x)^5$. Since the convergence is slightly faster for larger p, the coefficient of $1/\log(x)^5$ in the convergence rate function is smaller.

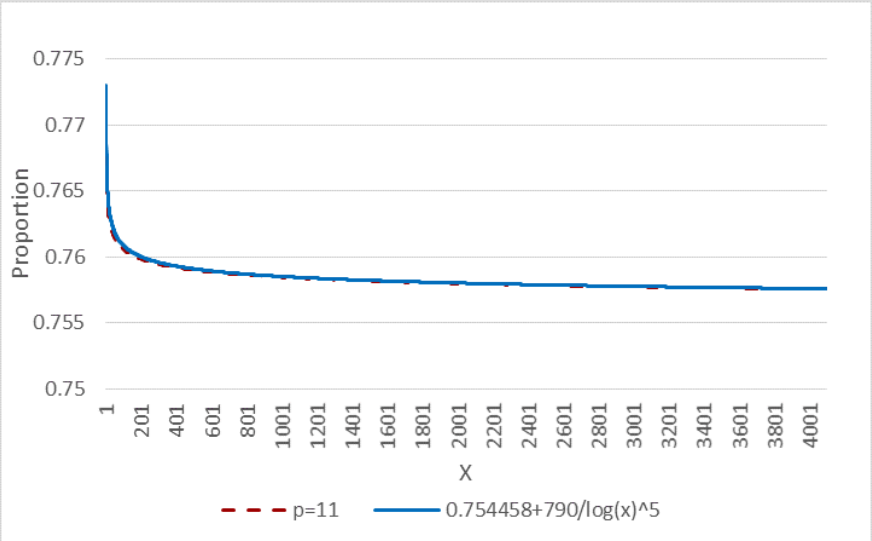

Figure 4.24: Convergence rate for $p = 11$ and $0.754458 + 790/\log(x)^5$

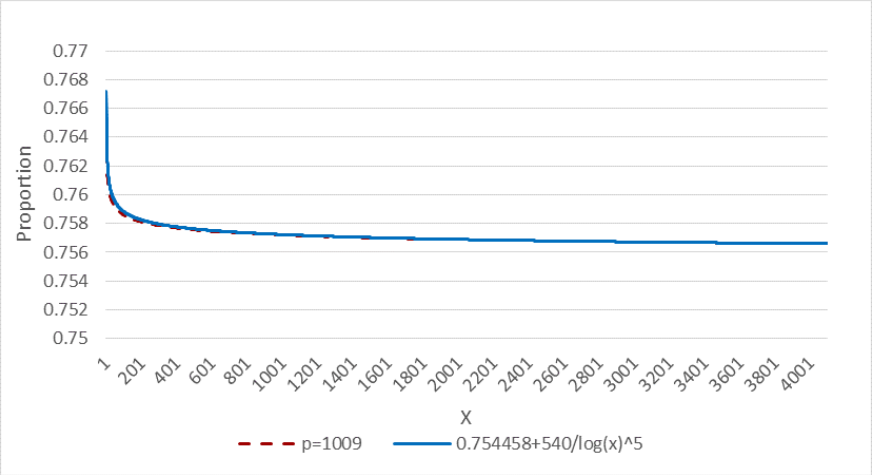

Figure 4.25: Convergence rate for $p = 1009$ and $0.754458 + 540/\log(x)^5$

Correctness of our numerical results: To check the correctness of the data, the author ran the program for prime discriminants $|D| < 2^{28}$, $p = 2, 3, 5, 7, 11$ and the results were exactly the same as Cohen's data [Coh13].

The p-Cohen-Lenstra heuristics for fixed discriminants: For the p-Cohen-Lenstra heuristic, a prime number is fixed and the computation is performed for discriminants up to a bound. The other perspective is to fix a fundamental discriminant and perform the computation for as many primes as possible. As we described in Section 3.5, for a fixed discriminant, the probability of primes p for which the odd part of class number equals one is related to the structure of Cl_K. If the odd part of Cl_K is not cyclic, the probability will be zero. If the odd part of Cl_K is cyclic and $h_K = 2^r H_1^{r_1} H_2^{r_2} ... H_m^{r_m}$, where $H_1^{r_1} H_2^{r_2} ... H_m^{r_m}$ is the prime factorization of the odd part of h_K, then the probability will be $\frac{H_1-1}{H_1}\frac{H_2-1}{H_2}...\frac{H_m-1}{H_m}$.

Note that we can write the class group Cl_K as a direct product of cyclic subgroups like

$$Cl_K \simeq C(m_1) \times ... \times C(m_s),$$

where the positive integers $m_i, m_2, ..., m_s$ satisfy $m_1 \geq 1$, $m_{j+1} \mid m_j$ for $1 \leq j < s$ and $C(x)$ denotes the cyclic group of order x. Then it is easy to determine whether or not the odd

part of Cl_K is cyclic. If there exists at most one m_i such that m_i has odd prime divisors, then the odd part of Cl_K is cyclic. Otherwise, the odd part of Cl_K is not cyclic.

