July 2024

Improvements in Computational Techniques For Determining Ideal Class Groups and Class Numbers

Muhammed Rashad Erukulangara
University of South Florida

Improvements in Computational Techniques for Determining Ideal Class Groups and Class Numbers

by

Muhammed Rashad Erukulangara

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
Department of Mathematics & Statistics
College of Arts and Sciences
University of South Florida

Major Professor: Jean-François Biasse, Ph.D.
Dmytro Savchuk, Ph.D.
Nataša Jonoska, Ph.D.
Giacomo Micheli, Ph.D.
Ruthmae Sears, Ph.D.

Date of Approval:
June 24, 2024

Keywords: Imaginary quadratic field, quadratic forms, cyclotomic field, norm relations, principal ideal problem

ACKNOWLEDGMENTS

I want to express my deep appreciation to Dr. Jean-François Biasse, my supervisor, for his exceptional guidance, unwavering support, and constant encouragement during my doctoral studies. His expertise and valuable insights were instrumental in completing my dissertation. I am also grateful to my committee members, Dr. Nataša Jonoska, Dr. Ruth-mae Sears, Dr. Giacomo Micheli, and Dr. Dmytro Savchuk, for their insightful comments and encouragement, which have significantly improved this dissertation. I'm also thankful to Dr. William Youmans for his assistance along the way. I extend sincere thanks to the Mathematics and Statistics Department at the University of South Florida for providing the necessary resources and facilities crucial for the completion of my research. Lastly, my heart-felt gratitude goes to my family for their enduring love, encouragement, and understanding throughout this journey. Their unwavering support has been my pillar of strength.

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

The ideal class group is a fundamental concept in algebraic number theory, providing insights into the structure and factorization properties of the ring of integers of a number field. It measures the extent to which unique factorization fails in the ring of integers. Efficiently computing the ideal class group is crucial for exploring unproved heuristics in number theory and solving Diophantine equations. Additionally, the computation of the ideal class group has several cryptographic applications, such as schemes based on the Discrete Logarithm Problem (DLP), the computation of isogenies, and groups of unknown order. Despite its importance, much about the ideal class group and its order, known as the class number, remains enigmatic due to the computational challenges involved.

In the first part of this thesis, we present a modified version of the Hafner and McCurley class group algorithm [41] for the ideal class Group computation of imaginary quadratic fields. Our modified version improves the asymptotic run time and achieves the conjectured run time of the Hafner and McCurley class group algorithm [41, Sec. 5]. This improvement relies on recent results regarding the properties of the Cayley graph of the ideal class group [46].

In the second part of this thesis, we introduce a new approach for unconditional class number computation of the maximal real subfield of cyclotomic fields. Our method for computing class numbers in the maximal real subfield of cyclotomic fields closely adheres to the methodology outlined by John C. Miller [54, 55, 56]. The cornerstone of our novel approach for unconditional class number computation of the maximal real subfield of cyclotomic fields lies in the *norm relations* techniques introduced by Biasse, Fieker, Hofmann, and Page [20]. In particular, we employ norm relation-based Principal Ideal Problem (PIP) technique as outlined in [43].

CHAPTER 1
INTRODUCTION

Algebraic number theory is a captivating and profound branch of mathematics that utilizes the techniques of abstract algebra to study integers, rational numbers, and their generalizations. At its core, algebraic number theory explores number fields, extensions of the field of rational numbers, and their intricate structures, such as the ring of integers. One of the most important properties of rational integers is the unique factorization, meaning integers can be expressed as the product of prime numbers in a unique way. However, this property can fail in the ring of integers of a general number field. This failure is measured by the ideal class group and its order, known as the class number. The ideal class group and its order, the class number, are perhaps the most important concepts in the study of number fields. Computing the structure and order of the ideal class group is considered a challenging problem, one of the four major tasks in computational number theory postulated by Pohst and Zassenhaus [62], alongside the computation of the unit group, the Galois group, and the ring of integers. Much about class groups and class numbers remains mysterious due to their computational difficulty. This thesis focuses on the computation of class groups for two important number fields in algebraic number theory. The first number field is the imaginary quadratic field, and the second is the maximal real subfield of a cyclotomic field. Specifically, for imaginary quadratic fields, we provide a proof for the conjectured run time of the Hafner and McCurley class group algorithm [41]. For the maximal real subfield of cyclotomic fields, we introduce a new technique for unconditional class number computation and determine the class numbers of a few maximal real subfields of cyclotomic fields that have not been documented in the literature. Our approach to class number computation for these maximal real subfields of cyclotomic fields closely follows the methodology of Miller [54, 55, 56].

1.1 Class Group Computation of Imaginary Quadratic Fields

The study of the ideal class group of imaginary quadratic field $Cl(-d)$ goes back to Gauss [85]. Gauss studied the class group of imaginary quadratic fields by using quadratic forms and presented an algorithm for the class computation with a run time of $O(d^{1/2})$, where $-d$ is the discriminant of the imaginary quadratic field. Later in 1968 Shanks [73, 74] proposed an algorithm for computing the ideal class group of quadratic number field by using the baby-step giant-step method. This algorithm had time complexity $O(e^{(1/4+\epsilon)\log d})$, or $O(e^{(1/5+\epsilon)\log d})$ under a generalization of the Riemann hypothesis (GRH) [48]. The input for the ideal class group computation of a quadratic field is its discriminant d, and its bit-length is polynomially bounded in $O(\log|d|)$. Hence, all the above class group computation algorithms for quadratic fields are exponential. For number fields of higher degree, a lattice reduction is needed for class group computation, and its time complexity depends on the degree and the discriminant of the number field. A breakthrough in the ideal class group computation came through Hafner and McCurley [41] in 1989. Hafner and McCurley introduced a subexponential algorithm for the ideal class group computation of an imaginary quadratic field under the Generalized Riemann hypothesis (GRH). After the breakthrough of the Hafner and McCurley class group algorithm, much research happened in the practical implementation of the Hafner and McCurley algorithm [6, 11, 16, 30, 44] and the ideal class group computations of higher degree number fields [10, 12, 14, 18, 20, 23]. Although these computations in higher-degree number fields have achieved reduced asymptotic running time [10, 12, 14, 18, 20, 23] , for imaginary quadratic fields until now the best known asymptotic complexity was the one stated by Hafner and McCurley [41].

In this thesis, we present a modified version of the Hafner-McCurley class group algorithm for the ideal class group computation of imaginary quadratic field under GRH. Our modified version improves the asymptotic run time and we achieve the conjectured run time of the Hafner and McCurley class group algorithm [41, Sec. 5]. Our modified version of the Hafner

and McCurley class group algorithm relies on recent results on the properties of the Cayley graph of the ideal class group [46]. The following is the main result we present on ideal class group computation of imaginary quadratic field.

Theorem 1. Under a generalization of the Riemann hypothesis, there is a Las Vegas algorithm which computes $Cl(-d)$ with probability $1 - \frac{1}{d^{1+o(1)}}$ in time

$$L(d)^{3/\sqrt{8}+o(1)} = e^{\left(3/\sqrt{8}+o(1)\right)\sqrt{\log d \log\log d}}.$$

1.2 Class Number Computation of Maximal Real Subfield of Cyclotomic Fields

Cyclotomic fields are one of the important number fields, and they have played a crucial role in the development of algebraic number theory due to their connection with Fermat's Last Theorem. However not much is known about the class numbers of cyclotomic fields due to computational difficulty. Schoof described the computation of class numbers for cyclotomic fields as a 'notoriously hard' problem [69]. The difficulty of this problem lies in the class number computation of the maximal real subfield $\mathbb{Q}(\zeta_m)^+$ of the cyclotomic field $\mathbb{Q}(\zeta_m)$. The class number of the maximal real subfield of a cyclotomic field is also known as the "plus part" of the class number and it is denoted by h^+. The classical method for calculating h^+ is by using the Minkowski bound and we will discuss it in Section 3.4. However, this method becomes impractical for cyclotomic fields with large discriminants. To address cyclotomic fields with large discriminants, Masley [51] and van der Linden [49] introduced a method for h^+ computation using Odlyzko's discriminant lower bounds. Unfortunately, this method is limited to cyclotomic fields with small root discriminants. Later, John C. Miller described a new approach for unconditional (without assuming GRH) h^+ computation [54, 55, 56]. Miller's approach finds an upper bound for h^+ by establishing nontrivial lower bounds for sums over prime ideals of the Hilbert class field. This upper bound, combined with some divisibility arguments, yields the exact h^+. In this thesis, we introduce a variant of Miller's technique for computing unconditional h^+. The key behind our new approach

for unconditional h^+ computation is the concept of norm relations introduced by Biasse, Fieker, Hofmann, and Page [20]. Specifically, we utilize a norm relation based Principal Ideal Problem (PIP) resolution subroutine as described in [43] as part of our new approach. The following is the summary of our results on class number computation of maximal real subfield of cyclotomic fields.

Theorem 2. The class number of $\mathbb{Q}(\zeta_m)^+$ is one for $m = 285, 540, 372, 396, 308, 231, 462$.

1.3 Outline

In Chapter 2, we discuss some foundational results in algebraic number theory necessary for the subsequent chapters. Chapter 3 covers various algorithms in the literature for ideal class group computation. Our modified version of the Hafner and McCurley class group algorithm is presented in Chapter 4. In Chapter 5, we examine the *norm relations* introduced by Biasse, Fieker, Hofmann, and Page [20] and explore various arithmetic applications of these norm relations. Chapter 6 introduces our new technique for unconditional h^+ computation. Chapter 4 is based on collaborative research with Jean-François Biasse, published in Advances in Mathematics of Communications (AMC) [13]:

Jean-François Biasse and Muhammed Rashad Erukulangara. "A proof of the conjectured run time of the Hafner-McCurley class group algorithm". In: Advances in Mathematics of Communications 17 (Jan. 2021). DOI: https://doi.org/10.3934/amc.2021055

Chapter 5 is based on the following joint work with Jean-François Biasse, Claus Fieker, Tommy Hofmann and William Youmans [19].

Jean-François Biasse,Claus Fieker, Tommy Hofmann ,William Youmans and Muhammed Rashad Erukulangara. "Mildly Short Vectors in Ideals of Cyclotomic Fields Without Quantum Computers". In: Mathematical Cryptology 2.1 (Nov. 2022), pp. 84–107. url: https://journals.flvc.org/mathcryptology/article/view/132573.

The content of Chapter 6 is derived from collaborative, unpublished work with Jean-François Biasse.

CHAPTER 2

BACKGROUND

In this chapter, we discuss some of the basic results in algebraic number theory that will be useful for the subsequent chapters.

2.1 Number Fields

A number field is a finite field extension K of $\mathbb{Q}$. In other words, a number field is a $\mathbb{Q}$-vector space of finite dimension. The dimension $[K : \mathbb{Q}]$ is called the degree of the number field K. An element in a number field is called an algebraic integer if it is a root of a monic polynomial with coefficients in $\mathbb{Z}$. The set of algebraic integers of a number field is called the ring of integers of K and it is denoted by $\mathcal{O}_K$. The ring of integers $\mathcal{O}_K$ is a ring and also a free abelian group whose rank is the degree of the corresponding field K. Orders generalize the notion of the ring of integers of a number field. An order of an algebraic number field K is a subring $\mathcal{O} \subseteq \mathcal{O}_K$ which is also a free abelian group of rank $n = [\, K : \mathbb{Q}]$.

A number field K of degree n over $\mathbb{Q}$ has n distinct embedding into $\mathbb{C}$. Let L/K be a degree m extension of number fields. Let $\sigma_1, ..., \sigma_m$ be the m distinct embeddings of L into $\mathbb{C}$ which fix K. Then for an element $\alpha \in L$, the norm is defined as

$$\mathrm{N}_{L/K}(\alpha) = \prod_{i=1}^{m} \sigma_i(\alpha).$$

Also, the trace of α is defined as

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{m} \sigma_i(\alpha)$$

The norm map is multiplicative and the trace map is additive. For an algebraic integer $\alpha \in K$, the norm and trace of α belong to $\mathbb{Z}$.

Definition 2.1 (Euclidean lattice)**.** Let $v_1, ..., v_n$ be linearly independent vectors in $\mathbb{R}^n$. Then, the lattice generated by these vectors is the set of all points $\sum_i a_i v_i$ with $a_i \in \mathbb{Z}$. The set $\{v_1, ..., v_n\}$ is called a basis of the lattice, and the dimension of the lattice is defined as the cardinality of this basis set.

Conceptually, a lattice can be viewed as a collection of points in a multi-dimensional space arranged in a regular, grid-like pattern. Let $\mathcal{L}$ be a lattice of dimension n with a basis $v_1, ..., v_n$. The fundamental domain of $\mathcal{L}$ with respect to the basis $v_1, ..., v_n$ is the region defined by

$$F(v_1, ..., v_n) = \{t_1 v_1 + t_2 v_2 + ... + t_n v_n : 0 \leq t_i < 1\}.$$

Let K be a number field of degree n. Let $\mathcal{O}_K$ be the ring of integers of K with a basis $w_1, ..., w_n$. We can define the embedding $\sigma : K \to \mathbb{C}^n$ by $\sigma(a) = (\sigma_1(a), ..., \sigma_n(a))$, where $\sigma_1, ..., \sigma_n$ are n distinct embeddings of K into $\mathbb{C}$. Then the image $\sigma(\mathcal{O}_K)$ can be considered as an n -dimensional lattice with basis $\sigma(w_1), ..., \sigma(w_n)$. Let V be the volume of the fundamental domain of the lattice $\sigma(\mathcal{O}_K)$. Then the discriminant of the number field K, denoted by d_K, is:

$$d_K = V^2.$$

The discriminant is an integer and it is independent of the choice of the basis of $\mathcal{O}_K$. The discriminant can be computed by using the following formula

$$d_K = \det(\mathrm{Tr}_{K/\mathbb{Q}}(w_i w_j)_{1 \leq i,j \leq n}).$$

The root discriminant of a number field is defined as $|d_K|^{1/n}$ and it is denoted by $rd(K)$.

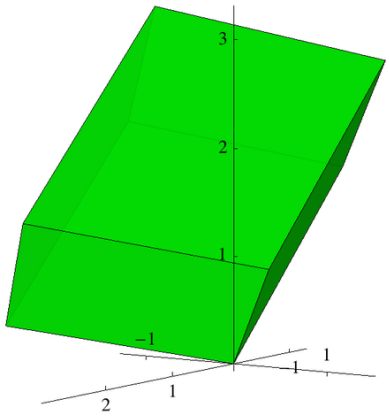


Figure 1. A fundamental domain of $\mathcal{O}_K$ for $K = \mathbb{Q}[x]/(x^3 - x^2 - 2x + 1)$ [67]

Let us consider a non-zero ideal I of $\mathcal{O}_K$, then the norm of the ideal I is defined by

$$\mathrm{N}(I) = |\mathcal{O}_K/I|.$$

For an element $\alpha \in \mathcal{O}_K$, consider the principal ideal $\alpha\mathcal{O}_K$ of $\mathcal{O}_K$. Then, $\mathrm{N}(\alpha\mathcal{O}_K) = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$, which means that the notions of norm of an element and of an ideal coincide. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. Since the prime ideals of $\mathbb{Z}$ are in the form $p\mathbb{Z}$, $\mathfrak{p} \cap \mathbb{Z}$ will be $p\mathbb{Z}$ for some prime number p and we say that $\mathfrak{p}$ lies above p. Every non-zero prime ideal of $\mathcal{O}_K$ is a maximal ideal. So, we can define the residue field $\mathcal{O}_K/\mathfrak{p}$ for $\mathfrak{p}$. Similarly we can define the residue field for $p\mathbb{Z}$ as $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. It can be easily verified that the residue field $\mathcal{O}_K/\mathfrak{p}$ is a finite dimensional $\mathbb{F}_p$-vector space and the dimension of $\mathcal{O}_K/\mathfrak{p}$ over $\mathbb{F}_p$ is called the inertial degree. We use $f_\mathfrak{p}$ to denote the inertia degree of $\mathfrak{p}$ and the norm of the prime ideal $\mathfrak{p}$ can be expressed as

$$\mathrm{N}(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}| = |\mathbb{F}_\mathfrak{p}|^{\dim_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p})} = |\mathbb{F}_\mathfrak{p}|^{f_\mathfrak{p}} = p^{f_\mathfrak{p}}.$$

One of the important algebraic structures inside a number field are the fractional ideals. A fractional ideal I is a finitely generated $\mathcal{O}_K$-module contained in K. The ideals of $\mathcal{O}_K$ are particular cases of fractional ideals of K. So, to avoid ambiguity we use the term integral

ideals for the ideals of $\mathcal{O}_K$. Now let us discuss the factorization of the fractional ideals. Let I be a non-zero fractional ideal of K. Then

$$I = \mathfrak{p}_1 ... \mathfrak{p}_r \mathfrak{q}_1^{-1} ... \mathfrak{q}_s^{-1},$$

where $\mathfrak{p}_1, ..., \mathfrak{p}_r, \mathfrak{q}_1, ..., \mathfrak{q}_s$ are prime integral ideals. This factorization is unique up to the permutation of the factors. The non-zero fractional ideals of a number field K form a multiplicative group. Let us denote it by I_K. Let P_K be the subgroup of I_K formed by the principal ideals of the form $\alpha\mathcal{O}_K$, where $\alpha \in K^*$. Then, the ideal class group, denoted by $Cl(K)$, is defined as $Cl(K) = I_K/P_K$. The cardinality of the class group is called the class number and it is denoted by h_K and it is finite [52]. We can also define the class group for an order in K which is not the maximal order $\mathcal{O}_K$. For a non-maximal order $\mathcal{O}$ of K, not every ideal is invertible. For a non-maximal order $\mathcal{O}$, the class group is defined as the following quotient of groups

$$Cl(\mathcal{O}) = \frac{\{\text{Invertible fractional ideals of } \mathcal{O}\}}{\{\text{Principal invertible fractional ideals of } \mathcal{O}\}}.$$

The cardinality of the class group $Cl(\mathcal{O})$ is called the class number of $\mathcal{O}$ and it is a multiple of h_K.

Units of a number field K are the elements of $\mathcal{O}_K$ that have an inverse in $\mathcal{O}_K$. The norm $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$ of an element α of $\mathcal{O}_K$ is equal to ± 1 if and only if α is a unit of K. As mentioned earlier the number field K of degree n has n distinct embeddings into $\mathbb{C}$. An embedding is called a real embedding if its image is contained in $\mathbb{R}$. Otherwise it is called a complex embedding. The complex embeddings come in conjugate pairs. Let r_1 be the number of real embeddings of K and r_2 be the number of pairs of complex embeddings of K. Then the group of units of K, denoted by $\mathcal{O}_K^*$, is given by the Dirichlet's Units theorem [36]. By

Dirichlet's Units Theorem, we have

$$\mathcal{O}_K^* \simeq \mathbb{Z}^{r_1+r_2-1} \times \mu(\mathcal{O}_K).$$

Here $\mu(\mathcal{O}_K)$ is the group of roots of unity in $\mathcal{O}_K$. Let $r = r_1 + r_2 - 1$. Then, there exist units $u_1, ..., u_r$ such that every element x of $\mathcal{O}_K^*$ can be written in a unique way as

$$x = \eta u_1^{n_1} \dots u_r^{n_r},$$

where η is a root of unity in K. Such a family (u_i) is called the fundamental units of K. Consider the first r_1+r_2 embeddings of K into $\mathbb{C}$. Here σ_i for $1 \leq i \leq r_1$ are real embeddings and the remaining embeddings are complex embeddings. The logarithmic embedding of K^* into $\mathbb{R}^{r_1+r_2}$ is defined by the map

$$L(x) = (\ln|\sigma_1(x)|, \dots, \ln|\sigma_{r_1}(x)|, 2\ln|\sigma_{r_1+1}(x)|, \dots 2\ln|\sigma_{r_1+r_2}(x)|)$$

for $x \in K^*$. Since the norm of a unit is ± 1, the image of the unit group $\mathcal{O}_K^*$ under the logarithmic embedding will be a lattice of rank r_1+r_2-1 in the hyperplane $\sum_{1\leq i\leq r_1+r_2} x_i = 0$ of $\mathbb{R}^{r_1+r_2}$. The volume of the fundamental domain of this lattice is called the regulator of K and it is denoted by R_K. The regulator can also be defined as the absolute value of the determinant of any $r \times r$ matrices extracted from the $r \times (r+1)$ matrix

$$\ln \|\sigma_j(u_i)\|_{1\leq i\leq r, 1\leq j\leq r+1}.$$

One of the important results in algebraic number theory which links different arithmetic invariants of a number field K is the class number formula [35] of Dedekind which is given by

$$\lim_{s\to 1}(s-1)\zeta_K(s) = 2^{r_1}(2\pi)^{r_2}\frac{h_K R_K}{w_K\sqrt{d_K}},$$

where ζ_K is the Dedekind zeta function of K and w_k is the number of roots of unity in K. The class number formula is one among numerous instances where the class number and regulator of a field are inextricably linked.