Mosunov has computed this decomposition for $|D|$ up to 2^{40} [Mos15]. The author picked the first 100 discriminants from the *cl3mod8, cl7mod8, cl4mod16 and cl8mod16* files with indices $0, 10, 100, 1000, 2000, 3000, 4000$, and ran the program for p tup to 30000. In Tables 4.8 and 4.9, we present some computation results from the file $cl3mod8.4000$ and $cl8mod16.0$ as examples. For the "Cl_K Decomposition" column, $m_1 \times ... \times m_s$ represents the decomposition $Cl_K \simeq C(m_1) \times ... \times C(m_s)$. The "Prop" and "Prob" columns show the proportion and the theoretical probability of fake real quadratic orders for which the odd part of the class number equals one. Note that the theoretical probability, $\frac{H_1-1}{H_1}\frac{H_2-1}{H_2}...\frac{H_m-1}{H_m}$, is based on the assumption that the ideal $\mathfrak{p}^{2^s}$ is randomly distributed where the order of $\mathfrak{p}$ is 2^sN for some $s \in \mathbb{Z}$ and some odd integer N.

Table 4.8: p-Cohen-Lenstra Heuristic for fixed $|D| \equiv 3 \pmod 8$ from the file $cl3mod8.4000$

D	h_K	h_K Factorization	Cl_K Decomposition	Prop	Prob
-1073741824003	161661	3×53887	161661	0.667802	0.666654
-1073741824011	471404	$2^2 \times 117851$	235702×2	1.000000	0.999991
-1073741824019	390630	$2 \times 3 \times 5 \times 29 \times 449$	390630	0.512270	0.513796
-1073741824195	229880	$2^3 \times 5 \times 7 \times 821$	229880	0.682416	0.684879
-1073741824203	193122	$2 \times 3^2 \times 10729$	64374×3	0.000000	0.000000
-1073741824299	242212	$2^2 \times 19 \times 3187$	242212	0.949439	0.947071
-1073741824339	177110	$2 \times 5 \times 89 \times 199$	177110	0.782073	0.787036
-1073741824371	346400	$2^5 \times 5^2 \times 433$	173200×2	0.802299	0.798152
-1073741824579	210840	$2^3 \times 3 \times 5 \times 7 \times 251$	210840	0.457362	0.455321
-1073741824707	209682	$2 \times 3^3 \times 11 \times 353$	209682	0.611174	0.604344

Table 4.9: p-Cohen-Lenstra Heuristic for fixed $|D| \equiv 8 \pmod{16}$ from the file $cl8mod16.0$

D	h_K	h_K Factorization	Cl_K Decomposition	Prop	Prob
-8	1	1	1	1.000000	1.000000
-24	2	2	2	1.000000	1.000000
-56	4	2^2	4	1.000000	1.000000
-104	6	2×3	6	0.667983	0.666667
-248	8	2^3	8	1.000000	1.000000
-296	10	2×5	10	0.801765	0.800000
-440	12	$2^2 \times 3$	6×2	0.668783	0.666667
-536	14	2×7	14	0.858303	0.857143
-1304	22	2×11	22	0.911920	0.909091
-1832	26	2×13	26	0.923853	0.923077

As we expected, only a few discriminants have probability 0. Most of them have probability greater than 60%. For $D = -1073741824003$, since the odd part of Cl_K is cyclic, the probability is given by $2/3 \times 53886/53887 = 0.66665... \approx 0.667802$. For $D = -1073741824011$, the probability is $117850/117851 = 0.999991... \approx 1.000000$. And for $D = -1073741824203$, as we can see, the odd part of Cl_K is not cyclic. So the probability for $D = -1073741824203$ is 0.

For $D = -8, -24, -56, -248$, since $h_K = 2^k$ for some $k \in \mathbb{Z}$, so the probability is 1. For $D = -104$, the probability is $2/3 = 0.666666... \approx 0.667983$. The probability for $D = -1832$ is given by $12/13 = 0.923076... \approx 0.923853$.

4.3 The p-Ankeny-Artin-Chowla Conjecture

For the p-Ankeny-Artin-Chowla conjecture, we need to check whether D divides the second coefficient of the fundamental unit. A special case is when $D = -3$, where as long as $\left(\frac{D}{p}\right) = 1$, every fake real quadratic order $\mathcal{O}_{K,p}$ is a counterexample for the p-Ankeny-Artin-Chowla conjecture. We have the following theorem.

Theorem 4.1. Let $K = \mathbb{Q}(\sqrt{-3})$. Then for any prime number p with $p \equiv 1 \pmod 3$, there exists a fundamental unit $\epsilon = \frac{a+b\sqrt{-3}}{2}$ of $\mathcal{O}_{K,p}$ such that $3 \mid b$.

Proof. For any prime p, we first prove that $p \equiv 1 \pmod 3$ is equivalent to $(\frac{-3}{p}) = 1$. When $p = 2$, we know that $2 \equiv -1 \pmod 3$ and $(\frac{-3}{2}) = -1$. So we just assume that p is an odd prime. Then we have

$$\left(\frac{-3}{p}\right) \cdot \left(\frac{p}{3}\right) = (-1)^{\frac{-3-1}{2}\frac{p-1}{2}} = (-1)^{-2\cdot\frac{p-1}{2}} = 1.$$

Thus, $(\frac{-3}{p}) = 1$ is equivalent to $(\frac{p}{3}) = 1$, which is equivalent to $p \equiv 1 \pmod 3$. So any p with $p \equiv 1 \pmod 3$ gives us a fake real quadratic order $\mathcal{O}_{K,p}$ where $K = \mathbb{Q}(\sqrt{-3})$.

Now suppose that $\epsilon_0 = \frac{a+b\sqrt{-3}}{2}$ is a fundamental unit of $\mathcal{O}_{K,p}$, where $a, b \in \mathbb{Z}$. Since the unit group of $\mathcal{O}_K$ is $\mathcal{O}_K^* = \{1, -1, \zeta, \zeta^2, -\zeta, -\zeta^2 : \zeta^2 + \zeta + 1 = 0\}$, then $\epsilon\zeta$ and $\epsilon\zeta^2$ are also fundamental units of $\mathcal{O}_{K,p}$. Without loss of generality, we take $\zeta = \frac{-1-\sqrt{-3}}{2}$ and $\zeta^2 = \frac{-1+\sqrt{-3}}{2}$. That is,

$$\epsilon_1 = \epsilon_0\zeta = \frac{a+b\sqrt{-3}}{2} \cdot \frac{-1-\sqrt{-3}}{2} = \frac{1}{2} \cdot \frac{-a+3b-(a+b)\sqrt{-3}}{2}$$

and

$$\epsilon_2 = \epsilon_0\zeta^2 = \frac{a+b\sqrt{-3}}{2} \cdot \frac{-1+\sqrt{-3}}{2} = \frac{1}{2} \cdot \frac{-a-3b+(a-b)\sqrt{-3}}{2}$$

are both fundamental units of $\mathcal{O}_{K,p}$.

By Theorem 3.5, ϵ is a generator of $\mathfrak{p}^{o(\mathfrak{p})}$. That is, $N(\epsilon) = p^{o(\mathfrak{p})}$, i.e., $a^2 + 3b^2 = 4p^{o(\mathfrak{p})}$. Now $3 \mid a$ implies $3 \mid p$, which is not possible as p is prime and $p \neq 3$. So either $a \equiv 1 \pmod$

3) or $a \equiv 2 \pmod 3$.

If $3 \mid b$, we are done. Otherwise, $b \equiv 1 \pmod 3$ or $b \equiv 2 \pmod 3$. So either $3 \mid (a-b)$ or $3 \mid (a+b)$. That is, either ϵ_1 or ϵ_2 is a fundamental unit with 3 dividing the second coefficient. □

So all fake real quadratic orders derived from $K = \mathbb{Q}(\sqrt{-3})$ violate the p-Ankeny-Artin-Chowla conjecture. From now on, we only look at the case when $D \neq -3$.

To find counterexamples and their behavior, the author did tests in two dimensions. First, we fixed small primes $p = 2, 3, 5, 7, 11, 101, 1009$ and ran the program for all prime discrimiants up to 2^{40}. In this case, only one counterexample was found for a small discriminant:

- The fake real quadratic order $\mathcal{O}_{K,p}$ for $D = -89716079$, $p = 11$ violates the p-Ankeny-Artin-Chowla conjecture, the fundamental unit is given in Appendix A.

Then tests were done for relatively small discriminants, $|D| < 10 \cdot 2^{28}$, with more prime numbers, p up to 30000. In this case, thousands of counterexamples were found, especially for extremely small discriminants like $D = -7, -11$. The largest counterexamples we found is for $D = -2524520819$.

To check whether counterexamples exist for big discriminants, the author picked the largest prime discriminants from the files with indices $2^k - 1$ where $k = 0, 1, ...12$. The computations were done for as many primes as possible given our time constraints. Three counterexamples were found for p up to 10^{11} and the largest one is for $D = -2147483647$ (index=7) and $p = 268435561$. To find a counterexample for $|D| \approx 2^{40}$, the expected upper bound on p is more than 10^{13} since we expect to encounter a counterexample for the first 2^{41} primes as explained below. This bound on p is far beyond our search.

The existence of more counterexamples for smaller discriminants is reasonable since the counterexample satisfies the condition that $D \mid b$, and for large discriminants, the probability of the existence of such coefficients b is much smaller. To check whether b behaves randomly

with respect to divisibility by D, the author randomly picked several prime discriminants, searched counterexamples with p up to 10^{10} and looked for a pattern of proportions of counterexamples. For fixed D, we expect that the proportion of counterexamples converges to $1/|D|$. Table 4.10 shows the number of fake real quadratic orders and number of counterexamples for selected discriminants with p up to 10^{10}.