Another important invariant of a number field is the S-unit group. For a set S of prime ideals of $\mathcal{O}_K$, the S-units are the elements $x \in K^*$ such that $v_{\mathfrak{p}}(x) = 0$ for all $\mathfrak{p} \notin S$. Here $v_{\mathfrak{p}}(x)$ denotes the valuation of x at the prime ideal $\mathfrak{p}$. The group of S-units is denoted by $\mathcal{O}_{K,S}^*$, and it is called the S-unit group of K.

2.2 Class Groups of Imaginary Quadratic Fields and Binary Quadratic Forms

A field K is called an imaginary quadratic field if $[K : \mathbb{Q}] = 2$ and if its signature is $r_1 = 0, r_2 = 1$. The study of the class groups of imaginary quadratic fields is an old one and it was initiated by Gauss who studied this by using binary quadratic forms. The discriminant of an imaginary quadratic field is negative and it is congruent to 0 or 1 mod 4. Every order $\mathcal{O}$ of K has discriminant $d = d_k f^2$, where d_k is the fundamental discriminant (discriminant of K) and f is a positive integer called the conductor of $\mathcal{O}$. Also, if d is a non square integer such that $d \equiv 0$ or $1 \mod 4$, then $d = d_k f^2$, and there is a unique quadratic order $\mathcal{O}$ of discriminant d.

A polynomial $g = ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y]$ with $b^2 - 4ac = d$ is called a binary quadratic form of discriminant d. If $d < 0$ and $a > 0$, then the binary quadratic form is called positive definite. If $gcd(a, b, c) = 1$, then we say that the corresponding binary quadratic form is primitive. We usually denote a binary quadratic form $ax^2 + bxy + cy^2$ of discriminant d by (a, b, c) or by (a, b) since c is determined by the discriminant. Let $g_1 = (a_1, b_1, c_1)$ and $g_2 = (a_2, b_2, c_2)$ be two quadratic forms of the same discriminant d. Let $s = (b_1 + b_2)/2$, $n = (b_1 - b_2)/2$. Consider the integers u, v, w and d' which satisfy

$$ua_1 + va_2 + ws = d' = \gcd(a_1, a_2, s).$$

Also consider the integer $d_0 = \gcd(d', c_1, c_2, n)$. Then the composition of two quadratic forms g_1 and g_2 is defined as

$$(a_3, b_3, c_3) = \left(d_0 \frac{a_1 a_2}{d'^2}, b_2 + \frac{2a_2}{d'}(v(s - b_2) - wc_2), \frac{b_3^2 - d}{4a_3} \right).$$

The composition of two quadratic forms can be computed by using Algorithm 5.4.7 of [29]. Let $g_1 = a_1x^2 + b_1xy + c_1y^2$ and $g_2 = a_2x^2 + b_2xy + c_2y^2$ be positive definite binary quadratic forms. We say g_1 and g_2 are equivalent if there is a matrix $A = \left(\begin{smallmatrix} \alpha & \gamma \\ \beta & \delta \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ such that

$$a_2r^2 + b_2rt + c_2t^2 = a_1x^2 + b_1xy + c_1y^2;$$

where $r = \alpha x + \gamma y$ and $t = \beta x + \delta y$. Under this notion of equivalence, the binary quadratic forms of discriminant d partition themselves into equivalence classes. These equivalence classes form a group under the composition of forms. This group is isomorphic to the class group of the quadratic order $\mathcal{O}$ of discriminant d. The correspondence between equivalence classes of binary quadratic forms and ideal classes of quadratic order $\mathcal{O}$ of discriminant d is given by the following map:

$$ax^2 + bxy + cy^2 \to \left(a\mathbb{Z} + \frac{b + \sqrt{d}}{2}\mathbb{Z} \right).$$

Since we have a natural bijection between equivalence classes of binary quadratic forms and ideals, we can transport the class group structure of an imaginary quadratic order to the group of equivalence classes of quadratic forms. The multiplication between ideals corresponds to the composition of quadratic forms.

2.3 Properties of the Ideal Class Groups

In this section, we discuss some properties of the ideal class groups that will be crucial to the design and analysis of algorithms presented in subsequent chapters.

2.3.1 Generalized Riemann Hypothesis(GRH)

The Riemann zeta function, denoted by ζ, is a function of a complex variable defined as

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

for $\mathrm{Re}(s) > 1$. One of the most important conjectures in mathematics is about the Riemann zeta function, and is known as the Riemann Hypothesis. This hypothesis states that the Riemann zeta function has zeroes only at negative even integers and complex numbers with a real part of $\frac{1}{2}$. The Riemann Hypothesis is considered one of the most significant unsolved problems in mathematics and is one of the Millennium Prize Problems of the Clay Mathematics Institute.

The Riemann Hypothesis implies profound results about the distribution of prime numbers and is of great importance in number theory [66]. There have been several generalizations of the Riemann Hypothesis, and the vast majority of the mathematical community believes these generalizations to be true. One such generalization concerns Hecke L-functions and is known as the Generalized Riemann Hypothesis (GRH). This same assumption is sometimes referred to as the Extended Riemann Hypothesis (ERH), particularly in [41] and [4].

Consider a finite field extension E of K with an abelian Galois group $G = \mathrm{Gal}(E/K)$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ that is unramified in the abelian extension E. Consider a prime ideal $\mathfrak{P}$ of $\mathcal{O}_E$ that lies above $\mathfrak{p}$. There is a unique element σ in the Galois group G such that for any element $\alpha \in \mathcal{O}_E$,

$$\sigma(\alpha) \equiv \alpha^{\mathrm{N}(\mathfrak{p})} \bmod \mathfrak{P}.$$

This unique element σ of G is called the Artin symbol of $\mathfrak{p}$ and is denoted by $\left(\frac{\mathfrak{p}}{E/K}\right)$. A Hecke character χ is defined on the ideals of $\mathcal{O}_K$ as follows. Let φ be a homomorphism from G into the complex roots of unity. This homomorphism induces a function on the prime ideals of $\mathcal{O}_K$, given by

$$\chi(\mathfrak{p}) = \varphi\left(\frac{\mathfrak{p}}{E/K}\right)$$

when $\mathfrak{p}$ is unramified, and 0 otherwise. The Hecke character constructed in this manner can then be extended to all ideals by multiplicativity. If a character χ takes only the values $0, 1$, then the character is called a principal character. For any character χ there is an ideal $\mathfrak{f}$ of $\mathcal{O}_K$ such that $\chi((t)\mathcal{O}_K) = 1$ for all totally positive t congruent to 1 modulo $\mathfrak{f}$. Then we say χ is defined modulo $\mathfrak{f}$. The ideal of the least norm with respect to which χ is defined is called its conductor. The Hecke L-function associated with a character χ is defined as

$$L(s, \chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}$$

where sum is over nonzero ideals of $\mathcal{O}_K$. When χ is a trivial character, then the Hecke L-function is called the Dedekind ζ function of K:

$$\zeta(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}.$$

The following is the Generalized Riemann hypothesis (GRH):

Conjecture 2.2 (GRH)**.** *Let K be a number field and χ be a Hecke character on K. Then the Hecke L-function given by $L(s, \chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}$ is zero free in the half-plane $\Re(s) > 1/2$.*

2.3.2 Small Generators of the Ideal Class Group

As we discussed in the previous section, the Generalized Riemann Hypothesis (GRH) asserts that all Hecke L-functions are zero-free in the half-plane $\Re(s) > 1/2$. By using GRH, Eric Bach made an estimate for $\sum_\rho \frac{1}{|\rho+a|^2}$ for $0 < a < 1$, where the sum is over the zeros of Hecke L- function and Dedekind ζ function [4, Lem. 5.6]. By using this critical estimate and the results derived from it, Eric Bach proved the following theorem:

Theorem 2.3 (Thm.4 of [4])**.** *Let K be a number field of degree greater than 1. Let d be the absolute value of the discriminant of K. Let χ be a non-principal character of the ideals of K that is defined modulo $\mathfrak{f}$. Then:*

$$\chi(p) \neq 1 \text{ occurs for } N(\mathfrak{p}) \leq 3\log^2(d^2 N(\mathfrak{f}))$$
$$\chi(p) \neq 0, 1 \text{ occurs for } N(\mathfrak{p}) \leq 12\log^2(d^2 N(\mathfrak{f}))$$
$$\chi(p) \neq 0, 1 \text{ and degree}(\mathfrak{p}) = 1 \text{ occurs for } N(\mathfrak{p}) \leq 18\log^2(d^2 N(\mathfrak{f})).$$

By using Theorem 2.3, we obtain the following important result on ideal class groups.

Corollary 2.4. *Let K be a number field with discriminant d. Then the ideal class group is generated by classes of prime ideals of norm at most $12\log^2(|d|)$.*

Proof. Since the ideal class group of K is arithmetically constructed from K, we can interpret Hecke characters as discrete characters of the ideal class group $Cl(K)$. Let H be the subgroup of the ideal class group generated by the classes of prime ideals of norm less than $3\log^2(d^2) = 12\log^2(d)$. Assume H is a proper subgroup of the ideal class group $Cl(K)$. Then there is a nontrivial character on $Cl(K)$ which is trivial on H. This character is trivial on the prime ideals of norm less than $12\log^2(d)$. This contradicts the first part of Theorem 2.3 with $\mathfrak{f} = \mathcal{O}_K$. So, $H = Cl(K)$, and $Cl(K)$ is generated by the classes of prime ideals of norm less than $12\log^2(d)$. □

So, the ideal class group has a finite generating set, and this result is very useful for the computation of the class groups and units of K.

2.3.3 Cayley Graph of the Ideal Class Group

A Cayley graph is a visual representation of a group, built using a particular set of generators for that group. Named after the mathematician Arthur Cayley, these graphs find applications in diverse fields like algebra, geometry, and computer science. Here is the definition of a Cayley graph.

Definition 2.5. Let G be a group generated by a subset of elements $S \subseteq G$. Then the Cayley graph $Cay(G, S)$ of G is a graph in which each vertex corresponds to an element of the group G. Also, there is a directed edge from vertex g_1 to vertex g_2 if and only if there is an element $s \in S$ such that $s.g_1 = g_2$.

If k is the cardinality of the generating set S of $Cay(G, S)$, then $Cay(G, S)$ is a k-regular graph. We can apply the definition of a Cayley graph to the class group of a number field K. Thus, we can select G as $Cl(K)$ and require a generating set S for G. Since the class group $Cl(K)$ is generated by the classes of prime ideals with norms less than $12\log^2|d|$, we can choose $S := \{\text{prime ideals of } \mathcal{O}_K \text{ with norm less than } \log^{2+\epsilon}|d| \text{ for any } \epsilon > 0\}$ and construct the Cayley graph $Cay(Cl(K), S)$. Expanding the generating set slightly does not have a significant impact on the overall cost of any of the algorithms being considered. The most intriguing result about $Cay(Cl(K), S)$ is that random walks in $Cay(Cl(K), S)$ reach arbitrary subsets of $Cl(K)$ with a probability at least proportional to the size of the subset. This rapid mixing property of $Cay(Cl(K), S)$ is highly beneficial, and we will briefly discuss it here.

The adjacency operator A acts on the functions over the vertices of a graph G by

$$(Af)(x) = \sum_{x \text{ and } y \text{ connected by an edge}} f(y).$$

For a k-regular graph, the constant function $\mathbb{1}(x) = 1$ will be an eigenfunction of the adjacency operator A with eigenvalue k. We denote this eigenvalue by λ_{triv}, which is the largest eigenvalue of the adjacency operator A. The spectral gap of a graph G is defined to be $\gamma(G) = \lambda_{triv} - \lambda_2$, where λ_2 is the largest non-trivial eigenvalue. We say G has spectral expansion γ if $\gamma(G) \geq \gamma$. A graph is called a good expander if it has a large expansion parameter γ.

Expansion properties of graphs are extensively studied across various fields of mathematics and computer science. The bounds on the eigenvalues of a good expander graph are particularly valuable for determining the number of paths between two sets of graph vertices. These bounds on the eigenvalues of a good expander yield the following important result.

Proposition 2.6 (Lem.2.1 of [46])**.** *Let G be a finite k-regular graph such that $\lambda < c$ for some $c < k$ for all eigenvalue $\lambda \neq \lambda_{triv}$. Then a random walk of length at least $\frac{\log 2|G|/|G_0|^{1/2}}{\log k/c}$ starting from v ends in G_0 with probability between $\frac{|G_0|}{2|G|}$ and $\frac{3|G_0|}{2|G|}$.*

Proof. Let G be a finite k-regular graph with the bound $\lambda < c$ for nontrivial eigenvalues λ for some $c < k$. Consider the characteristic function χ_{G_0} for a subset G_0 of vertices of the graph G. The characteristic function χ_{G_0} is defined by $\chi_{G_0}(x) = 1$ if $x \in G_0$ and $\chi_{G_0}(x) = 0$ if $x \notin G_0$. The L^2 inner product on the functions f, g over the vertices of the graph G is defined by $\langle f,\ g\rangle = \sum_x f(x)g(x)$. Now, consider a vertex v and a subset G_0 of the vertices of the graph G. For a given t, $A^t\chi_{\{v\}}(x)$ will be the number of paths of length t from the vertex v to the vertex x of the graph. So, the number of paths of length t from vertex v to the subset G_0 will be $\langle \chi_{G_0},\ A^t\chi_{\{v\}}\rangle$. Then, we get the following inequality by using the properties of the L^2 inner product and Cauchy-Schwartz inequality,

$$\langle \chi_{G_0},\ A^t\chi_{\{v\}}\rangle \leq \frac{|G_0|}{|G|}k^t + c^t|G_0|^2.$$

That is, we have a bound on the number of paths of length t between the vertex v and subset G_0 in terms of the eigenvalue bounds. If we take $t > \frac{\log 2|G|/|G_0|^{1/2}}{\log k/c}$, then we get the following inequality

$$\frac{|G_0|}{2|G|}k^t \leq \langle \chi_{G_0},\ A^t\chi_{\{v\}} \rangle \leq \frac{3|G_0|}{2|G|}k^t. \tag{2.1}$$

For a k-regular graph, the number of paths of length t from a given vertex is given by k^t. So, if we divide Inequality 2.1 by k^t, we get the result. □

Consider the Cayley graph $Cay(Cl(K), S)$. Since $Cl(K)$ is a finite abelian group, the eigenfunctions of the adjacency operator A are precisely the characters $\chi : Cl(K) \longrightarrow \mathbb{C}^*$. Indeed, we have the formula:

$$(A\chi)(x) = \sum_{s\in S} \chi(sx) = \lambda_\chi \chi(x) \text{ where } \lambda_\chi = \sum_{s\in S} \chi(s).$$

So, the spectrum of eigenvalues consists of the character sums $\lambda_\chi = \sum_{s\in S} \chi(s)$ ranging over the generating set S. Theorem 1.1 of Jao, Miller, and Venkatesan [46] gives eigenvalue bounds for these character sums under the assumption of GRH. So the Cayley graph $Cay(Cl(K), S)$ can be considered as a good expander graph, and we have the following result from [46, Cor. 1.3].

Theorem 2.7 (Cor.1.3 of [46])**.** *Let K be a number field of degree n and discriminant d, $\mathfrak{m}$ be an integral ideal of $\mathcal{O}_K$. Let G be the narrow ray class group relative to $\mathfrak{m}$, $\epsilon > 0$, and*

$$S := \left\{ \textit{prime ideals of norm less than } \log^{2+\epsilon}(N(\mathfrak{m})|d|) \textit{ and their inverses} \right\}.$$

Then there is a constant $C > 0$ such that for d sufficiently large, a random walk of length

$$t > C\frac{\log|G|}{\log\log(N(m)|d|)}$$

starting from any vertex ends in any $G_0 \subseteq G$ *with probability at least* $\frac{|G_0|}{2|G|}$.

The above result applies to a narrow ray class group of a number field K relative to a conductor $\mathfrak{m}$. However, it can be extended to the ideal class group of orders in K. As a result, asymptotically, random walks of length $O\left(\frac{\log|Cl(K)|}{\log\log|d|}\right)$ in the Cayley graph of $Cl(K)$ reach subsets of $Cl(K)$ that are distributed almost uniformly at random.

2.4 Finiteness of the Ideal Class Group

In this section, let's discuss the Class Number Theorem, which states that the ideal class group is finite. The backbone of the Class Number Theorem is the famous Minkowski's Theorem [52]. Minkowski's Theorem is stated as follows:

Theorem 2.8 (Minkowski's Theorem)**.** *Let* $\mathcal{L}$ *be a full lattice in an* n*-dimensional vector space* V *over* $\mathbb{R}$*. Let* Y *be a centrally symmetric, bounded, context subset of* V*. If* $vol(Y) > 2^n vol(\mathcal{L})$*, then* Y *contains a nonzero point of* $\mathcal{L}$*.*

By applying Minkowski's Theorem to the ideal lattices formed by the canonical embeddings of K, we obtain the result that every ideal class of $Cl(K)$ contains an integral ideal whose norm is at most $C_{r_1,r_2}\sqrt{|d|}$. Here, the constant C_{r_1,r_2} depends only on the number of real embeddings r_1 and the number of pairs of complex embeddings r_2 of K. That is, each ideal class contains a representative integral ideal whose norm is bounded by a constant depending only on the field. Then, by using the fact that there are only a finite number of integral ideals with a given norm, we obtain the result that the class group is finite.

CHAPTER 3

CLASS GROUP AND UNIT GROUP COMPUTATIONS

In this chapter, we discuss various algorithms for the computation of ideal class groups and unit groups of number fields.

3.1 Algorithms For Class Group and Unit Group Computations

The computation of the ideal class group and the unit group of a number field are primary challenges in computational algebraic number theory, along with the computation of the Galois group and the ring of integers, as postulated by Zassenhaus [62]. The theoretical results and computational experiences show these computations are very difficult tasks. Even under the assumption of the Generalized Riemann hypothesis (GRH), the fastest deterministic algorithm for the computation of the ideal class group and the unit group has exponential time complexity, i.e exponential in $\log(|d|)$, where d is the discriminant of the number field K. Computationally hard problems like class group computation can serve as the security assumption for certain cryptosystems. In 1968 Shanks [73, 74] proposed an algorithm for computing the ideal class group of a quadratic number field by using the baby-step giant-step method. This algorithm had exponential time complexity $O(e^{(1/4+\epsilon)\log|d|})$, or $O(e^{(1/5+\epsilon)\log|d|})$ under a generalization of the Riemann hypothesis (GRH) [48]. On input d with $|d|> 1$ and $0 < a, b < 1$, we define the subexponential function as

$$L_d(a, b) = e^{b\log(|d|)^a \log\log(|d|)^{1-a}}.$$

An algorithm is termed as subexponential algorithm if its running time grows according to a subexponential function with respect to its input size $\log|d|$. A breakthrough in the

ideal class group computation came through Hafner and McCurley [41] in 1989. Hafner and McCurley introduced a subexponential algorithm for the ideal class group computation of an imaginary quadratic field under the Generalized Riemann hypothesis. The expected running time of the Hafner and McCurley subexponential algorithm is $L_d(\frac{1}{2}, \sqrt{2} + o(1))$. After the breakthrough of the Hafner and McCurley class group algorithm, much research happened in the practical implementation of the Hafner and McCurley algorithm [6, 11, 16, 30, 44] and the ideal class group computations of higher degree number fields [10, 12, 14, 18, 20, 23]. All these algorithms have subexponential time complexity under the assumption of the Generalized Riemann hypothesis. Also, all these algorithms use the index calculus method as used in the Hafner and McCurley class group algorithm. The following is the outline of the index calculus method for ideal class group computations.