Table 4.10: Proportion of p-AAC counterexamples for selected D with p up to 10^{10}

D	#p with $(\frac{D}{p}) = 1$	# counterexamples	Proportions
-7	25423038	3631144	1/7.001385238
-19	25422848	1336786	1/19.01788918
-59	25421747	429750	1/59.15473415
-127	25422646	199306	1/127.5558488
-859	25421893	28839	1/881.5109054
-1367	25424175	17755	1/1431.944523
-2099	25423040	11360	1/2237.943662
-12647	25422928	2012	1/12635.65010
-100019	25422313	250	1/101689.2520

Within our search, it is apparent that the proportion of counterexamples for each D converges to $1/|D|$ as expected. So for $|D| \approx 2^{40}$, the probability to find a counterexample is very small. This explains why no counterexamples have been found for extremely large $|D|$. We also present the graphs that show the convergence trend of the proportions of counterexamples for $D = -7, -859, 100019$. In Figures 4.26-4.28, the upper bound of p at a specific point is given by $X \cdot 10^7$ where $1 \leq X \leq 1000$ is the X-coordinate of that point. The Y-coordinate represents the value of 1/proportion and is supposed to converge to $|D|$.

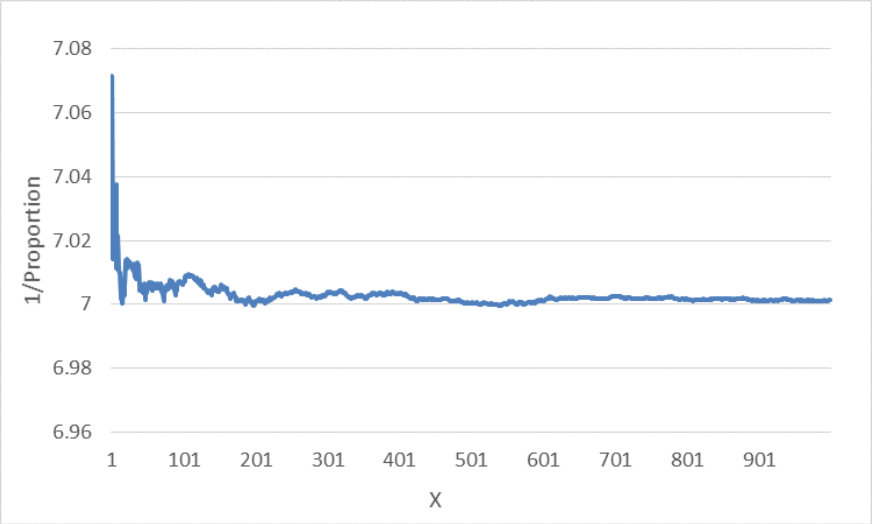

Figure 4.26: Proportion of p-AAC counterexamples for $D = -7$ with p up to $X \cdot 10^7$

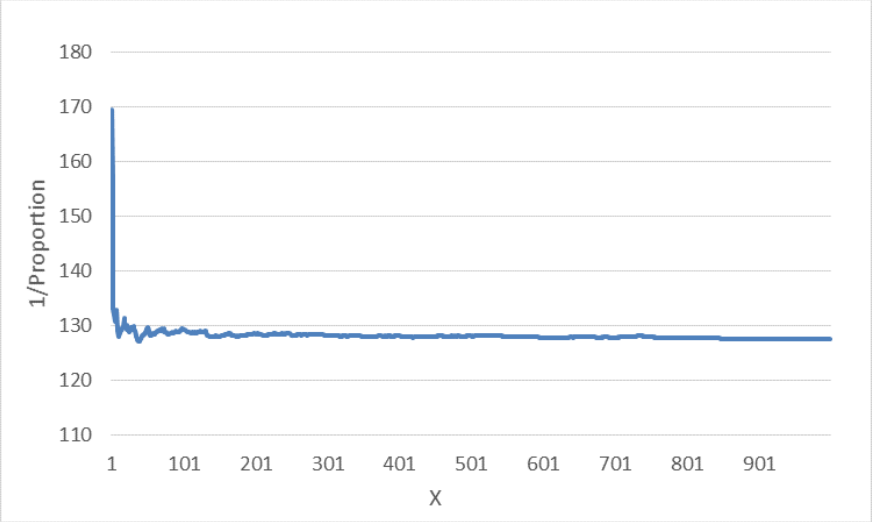

Figure 4.27: Proportion of p-AAC counterexamples for $D = -127$ with p up to $X \cdot 10^7$

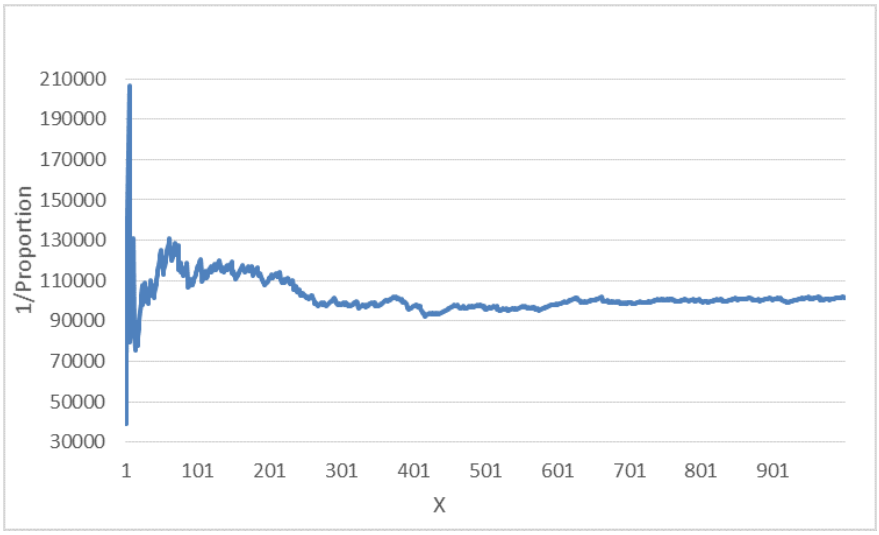

Figure 4.28: Proportion of p-AAC counterexamples for $D = -100019$ with p up to $X \cdot 10^7$

Finally, we present some counterexamples to the p-Ankeny-Artin-Chowla conjecture in fake real quadratic orders. For the larger examples, we also list all the relative generators $\{g_i \mid 0 < i < l\}$ where l is the number of bits in the binary representation of the order of $[\mathfrak{p}]$. We know that $\epsilon = g_1^{2^{l-2}} g_2^{2^{l-3}} ... g_{l-1}$. Most of the counterexamples are too long to put in the thesis. Readers please refer to [Wan16] for more information.

$D = -7$, $p = 29983$, $\epsilon = 164 + 21\sqrt{-7}$

$D = -11$, $p = 29401$, $\epsilon = -325/2 - 33/2\sqrt{-11}$

$D = -823$, $p = 21107$, $\epsilon = -642110 - 104521\sqrt{-823}$

$D = -34327$, $p = 24841$, $\epsilon = 744065602968799064239392111357642884840872394793205927819$
$758006669225594403 01 - 189968479230545312697694489938448658998719975132028716015326823676539031020\sqrt{-34327} = g_1^{16} \cdot g_2^8 \cdot g_3^4 \cdot g_4^2 \cdot g_5$

$g_1 = 128165/16 - 311/16\sqrt{-34327}$

$g_2 = 1$

$g_3 = -723/68 - 1/68\sqrt{-34327}$

$g_4 = -74971/98 - 15/98\sqrt{-34327}$

$g_5 = 3893 - 36\sqrt{-34327}$

$D = -110587, p = 28961, \epsilon = 48327505282999056547310698979601687036994536513666533926$
$692786508712957041432661347/2+151934277179228386483814070411617774970608993828089 1$
$880310080921661521404649412 15/2\sqrt{-110587} = g_1^{16} \cdot g_2^8 \cdot g_3^4 \cdot g_4^2 \cdot g_5$

$g_1 = 704629/298 - 175/298\sqrt{-110587}$

$g_2 = -386/362 + 12/362\sqrt{-110587}$

$g_3 = 350707/326 - 2117/326\sqrt{-110587}$

$g_4 = -2373/158 - 5/158\sqrt{-110587}$

$g_5 = -1951 - 40\sqrt{-110587}$

$D = -1071739, p = 281, \epsilon = 65604922183630814188030129877363936067286299153553367478 2$
$067145487738739996510330164217421936583389765000426207717832982022695548437164650 7$
$027800258283299677721907814012242046127/2+171230572500521632509068795921397111355$
$954385564169668847379494742312161486349900453427747272921256127830454884145971469 8$
$619851544718768553615791441284724566585912538782392485/2\sqrt{-1071739} = g_1^{64} \cdot g_2^{32} \cdot g_3^{16} \cdot$
$g_4^8 \cdot g_5^4 \cdot g_6^2 \cdot g_7$

$g_1 = 8102/850 + 8/850\sqrt{-1071739}$

$g_2 = -6940/430 + 10/430\sqrt{-1071739}$

$g_3 = -84343/662 + 97/662\sqrt{-1071739}$

$g_4 = 4139/670 + 11/670\sqrt{-1071739}$

$g_5 = -3802/370 + 8/370\sqrt{-1071739}$

$g_6 = -4869/362 - 1/362\sqrt{-1071739}$

$g_7 = -3167/2 - 5/2\sqrt{-1071739}$

$D = -2147483647, p = 268435561, \epsilon = -16523777968842241087444610672008214350703297245$

$755530638718726952628644710978055910231295505886510842200489816125105442037 9-64640$

$734667080971294992512025395118428587383028721385469294340690007960750611541510969 9$

$0668348649325786747497157166 0\sqrt{-2147483647} = g_1^8 \cdot g_2^4 \cdot g_3^2 \cdot g_4$

$g_1 = -46707763225/16 + 536870281/16\sqrt{-2147483647}$

$g_2 = -29/4 + 1/4\sqrt{-2147483647}$

$g_3 = 1$

$g_4 = -536870919/2 - 7/2\sqrt{-2147483647}$

Correctness of our numerical results: After we found all relative generators, we computed $N(\epsilon) = N(g_1)^{2^{l-2}} N(g_2)^{2^{l-3}} ... N(g_{l-1})$ to check if it is equal to $p^{o(\mathfrak{p})}$. If not, a message "wrong unit for D=... and p=..." was printed. The norm test was performed for each fake real quadratic order, which ensures the correctness of our result. Moreover, the author searched counterexamples for $|D| < 1072000$, $p < 1000$ and the results matched Cohen's data [Coh13].