3.1.1 Index Calculus Method For Ideal Class Group Computation

One of the important steps in the index calculus method is the computation of the SNF of a matrix, which is defined as follows.

Definition 3.1. Let $A = (a_{ij})$ be a $n \times n$ matrix with integer entries. Then the matrix A is in SNF if

1. $a_{ij} = 0$ for $i \neq j$.
2. For some k with $0 \leq k \leq n$, $a_{ii} \neq 0$ for $i \leq k$, and $a_{ii} = 0$ for $i > k$.
3. $a_{11} \mid a_{22} \mid \ldots \mid a_{kk}$.

For any integer $n \times n$ matrix with non-zero determinant, there exists a unique Smith norm form corresponding to the matrix [29, Th. 2.4.12] and it can be computed by using Algorithm 2.4.14 of [29]. Let G be a finite abelian group. Then G is isomorphic to a quotient $\mathbb{Z}^n/L$ where L is a submodule of $\mathbb{Z}^n$ of rank n [29, Th. 2.4.1]. We can represent the finite abelian group G by an $n \times n$ matrix A, where the columns of A correspond to coordinates

of a $\mathbb{Z}$-basis of L with respect to some $\mathbb{Z}$-basis of $\mathbb{Z}^n$. Then we can determine the structure of G from the SNF of A. In fact, we have the following isomorphism

$$G \cong \bigoplus_{1 \leq i \leq n} (\mathbb{Z}/d_i\mathbb{Z}),$$

where d_i are the diagonal elements of the SNF of A.

Let $\mathcal{B} = \mathfrak{p}_1, \ldots, \mathfrak{p}_N$ be a set of invertible prime ideals of the ideal class group $Cl(\mathcal{O})$ of order $\mathcal{O}$ of the number field K such that it generates $Cl(\mathcal{O})$. Then, we can define the surjective homomorphism

$$\begin{aligned} \mathbb{Z}^N \xrightarrow{\phi} \quad I \quad &\xrightarrow{\pi} Cl(\mathcal{O}) \\ (e_1, ..., e_N) \longrightarrow \prod_i \mathfrak{p}_i{}^{e_i} &\longrightarrow \prod_i [\mathfrak{p}_i]^{e_i}. \end{aligned}$$

The ideal class group $Cl(\mathcal{O})$ is isomorphic to $\mathbb{Z}^n/\mathrm{Ker}(\pi \circ \phi)$. Therefore, computing the ideal class group $Cl(\mathcal{O})$ is equivalent to computing $\mathrm{Ker}(\pi \circ \phi)$. The elements of $\mathrm{Ker}(\pi \circ \phi)$ are the vectors $(e_1, \ldots, e_N)$ in the lattice $\mathbb{Z}^n$ such that $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_N^{e_N} = (\alpha)$, where $\alpha \in \mathcal{O}$.

For the index calculus strategy, we aim to collect relations of the form $\prod_i \mathfrak{p}_i^{e_i^{(j)}} = (\alpha_j)$, and we store these relations as the rows of the matrix $M = (e_i^{(j)})$. After gathering enough relations, the SNF of the matrix M reveals the class group structure of $Cl(\mathcal{O})$.

Additionally, if a vector $(x_1, \ldots, x_N)$ belongs to the left kernel of the matrix M, it provides us with the unit $\gamma = \alpha_1^{x_1} \cdots \alpha_N^{x_N}$. Using this method, we can compute the unit group of $Cl(\mathcal{O})$ from the left kernel of M.

Input : Number field K with an order $\mathcal{O}$, factor base $\mathcal{B} = \{\mathfrak{p} \subseteq \mathcal{O} \mid \mathrm{N}(\mathfrak{p}) \leq B\}$ that generates the class group $Cl(\mathcal{O})$
Output: Class group and unit group of $\mathcal{O}$
1 Generate a $\mathbb{Z}$-lattice L of random relations in $Cl(\mathcal{O})$ between the classes of elements of $\mathcal{B}$;
2 Consider a matrix M for a generating system of L;
3 Compute the left kernel $ker(M)$ of the matrix M;
4 Compute the class group structure of $Cl(\mathcal{O})$ from the Smith norm form of M;
5 Compute a generating set for the units of the form γX obtained from $Ker(M)$;
6 Certify the result;

Algorithm 1: Index calculus method

3.2 Hafner and McCurley Algorithm

As mentioned in the previous section, a breakthrough in the ideal class group computation came through Hafner and McCurley [41] in 1989. By using the properties of binary quadratic forms, Hafner and McCurley introduced a subexponential algorithm for the ideal class group of imaginary quadratic fields. So, Let us briefly discuss imaginary quadratic fields and the Hafner and McCurley algorithm in this section.

Imaginary quadratic fields contain only a finite number of units. For $d > 0$, we consider the imaginary quadratic order $\mathcal{O}_{-d}$ of discriminant $-d$. The imaginary quadratic order of discriminant $-d$ is a $\mathbb{Z}$-module $\mathcal{O}_{-d} = \mathbb{Z} + \frac{-d+\sqrt{-d}}{2}\mathbb{Z}$. If $-d$ is a fundamental discriminant, then the imaginary quadratic field of discriminant $-d$ is a $\mathbb{Q}$-vector space $\mathbb{Q}(\sqrt{-d}) = \mathbb{Q} + \mathbb{Q}\sqrt{-d}$. An ideal of $\mathcal{O}_{-d}$ is a two-dimensional $\mathbb{Z}$-module $\mathfrak{a} = m(a\mathbb{Z} + \frac{b+\sqrt{-d}}{2}\mathbb{Z})$, where $a, b, m \in \mathbb{Z}$ and $4a|b^2 + d$. The integers a and m are unique, and b is defined modulo $2a$. The ideal $\mathfrak{a}$ is said to be primitive if $m = 1$. The norm of an ideal is $N(\mathfrak{a}) = am^2$. The prime ideals of $\mathcal{O}_{-d}$ have the form $\mathfrak{p} = p\mathcal{O}_{-d}$ for p prime with Kronecker symbol $\left(\frac{-d}{p}\right) = -1$ and $\mathfrak{p} = p\mathbb{Z} + \frac{b_p+\sqrt{-d}}{2}\mathbb{Z}$ for primes p with Kronecker symbol $\left(\frac{-d}{p}\right) \neq -1$ and b_p the uniquely determined square root b of $-d$ modulo $4p$ in $[0, p]$. In both cases, we say that $\mathfrak{p}$ lies over p and we denote this by $\mathfrak{p} \mid p$. When $\left(\frac{-d}{p}\right) \leq 0$, only one prime ideal lies over p. When $\left(\frac{-d}{p}\right) = 1$, there are two prime ideals lying over p, which correspond to the two possible

roots modulo p. If the prime ideal $\mathfrak{p}$ corresponds to the choice of root b_p, then its conjugate $\overline{\mathfrak{p}}$ corresponds to $-b_p \bmod 4p$.

In the previous chapter, we discussed the natural correspondence between the classes of binary quadratic forms and the ideal class group of an imaginary quadratic order. So, we have the following correspondence between the prime ideals of the imaginary quadratic order and prime binary quadratic forms of discriminant $-d$:

$$p\mathbb{Z} + \frac{b_p + \sqrt{-d}}{2}\mathbb{Z} \to (p, b_p, .)$$

Since we can transport the class group structure of an imaginary quadratic order to the set of equivalence classes of quadratic forms, we use the same notation $Cl(-d)$ for the ideal class group of imaginary quadratic order of discriminant $-d$ and the class group of equivalence classes of binary quadratic forms of negative discriminant $-d$. We use $h(-d)$ to denote the class number of $Cl(-d)$. Working on equivalence classes of binary quadratic forms is more practical than the ideal class group of imaginary quadratic fields. We have the following result for the set of generators of the class group $Cl(-d)$ of binary quadratic forms of negative discriminant $-d$.

Theorem 3.2 (Thm.4 of [4]). *Let p_i be the ith prime with $\left(\frac{-d}{p_i}\right) = 1$, and let*

$$b_i = \min\{b \in \mathbb{Z}_{\geq 0} : b^2 \equiv -d \bmod 4p_i\}.$$

Then, under GRH, there exists an absolute, effectively computable constant c such that the classes $[(p_i, b_i, .)]$, $1 \leq i \leq n_0$, generate $Cl(-d)$, where n_0 is the largest integer such that $p_{n_o} \leq c \log^2 d$.

Let $\mathcal{P}$ be a set that contains primes p such that $(-d/p) = 1$ and $p < c \log^2 d$, then the classes of prime forms $[(p_i, b_i, .)]$ for $p_i \in \mathcal{P}$ will generate the class group. Let us use f_i to denote the reduced prime form $(p_i, b_i, .)$ and let $n = |\mathcal{P}|$. Then we have a homomorphism

$\varphi : \mathbb{Z}^n \to Cl(-d)$ by

$$\varphi(x_1, ..., x_n) = \prod_{i=1}^{n} f_i^{x_i}.$$

An integer relation on $f_1, ..., f_n$ is a vector $(x_1, ..., x_n) \in \mathbb{Z}^n$ such that $\varphi(x_1, ..., x_n) = \prod_{i=1}^{n} f_i^{x_i} = 1_{Cl(-d)}$ where $1_{Cl(-d)}$ is the identity element of the class group $Cl(-d)$. Relations in $f_1, ..., f_n$ form an additive subgroup of $\mathbb{Z}^n$ (i.e. a Euclidean lattice) which we denote as Λ. Since φ is surjective, we have

$$\mathbb{Z}^n/\Lambda \cong Cl(-d).$$

Therefore, the computation of $Cl(-d)$ reduces to the search for relations between the $f_1, \ldots, f_n$. Once enough relations are collected to generate Λ, a polynomial time linear algebra phase yields the quotient $\mathbb{Z}^n/\Lambda$, and therefore the ideal class group $Cl(-d)$ and class number $h(-d) = |\det(\Lambda)|$.

Let us denote the box $\{x \in \mathbb{Z}^n,\ ||x||_\infty \leq t\}$ by $W_n(t)$. Algorithm 2 outlines the Hafner and McCurley class group algorithm.

Input : $d > 4$ with $d \equiv 0$ or $3 \bmod 4$
Output: The class number $h(-d)$ and the invariants of the class group $Cl(-d)$

1 Compute a rational number B such that $B/2 \leq h(-d) < B$ as explained in [53];
2 By using the relation search strategy of Seysen [72], generate n relations $w_1, ..., w_n$ on the generators $f_1, ..., f_n$ from $W_n(n^2 d)$;
3 Compute the determinant h_0 of the $n \times n$ matrix A_0 formed by the columns $w_1, ...w_n$;
4 Create new relations $v_1, ..., v_m$ from $W_n(d^2)$;
5 Compute the Hermite normal form H of the $n \times (n + m)$ matrix formed by the columns $w_1, ..., w_n, v_1, ..., v_m$;
6 Let h be the product of the diagonal entries of the Hermite normal form H. If $h > B$ go back to Step 3. Otherwise, compute the SNF S of H and output the diagonal entries of S;

Algorithm 2: Hafner and McCurley Class group algorithm

3.2.1 Running Time of the Hafner and McCurley Algorithm

In this section, we discuss the running time of the Hafner and McCurley class group algorithm as explained in [41, Sec. 4]. The crucial part of Hafner and McCurley's class group computation strategy is the finding of a generating set for the lattice of the relations Λ. We have to choose $\mathcal{B}$ such that it generates the class group and is optimum for the generation of the lattice of the relations Λ. Let

$$\mathcal{B} = \left\{ p \leq B, \left(\frac{-d}{p}\right) \neq -1 \right\},$$

for a suitable B. According to Hafner and McCurley B should be taken as $L(d)^z$ with a parameter z, where

$$L(d) = e^{\sqrt{\log d \log\log d}}.$$

Then the the cardinality n of set $\mathcal{B}$ will be $L(d)^{z+o(1)}$.

Theorem 3.3. *The expected running time of Hafner and McCurley class group algorithm is* $L(d)^{\sqrt{2}+o(1)}$ *bit operations.*

Proof. Step 1 of Hafner and McCurley algorithm takes at most $n^{1+o(1)}$ bit operations [41]. For testing a relation in either Step 2 or Step 4, we have to do the composition and reduction of quadratic forms. The reduction algorithm is a variant of Euclid's algorithm as in Algorithm 5.4.2 of [29]. The composition of quadratic forms can be done by using Algorithm 5.4.7 of [29]. Both composition and reduction of quadratic forms can be done in $O(\log^2 d)$ bit operations. So, the running time to test a single relation in either Step 2 or Step 4 is $n^{1+o(1)}$ bit operations. Also, the probability for a random vector to generate a relation in either Step 2 or Step 4 is $L(d)^{-1/4z+o(1)}$. So, the expected running time to create all the relations for Step 2 and Step 4 is

$$(n+m)n^{1+o(1)}L(d)^{1/4z+o(1)}$$

Hafner and McCurley [41] proved that the number of relations m needed in Step 3 should be $n^{1+o(1)}$. So the total expected time for relations collection steps will be $n^{2+o(1)}L(d)^{1/4z+o(1)}$ bit operations. By using the Gaussian elimination and the Chinese remainder theorem Step 2 can be done by $O(n^{4+o(1)})$ bit operations. The Hermite normal form computation in Step 5 can be done by using fast integer multiplication methods [2] and we get the running time of $O(n^{4+o(1)})$ bit operations. Also, the SNF computation in Step 5 can be done by $O(n^3 \log^4(d))$ bit operations. Since we have $n = L(d)^{z+o(1)}$, the total running time for the Hafner and McCurley class group algorithm will be

$$L(d)^{2z+1/4z+o(1)} + L(d)^{4z+o(1)}.$$

So, with optimum choice $z = 1/\sqrt{8}$, the expected running time of the Hafner McCurley class group algorithm is $L(d)^{\sqrt{2}+o(1)}$ bit operations.

□

In [41, Sec. 5], Hafner and McCurley observed that the collection of relations in the subexponential class group computation method could be improved and made the following conjecture.

Conjecture 3.4. *Under the Generalized Riemann Hypothesis (GRH), the class group $Cl(-d)$ can be computed with an expected runtime of $L(d)^{2/\sqrt{3}+o(1)}$.*

In Chapter 4, we modify the relation collection phase of Hafner and McCurley class group algorithm and prove Conjecture 3.4. In fact, by using better linear algebra methods we achieve a run time of $L(d)^{3/\sqrt{8}+o(1)}$.

3.3 Class Group Computations in Higher Degree Number Fields

As mentioned in Section 3.1, the subexponential algorithms for the ideal class group computation of number fields are based on the index calculus method. The crucial part of the index calculus method is the relation collection phase. Let K be a number field of degree n and $\mathcal{O}$ be an order in K. For the relation collection phase of class group computation of $Cl(\mathcal{O})$, we have to find the relations of the form $\mathfrak{a} = (\phi)\mathfrak{p}_1^{e_1}...\mathfrak{p}_k^{e_k}$ for a given ideal $\mathfrak{a} \subseteq \mathcal{O}$ and $B > 0$, where $\mathfrak{p}_\mathfrak{i}$ are invertible prime ideals and belong to the factor base $\mathcal{B} = \{\mathfrak{p} \mid \mathrm{N}(\mathfrak{p}) \leq B\}$. We aim to achieve a subexponential class group algorithm when the bound B on the factor base is subexponential. In other words, we want the running time of the relation collection phase in $L_d(a_1, b_1)$ for $0 < a_1 < 1$ and $b_1 > 0$ when the bound B is in $L_d(a_2, b_2)$ for $0 < a_2 < 1$ and $b_2 > 0$. The classical method to produce a relation is by testing the smoothness of the power product of the ideals $\mathfrak{a} \cdot \prod \mathfrak{p}_i^{e_i}$ over the factor base $\mathcal{B}$ where $\mathrm{N}(\mathfrak{p}_\mathfrak{i}) \leq 48 \log|d|^2$ and $e_i \leq |d|$ where d is the discriminant of the order $\mathcal{O}$. We have to do ideal reduction before testing the smoothness of the product $\mathfrak{a} \cdot \prod \mathfrak{p}_i^{e_i}$. That is, we have to find an ideal $\mathfrak{b} \subseteq \mathcal{O}$ of small norm in the same equivalence class of $\mathfrak{a}' = \mathfrak{a} \cdot \prod \mathfrak{p}_i^{e_i}$. The following is the procedure for the ideal reduction.

Ideal reduction Let A be fractional ideal of the number field K of degree n. Consider the embeddings $(\sigma_i)_{1 \leq i \leq n}$ of K into $\mathbb{C}$. Then the Minkowski map from K to $\mathbb{R}^n$ is defined as follows

$$x \longrightarrow (\sigma_1(x), ..., \sigma_{r_1}(x), Re\,\sigma_{r_1+1}(x), Im\,\sigma_{r_1+1}(x), ..., Re\,\sigma_{r_1+r_2}(x), Im\,\sigma_{r_1+r_2}(x)).$$

The image of A under the Minkowski map is an n-dimensional lattice in $\mathbb{R}^n$. We compute a shortest non zero vector $\vec{\alpha}$ in this lattice. We find a short element α in A corresponding to

this shortest vector. Then for some $t \in \mathbb{Z}$ the ideal $\frac{t}{\alpha}A$ is an integral ideal and has a small norm. We call this ideal $\frac{t}{\alpha}A$ a reduced ideal in the equivalence class of A.

The subexponential class group algorithms apply the reduction procedure described above to the ideal $\mathfrak{c} = l\ \mathfrak{a}'^{-1}$ with $l \in \mathbb{Z}$. The reduction procedure provides $\phi \in \mathfrak{c}$ that satisfies

$$||\phi|| \leq \lambda_{\mathcal{O}} |d|^{\frac{1}{2n}} \mathrm{N}(\mathfrak{c})^{\frac{1}{n}}.$$

So we have the ideal $\mathfrak{b} = \frac{\phi}{l}\mathfrak{a}'$ of a small bounded norm where the approximation factor $\lambda_{\mathcal{O}}$ depends on the reduction procedure we use. The reduced ideal $\mathfrak{b}$ satisfies

$$\mathrm{N}(\mathfrak{b}) \leq \lambda_{\mathcal{O}}^{n} \sqrt{|d|}$$

and it will be in the same class of $\mathfrak{a}'$. The following is the summary of ideal reduction.

Proposition 3.5. *Let K be a number field of degree n. Let $\mathcal{O}$ be an order of K with discriminant d. Given an ideal $\mathfrak{a}$ of $\mathcal{O}$, the ideal reduction provides an ideal $\mathfrak{b}$ of bounded norm in the same ideal class of $\mathfrak{a}$ that satisfies*

$$\mathrm{N}(\mathfrak{b}) \leq \lambda_{\mathcal{O}}^{n} \sqrt{|d|},$$

where the approximation factor $\lambda_{\mathcal{O}}$ depends on the reduction procedure.

Input : Number field K of degree n, ideal $\mathfrak{a} \subseteq \mathcal{O}$ with discriminant d.
Output: Ideal $\mathfrak{b} \subseteq \mathcal{O}$ with $\mathrm{N}(\mathfrak{b}) \leq \lambda_{\mathcal{O}}^{n} \sqrt{|d|}$, where $\lambda_{\mathcal{O}}$ is the approximation factor.

1 $\mathfrak{c} = l\mathfrak{a}^{-1}$ with $l \in \mathbb{Z}$;
2 Let $\mathcal{L} = \Phi(\mathfrak{c})$ be the image of $\mathfrak{c}$ under the Minkowski map Φ;
3 Find a shortest vector v in $\mathcal{L}$;
4 Find the short element $\phi \in \mathfrak{c}$ corresponding to v;
5 **return** $\mathfrak{b} = \frac{\phi}{l}\mathfrak{a}$

Algorithm 3: Ideal reduction

After obtaining the reduced ideal $\mathfrak{b}$, we try to decompose the ideal $\mathfrak{b}$ over the factor base $\mathcal{B}$ to obtain a relation. Using the above strategy in 1990 Buchmann [23] generalized the Hafner

and McCurley subexponential algorithm for arbitrary number fields under the Generalized Riemann hypothesis (GRH). In [23], Buchmann achieved a heuristic time complexity of $L_d(\frac{1}{2}, 1.7 + o(1))$. Later [30] provided the practical implementation of Buchmann's strategy. In [30], Cohen, Diaz Y Diaz and Olivier used LLL-reduction for the ideal reduction procedure. One important observation to make here is that the reduction procedure is easy for the Hafner and McCurley class group algorithm of imaginary quadratic fields. For the class group computation of an imaginary quadratic field, we can work with binary quadratic forms, and the reduction procedure is easy and can be performed in $O(\log^2|d|)$ bit operations where d is the discriminant of the binary quadratic form. But we can no longer work on quadratic forms for higher degree number fields. Another key difference between the class group computation of quadratic fields and the higher degree fields is the smoothness probability of the reduced ideals. For imaginary quadratic fields, we have a theorem due to Seysen [72] which gives a probability for the smoothness of the reduced form over the factor base. The same theorem can be applied to real quadratic fields as well. But for higher degree number fields we don't have any such theorem and we have to depend on heuristics such as Corollary 2.1 of [12] for the class group computations. Also these heuristics on the probability of smoothness of reduced ideals depend on the norm of the reduced ideal. That is, the smaller the norm of the reduced ideal, the higher the smoothness probability, and vice versa.

Buchmann's algorithm's time complexity is valid only for classes of number fields of fixed degree with a discriminant that tends to infinity. We will explain the reason for this limitation shortly. In 2014 Biasse [10] introduced a method to compute the class group and the unit group of an equation order $\mathbb{Z}[\theta]$ with a heuristic subexponential time complexity $L_d(1/3, c)$ for some $c > 0$ in certain classes of number fields under GRH. The results presented in [10] deal with the instances where the degree and the discriminant of the extension grow to infinity under certain conditions. This method was influenced by the $L(1/3)$ algorithm of Enge, Gaudry, and Thomé [37] which computes discrete logarithms in the Jacobian of certain classes of algebraic curves. Later in [12, 14] Biasse and Fieker introduced a heuristic

subexponential algorithm for the class group computation of all classes of number fields under GRH. Biasse and Fieker deal with instances where the degree of the number field goes to infinity. The main idea behind the subexponential algorithm of Biasse and Fieker is the use of the BKZ [68] reduction for the ideal reduction procedure. The following is the outline of BKZ [68] ideal reduction.

For classes of number fields for which the degree $n \to \infty$, we have $n \leq \log|d|$. The BKZ reduction offers a trade-off between the time spent for the reduction and approximation factor $\lambda_{\mathcal{O}}$. In other words, it offers trade-off between the time spent for the reduction and the bound on the norm of the reduced ideal $\mathfrak{b}$. The approximation factor for the BKZ reduction is $\lambda_{\mathcal{O}} = k^{\frac{n}{2k}}$ for a parameter $k \leq n$ and it has a running time of $2^{O(k)} \cdot P(n)$ where P is a polynomial. So we have the bound on the norm of the reduced ideal

$$\mathrm{N}(\mathfrak{b}) \leq k^{\frac{n^2}{2k}} \sqrt{|d|}.$$

If we choose $k = \log(|d|)^{\frac{2}{3}} \log\log(|d|)^{\frac{1}{3}}$, the bound on the norm of the reduced ideal becomes $L_d(4/3, e_1)$ for some $e_1 > 0$. Also if we choose a subexponential bound $B = L_d(2/3 + \epsilon)$ for the factor base for some $\epsilon > 0$, then by using the heuristic on smoothness probability as in Corollary 2.1 of [12], the expected number of BKZ_k reduced ideals we have to draw to find a B-smooth ideal is $L_d(2/3+\epsilon, O(1))$ and we get $L_d(2/3+\epsilon)$-time algorithm to compute the class group $Cl(\mathcal{O})$. But if we use LLL-reduction as in [30] then the approximation factor will be $\lambda_{\mathcal{O}} = 2^{\frac{n}{2}}$ and the bound on the reduced ideal will be

$$\mathrm{N}(\mathfrak{b}) \leq 2^{\frac{n^2}{2}} \sqrt{|d|} \leq L_d(2, e_2)$$

for some $e_2 > 0$. Then for a subexponential bound on the factor base $B = L_d(\alpha, c)$ for some $0 < \alpha < 1$ and $c > 0$, the expected time to find a $B-$smooth ideal will be $L_d(2 - \alpha, e_3)$ for some $e_3 > 0$. So it's impossible to find a subexponential algorithm for the class group

computation by using LLL-reduction for the classes of number fields where degree tends to infinity. The following is the summary of BKZ ideal reduction method.

Proposition 3.6. *Let K be a number field of degree n. Let $\mathcal{O}$ be an order of K with discriminant d. Given an ideal $\mathfrak{a}$ of $\mathcal{O}$, the BKZ ideal reduction provides the ideal $\mathfrak{b}$ of bounded norm in the same ideal class of $\mathfrak{a}$ that satisfies*

$$\mathrm{N}(\mathfrak{b}) \leq k^{\frac{n^2}{2k}} \sqrt{|d|},$$

for a parameter k and it has a running time of $2^{O(k)} \cdot P(n)$ where P is a polynomial.

Beyond the subexponential complexity In 2019, motivated by the work of [5], Biasse and van Vredendaal [18] presented a heuristics algorithm for the S-unit computation in real multiquadratic fields $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$ under GRH. This algorithm has a heuristic time complexity of $\mathrm{Poly}\Big(\log(|d|), \mathrm{Size}(S)\Big) e^{\tilde{O}(\sqrt{\log|d_0|})}$ where $d_0 = d_1 \cdots d_n$ and d is the discriminant of the multiquadratic field K. Since the ideal class group of the field can be obtained from the S-unit group computation when S generates the ideal class group, the method of Biasse and van Vredendaal gives the ideal class group in time $\mathrm{Poly}\Big(\log(|d|)\Big) e^{\tilde{O}(\sqrt{\log|d_0|})}$. The key idea behind the algorithm of [18] is a recursive strategy that takes advantage of the computation in subfields. Later Biasse, Fieker, Hofmann and Page [20] generalized the strategy of [18]. In [20], they presented a systematic method to leverage the computations in subfields for the computation of rings of integers, S-unit groups, and class groups. The strategy of [20] was used for computing the class group of $K = \mathbb{Q}(\zeta_{6552})$ of degree 1728 with a 5258-digit discriminant and other number fields of large degree and discriminant under the assumption of GRH.

3.4 Unconditional Class Group Computations

The index calculus algorithms we discussed earlier for ideal class group computations depend on the Generalized Riemann Hypothesis (GRH) and other heuristics. In this section, we discuss the unconditional class group computational results, meaning the class group computations without assuming GRH, as documented in the literature, and we analyze their time complexity compared to index calculus algorithms. In 1968, Shanks [73] introduced the powerful technique called baby-steps-giant-steps. Using this technique the class number of the imaginary quadratic field of discriminant d can be computed unconditionally with a running time of $O(|d|^{1/4+\epsilon})$. Later, Buell [28] did a comprehensive computation of imaginary quadratic fields. Buell unconditionally computed the class group of imaginary quadratic fields with discriminants $0 < |d| < 2.2 \cdot 10^9$. Buell's unconditional computation was based on counting the number of reduced binary quadratic forms. This strategy took $O(|d|^{1/2})$ steps for each discriminant d. In 2006, Jacobson et al. [45] tabulated the class groups of all imaginary quadratic fields for $0 < |d| < 10^{11}$. They used an algorithm given by Buchmann, Jacobson, and Teske (BJT) [24] for their computation and its correctness is conditional on GRH. But Jacobson et al. verified their results unconditionally using a verification algorithm based on the Eichler Selberg Trace Formula [71]. Overall this approach takes $O(|d|^{1/4+\epsilon})$ steps per discriminant. Using the same approach of [45], Ramachandran [64] extended the bound on discriminant to $|d| < 2 \cdot 10^{11}$ with same number of steps per discriminant. In 2016, Mosunov and Jacobson [57] presented an improved algorithm for unconditional class group tabulation of imaginary quadratic fields up to the discriminant 2^{40}. Mosunov and Jacobson's method [57] was inspired by that of Hart et al. [42] and they used certain class number generating functions and a product of two large-degree power series for their class group computations.

For the class group computation of real quadratic fields Lenstra [48] and Schoof [70] introduced a modified version of Shanks' baby-steps-giant-steps algorithm. These modified

algorithms could compute the class groups of real quadratic fields unconditionally with a probabilistic running time of $O(d^{1/4+\epsilon})$. Later, in 1998 Srinivasan [78] presented a probabilistic algorithm, a version of Shanks's algorithm, that could compute the class group of real quadratic field. Srinivasan's algorithm did not assume GRH and has an expected running time of $O(d^{1/5+\epsilon})$. In 2023, Bian et al. [9] introduced a modified generic group structure algorithm of Buchmann and Schmidt [25] for class group computation of real quadratic fields. They also used the Selberg trace formula for Maaß forms to verify the class groups and regulators. This algorithm could compute the class group and the regulator for discriminant $d < X$ in time $O(X^{5/4+o(1)})$. Bian et al. [9] were able to compute unconditionally correct class groups and regulators of real quadratic fields up to discriminant 10^{11}. It is important to observe that there are currently no unconditional subexponential class group computation methods available for both real and imaginary quadratic fields.

The case of cyclotomic fields The computation of the class number of cyclotomic fields is considered a computationally hard problem. The difficulty lies within the computation of the class number of the maximal real subfield of cyclotomic fields. The classical method for unconditional computation of the class number of maximal real subfield of cyclotomic fields is by using Minkowski's bound, which is defined as

$$M_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d|}.$$

This method involves checking whether prime numbers below Minkowski's bound factor into principal ideals. Since the Minkowski bound is proportional to the square root of the discriminant, this method becomes impractical for large discriminants. Based on Odlyzko's discriminant lower bounds [60], Masley [51] computed the class numbers of maximal real subfield of cyclotomics fields unconditionally. Later Van der Linden [49] extended Masley's results and performed unconditional computations of composite conductors up to conductor 200. But the methods of Masley [51] and Van der Linden [48] become too difficult when

the root discriminant of the field becomes large. To overcome this difficulty, Miller [54] introduced a new approach for class number upper bound that applies to number fields of large root discriminants. Miller's method involved establishing a lower bound for the sums of prime ideals of the Hilbert class field, consequently yielding an upper limit for the class number of the maximal real subfield of a cyclotomic field. By using this method, Miller computed unconditional class numbers of maximal real subfield of cyclotomic fields of composite conductors with degree up to 116 [54]. Later this method was extended to prime conductors in [56]. In [56], Miller presented unconditional computation of the class numbers of the maximal real subfield of cyclotomic fields for all prime conductors less than 151. In Chapter 6, we introduce a new technique for unconditional class number computation of maximal real subfield of cyclotomic fields and present a few class numbers that are not documented in the literature.

3.5 Applications of Ideal Decomposition

As we discussed in the Section 3.3, a key step in the computation of the ideal class group and the unit group of order $\mathcal{O}$ in a number field K is to decompose a given ideal $\mathfrak{a}$ as $\mathfrak{a} = (\phi)\mathfrak{p}_1^{e_1}...\mathfrak{p}_N^{e_N}$, where the $\mathfrak{p}_\mathfrak{i}$ are invertible prime ideals and belong to the factor base $\mathcal{B} = \{\mathfrak{p} \,|\, \mathrm{N}(\mathfrak{p}) \leq B\}$. This way of representing an ideal as a power product of ideals of smaller norms is called ideal decomposition. If we replace the LLL-reduction method of Buchmann [23] with the BKZ-reduction, then we can obtain a subexponential method for ideal decomposition [12, 14]. One of the main applications of the ideal decomposition is the computation of the ideal class group and fundamental units of $\mathcal{O}$. This is done by deriving relations in $Cl(\mathcal{O})$ of the form $\prod \mathfrak{p}_i^{e_i} = (\phi)$. There are also other important applications for the ideal decomposition method. Let's briefly discuss a few of them.

3.5.1 Principal Ideal Problem

Given an arbitrary ideal $\mathfrak{a} \subseteq \mathcal{O}$, the principal ideal problem is checking whether the ideal is principal, and if it is principal find the ϕ such that $\mathfrak{a} = (\phi)$. An algorithm for the principal ideal problem by using ideal decomposition is presented in [12] and it is as follows. First, we do the ideal decomposition of $\mathfrak{a}$ over a factor base $\mathcal{B} = \mathfrak{p}_1, ..., \mathfrak{p}_N$. Let the ideal decomposition of $\mathfrak{a}$ be $\mathfrak{a} = (\phi)\mathfrak{p}_1^{b_1}...\mathfrak{p}_N^{b_N}$. Let $b = (b_1, ..., b_N)$. Using the ideal decomposition, we can also find the relations between the elements of $\mathcal{B}$. That is vectors of the form (e_i) such that $\prod \mathfrak{p}_i^{e_i} = (\phi)$ for some $\phi \in K$. Let M be an $N \times N'$ matrix whose rows generate all relations over the factor base $\mathcal{B}$. If we can show that b belongs to the lattice spanned by the row vectors of M, then the ideal $\mathfrak{a}$ should be principal by the construction. In other words, if $XM = b$ has a solution, then $\mathfrak{a}$ is principal and otherwise not. The generator of the principal ideal can be obtained from the solution X of $XM = b$. Since ideal decomposition can be done in subexponential time as in [12, 14], the principal ideal problem can also be done in subexponential time under GRH.

3.5.2 S-Unit Group Computation

Let S be a finite set of prime ideals of a field K. An element $x \in K$ is called an S-integer if $v_{\mathfrak{p}}(x) \geq 0$ for all $\mathfrak{p} \notin S$. We denote the ring of S-integers by $\mathcal{O}_{K,S}$. An element $x \in K$ is called S-unit if $v_{\mathfrak{p}}(x) = 0$ for all $\mathfrak{p} \notin S$. We denote the multiplicative group of S-units by $U_{K,S}$. The S-unit group $U_{K,S}$ can also be considered as the set of all invertible elements of the ring of S-integers $\mathcal{O}_{K,S}$. The S-unit group is finitely generated and each S-unit can be written as a power product of its fundamental S-units. In [75], Simon presented an algorithm for the computation of fundamental S-units by using the ideal decomposition. This is another application of ideal decomposition for solving computationally hard number theory problems. We briefly discuss Simon's S-unit computation here. Let's start with the definition of Hermite normal form computation, which is crucial for Simon's method.

Definition 3.7. An m by n matrix A with integer entries has a Hermite normal form $H = (h_{ij})$ if there is a square unimodular matrix U such that $H = UA$ and H satisfies the following conditions:

1. $\forall j < i,\ 0 \leq h_{ij} < h_{jj}$.

2. $\forall j > i,\ h_{ij} = 0$.

The Hermite normal form of a matrix can be computed by using the Algorithm.2.4.4 of [29]. The strategy of Simon's S-unit computation [75] is as follows. For a vector V with l elements and a $k \times l$ matrix U, we define a k element vector $W = V^U$ as $W_i = \prod_j V_j^{U_{i,j}}$. Also, we use $\begin{pmatrix} A \\ B \end{pmatrix}$ to denote the concatenation of two matrices A and B. Let $S = \{\mathfrak{p}_1, ..., \mathfrak{p}_s\}$. Also, let $d_1, ..., d_r$ be the elementary divisors of the ideal class group $Cl(K)$ and $\mathfrak{g}_1, ..., \mathfrak{g}_r$ be the generators corresponding to cyclic subgroups corresponding to the elementary divisors. Consider the matrix

$$M = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix}$$

Since $\mathfrak{g}_i$ is the generator of the cyclic subgroup of order d_i, we have $\mathfrak{g}_i^{d_i} = (\beta_i)\mathcal{O}_K$ for some $\beta_i \in K^*$ and let $V = (\beta_1, ..., \beta_r)$ be the vector corresponding to $\mathfrak{g}_1, ..., \mathfrak{g}_r$. Now we do the ideal decomposition of prime ideals $\mathfrak{p}_i$ in S over the factor base $\mathfrak{g}_1, ..., \mathfrak{g}_r$. That is we do the decomposition

$$\mathfrak{p}_j = \prod_i \mathfrak{g}^{e_{i,j}} \alpha_j$$

for $\alpha_j \in K^*$ and $e_{i,j} \in \mathbb{Z}$. Then, consider the matrix $M' = -(e_{i,j})$ and the vector $V' = (\alpha_1, ..., \alpha_s)$. We compute the Hermite normal form of the concatenated matrix $\begin{pmatrix} M \\ M' \end{pmatrix}$ and get the unimodular matrix U such that

$$U \begin{pmatrix} M \\ M' \end{pmatrix} = \begin{pmatrix} H \\ 0 \end{pmatrix},$$

where H is the Hermite normal form. Then compute

$$(W \mid W') = (V \mid V')^U$$

and the elements in W will be the generators of the S-unit group modulo the units of K. If we use ideal decomposition as in [12, 14], then the S-unit group computation can also be done in subexponential time under GRH.

One of the applications of subexponential S-unit computation mentioned above is solving the so-called norm equations. The norm equation is $N_{L/K}(x) = a$ for a given arbitrary extension of number fields L/K and an algebraic number field element a of K. In [76], Denis Simon introduced an algorithm to solve the norm equation when a is an S-unit, and when we need the solution x to be also an S-unit for a given S. So, the subexponential S-unit group computation can be used here to solve the norm equation. Another noteworthy observation is that one of the traditional approaches to solving Pell's equation involves calculating numerous elements with small norms in a quadratic field. Hence, solving norm equations contributes to addressing Pell's equations.

3.6 Applications to Cryptography

Ideal class groups play a significant role in cryptography due to their algebraic properties, which can be harnessed to create secure cryptographic systems. Ideal class group computation has applications in schemes based on the discrete logarithm problem, elliptic curve cryptography, and lattice-based cryptography. These applications span various cryptographic primitives and protocols, advancing secure communication and data protection.

In this section, we briefly discuss some of these applications of ideal class group computation in cryptography.

Schemes based on the discrete logarithm problem Schemes based on the discrete logarithm problem are the most obvious applications of ideal class group computations in cryptography. For an order $\mathcal{O}$ in a number field K, the ideal decomposition of an ideal $\mathfrak{a} \subseteq \mathcal{O}$ is used for solving discrete logarithm problems in the ideal class group $Cl(\mathcal{O})$. Buchmann and Williams [26, 27] introduced schemes based on discrete logarithm problems in the ideal class groups in 1980. They described two types of schemes: those utilizing imaginary fields and those utilizing real fields. In the imaginary field case, cryptosystems rely on arithmetic operations within the ideal class group, and security is based on solving the discrete logarithm problem. In the real field scenario, a structure known as the infrastructure is used, and security is based on a problem analogous to the discrete logarithm problem, namely the principal ideal problem. The latest security estimates, derived from computational data on solving the underlying challenging problems (which stem from the difficulty of computing the ideal class group), have been provided by Biasse, Jacobson, and Silvester [17].