Chapter 5

Conclusion and Future Work

In this thesis, we presented the basic concepts and properties of fake real quadratic orders based on the result from Cohen's manuscript [Coh13] and Oh's thesis [Oh14]. Class groups of fake real quadratic orders were investigated. In addition, we discussed fundamental units and infrastructures of fake real quadratic orders. Then we focused on the p-Cohen-Lenstra heuristics and the p-Ankeny-Artin-Chowla conjecture. For the first heuristic, computations were performed for $|D| < 2^{40}$ and primes $p = 2, 3, 5, 7, 11, 101, 1009$. With the increase of the upper bound of $|D|$, the convergence is slow but still tends to the expected number $C \approx 0.75$. For the p-Ankeny-Artin-Chowla conjecture, only one counterexample was found for $|D|$ up to 2^{40}, $D \neq -3$ with small primes $p = 2, 3, 5, 7, 11, 101, 1009$. When we focused on small discriminants, $|D| < 10 \cdot 2^{28}$, and ran the program for p up to 30000, thousands of counterexamples were found, especially for extremely small discriminants like $D = -7$ and $D = -11$. Moreover, we found that the proportion of counterexamples converges to $\frac{1}{|D|}$ for a fixed prime discriminant D. All the numerical data was saved on the penguin1 server in the Department of Computer Science at the University of Calgary. To get access to the data, please contact the author or her supervisor Dr. Michael J. Jacobson, Jr., at hongyan.wang@ucalgary.ca or jacobs@ucalgary.ca, respectively.

5.1 Future Work

For the p-Cohen-Lenstra heuristics, the author only performed computations to find the probability of discriminants for which the odd part of the class number equals one. Cohen and Lenstra also gave a hypothesis on the probability that the odd part of the class number equals any odd number, like $3, 5, 7...$ [CL84]. It will be interesting to perform similar tests on fake real quadratic orders to find probabilities corresponding to these odd numbers. We believe that the result will support the Cohen-Lenstra heuristic in fake real quadratic orders.

In addition, for real quadratic fields, Cohen and Lenstra [CL84] hypothesized that the probability that q divides h_K is equal to

$$1 - \prod_{k \geq 2}(1 - q^{-k}) = q^{-2} + q^{-3} + q^{-5} - q^{-7} - ...$$

where q is any prime number. So for fake real quadratic orders, we believe that the probability that q divides $h_{K,p}$ is the same.

Moreover, Cohen and Lenstra also conjectured that, in real quadratic fields, the probability that the q-rank of Cl_K equals r is

$$q^{-r(r+1)} \prod_{k \geq 1}(1 - q^{-k}) \prod_{1 \leq k \leq r}(1 - q^{-k})^{-1} \prod_{1 \leq k \leq r+1}(1 - q^{-k})^{-1},$$

where q is an odd prime number. In fake real quadratic orders, we expect that the probability that the q-rank of $Cl_{K,p}$ equals r is the same number. These problems are worthy of further study.

For the p-Ankeny-Artin-Chowla Conjecture, as was mentioned in Chapter 4, counterexamples were found for both small and large discriminants. Our data suggests that, as expected, the proportion of counterexamples converges to $\frac{1}{|D|}$ for a fixed D. This is worth checking for larger discriminants with more prime numbers. We give our conjecture regarding the p-Ankeny-Artin-Chowla Conjecture as follows.

Conjecture 5.1. For any prime discriminant D, there exists infinitely many primes p such that $\mathcal{O}_{K,p}$ violates the p-Ankeny-Artin-Chowla Conjecture. Moreover, the probability of counterexamples is equal to $1/|D|$.

Our data showed exactly that the proportion of counterexamples for the p-Ankeny-Artin-Chowla Conjecture converges to $1/|D|$ for any fixed D. Thus, the divisibility of b by D behaves randomly for any fake real quadratic order $\mathcal{O}_{K,p}$ with fundamental unit $\epsilon = \frac{a+b\sqrt{D}}{2}$. Since fake real quadratic orders behave similarly to real quadratic orders, we believe that the divisibility of b by D also behaves randomly for any real quadratic field $K = \mathbb{Q}(\sqrt{D})$ with fundamental unit $\epsilon = \frac{a+b\sqrt{D}}{2}$. Thus, the "log log" statement is correct and the expected number of counterexamples for D up to $2 \cdot 10^{11}$ is no more than 1.4. We will find counterexamples as long as we perform enough experiments. Therefore, we believe that the Ankeny-Artin-Chowla conjecture is false for real quadratic fields.

In the end, we look at the runtimes of our program. As we discussed in Section 4.1, the test of the p-Ankeny-Artin-Chowla conjecture takes most of the total runtime. Since the norm test caused the bottleneck in our program, a big improvement will be finding a more efficient way to test the correctness of the fundamental unit we compute. In addition, normal multiplications are performed when looking for relative generators. Since NUCOMP is much faster than the normal composition, if we can find relative generators in the process of NUCOMP, the program will likely be much faster. This problem is worthy of further study.