Evaluation of isogenies An elliptic curves E defined over a finite field F_q is an algebraic group given by the equation

$$E : y^2 = x^3 + ax + b,\ a, b \in F_q,\ 4a^3 + 27b^2 \neq 0.$$

For elliptic curves E, E' defined over F_q, an isogeny is a non-constant rational map between E and E'. It is also a group homomorphism. An endomorphism of E is an isogeny $E \to E$. The set of all endomorphisms of E forms a ring under pointwise addition and multiplication. This ring is called the endomorphism ring of E. In ordinary elliptic curves defined over finite fields, as well as in supersingular elliptic curves defined over prime fields, the ring of endomorphisms is isomorphic to an order in an imaginary quadratic field. Isomorphism

classes of curves are in correspondence with classes of ideals in $Cl(-d)$, and the class of a split prime ideal of norm ℓ acts as an isogeny of degree ℓ. As shown by Biasse, Fieker and Jacobson in [15, Prop. 6.2], the computation of a reduced basis of relations yields efficient ideal decompositions in $Cl(-d)$, which in turn allows the fast evaluation of isogenies of large degrees. This strategy was used in the signature scheme CSI-FiSh [8] where the pre-computation of the class group of a 154-digit discriminant field enables good performances because signing involves the evaluation of large degree isogenies through the decomposition of the corresponding ideal class.

Short generator of a principal ideal In 2009 Gentry [39, 40] presented the first fully homomorphic encryption scheme. The scheme was based on hardness of finding short vectors in ideal lattices. Later Vercauteren and Smart [77] showed that finding a short generator of principal ideal could break some variations of Gentry's scheme. This is an application of ideal decomposition or principal ideal problem to the cryptanalysis of homomorphic encryption schemes. In 2013 Lyubashevsky et al. [50] introduced a lattice-based cryptosystem called Ring Learning With Error (RLWE). RLWE is based on finding short vectors in the ideal lattices of cyclotomic fields. Later [31, 32, 33] showed that there was an efficient heuristic quantum reduction from the search for short vectors in ideal lattices to generators of principal ideal problem. The bottleneck of this ideal lattice-based cryptosystem is the ideal decomposition in the ideal class group.

CHAPTER 4

CONJECTURED RUN TIME OF THE HAFNER-MCCURLEY CLASS GROUP ALGORITHM

In this chapter[1], we present a modified version of the Hafner-McCurley class group algorithm and prove the conjectured runtime of the Hafner-McCurley class group algorithm [41, Sec. 5]. In this modified version, we demonstrate that the class group algorithm of Hafner and McCurley runs in expected time $e^{\left(3/\sqrt{8}+o(1)\right)\sqrt{\log d \log\log d}}$, where $-d$ is the discriminant of the input imaginary quadratic order. In the original paper, an expected runtime of $e^{\left(\sqrt{2}+o(1)\right)\sqrt{\log d \log\log d}}$ was proven, and better bounds were conjectured. To achieve a proven result, we rely on a mild modification of the Hafner and McCurley algorithm and recent results on the properties of the Cayley graph of the ideal class group [46]. This chapter is based on collaborative research work with Jean-François Biasse, published in Advances in Mathematics of Communications (AMC) [13]. The following is the main result of our publication.

Theorem 4.1. *Under a generalization of the Riemann hypothesis, there is a Las Vegas algorithm that computes $Cl(-d)$ with probability $1 - \frac{1}{d^{1+o(1)}}$ in time*

$$L(d)^{3/\sqrt{8}+o(1)} = e^{\left(3/\sqrt{8}+o(1)\right)\sqrt{\log d \log\log d}}.$$

The complexity proved in the main result is not surprising. Indeed, as early as 1988, McCurley [53] gave heuristic arguments showing that $|Cl(-d)|$ should be computable in time $L(d)^{3/\sqrt{8}+o(1)}$ (note that this conjecture only concerns the computation of the cardinality of

[1]This chapter is based on collaborative research work with Jean-François Biasse, published in Advances in Mathematics of Communications (AMC) [13]

$Cl(-d)$, not the group structure itself). Then, in [41, Sec. 5], Hafner and McCurley described conjectural improvements to their subexponential techniques for computing $Cl(-d)$ that included the observation that the collection of the relations could be improved and that such an improvement would yield a run time of $L(d)^{2/\sqrt{3}+o(1)}$. Combined with better linear algebra methods than the ones used in [41], this yields the run time of $L(d)^{3/\sqrt{8}+o(1)}$ we prove in this chapter. In 2000, Vollmer even claimed a proof of this run time [82, Th. 2]. However, this claim was retracted in the Corrigendum of a 2002 follow-up paper [81]. In 2016, Biasse, Fieker, and Jacobson conjectured the main result of this chapter [15, Conj. 1].

Our methods rely on a result from Jao, Miller, and Venkatesan [46] showing that under the GRH, the Cayley graph of $Cl(-d)$ is an expander graph (for a good choice of edges). This allowed us to show that relations between generators of $Cl(-d)$ could be obtained from short products of generators. With that knowledge, we prove that a minor modification of the original algorithm of Hafner and McCurley yields the conjectured expected run time. We do not rule out the existence of a more elementary proof involving techniques available at the time of Hafner and McCurley's paper [41] in addition to cubic complexity linear algebra methods (as observed in [41, Sec. 5], linear algebra with quartic complexity can only yield a total run time of $L(d)^{2/\sqrt{3}+o(1)}$).

On the other hand, we do not foresee any improvement of these methods that would yield a subexponential run time that is not conditional on a generalization of the Riemann Hypothesis being true. Indeed, all variations around the subexponential algorithm of [41] rely on the manipulation of vectors whose length is given by the first n primes generating the class group. So far, the only known unconditional bounds on the length of such vectors are all exponential in the input size. We assume a generalization of the Riemann hypothesis in this chapter as described in Conjecture 2.2 and we abbreviate it by "GRH". Note that the same assumption is sometimes referred to as the Extended Riemann Hypothesis (ERH), in particular in [4] and [41].

4.1 Overview of the Algorithm

As we have seen in Section 3.2, the subexponential algorithm of Hafner and McCurley consists in the choice of a factor basis $f_1, \ldots, f_n$, and the resolution of the following two main tasks:

- Finding a generating set of elements of Λ, the lattice of relations between factor basis elements.
- Computing the quotient $\mathbb{Z}^n/\Lambda$.

The quotient computation is well understood and essentially corresponds to the computation of the Smith Normal Form (SNF) of the matrix representing a basis for Λ. Such a basis is typically obtained by computing the Hermite Normal Form (HNF) of a rectangular matrix representing a generating set for Λ. Polynomial time methods for the computation of HNF and SNF of integer matrices are known. Therefore, the main challenge of the algorithm is the calculation of a generating set for Λ as we discussed in Section 3.2.

The main issue with computing a basis of Λ is that we cannot easily sample random elements of Λ. In practice, products of the generators $f_1, \ldots, f_n$ with exponents drawn uniformly at random seem to be equivalent to random smooth form, and thus yield relations between the generators that appear to be distributed closely to the uniform distribution. This explains why in practical implementations [6, 11, 16, 30, 44], the randomization of the elements in Λ that are calculated is never an issue, and the number m of elements of Λ we need to draw is never significantly larger than n. At the end of the procedure, we can efficiently test whether enough relations were collected, thus certifying the computation. This test is based on a bound h^* as mentioned in Step 1 of the class group algorithm of [41] that we can efficiently compute, which satisfies $h^* \leq \det(\Lambda) < 2h^*$. If $\det(\Lambda) \geq 2h^*$, then more relations are needed.

Making a formal case for the run time without the heuristic that elements sampled in Λ are distributed uniformly at random is more difficult. This was achieved by Hafner and

McCurley in their original paper [41] at the price of a procedure that makes relation collection artificially more expensive than what is done in practical implementations in order to prove its expected run time under GRH. In this chapter, we show how to enhance this phase of the algorithm without having to rely on additional heuristics. The relation collection can be divided into phases. The original algorithm of Hafner and McCurley has two phases. The first one consists in the creation of n relations that are linearly independent. This means that at the end of it, we know $\Lambda_0 \subseteq \Lambda$ of full rank. However, since we typically have $\det(\Lambda_0) \gg \det(\Lambda)$, more relations are needed to find a generating set of Λ. Then the second phase consists of creating new relations with an expensive randomization strategy such that the the corresponding lattices $(\Lambda_i)_{i \leq m}$ they generate satisfy

$$\Lambda_0 \subseteq \Lambda_1 \subseteq ... \subseteq \Lambda_m \subseteq \Lambda$$

Our algorithm introduces an intermediate phase before the expensive randomization strategy of Hafner and McCurley in order to make sure that Λ_1 has a moderate determinant. We label our phases from 1 to 3.

Phase 1- For each $k = 1, \ldots, n$, we compute a relation whose k-th coefficient is significantly larger than the others. This method due to Seysen [72] ensures the fact that at the end of the collection of the first n relations, the lattice Λ_0 they generate has full rank.

Phase 2- We construct additional relations in order to ensure that at the end of this phase, the lattice Λ_1 they generate satisfies $\det(\Lambda_1) \in 2^{O(\log^4 d)}$. This is our main technical addition to the original method from [41]. We achieve this by observing that as long as $\det(\Lambda_1) > e^{\log^4 d}$, the lattice Λ_1 is very sparse within Λ, and therefore we can ensure the creation of new relations outside of Λ_1 with large enough probability.

Phase 3- Once we have $\det(\Lambda_1) \in 2^{O(\log^4 d)}$, we resume the creation of new relations with the expensive last phase of [41]. Since $|\Lambda/\Lambda_1|$ is small, the number of expensive steps is significantly smaller than in [41].

4.2 Phase 1

In this section, we show how to create n linearly independent relations between the $(f_i)_{i\leq n}$. We follow the approach of Seysen [72, Sec. 4] which consists in ensuring that the matrix $(a_{i,j})$ whose rows are the relation vectors satisfies $|a_{ii}|> \sum_{j\neq i}|a_{i,j}|$, which in turns guarantees that the matrix $(a_{i,j})$ has full rank. To improve on the run time of Seysen, we use the fact that the Cayley graph of $Cl(-d)$ is an expander graph as we discussed in Theorem 2.7. According to Theorem 2.7 a random walk of length at least $C\frac{\log|Cl(-d)|}{\log\log d}$ starting from any vertex of the Cayley graph of $Cl(-d)$ ends on a node whose distribution is close to the uniform one.

We can use this result to produce an analogue of the method of Seysen [72, Sec. 4] which requires only short products in order to produce a sparse relation with a dominant i-th coefficient. Here, we assume that

$$\mathcal{B} = f_1, \ldots, f_n = \left\{\text{Prime forms corresponding to } p \leq L(d)^z \text{ and } \left(\frac{d}{p}\right) \neq 1\right\},$$

which means that $n = L(d)^{z+o(1)}$. Choosing $t = \log(d) \gg C\frac{\log|Cl(-d)|}{\log\log d}$, we draw random vectors $\vec{x}$ of ℓ_1-norm t until $f \cdot \left(\prod_{i\leq n_0} f_i^{x_i}\right)$ factors as a product of elements of $\mathcal{B}$ (i.e. is $\mathcal{B}$-smooth). The cost and the chances of success are given by Theorem 2.7 applied to the set G_0 of $\mathcal{B}$-smooth reduced forms. We fix an amount of attempts such that the probability of obtaining the desired decomposition is high enough. To test for smoothness, we use Bernstein's batch smoothness test [7] rather than trial division. Bernstein's batch smoothness test allows us to test the smoothness of a set of elements together over a factor base. Given a finite set P of primes and a set S of positive integers, Bernstein's batch smoothness test finds P-smooth elements in S with a running time of $b(\log b)^{2+o(1)}$, where b is the total number of bits in P and S. In contrast, with trial division, we have to test the smoothness of each element in S separately, resulting in a running time of $b^{2+o(1)}$. Therefore, Bernstein's batch smoothness test allows us to reduce the asymptotic complexity. If at the end of the

procedure, no smooth form was found, we declare a failure. If not, the result is guaranteed to be correct. This is compatible with a Las Vegas algorithm. All procedures presented throughout this chapter satisfy this property.

Input : Fundamental discriminant $-d < 0$, reduced form f, set of prime forms $\mathcal{B} = \{f_1, \ldots, f_n\}$, $\varepsilon > 0$
Output: $\vec{x} \in \mathbb{Z}^n$ such that $\prod_{i \leq n} f_i^{x_i} = f$, or FAILURE

$B \leftarrow 4 \cdot e^{u(\log u + \log\log u + c(\varepsilon))}$ for $c(.)$ as in [72, Th. 5.2] and $u = \frac{\log\left(\sqrt{d}/2\right)}{\log(L(d)^z)}$;
$f'_1, \ldots, f'_{n_0} \leftarrow \left\{\text{Prime forms with } p \leq \log^{2+\varepsilon}(d) \text{ and } \left(\frac{d}{p}\right) \neq 1\right\}$;
if $(f_i)_{i \leq n_0} \neq (f'_i)_{i \leq n_0}$ **then**
  return: FAILURE
end
$t \leftarrow \log d$. Initiate an empty list L_{forms};
for $k \leftarrow 1$ **to** $\lceil B \rceil$ **do**
  Draw $\vec{y} \in \mathbb{Z}^{n_0}$ uniformly at random among the ℓ_1-norm t vectors;
  Store $\vec{y}$ and $\left(\prod_{i \leq n_0} f_i^{y_i}\right) \cdot f$ in L_{forms};
end
Test the $\mathcal{B}$-smoothness of all forms in L_{forms} using [7];
if *There is* $\left(\prod_{i \leq n_0} f_i^{y_i}\right) \cdot f$ *that is* $\mathcal{B}$*-smooth in* L_{forms} **then**
  Let $\vec{x'} \in \mathbb{Z}^n$ with $\left(\prod_{i \leq n_0} f_i^{y_i}\right) \cdot f = \prod_{i \leq n} f_i^{x'_i}$ and $\vec{y'} = (\vec{y} \,||\, \vec{0}) \in \mathbb{Z}^n$;
  return: $\vec{x} = \vec{x'} - \vec{y'}$;
else
  return: FAILURE
end

Algorithm 4: Relation search algorithm

Proposition 4.2. *Under GRH, Algorithm 4 with input*

$$\mathcal{B} = \left\{ \textit{Prime forms corresponding to } p \leq L(d)^z \textit{ and } \left(\frac{d}{p}\right) \neq 1 \right\},$$

succeeds with probability at least $1 - \frac{1}{d^{1+o(1)}}$ *in time* $L(d)^{1/4z+o(1)} + L(d)^{z+o(1)}$ *and returns a vector* $\vec{x}$ *whose* ℓ_1*-norm is in* $O(\log d)$.

Proof. We denote by S the set of $\mathcal{B}$-smooth reduced forms of $Cl(-d)$. From the proof of [72, Prop. 4.4], we know that the probability $\frac{|S|}{2|Cl(-d)|}$ that a single product of the form

$\left(\prod_{i\leq n_0} f_i^{y_i}\right)\cdot f$ be $\mathcal{B}$-smooth satisfies

$$\frac{|S|}{2|Cl(-d)|}\geq\frac{\psi_{-d}(\sqrt{d}/2,L(d)^z)}{2\sqrt{d}\log d},$$

where the function $\psi_{-d}(x,y):=\{a\leq x:\text{Any prime dividing } a \text{ satisfies } p\leq y \text{ and } (\frac{-d}{p})=1\}$. The function $\psi_{-d}(x,y)$ satisfies the inequality

$$\psi_{-d}(x,y)\geq x\cdot e^{-u(\log u+\log\log u+c(\varepsilon))} \text{ for } u=\frac{\log x}{\log y},$$

provided that $x>10$ and $\log(x)^{1+\varepsilon},\log^{2+\varepsilon}(d)\leq y\leq e^{\log^{1-\varepsilon}d}$. The pair $x=\sqrt{d}/2$ and $y=L(d)^z$ satisfies these constraints, and we can thus deduce that

$$\frac{\psi_{-d}(\sqrt{d}/2,L(d)^z)}{2\sqrt{d}\log d}\geq\frac{1}{4\log d}e^{-u(\log u+\log\log u+c(\varepsilon))} \text{ for } u=\frac{\log\left(\sqrt{d}/2\right)}{\log\left(L(d)^z\right)}.$$

Let us denote by p_s the probability of smoothness of one of the forms in the list. We repeat the experiment $\lceil B\rceil$ times where $B\geq\frac{\log d}{p_s}$. Therefore the probability of failure is given by

$$(1-p_s)^{\lceil B\rceil}=e^{-\lceil B\rceil p_s(1+o(1))}\leq e^{-\log d(1+o(1))}.$$

Moreover, as shown in the proof of [72, Prop. 4.4], the number of times Steps 8 and 9 are repeated satisfies $\lceil B\rceil=L(d)^{1/4z+o(1)}$.

To test the $\mathcal{B}$-smoothness of the elements of L_{forms}, we use Bernstein's batch smoothness test [7] on the set $\mathcal{S}$ of first coefficients of the corresponding reduced form, with the set of primes $\mathcal{P}$ that are bounded by $L(d)^z$. This algorithm takes time $b\log(b)^{2+o(1)}$ where b is the total number of bits of all integers in $\mathcal{S}$ and $\mathcal{P}$ combined, which is in $L(d)^{1/4z+o(1)}+L(d)^{z+o(1)}$. Therefore, the time taken for this step is in $L(d)^{1/4z+o(1)}+L(d)^{z+o(1)}$. □

Algorithm 4 will be used for different input forms f in the rest of this chapter. To use it in the context of Seysen's relation collection method [72], we set $f = f_i^{2nd}$ to ensure the creation of a row vector of the relation matrix that satisfies $|a_{ii}| > \sum_{j \neq i} |a_{i,j}|$.

Input : Fundamental discriminant $-d < 0$, set of prime forms $\mathcal{B} = \{f_1, \ldots, f_n\}$, $\varepsilon > 0$
Output: Matrix $(a_{i,j})$ with $\forall i$, $\prod_j f_j^{a_{i,j}} = 1_{Cl(-d)}$, $|a_{ii}| > \sum_{j \neq i} |a_{i,j}|$, or FAILURE

$(a_{i,j}) \leftarrow 0^{n \times n}$;
for $i \leq n$ **do**
  Use Algorithm 4 with input $f = f_i^{2nd}$, $\mathcal{B}$ and ε and add the vector $\vec{x} - 2nd\vec{e_i}$ to the i-th row of $(a_{i,j})$;
  if Algorithm 4 outputs FAILURE **then return** FAILURE;
end
return $(a_{i,j})_{i,j}$;

Algorithm 5: Phase 1

Proposition 4.3. *Assuming GRH, Algorithm 5 is valid, and succeeds with probability at least* $1 - \frac{1}{d^{1+o(1)}}$ *in time*

$$L(d)^{z+o(1)} \left(L(d)^{z+o(1)} + L(d)^{1/4z+o(1)} \right).$$

Proof. The running time for Algorithm 4 is $L(d)^{1/4z+o(1)} + L(d)^{z+o(1)}$. So the running time for Algorithm 5 is $n.\left(L(d)^{z+o(1)} + L(d)^{1/4z+o(1)}\right)$. Since $n = L(d)^{z+o(1)}$, the running time for Algorithm 5 is $L(d)^{z+o(1)} \left(L(d)^{z+o(1)} + L(d)^{1/4z+o(1)} \right)$. The probability of success of Algorithm 5 is at least $(1 - \frac{1}{d^{1+o(1)}})^n$. Since $n/d^{1+o(1)} \ll 1$ for large d, we can use the binomial approximation, $(1+x)^\alpha \approx 1 + x\alpha$, which yields $(1 - \frac{1}{d^{1+o(1)}})^n = 1 - \frac{n}{d^{1+o(1)}}(1 + o(1))$. Then, since $n = d^{o(1)}$, the Algorithm 5 succeeds with probability at least $1 - \frac{1}{d^{1+o(1)}}$.

□

4.3 Phase 2

The second phase is where a modification of the strategy of Hafner and McCurley needs to be made in order to lower the cost of the search for relations with good guarantees of randomness. From a high level perspective, we quantify how sparse the relation lattice Λ' is at a given step to measure the chances of drawing a relation outside of it. When the determinant of $\Lambda' \subseteq \Lambda$ is large enough, new relations are outside of Λ' with overwhelming probability. When this happens, the addition of a new vector to Λ' means that its determinant gets divided by at least a factor 2. At some point, success in enriching Λ' with new relations results in a determinant that is no longer large enough to guarantee the probability that new relations are outside of it. At this point, we need to switch to Phase 3 to finish the calculation of Λ. We fix the target determinant for the switch to $e^{\log^4 d}$. The determinant is calculated only once after collecting $n^{1+o(1)}$ relations. If it does not fall below the required bound, then the procedure returns a failure.

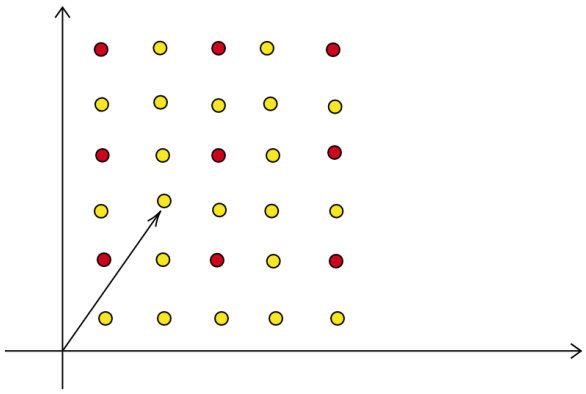


Figure 2. Finding relations outside Λ' (red dots)

The specificity of the method to search for relations in Phase 2 is that for each new attempt at finding a relation, we first draw a large vector of exponents $\vec{x} = (x_1, \ldots, x_n)$ and compute the form $f = \prod_i f_i^{x_i}$. This product is expensive to evaluate, and the odds of f being $\mathcal{B}$-smooth are low. Then, rather than drawing a new f, we multiply short random products to f in order to generate a relation involving f via Algorithm 4. Due to the properties of

Algorithm 4 analyzed in the previous section, each short product, which is inexpensive to evaluate, has a reasonable chance to yield a relation. Moreover, once a relation $\vec{v} \in \Lambda$ is found, we have that $\|\vec{v} - \vec{x}\|$ is short, which means that if we were able to argue that $\vec{x}$ was far enough from Λ', then we know that the new relation satisfies $v \notin \Lambda'$.

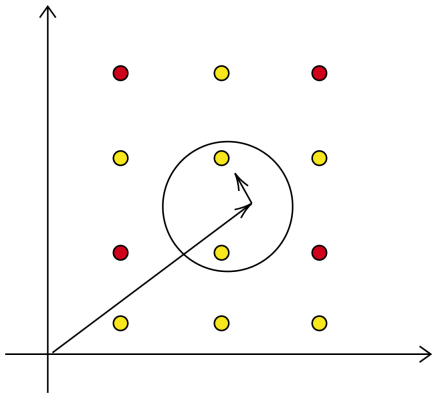


Figure 3. Phase 2 - Multiplying small random products

To efficiently test the determinant at the end of Phase 2, we need to introduce a new building block to the algorithm. The original Hafner-McCurley algorithm [41] proceeds with computing the (row) Hermite Normal Form of the integer matrix whose rows are the vectors of exponents of the relations that are collected (i.e. the *relation matrix*). However, the Hermite Normal Form takes time $n^{4+o(1)}$ to compute for a $n^{1+o(1)} \times n$ matrix with polynomial sized entries such as the one we have at the end of Phase 2. Better techniques are now available to find the Smith Normal Form (SNF) of a basis of the lattice generated by the rows of the relation matrix without having to compute the Hermite Normal Form at all. The advantage of using such a method is two-fold:

- It allows the intermediate verification of the determinant of a full-rank $\Lambda' \subseteq \Lambda$ at a lower cost.

- Once a generating set for Λ is found, the SNF of a basis for Λ is $\mathrm{diag}(d_1, \ldots, d_n)$ where $Cl(-d) = \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z}$, thus giving us the final result of the class group algorithm.

Lemma 4.4. *Given $n^{1+o(1)}$ vectors in $\mathbb{Z}^n$ with polynomial-sized entries that generate a full-rank sublattice $\Lambda_1 \subseteq \Lambda$, there is a Las Vegas algorithm to compute the SNF of a basis for Λ_1 in time $n^{3+o(1)}$.*

Proof. First, we need to reduce the problem to the computation of the SNF of a square matrix. This is a direct application of [79, Th. 58] which states that there is a Las Vegas algorithm to compute a matrix $B \in \mathbb{Z}^{(2m+5)\times(2m+5)}$ (where $m = n^{1+o(1)}$ is the number of input vectors) whose Hermite Normal Form has the shape $\begin{pmatrix} H & (0) \\ (0) & I \end{pmatrix}$ with entries of polynomial bit-size, in time $n^{\omega+o(1)}$, where $\omega \leq 3$ is the exponent for the complexity of matrix multiplication. This directly implies that the SNF of B is $\mathrm{diag}(d_1, \ldots, d_n, 1 \ldots, 1)$ where $\mathrm{diag}(d_1, \ldots, d_n)$ is the SNF of H, which is a basis of Λ_1. The Las Vegas SNF algorithm recently introduced in [21] allows us to compute the SNF of B in time $n^{3+o(1)}$, which concludes this proof. □

We summarize Phase 2 in Algorithm 6. We analyze its run time and correctness separately from its probability of success, as the former is straightforward, while the latter requires a careful analysis of the odds of the random vector $\vec{z}$ being far enough from the lattice Λ_1 in Step 3.

Proposition 4.5. *Algorithm 6 is valid and terminates in time*

$$L(d)^{3z+o(1)} + L(d)^{z+1/4z+o(1)}.$$

Proof. The validity immediately derives from the results previously stated. In particular, note that if $f = \prod_i f_i^{z_i} = \prod_i f_i^{x_i}$ where $\vec{x}$ is the output of Algorithm 4 on input f, then $\vec{x} - \vec{z} \in \Lambda$. The running time of the "for loop" of Steps 2 to 11 is $L(d)^z(L(d)^{z+o(1)} + L(d)^{1/4z+o(1)})$

as Algorithm 4 is repeated $n^{1+o(1)}$ times. Then Step 12 takes time $L(d)^{3z+o(1)}$, and therefore the overall time is

$$L(d)^z(L(d)^{z+o(1)} + L(d)^{1/4z+o(1)}) + L(d)^{3z+o(1)} = L(d)^{3z+o(1)} + L(d)^{z+1/4z+o(1)}.$$

□

Input : Fundamental discriminant $-d < 0$, $\mathcal{B} = (f_i)_{i \leq n}$ for $n = L(d)^z$, $\varepsilon > 0$, and n generators of $\Lambda_0 \subseteq \Lambda$ of full rank
Output: $n + \log_2\left(n^{5n/2}d^n\right)$ generators of $\Lambda_1 \subseteq \Lambda$ with $\det(\Lambda_1) \leq e^{\log^4 d}$ or FAILURE

1 $\Lambda_1 \leftarrow \Lambda_0$;
2 **for** $i \leq \log_2\left(n^{5n/2}d^n\right)$ **do**
3 Choose $\vec{z} \in [-d^2, d^2]^n$ uniformly at random ;
4 $\tilde{f} \leftarrow \prod_{k=1}^n f_k^{z_k}$;
5 Use Algorithm 4 with input $f = \tilde{f}$, $\mathcal{B}$ and ε ;
6 **if** *Algorithm 4 outputs FAILURE* **then**
7 **return** FAILURE;
8 **else**
9 $\Lambda_1 \leftarrow \Lambda_1 + \mathbb{Z}(\vec{x} - \vec{z})$;
10 **end**
11 **end**
12 Compute the determinant h_1 of Λ_1 using Lemma 4.4;
13 **if** $h_1 > e^{\log^4 d}$ **then**
14 **return:** FAILURE
15 **else**
16 **return:** the $n + \log_2\left(n^{5n/2}d^n\right)$ generators of Λ_1
17 **end**

Algorithm 6: Phase 2

We now turn to the analysis of the probability of success of Algorithm 6. Whenever we generate a new relation in Step 5, we need to find a bound on the probability that it does not belongs to Λ_1 already. Each time $\vec{x} - \vec{z} \notin \Lambda_1$, the update Step 9 divides the index Λ_1 within Λ by a factor at least 2, thus getting us one step closer to passing the test of Step 13 on the determinant of Λ_1. Let us denote the box $\{x : x \in \mathbb{Z}^n, \|x\|_\infty \leq d^2\}$ by $W_n(d^2)$ as in [41]. We also denote an n-dimensional sphere of radius r for the Euclidean distance, centered at x by

$B(x, r)$. We define the subspace of $W_n(d^2)$,

$$V := \left\{ \bigcup B(x, (2+\varepsilon)\log d) : x \in \Lambda_1 \cap W_n(d^2) \right\} \cap W_n(d^2)$$

By construction, the relations added to the sublattice Λ_1 on Step 9 of Algorithm 6 are within distance $\log(d)$ for the ℓ_1-norm of a vector $\vec{x} \in W_n(d^2)$ drawn uniformly at random. This means that they are also at distance $\log(d)$ of $\vec{x}$ for the Euclidean distance. By the triangular inequality, they cannot be in Λ_1 as long as the random vector $\vec{x}$ is outside of V.

Lemma 4.6. *Let Λ_1 be a full rank sublattice of Λ with discriminant greater than $e^{\log^4 d}$. Then the probability that a vector $\vec{x}$ drawn uniformly at random in $W_n(d^2)$ be outside of V is at least $1 - \frac{1}{e^{\log^4 d(1+o(1))}}$.*

Proof. We obtain a lower bound on the cardinality $W_n(d^2) \setminus V$ by subtracting an upper bound on the total number of integer points contained inside V from $|W_n(d^2)|$. According to [65, Corollary 1.4], the number of integer elements contained inside each individual n-dimensional sphere is bounded from above by $\frac{3.e^{\pi.k^2.r^2}}{2}$, where r is the radius of the sphere and $k = 10(\log n + 2)$. According to [41, Lem. 1], the number of elements of Λ_1 inside the box $W_n(d^2)$ is $\frac{(2d^2)^n}{\det(\Lambda_1)}.(1 + O(nD/d^2))$, where D is a bound on the diameter of the fundamental domain of Λ_1. In the proof of [41, Lem. 2], it is specified that the diameter of the fundamental domain of Λ_0 is in $O(n^2 d)$ by a triangular inequality argument on the vectors of the basis of Λ_0. Since the fundamental domain of Λ_1 is contained in that of Λ_0, it satisfies the same bound and

$$\left|\Lambda_1 \cap W_n(d^2)\right| \in \frac{(2d^2)^n}{\det(\Lambda_1)}. \left(1 + O\left(\frac{n^3}{d}\right)\right).$$

Therefore, the number of integer elements inside V is bounded from above by

$$\frac{(2d^2)^n}{\det(\Lambda_1)}. \left(1 + O\left(\frac{n^3}{d}\right)\right). \frac{3.e^{\pi.k^2.r^2}}{2}$$

In turn, this implies that the number of integer elements on the space $W_n(d^2) \setminus V$ is at least

$$(2d^2)^n - \frac{(2d^2)^n}{\det(\Lambda_1)} \cdot \left(1 + O\left(\frac{n^3}{d}\right)\right) \cdot \frac{3.e^{\pi.k^2.r^2}}{2}$$

So the probability to draw an $\vec{x}$ in $W_n(d^2) \setminus V$ is at least

$$1 - \frac{3.e^{\pi.k^2.r^2}}{2\det(\Lambda_1)}(1 + o(1)) = 1 - \frac{1}{e^{\log^4 d(1+o(1))}}$$

because $r = (2+\varepsilon)\log d$, $n = L(d)^{z+o(1)}$, $k = 10(\log n + 2)$, and $\det(\Lambda_1) \geq e^{\log^4 d}$. □

Note that we did not discuss the probability of success of the Las Vegas SNF method used in Step 12 of Algorithm 6. The probability of success of the methods described in [21, 79] is at least 1/2. Therefore, we can achieve a probability of success of $1 - \frac{1}{e^{\log^c d}}$ for any constant $c > 0$ without (asymptotically) increasing the cost by repeating the procedure a polynomial amount of times. To assess the overall success probability of Algorithm 6, we need to find a lower bound on the probability of finding enough relations outside of Λ_1 so that at the end of the procedure $\det(\Lambda_1) \leq e^{\log^4 d}$.

Proposition 4.7. *Under GRH, the probability of success of Algorithm 6 is at least* $1 - \frac{1}{d^{1+o(1)}}$.

Proof. We derive a conservative lower bound on the success probability of Algorithm 6 by first noticing that according to the Hadamard inequality, $\det(\Lambda_0) < n^{5n/2}d^n$. This means that the number of times a vector $\vec{x} - \vec{z} \notin \Lambda_1$ needs to be added on Step 9 of Algorithm 6 is less than the number $\log_2\left(n^{5n/2}d^n\right) = n^{1+o(1)}$ of relation collected. The probability of drawing enough random vectors $\vec{z}$ outside of V in Step 4 is higher than $\left(1 - \frac{1}{e^{\log^4 d(1+o(1))}}\right)^{n^{1+o(1)}}$. Combining this with the probability $1 - \frac{1}{d^{1+o(1)}}$ of success of Algorithm 4, we get that the probability of finding enough relations to bring $\det(\Lambda_1)$ below $e^{\log^4 d}$ is higher than

$$\left(1 - \frac{1}{e^{\log^4 d(1+o(1))}}\right)^{n^{1+o(1)}} \cdot \left(1 - \frac{1}{d^{1+o(1)}}\right)^{n^{1+o(1)}}.$$

Since $n = L(d)^{z+o(1)}$, we have $\frac{n^{1+o(1)}}{e^{\log^4 d(1+o(1))}} \ll 1$ and $\frac{n^{1+o(1)}}{d^{1+o(1)}} \ll 1$ for very large d. Therefore, we can use the binomial approximation $(1+x)^\alpha \approx 1 + x\alpha$ as in the proof of Proposition 4.3. Moreover, we have $n = d^{o(1)}$ and $d = e^{o(1)\cdot\log^4 d}$, therefore,

$$\left(1 - \frac{1}{e^{\log^4 d(1+o(1))}}\right)^{n^{1+o(1)}} \cdot \left(1 - \frac{1}{d^{1+o(1)}}\right)^{n^{1+o(1)}} = 1 - \frac{1}{d^{1+o(1)}}.$$

□

4.4 Phase 3

The last phase of the relation search uses the exact same method described in [41, Sec. 3]. In a nutshell, it consists in creating a tower of sublattices $(\Lambda_i)_{2\leq i\leq m}$ of the lattice of relations such that

$$\Lambda_0 \subseteq \Lambda_1 \subseteq \ldots, \subseteq \Lambda_m = \Lambda.$$

The key observation proved in [41, Lem. 2] is that when relations are obtained simply by testing the $\mathcal{B}$-smoothness of elements $f = \prod_i f_i^{x_i}$ for a vector $\vec{x}$ drawn uniformly at random in $W_n(d^2)$, the probability that they belong to a given coset in Λ/Λ_1 is essentially given by $\det(\Lambda)/\det(\Lambda_1)$. This means that new relations have somewhat comparable chances of landing in different cosets of Λ/Λ_1. Once every coset has been hit at least once, the relation collection is complete. What makes Phase 3 less expensive than the analogue procedure in [41, Sec. 3] is the fact that we start the procedure from Λ_1 where $|\Lambda/\Lambda_1| \leq e^{\log^4 d}$ instead of starting from Λ_0 which is only known to satisfy the more pessimistic bound $|\Lambda/\Lambda_0| < n^{5n/2}d^n$, thus requiring the drawing of exponentially more vectors to complete the lattice of relations.

Proposition 4.8. *Under GRH, Algorithm 7 returns $Cl(-d)$ with probability at least $1-\frac{1}{d^{1+o(1)}}$ in time*

$$L(d)^{3z+o(1)} + L(d)^{z+1/4z+o(1)}$$

Input : Fundamental discriminant $-d < 0$, $\mathcal{B} = (f_i)_{i \leq n}$ for $n = L(d)^z$, $\varepsilon > 0$, and $m = n^{1+o(1)}$ generators of $\Lambda_1 \subseteq \Lambda$ of full rank with $\det(\Lambda_1) \leq e^{\log^4 d}$

Output: $Cl(-d)$, or FAILURE

$B \leftarrow 4 \cdot e^{u(\log u + \log\log u + c(\varepsilon))}$ for $c(.)$ as in [72, Th. 5.2] ;
for $k \leftarrow 1$ **to** $\frac{\log^4 d + \log d}{\log(1.5)}$ **do**
  Initiate an empty list L_{forms};
  for $r \leftarrow 1$ **to** $\lceil B \rceil$ **do**
    Choose $\vec{x}$ uniformly at random in $W_n(d^2)$. $f \leftarrow \prod_{i=1}^{n} f_i^{x_i}$;
    Store $f, \vec{x}$ in L_{forms};
  end
  Test the $\mathcal{B}$-smoothness of all forms in L_{forms} using [7];
  if *there is f that is $\mathcal{B}$-smooth in L_{forms}* **then**
    Let $\vec{y} \in \mathbb{Z}^n$ with $f = \prod_{i \leq n} f_i^{y_i}$. $\Lambda_{k+1} \leftarrow \Lambda_k + \mathbb{Z}(\vec{x} - \vec{y})$;
  else
    return: FAILURE
  end
end
Compute h^* such that $h^* \leq \det(\Lambda) < 2h^*$;
Compute $d_1, \ldots, d_n$ such that $\Lambda / \Lambda_k = \prod_i \mathbb{Z}/d_i\mathbb{Z}$ using Lemma 4.4;
if $\prod_i d_i \geq 2h^*$ **then**
  return: FAILURE
else
  return: $\mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z}$
end

Algorithm 7: Phase 3

Proof. We rely on [41, Lem. 3] which states that if we generate at least $\frac{\log|\Lambda/\Lambda_1|+\log d}{\log(2/\alpha)}$ new relations stemming from a random choice of $\vec{x} \in W_n(d^2)$ as in Step 5 with $\alpha = 1 + O\left(\frac{n^3}{d}\right)$, then we have a probability at least $1-\frac{1}{d}$ of generating $Cl(-d)$. For d large enough, $\log(2/\alpha) \geq \log(1.5)$, which ensures that if all attempts at finding relations in the "for loop" of Steps 3 to 14 succeed then we have a probability $1 - \frac{1}{d}$ of obtaining $Cl(-d)$. The probability of succeeding in finding these relations is at least

$$\left(1 - \frac{1}{d^{1+o(1)}}\right)^{\frac{\log^4 d+\log d}{\log(1.5)}} = 1 - \frac{1}{d^{1+o(1)}},$$

which proves the result on the probability of success. The evaluation of a product in Step 5 takes time $n^{1+o(1)}$, The number $\lceil B \rceil$ of attempts to generate a relation with probability $1 - \frac{1}{d^{1+o(1)}}$ is $L(d)^{1/4z+o(1)}$. This means that the loop between Step 2 and Step 14 costs $L(d)^{z+1/4z+o(1)}$. The computation of h^* runs in polynomial time under the ERH, and the computation of $d_1, \ldots, d_n$ via the SNF costs $L(d)^{3z+o(1)}$ as seen before. □

Corollary 4.9. *Assuming GRH, there is a Las Vegas algorithm to compute $Cl(-d)$ in time $L(d)^{3/\sqrt{8}+o(1)}$ with probability at least $1 - \frac{1}{d^{1+o(1)}}$.*

Proof. The setup of the algorithm for computing $Cl(-d)$ consists in computing $\mathcal{B}$ in time $L(d)^{z+o(1)}$. The time of the subsequent phases is bounded by $L(d)^{3z+o(1)} + L(d)^{z+1/4z+o(1)}$. Therefore, the total run time is optimal for $z = 1/\sqrt{8}$. □

CHAPTER 5

NORM RELATIONS AND ARITHMETIC APPLICATIONS

In this chapter[1], we discuss norm relations and the necessary and sufficient criteria for the existence of norm relations. Additionally, we explore subfield-based algorithms for the computation of the S-unit group, the principal ideal problem (PIP), and the ideal decomposition using norm relations. Sections 5.1, 5.2, 5.4, and 5.6 of this chapter are based on joint work with Jean-François Biasse, Claus Fieker, Tommy Hofmann, and William Youmans, published in Mathematical Cryptology (MC) [19].