Bibliography

[AAC52] Nesmith C. Ankeny, Emil Artin, and Sarvadaman D. S. Chowla. The class-number of real quadratic number fields. *Ann. of Math.* (2), 56:479–493, 1952.

[Arn92] Steven Arno. The imaginary quadratic fields of class number 4. *Acta Arith.*, 60(4):321–334, 1992.

[ARW98] Steven Arno, Michael L. Robinson, and Ferrell S. Wheeler. Imaginary quadratic fields with small odd class number. *Acta Arith.*, 83(4):295–330, 1998.

[Bak67] Alan Baker. Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika* 13 (1966), 204-216; ibid. 14 (1967), 102-107*; ibid.*, 14:220–228, 1967.

[Bak71] Alan Baker. Imaginary quadratic fields with class number 2. *Ann. of Math.* (2), 94:139–152, 1971.

[BW00] David Bressoud and Stan Wagon. *A Course in Computational Number Theory.* Key College Publishing, Emeryville, CA; in cooperation with Springer-Verlag, New York, 2000.

[BWZ71] Brent D. Beach, Hugh C. Williams, and Robert C. Zarnke. Some computer results on units in quadratic and cubic fields. Proceedings of the Twenty-Fifth Summer Meeting of the Canadian Mathematical Congress, pages 609–1971.

University of Manitoba, Department of Computer Science, Lakehead Univ., Thunder Bay, Ont., 1971.

[CL84] Henry Cohen and Hendrik W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[Coh00] Henri Cohen. *Advanced Topics in Computational Number Theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[Coh13] Henri Cohen. Experiments on fake real quadratic orders. 2013. Unpublished Manuscript.

[Cor08] Giuseppe Cornacchia. Su di un metodo per la risoluzione in numeri interi dell'equazione $\sum_{h=0}^{n} C_h x^{n-h} y^h = P$. *Giornale di Matematiche di Battaglini*, 46:33–90, 1908.

[FS16] Francesc Fité and Andrew V. Sutherland. Sato-Tate groups of $y^2 = x^8 + c$ and $y^2 = x^7 - cx$. In *Frobenius distributions: Lang-Trotter and Sato-Tate conjectures*, volume 663 of *Contemp. Math.*, pages 103–126. Amer. Math. Soc., Providence, RI, 2016.

[FUW99] Glenn J. Fox, Jerzy Urbanowicz, and Kenneth S. Williams. Gauss' congruence from dirichlet's class number formula and generalizations. *Number Theory in Progress (Za-kopane, 1997)*, 2:813–839, 1999.

[Gau66] Carl F. Gauss. *Disquisitiones Arithmeticae*. Translated into English by Arthur A. Clarke, S. J. Yale University Press, New Haven, Conn.-London, 1966.

[JJSW06] Michael J. Jacobson Jr, Reginald E. Sawilla, and Hugh C. Williams. Efficient ideal reduction in quadratic fields. *Int. J. Math. Comput. Sci.*, 1(1):83–116, 2006.

[JS14] Michael J. Jacobson, Jr. and Renate Scheidler. Infrastructure: structure inside the class group of a real quadratic field. *Notices Amer. Math. Soc.*, 61(1):36–46, 2014.

[JW09] Michael J. Jacobson, Jr. and Hugh C. Williams. *Solving the Pell Equation*. CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC. Springer, New York, 2009.

[Len82] Hendrik W. Lenstra, Jr. On the calculation of regulators and class numbers of quadratic fields. *Cambridge Univ. Press, Cambridge*, 56:123–150, 1982.

[Mil14] James S. Milne. Algebraic Number Theory(v3.06), 2014. Available at www.jmilne.org/math/.

[Mor60] Louis J. Mordell. On a pellian equation conjecture. *Acta Arithmetica*, 2(6):137–144, 1960.

[Mos15] Anton S. Mosunov. Unconditional class group tabulation of imaginary quadratic fields to 2^{40}. *Master's Thesis, University of Calgary*, 2015.

[Oes85] Joseph Oesterlé. Nombres de classes des corps quadratiques imaginaires. *Séminaire Bourbaki*, 26:309–323, 1985.

[Oh14] Richard M. Oh. Fake real quadratic orders. *Doctoral Dissertation, University of South Carolina*, 2014.

[Say13] Maxwell Sayles. *optarith* and *qform* libraries for fast binary quadratic forms arithmetic. `http://github.com/maxwellsayles`, 2013.

[Sch91] Arnold Schönhage. Fast reduction and composition of binary quadratic forms. Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation:128–133, 1991.

[Sol86] Ragnar Soleng. A computer investigation of units in quadratic number fields. *Unpublished Manuscript*, 1986.

[Spi69] Robert Spira. Calculation of Dirichlet L-functions. *Math. Comp.*, 23:489–497, 1969.

[SS71] Doz Dr A Schönhage and Volker Strassen. Schnelle multiplikation grosser zahlen. *Computing*, 7(3-4):281–292, 1971.

[Sta67] Harold M. Stark. A complete determination of the complex quadratic fields of class-number one. *Michigan Math. J.*, 14:1–27, 1967.

[Sta75] Harold M. Stark. On complex quadratic fields with class-number two. *Math. Comp.*, 29:289–302, 1975.