Let K/F be a normal extension of number fields, and let G be the Galois group of the extension K/F. Exploring relations between the arithmetic invariants of a number field and its subfields has been an important topic in algebraic number theory since its inception. The first investigation in this area was conducted by Dirichlet in 1842 [34]. According to Dirichlet [34], in the case of biquadratic fields $K = \mathbb{Q}(\sqrt{m}, \sqrt{-m})$, the class number of K can be expressed as either the product of the class numbers of its subfields $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{-m})$, or half of this product. Dirichlet also offered a simple rule to figure out which situation applies to a given value of m. Later Walter [83] generalized this to the biquadratic fields of the form $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$. For the quadratic subfields $K_1 = \mathbb{Q}(\sqrt{m})$, $K_2 = \mathbb{Q}(\sqrt{n})$ and $K_3 = \mathbb{Q}(\sqrt{mn})$ of K, Walter [83] presented the class number formula

$$h(K) = 2^i h(K_1)h(K_2)h(K_3)$$

where $i \in \mathbb{Z}$ depends on the index of certain unit groups. Hence, once we have the class numbers of these quadratic subfields, we can obtain the class number of K.

[1]This chapter is based on the paper published in Mathematical Cryptology (MC) [19]

A more organized study of these class number formulae of number fields was done by Brauer [22] and Kuroda [47]. They showed that relations between the permutation characters of the subgroups of the Galois group G of the number field K can give us the relations between the arithmetic invariants of the corresponding intermediate fields. For a subgroup $H \leq G$, let's denote the permutation character of G induced by the trivial character of H by $\mathrm{Ind}_{G/H}(1_H)$. Then, a relation of the form

$$\sum_{H \leq G} a_H \mathrm{Ind}_{G/H}(1_H) = 0$$

is called a Brauer relation. According to Brauer [22], the existence of a Brauer relation implies the existence of relations between zeta functions and arithmetic invariants of the corresponding fixed fields K^H of K.

Relations closely related to Brauer relations are relations of norms of subgroups of G. For $H \leq G$, we define the corresponding norm as $N_H = \sum_{h \in H} h \in \mathbb{Q}[G]$. Then, the equality of the form

$$0 = \sum_{H \leq G} a_H N_H$$

for $a_H \in \mathbb{Z}$ is a relation of norms of subgroups of G. Walter [83] proved a correspondence between Brauer relations and relations of norms of subgroups. In other words, the existence of relations of norms of subgroups of G implies the existence of relations between the arithmetic invariants of K and its subfields. Bauch, Bernstein, de Valence, Lange and van Vredendaal [5] and Biasse and van Vredendaal [18] implicitly used these kinds of relations of norms of subgroups of G in their recursive approaches. Bauch, Bernstein, de Valence, Lange, and van Vredendaal [5] presented a recursive method to reduce the computation of principal ideal generators of multiquadratic fields to quadratic subfields by using the information from the subfields. Biasse and van Vredendaal [18] generalized this strategy for the computation of the S-unit group of multiquadratic fields. In 2020, Biasse, Fieker, Hofmann, and Page [20] generalized the idea of relations of norms of subgroups and introduced the relations of the

form

$$d = \sum_{i=1}^{l} a_i \mathrm{N}_{H_i} b_i,$$

where $d \in \mathcal{N}_{>0}$ and $a_i, b_i \in \mathbb{Z}[G]$. These relations are called *norm relations*, and they help leverage the computations in subfields for the computation of rings of integers, S-unit groups, and class groups of a number field.

One of the crucial applications of norm relations is the resolution of the principal ideal problem (PIP). Norm relations help us solve PIP recursively by utilizing the subfield information. In the next chapter, we present a variant of Miller's technique [55] for the computation of class numbers of maximal real subfields of cyclotomic fields. The core idea behind this variant is the recursive PIP computation by using norm relations. More specifically, we use the norm relation-based PIP algorithm as described in [43]. In this chapter, we discuss norm relations and the necessary and sufficient criteria for their existence. Also, we discuss the subfield-based algorithms for the computation of S-unit group and principal ideal problem by using norm relations.

5.1 Definition

Let K be a Galois number field with Galois group $G = Gal(K/\mathbb{Q})$. For a subgroup $H \leq G$ we denote by $N_H = \sum_{h \in H} h \in \mathbb{Q}[G]$ the norm of H as an element of the group algebra $\mathbb{Q}[G]$. A *norm relation of* G is an equality of the form $1 = \sum_{i=1}^{l} a_i \mathrm{N}_{H_i} b_i$ in $\mathbb{Q}[G]$ with $a_i, b_i \in \mathbb{Q}[G]$ and subgroups $1 \neq H_i \leq G$. By clearing denominators, a norm relation can always be written as

$$d = \sum_{i=1}^{l} a_i \mathrm{N}_{H_i} b_i \tag{5.1}$$

with $d \in \mathbb{N}_{>0}$ minimal such that $a_i, b_i \in \mathbb{Z}[G]$. We call d the *denominator* of the norm relation.

The relation between arithmetic objects of the number field K and its subfields can be obtained from norm relation (see [20]). Equation (5.1) implies that for all $x \in K^\times$ we have

$$x^d = \prod_{i=1}^{l} \mathrm{N}_{K/K^{H_i}}(x^{b_i})^{a_i}, \tag{5.2}$$

where $K^H = \{x \in K \mid \sigma(x) = x \text{ for all } \sigma \in H\}$ is the fixed field of H, $x^a = \prod_{g\in G} g(x)^{a_g}$ for all $x \in K^\times$, and $a = \sum_{g\in G} a_g g \in \mathbb{Z}[G]$. We mostly use Equality (5.2) when we refer to a norm relation. Let us consider a fractional ideal $\mathfrak{a}$ of the number field K. Then from [58, Chapter III, §1, Proposition 1.6] we can obtain the following equality for a subgroup $H \leq G$: $\mathrm{N}_{K/K^H}(\mathfrak{a})\mathcal{O}_K = \prod_{\sigma\in H} \sigma(\mathfrak{a}) = \mathfrak{a}^{N_H}$. That is, we have the following result from Equation (5.1)

$$\mathfrak{a}^d = \prod_{i=1}^{l} \mathrm{N}_{K/K^H}(\mathfrak{a}^{b_i})^{a_i}\mathcal{O}_K. \tag{5.3}$$

.

Example 5.1 (Ex.2.5 of [20])**.** Consider a biquadratic field $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ where d_1, d_2 are squarefree coprime integers. The Galois group of K is $Gal(K/\mathbb{Q}) = \langle\sigma\rangle \times \langle\tau\rangle \cong C_2 \times C_2$. Then we have the norm relation

$$2 = N_{\langle\sigma\rangle} + N_{\langle\tau\rangle} - \sigma N_{\langle\sigma\tau\rangle}.$$

Let's denote the quadratic subfields fixed by σ, τ and $\sigma\tau$ as K_σ, K_τ and $K_{\sigma\tau}$ respectively. Then for $\alpha \in K^*$, we have the following identity:

$$\alpha^2 = \frac{\mathrm{N}_{K/K_\sigma}(\alpha)\mathrm{N}_{K/K_\tau}(\alpha)}{\sigma(\mathrm{N}_{K/K_{\sigma\tau}}(\alpha))}.$$

Due to Funakura [38] we have the following simple criterion for the existence of norm relations for abelian groups G.

Theorem 5.2 (Thm.2.27 of [20]). *Let G be a finite abelian group, and write $G \cong C \times Q$ where C is the largest cyclic factor of G.*

1. *The group G admits a norm relation with denominator 1 if and only if $|Q|$ is divisible by at least two distinct primes. If the condition is satisfied, then G admits a norm relation with $a_i \in \mathbb{Z}$, denominator 1, and where all H_i satisfy that G/H_i is a p_i-group times a cyclic group, for some prime number p_i.*

2. *Assume that Q is a p-group. Then G admits a norm relation if and only if $Q \neq 1$. If the condition is satisfied, then G admits a norm relation with $a_i \in \mathbb{Z}$, denominator a power of p and where all H_i satisfy that G/H_i is a cyclic group.*

Basically, the theorem states that norm relations exist if and only if the finite abelian group G is not cyclic.

5.2 Saturation Techniques

Equation (5.2) shows us that if a norm relation of denominator d involving the fields $K_1, \ldots, K_l$ exists, then we know that the d-th powers of all elements $x \in K$ can be expressed as products of elements in $K_1, \ldots, K_l$. Suppose we want to compute a generating set of a multiplicative group $U \subseteq K^\times$ (typically the group of units, of the S-unit group for a certain set S), we can use the following recursive strategy:

1. Compute a subgroup $V \subseteq U$ such that $V \cap (K^\times)^d = U^d$.

2. Compute generators $v_1, \ldots, v_k$ of $V \cap (K^\times)^d$.

3. Take the d-th roots of the v_i and deduce generators of U.

When U is the S-unit group for a set of prime ideals S that is stable under the action of the Galois group, we can take V to be the subgroup of U generated by all the S_i-unit groups of K_i, where S_i is the set of prime ideals of K_i lying under the primes of S. Then, since V

contains all $\mathrm{N}_{K/K_i}(U)$, we know from Equation (5.2) that it contains all d-th powers of U. Additionally, if $x^d \in V$, then x must be only divisible by elements of S, hence $x \in U$ and $V \cap (K^\times)^d = U^d$. Step (2) is known as a *saturation* technique. We define the *d-saturation* W of V as the smallest group $W \subseteq K^\times$ with $V \subseteq W$ and $K^\times/W$ being d-torsion free. The group V is d-saturated if it equals its d-saturation. The saturation technique takes the subgroup V of the group U that we desire to compute, with the guarantee that U equals the d-saturation of V, and computes generators for $(V \cap (K^\times)^d)/V^d$.

When dealing with an arbitrary denominator d, we first factor d as a product of prime powers, and we repeat Steps (2) and (3) for all prime powers dividing d. Thus, from now on, we will assume that d is a prime power. Saturation employs local computations to detect global powers. This is a well-known technique in computational algebraic number theory, used, for example, in the class and unit group computation of number fields ([62, Section 5.7]) or the number field sieve ([1]). Note that, in contrast to previous applications of this technique, in our case the number d is in general not a prime. As a consequence, we will rely on the Grunwald–Wang theorem (see [3, Chapter X] or [59, Chapter IX, §1]) and therefore have to consider the following dichotomy. For $k \in \mathbb{Z}_{\geq 1}$ denote by ζ_k a primitive k-th root of unity and set $\eta_k = \zeta_k + \zeta_k^{-1}$. Let $s \geq 2$ be an integer such that $\eta_s \in K$ but $\eta_{s+1} \notin K$. Moreover, let S be a finite set of prime ideals of O_K. Recall that d is a prime power. We say that we are in the *bad case* when the following conditions are simultaneously satisfied:

1. The number $d = 2^t$ is even and $t > s$.

2. The elements $-1, 2 + \eta_s$ and $-(2 + \eta_s)$ are non-squares in K.

3. We have $\{\mathfrak{p} \mid 2 \in \mathfrak{p}$ and $-1, 2 + \eta_s\}$ and $-(2 + \eta_s)$ are non-squares in $K_\mathfrak{p} \subseteq S$

If we are not in the bad case, we say that we are in the *good case*. The terminology is explained by the theorem of Grunwald–Wang, which gives the following connection between global and local d-th powers.

Theorem 5.3 (Grunwald–Wang)**.** *Consider the canonical map $K^\times/(K^\times)^d \longrightarrow \prod_{\mathfrak{p}\notin S} K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^d$. If we are in the good case, this map is injective. If we are in the bad case, the kernel of the map is $\langle\bar{\eta}_s\rangle \cong \mathbb{Z}/2\mathbb{Z}$.*

The good case Finding d-th powers in the good case can be done exclusively by detecting local d-th powers modulo a set of prime ideals.

Proposition 5.4 ([20, Proposition 4.5])**.** *Assume that $\mathfrak{p}$ is a non-zero prime ideal with $d \notin \mathfrak{p}$ and let $\varpi \in K$ be a local uniformizer at $\mathfrak{p}$, that is, an element with $v_\mathfrak{p}(\varpi) = 1$. Then the map*

$$K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^d \longrightarrow \mathbb{Z}/d\mathbb{Z} \times k_\mathfrak{p}^\times/(k_\mathfrak{p}^\times)^d, \quad \bar{x} \longmapsto (\overline{v}, \overline{x\varpi^{-v}}) \text{ where } v = v_\mathfrak{p}(x),$$

is an isomorphism.

Proposition 5.5. *Assume that we are in the good case of Grunwald–Wang. For a multiplicative finitely generated subgroup $V \subseteq K^\times$ we have*

$$(V \cap (K^\times)^d)/V^d = \bigcap_{d\notin\mathfrak{p}} \ker(V/V^d \to \mathbb{Z}/d\mathbb{Z} \times k_\mathfrak{p}^\times/(k_\mathfrak{p}^\times)^d).$$

There exists $c_0 \in \mathbb{R}_{>0}$ (depending on K, V and d) such that

$$(V \cap (K^\times)^d)/V^d = \bigcap_{d\notin\mathfrak{p},\mathrm{N}(\mathfrak{p})\leq c_0} \ker(V/V^d \to \mathbb{Z}/d\mathbb{Z} \times k_\mathfrak{p}^\times/(k_\mathfrak{p}^\times)^d).$$

The general case In the general case, d is a power of 2, but the approach we sketch here applies to $d = p^t$ a power of an arbitrary prime p. In essence, it consists in inductively computing the p-saturation of V and replacing it with its p-saturation t times. At each step, p-th roots of generators of $(V \cap (K^\times)^p)/V^p$ need to be computed, which makes this process in practice more computationally expensive than in the so-called good case, but does not change the overall asymptotic complexity.

5.3 S-Unit Group Computation With Norm Relation

Let K/F be a normal extension of algebraic number fields with Galois group G. Let us assume G admits a norm relation of denominator d of the form

$$d = \sum_{i=1}^{l} a_i \mathrm{N}_{H_i} b_i.$$

Here $H_i \subseteq G$, $d \in \mathbb{N}_{>0}$, $a_i, b_i \in \mathbb{Z}[G]$. Consider a finite set S of G-stable non-zero prime ideals of $\mathcal{O}_K$. We can use the following steps to compute a $\mathbb{Z}$-basis of the S-unit group as described in [20, Alg. 4.16].

1. For each fixed field $K_i = K^{H_i}$ of K, compute a basis of the S-unit group $\mathcal{O}_{K_i,S}^{\times}$
2. Determine the group $V = (\mathcal{O}_{K_1,S}^{\times})^{a_1} ... (\mathcal{O}_{K_l,S}^{\times})^{a_l} \subseteq \mathcal{O}_{K,S}^{\times}$.
3. Compute the d-saturation of V as explained in Section 5.2.

By this approach we obtain a polynomial reduction for the S-unit group computation of K to the S-unit group computation of subfields K_i with the help of norm relation.

5.4 Principal Ideal Problem With Norm Relations

The S-unit group computation discussed above can be used to solve the PIP. We use the following method to solve the PIP by using the S-unit group as discussed in [19, Sec. 6]. Given an ideal $\mathfrak{a}$ of the number field K, we enumerate small linear combinations of LLL-reduced basis of $\mathfrak{a}$ until we find $\alpha \in \mathfrak{a}$ such that $(\alpha)/\mathfrak{a} = \mathfrak{p}$ is a prime ideal. Consider the set of prime ideal $S = \{\mathfrak{p}^{\sigma} \,|\, \sigma \in Gal(K/\mathbb{Q})\}$, the set of all conjugates of $\mathfrak{p}$ under the action of $Gal(K/\mathbb{Q})$. Then by using the method discussed above, we can find a generating set $\alpha_1, ..., \alpha_{r+s}$ of the S-unit group, where r is the rank of the unit group $\mathcal{O}_K^{\times}$ and s is the cardinality of the set S. Let $\vec{v_1}, ..., \vec{v}_{r+s} \in \mathbb{Z}^s$ represent the vectors corresponding to the valuations of α_i at the primes in S. Then by solving a linear system, we can find a vector

$\vec{x} \in \mathbb{Z}^{r+s}$ such that $\sum x_i \vec{v_i}$ is a vector with zeros everywhere except for a 1 in the entry corresponding to the prime ideal $\mathfrak{p}$. Then $\prod_i \alpha_i^{x_i}$ will be a generator of $\mathfrak{p}$. Since $(\alpha)/\mathfrak{a} = \mathfrak{p}$, we have $\alpha . \prod_i \alpha_i^{-x_i}$ as a generator of the ideal $\mathfrak{a}$ and as solution to PIP.

5.5 Principal Ideal Problem Without S-Unit Group Computation

In this section, we explore solving the PIP through norm relations, without relying on the S-unit group computation discussed in the previous section. Let K be a Galois number field with Galois group $G = Gal(K/\mathbb{Q})$. Let's assume G admits a norm relation of the form

$$d = \sum_{i=1}^{l} a_i \mathrm{N}_{H_i} b_i \tag{5.4}$$

with subfields $H_1, H_1, ..., H_l$. Then we use the following crucial result for solving the PIP in K by using the information from the subfields.

Lemma 5.6 (Lem. 4.1 of [43])**.** *Let $\mathfrak{a}$ be a fractional ideal of a number field K. If $\mathfrak{a}$ is a principal ideal, then $\mathrm{N}_{K/K_i}(\mathfrak{a}^{b_i})$ is also a principal ideal in the fixed field $K_i = K^{H_i}$ of H_i for $1 \leq i \leq l$. If $d = 1$, then the converse is also true and the generator of $\mathfrak{a}$ is given by $\prod_{i=1}^{l} (\alpha_i)^{a_i}$, where $\alpha_i \mathcal{O}_K = \mathrm{N}_{K/K_i}(\mathfrak{a}^{b_i})$ for $1 \leq i \leq l$.*

The previous lemma states that if the denominator d is one, then the PIP in K can be reduced to PIP instances in the subfields K_i. But if the denominator is not equal to one, we can not solve the PIP in K directly from the subfields K_i, and more work is needed. If the denominator is greater than one, we get the generator of $\mathfrak{a}^d$ from the subfield computations. That is we have

$$\mathfrak{a}^d = \beta \mathcal{O}_K.$$

If there exists a $u \in \mathcal{O}_K^{\times}$ such that $u\beta = \alpha^d$, then $\mathfrak{a} = \alpha \mathcal{O}_K$ and we have the solution α for the PIP in K. We use the saturation technique as explained in Section 5.2 to find the d-th power modulo unit group. Proposition 4.4 of [43] shows that we can even work on a smaller

group U generated by the subgroups of $\mathcal{O}_{K_i}$ instead of the full unit group for the saturation method. We use Algorithm 8 to solve the PIP by using norm relations as described in [43, Alg. 1].