[SW88] Alan J. Stephens and Hugh C. Williams. Some computational results on a problem concerning powerful numbers. *Math. Comp.*, 50(182):619–632, 1988.

[vdPtRW01] Alfred J. van der Poorten, Herman J. J. te Riele, and Hugh C. Williams. Computer verification of the Ankeny-Artin-Chowla conjecture for all primes less than 100 000 000 000. *Math. Comp.*, 70(235):1311–1328, 2001.

[Wag96] Christian Wagner. Class number 5, 6 and 7. *Math. Comp.*, 65(214):785–800, 1996.

[Wan16] Hongyan Wang. Fake real quadratic orders. `http://github.com/hongyanwang`, 2016.

[Wat04] Mark Watkins. Class numbers of imaginary quadratic fields. *Math. Comp.*, 73(246):907–938, 2004.

Appendix A

Counterexamples for the p-Ankeny-Artin-Chowla Conjecture

$D = -89716079$, $p = 11$, $\epsilon = 36387774605376039237113262167623706994225588540809271$
$47983442098897667636165187117224972351836137866209291903542432954299304715124$9
$43238060157080227241286509383904536940754667365474660368835275757823499504754$9
$15842027579802120298900398545511619051363072560921985446104406416750181915707$3
$49617646192390809279259909442898347800317187051089415138397628968379664447533$3
$70492371422505703713725735442464288023279655169597327569925790813566840210146$7
$30360966896960468201124268844318778055144951898281330783186786692852678969251$8
$28415995556261826654308767129741962273797999312298709723654758593556906287484$3
$86791933753964560635447694651331784762271674502699203712618270837656765425496$8
$05322654746826962733626315607888926987050919083103892987014045695930797925669$5
$13674653841009459145787760304941001626084953616547963531643948172366172333973$0
$93440023894496388707136454042973494086053491172336082108685559864042260373$4 $-$
$94547112813650249056098286225521572674479789054570951558773067104570264572575$2
$38002591525163240811660695246343830880399925428978883391558081900341626137154$8
$76463161549453694126122359174800938039391449460135390873391812875302499340143$6

$$0822566690635928115376622008153039086467994592977296076640464030094901767856867492083275409624216022833538123110339496095653762979532105209495871415166931467185670236494083351144497166900737360561348627838810598528624093834367002376533931190281193868558702507272147436077535890456694308744289174304927733368239575439972112681204827441397030458580821482348957638314756457900894432667732553794193928927285176118626361450199136131832130821249537849284585188342248928151698250294387057862318177327838361256785427189237115371303063495329472845677626657172653209795502220168380204066151954868684585848931262639178728659942826617577292864921702890444244868426101869287335858951\sqrt{-89716079} = g_1^{512} \cdot g_2^{256} \cdot g_3^{128} \cdot g_4^{64} \cdot g_5^{32} \cdot g_6^{16} \cdot g_7^{8} \cdot g_8^{4} \cdot g_9^{2} \cdot g_{10}$$

$$g_1 = 1$$

$$g_2 = -118073/9632 - 15/9632\sqrt{-89716079}$$

$$g_3 = -261685/7962 + 211/7962\sqrt{-89716079}$$

$$g_4 = 1373557/5504 + 19/5504\sqrt{-89716079}$$

$$g_5 = -268799/8472 + 25/8472\sqrt{-89716079}$$

$$g_6 = -247405/5128 + 37/5128\sqrt{-89716079}$$

$$g_7 = 536845/4152 - 59/4152\sqrt{-89716079}$$

$$g_8 = -665627/5832 + 35/5832\sqrt{-89716079}$$

$$g_9 = -256919/1060 + 1/1060\sqrt{-89716079}$$

$$g_{10} = -4639/2 - 1/2\sqrt{-89716079}$$

$D = -2655581107$, $p = 11299$, $\epsilon = -3196383859544444676462606090620857251936943822118823467335153111643620566873058318480533737591449492820712566188724386827106745580481324220772357925916643252553793662469326566422779216095393452830837155261659075613048396109210805801497033134050272628972049873424687301223632/2 + 147491533607102276963671353962264794373714318374889713989787362390558214359991913151039924725529751834091717684630447134607548187286292000508745069199307391397009$

$$308302938999850619563491436673331152214774787965389111859480073296813247055150$$

$$3521152578996304884850274683 69/2\sqrt{-2655581107} = g_1^{64} \cdot g_2^{32} \cdot g_3^{16} \cdot g_4^{8} \cdot g_5^{4} \cdot g_6^{2} \cdot g_7$$

$$g_1 = -689923/7366 + 23/7366\sqrt{-2655581107}$$

$$g_2 = -190781/13186 + 11/13186\sqrt{-2655581107}$$

$$g_3 = 382135/4154 - 9/4154\sqrt{-2655581107}$$

$$g_4 = -177197/40882 - 11/40882\sqrt{-2655581107}$$

$$g_5 = 621602073/54122 - 6851/54122\sqrt{-2655581107}$$

$$g_6 = -371382151/17011 + 1032/17011\sqrt{-2655581107}$$

$$g_7 = 128652 + 35\sqrt{-2655581107}$$