Input : A fractional ideal $\mathfrak{a}$ of K which satisfies $\mathfrak{a}^d = \prod_{i=1}^{l} \mathrm{N}_{K/K_i}(\mathfrak{a}^{b_i})^{a_i}\mathcal{O}_K$.
Output: Whether a is a principal ideal and a generator in case it is

$y \leftarrow 1$;
for $i \leftarrow 1$ to l **do**
  if $\mathrm{N}_{K/K_i}(\mathfrak{a}^{b_i})$ *is principal* **then**
    Find α_i of K_i such that $\mathrm{N}_{K/K_i}(\mathfrak{a}^{b_i}) = \alpha_i\mathcal{O}_{K_i}$;
  else
    return: $\mathfrak{a}$ is not principal
  end
end
$\beta = \alpha_1^{a_1}...\alpha_l^{a_l}$;
Compute $U = V_1^{a_1}...V_l^{a_l}$, where V_i are subgroups of $\mathcal{O}_{K_i}$ with index coprime to d ;
if β *is a d-th power modulo* U **then**
  return: $\alpha \in K^\times$ such that $\beta/\alpha^d \in U$;
else
  return: $\mathfrak{a}$ is not principal
end

Algorithm 8: PIP With Norm Relations

5.6 Ideal Decomposition With Norm Relations

Let K be a number field and let $\mathfrak{a} \subseteq K$ be an ideal of K. As we discussed in Section 3.5, the ideal decomposition of $\mathfrak{a}$ consists in representing $\mathfrak{a}$ as $\mathfrak{a} = (\phi)\mathfrak{p}_1^{e_1}...\mathfrak{p}_N^{e_N}$, where p_i belongs to a set of prime ideals S. In this section, we discuss how to leverage norm relations for the decomposition of an ideal by using subfield computations. Let $S = \{\mathfrak{p}_i\}_{i\leq k}$ be a set prime ideals of $\mathcal{O}_K$ that is stable under the action of $G = Gal(K/\mathbb{Q})$, and let $[\mathfrak{a}] \in \langle S\rangle$. Assume K admits a norm relation with subfields $(K_i)_{i\leq l}$. That is, we have the equation $\mathfrak{a}^d = \prod_{i=1}^{l} \mathrm{N}_{K/K_i}(\mathfrak{a}^{b_i})^{a_i}\mathcal{O}_K$. Then for each i, we find the decomposition of $\mathrm{N}_{K/K_i}(\mathfrak{a}^{b_i})$ in $Cl(\mathcal{O}_{K_i})$ with respect to $\mathfrak{p} \cap K_i$ for $\mathfrak{p} \in S$. From this decomposition of $\mathrm{N}_{K/K_i}(\mathfrak{a}^{b_i})$, we can get the corresponding decomposition of $\mathrm{N}_{K/K_i}(\mathfrak{a}^{b_i})^{a_i}\mathcal{O}_K$ in $Cl(\mathcal{O}_K)$ with respect to S. That

is, we have the decomposition

$$\mathfrak{a}^d \sim \prod_i \mathfrak{p}_i^{x_i}$$

for some vector $\vec{x}$. For each subfield K_i, by using ideal decomposition and PIP in $Cl(\mathcal{O}_{K_i})$, we can get an identity of the form

$$\mathrm{N}_{K/K_i}(\mathfrak{a}^{b_i})^{a_i}\mathcal{O}_K = (\alpha_i)\prod_j \mathfrak{p}_j^{x_{i,j}}.$$

By combining all the identities from the subfields as above and by using the form $\mathfrak{a}^d \sim \prod_i \mathfrak{p}_i^{x_i}$, we can get the ideal decomposition for $\mathfrak{a}^d$

$$\mathfrak{a}^d = (\alpha)\prod_i \mathfrak{p}_i^{y_i}. \tag{5.5}$$

Now we have the ideal decomposition for $\mathfrak{a}^d$. We would like to get the ideal decomposition of $\mathfrak{a}$ from $\mathfrak{a}^d = (\alpha)\prod_i \mathfrak{p}_i^{y_i}$. We use the following strategy as described in [19, Sec. 5.1] for this purpose.

Since the class of $\mathfrak{a}$ is a product of the classes of S, there must exist $\vec{z} \in \mathbb{Z}^k$ and $\beta \in K$ such that $\mathfrak{a} = (\beta)\prod_i \mathfrak{p}_i^{z_i}$, which means that

$$\mathfrak{a}^d = (\beta^d)\prod_i \mathfrak{p}_i^{dz_i}.$$

Since $\mathfrak{a}^d = (\alpha)\prod_i \mathfrak{p}_i^{y_i}$, we obtain the equality

$$(\beta^d)\prod_i \mathfrak{p}_i^{dz_i} = (\alpha)\prod_i \mathfrak{p}_i^{y_i}.$$

Since α is not necessarily β^d, we don't necessarily have $y_i = dz_i$. However, we know that $\prod_i \mathfrak{p}_i^{y_i} \sim \mathfrak{p}_i^{dz_i}$ so we must have $\vec{y} - d\vec{z} \in \mathcal{L}$ where $\mathcal{L} \subseteq \mathbb{Z}^k$ is the lattice of relations between the $\mathfrak{p}_i$, i.e. the lattice of vectors $\vec{u}$ such that $\prod_i \mathfrak{p}_i^{u_i}$ is a principal ideal. Our goal is to express α as $\alpha = \beta'^d \cdot \delta$ where δ is an S-unit with $(\delta)\mathcal{O}_K = \prod_i \mathfrak{p}_i^{u_i}$ such that $\vec{u} + \vec{y} \in d\mathbb{Z}^k$. If we

can express $\alpha = \beta'^d \cdot \delta$, then we have the equality $\mathfrak{a}^d = (\beta'^d) \prod_i \mathfrak{p}_i^{dz'_i}$ where $\vec{z'} := \vec{u} + \vec{y}$. The decomposition of the ideal $\mathfrak{a}$ follows from this equality. Once we find a S-unit δ_0 such that $(\delta_0) = \prod_i \mathfrak{p}_i^{u_i^0}$ with $\vec{u}^{(0)} + \vec{y} \in d\mathbb{Z}^k$, then any other solution δ is of the form $\delta = \delta_0 \delta'$ where δ' is an S-unit satisfying $(\delta')\mathcal{O}_K = \prod_i \mathfrak{p}_i^{u'_i}$ with $\vec{u'} \in d\mathbb{Z}^k$. The set of such δ' is a subgroup of the S-unit group.

By using the saturation methods as discussed in Section 5.2, we can find generators $\alpha_1, \ldots, \alpha_{r+k+1}$ of the S-unit group, where r is the rank of the unit group. Consider the matrix $M \in \mathbb{Z}^{(r+k+1)\times k}$ whose rows are the valuations of the α_i according to the primes in S. Since we have $\vec{y} - d\vec{z} \in \mathcal{L}$, there is $\vec{x} \in \mathbb{Z}^{r+k+1}$ such that $\vec{y} = \vec{x}M + d\vec{z}$, i.e.

$$\vec{y} = \vec{x}M \bmod d.$$

This system does not have a unique solution. However, we can put M in row reduced echelon form modulo d and find

1. a solution $\vec{x}^{(0)}$ to $\vec{y} = \vec{x}M \bmod d$,
2. a basis $\vec{x}^{(1)}, \ldots, \vec{x}^{(m)}$ of the left kernel of $M \bmod d$.

So all the $\vec{x}$ such that $\vec{y} = \vec{x}M \bmod d$ are of the form $\vec{x} = \vec{x}^{(0)} + \sum_j a_j \vec{x}^{(j)}$, including the one that satisfies $\vec{y} = \vec{x}M + d\vec{z}$ for $\vec{z}$ defined above. We denote by $\vec{x}^{(j)}M_i$ the i-th coefficient of $\vec{x}^{(j)}M$, and by $\alpha_i \in K$ the element that satisfies $\prod_j \mathfrak{p}_j^{M_{i,j}} = (\alpha_i)\mathcal{O}_K$. With the notation previously used, $\delta_0 = \prod_i \alpha_i^{x_i^{(0)}}$, while the subgroup of δ''s is generated by $\delta_i := \prod_i \alpha_i^{x_i^{(j)}}$ for $i = 1, \ldots, m$. Therefore, we have

$$
\begin{aligned}
(\alpha)\prod_i \mathfrak{p}_i^{y_i} &= (\alpha)\prod_i \mathfrak{p}_i^{\vec{x}M_i}\cdot\prod_i \mathfrak{p}_i^{y_i-\vec{x}M_i} \\
&= (\alpha)\prod_i \mathfrak{p}_i^{\vec{x}^{(0)}M_i}\cdot\prod_{j\le m}\left[\prod_i \mathfrak{p}_i^{\vec{x}^{(j)}M_i}\right]^{a_j}\cdot\prod_i \mathfrak{p}_i^{y_i-\vec{x}M_i} \\
&= (\alpha)\left(\prod_i \alpha_i^{x_i^{(0)}}\right)\cdot\left(\prod_{j\le m}\left[\prod_i \alpha_i^{x_i^{(j)}}\right]^{a_j}\right)\cdot\prod_i \mathfrak{p}_i^{y_i-\vec{x}M_i} \\
&= (\alpha')\left(\prod_j \delta_j^{a_j}\right)\cdot\prod_i \mathfrak{p}_i^{dz_i'} \quad \text{for some } z_i'\in\mathbb{Z}
\end{aligned}
$$

where we have a product representation of $\alpha' \in K$ and the $\delta_j \in K$.

If we can find $(a_j)_{i\le m}$ such that $\alpha'\cdot\prod_j \delta_j^{a_j} = \beta'^d$ for some $\beta' \in K$, we can obtain the identity

$$\mathfrak{a}^d = (\beta'^d)\prod_i \mathfrak{p}_i^{dz_i'}.$$

$\beta' = \beta$ and $z_i' = z_i$ provides us one solution to the above identity. Other choices of $(a_i)_{i\le m}$ can provide to other solutions. Once a solution is found, we have $\mathfrak{a} = (\beta')\prod_i \mathfrak{p}_i^{z_i'}$, which solves the ideal class decomposition problem.

Now the question is how to find the desired $(a_i)_{i\le m}$. Since there is a solution, we know that α' is a d-th power modulo U for $U = \langle\delta_1,\ldots,\delta_m\rangle$. This means that there are $x \in K^\times$ and $u \in U$ such that $\alpha' = u\cdot x^d$. To find the a_i, we apply a variation of the saturation methods described in Section 5.2. More precisely, we use Proposition 3 of [19] for finding $(a_i)_{i\le m}$ such that $\alpha'\cdot\prod_j \delta_j^{a_j} = \beta'^d$. We summarize the ideal decomposition with Algorithm 9.

Input : Number field K of unit rank r, norm relation $d = \sum_i a_i \mathrm{N}_{H_i} b_i$ where d is a prime power in the good case of Grunwald–Wang, ideal $\mathfrak{a}$ and set S of k primes stable under the action of $G = \mathrm{Gal}(K/\mathbb{Q})$, together with $\alpha, \vec{y}$ such that $\mathfrak{a}^d = (\alpha) \prod_i \mathfrak{p}_i^{y_i}$.

Output: $\beta', \vec{z'}$ such that $\mathfrak{a} = (\beta') \prod_i \mathfrak{p}_i^{z'_i}$.

1 Compute a basis $(\alpha_i)_{i \leq k+r+1}$ for the S-unit group (using recursive norm relation techniques), and let $M \in \mathbb{Z}^{(r+k+1)\times k}$ such that $(\alpha_i) = \prod_j \mathfrak{p}_j^{M_{i,j}}$;

2 Put M in row reduced echelon form mod$d$. Find $\vec{x}^{(0)}$ solution to $\vec{y} = \vec{x}M \bmod d$;

3 Compute $\vec{x}^{(1)}, \ldots, \vec{x}^{(m)}$ basis of the left kernel of M mod d ;

4 $\alpha' \leftarrow (\alpha) \left(\prod_i \alpha_i^{x_i^{(0)}} \right)$. For $j \leq m$: $\delta_j \leftarrow \prod_i \alpha_i^{x_i^{(j)}}$.$U \leftarrow \langle \delta_1, \ldots, \delta_m \rangle$. Let $c \leq c_0$ large enough. ;

5 Compute a $(\mathbb{Z}/d\mathbb{Z})$-generating set $\overline{\delta_1 \alpha'^{n_1}}, \ldots, \overline{\delta_m \alpha'^{n_m}}$ of

$$\bigcap_{p \notin \mathfrak{p}, \mathrm{N}(\mathfrak{p}) \leq c} \ker(\langle U, \alpha' \rangle / \langle U, \alpha' \rangle^d \to \mathbb{Z}/d\mathbb{Z} \times k_{\mathfrak{p}}^{\times} / (k_{\mathfrak{p}}^{\times})^d)$$

Compute $k, a_i \in \mathbb{Z}$, $1 \leq i \leq m$, with $1 = kd + \sum_{i=1}^m a_i n_i$;

6 Let $\vec{x} \leftarrow \vec{x}^{(0)} + \sum_{j \leq m} a_j \vec{x}^{(j)}$;

7 **return:** $\sqrt[d]{\alpha' \cdot \prod_j \delta_j^{a_j}}, \frac{1}{d} (\vec{y} - \vec{x}M)$

Algorithm 9: Ideal Decomposition With Norm Relations

CHAPTER 6

CLASS NUMBER OF MAXIMAL REAL SUBFIELD OF CYCLOTOMIC FIELDS

The computation of class numbers of cyclotomic fields is known as a "notoriously hard problem" [69]. The difficulty of this problem lies in the class number computation of the maximal real subfield of cyclotomic field [69, Sec. 1]. The class number of the maximal real subfield of a cyclotomic field is also known as the "plus part" of the class number of a cyclotomic field and it is denoted by h^+. The classical method to calculate h^+ is by using Minkowski's bound. But this method becomes impractical for cyclotomic fields of large discriminant. To address the cyclotomic fields of large discriminants, Masley [51] and van der Linden [49] introduced a method for h^+ computation by using Odlyzko's discriminant lower bounds. However, this method could only be applied to cyclotomic fields of small root discriminants, thus limiting their applicability. Later Miller described a new approach for h^+ computation [54, 55, 56]. Miller's approach finds an upper bound for h^+ by establishing nontrivial lower bounds for sums over prime ideals of the Hilbert class field. This upper bound, together with some divisibility arguments, gives the exact h^+. The crucial part of Miller's technique is finding a large number of principal prime ideals of the maximal real subfield of the cyclotomic field. In this chapter, we introduce a variant of Miller's technique for computing h^+ unconditionally. Then, we apply it to determine the class numbers of a few maximal real subfields of cyclotomic fields that are not documented in the literature. The key component of our new approach is the implementation of Algorithm 8 for the PIP resolution. These PIP methods were introduced in Chapter 5.

6.1 Miller's Approach For h^+ Computation

In this section, we discuss Miller's approach for h^+ computation [54, 55]. A Schwartz class function on $\mathbb{R}$ is a complex-valued smooth function $f : \mathbb{R} \to \mathbb{C}$ that decays rapidly to zero. That is, for all $m, n \in \mathbb{Z}_{\geq 0}$ we have

$$\sup_{x\in\mathbb{R}}|x^m f^{(n)}(x)|< \infty,$$

where $f^{(n)}$ denotes the n-th derivative of f. Consider a Schwartz class function F on R with the condition $F(0) = 1$ and $F(-x) = F(x)$. Let Φ be the function defined by

$$\Phi(s) = \int_{-\infty}^{\infty} F(x)e^{(s-1/2)x}\,dx.$$

Then Poitou's version [63] of Weil's "explicit formula" for a number field K of degree n and r_1 real embeddings will be of the form

$$\begin{aligned}\log d(K) =& r_1\frac{\pi}{2} + n(\gamma + \log 8\pi) - n\int_0^\infty \frac{1-F(x)}{2\sinh\frac{x}{2}}\,dx \\ &- r_1\int_0^\infty \frac{1-F(x)}{2\cosh\frac{x}{2}}\,dx - 4\int_0^\infty F(x)\cosh\frac{x}{2}\,dx \\ &+ \sum_\rho \Phi(\rho) + 2\sum_{\mathfrak{P}}\sum_{m=1}^{\infty}\frac{\log N\mathfrak{P}}{N\mathfrak{P}^{m/2}}F(m\log N\mathfrak{P})\end{aligned} \tag{6.1}$$

where γ is Euler's constant. Here the first summation is over nontrivial zeros of the Dedekind zeta function of the number field K. The second summation is over the prime ideals of K. When K is a totally real field we can apply Weil's explicit formula to the Hilber class field of K and deduce the following result, which is crucial for Miller's h^+ computation approach.

Theorem 6.1 (Thm. 2.3.1 of [55]). *Let K be a totally real field of degree n. For a positive constant c, consider the function*

$$F(x) = \frac{e^{-(x/c)^2}}{\cosh \frac{x}{2}}.$$

Let S be a subset of prime integers which totally split into principal prime ideals of K. Let

$$\begin{aligned} B =& \frac{\pi}{2} + \gamma + \log 8\pi - \log \mathrm{rd}(K) - \int_0^\infty \frac{1 - F(x)}{2} \left(\frac{1}{\sinh \frac{x}{2}} + \frac{1}{\cosh \frac{x}{2}} \right) dx \\ &+ 2 \sum_{p \in S} \sum_{m=1}^{\infty} \frac{\log p}{p^{m/2}} F(m \log p). \end{aligned} \tag{6.2}$$

If $B > 0$ then we have the following upper bound for the class number h of K,

$$h < \frac{2c\sqrt{\pi}}{nB}.$$

We denote the class number of the cyclotomic field $\mathbb{Q}(\zeta_m)$ of conductor m as h_m and the class number of its maximal real subfield $\mathbb{Q}(\zeta_m)^+$ as h_m^+. The main part of Miller's approach is finding sufficiently many algebraic integers x in $\mathbb{Q}(\zeta_m)^+$ such that $\mathrm{N}(x)$ is a prime integer p congruent to ± 1 modulo m. Consider an integral basis $\{b_0, b_1, ..., b_{n-1}\}$ of $\mathbb{Q}(\zeta_m)^+$ with $b_0 = 1$ and $b_j = 2\cos(\frac{2\pi j}{m})$ for $j = 1, ..., n-1$. Miller's approach searches "sparse vectors" over this integral basis, where almost all the coefficients are zero and the remaining coefficients are ± 1. Specifically, Miller searched over the vectors of the form

$$x = b_0 + b_1 + a_1 b_{j1} + a_2 b_{j2} + a_3 b_{j3} + a_4 b_{j4} + a_5 b_{j5} + a_6 b_{j6},$$

where $1 < j1 < j2 < j3 < j4 < j5 < j5 < j6 < n$ and $a_j \in \{-1, 0, 1\}$ for $1 \leq j \leq 6$. Once we find a vector x such that $\mathrm{N}(x)$ is a prime integer p congruent to ± 1 modulo m, then this prime integer p will split completely into principal ideals of $\mathbb{Q}(\zeta_m)^+$ and we can include p into the set S. Once we have a sufficient number of prime integers in S, we can use Equation 6.1 to get an upper bound for the class number h_m^+. Then by using various

divisibility theorems, we can obtain the exact class number from the upper bound. The following theorems are used for this purpose as described by van der Linden [49], Masley [51] and Washington [84]. We denote the relative class number $\frac{h_m}{h_m^+}$ by h_m^-.

Parity Check Theorem 6.2 (Thm. 2.21 of [51]). *If h_m^- is odd, then h_m^+ is odd.*

Reflection Theorem 6.3 (Thm. 2.22 of [51]). *For a prime integer p, consider the least common multiple M of p and the conductor m. If p does not divide the relative class number h_M^-, then p does not divide h_m^+.*

Pushing Down Theorem 6.4 (Thm. 10.4 of [84]). *Consider a Galois extension L/K with degree power of a prime p. Suppose at most one prime of K ramifies in L. Then if p does not divide h_K, then p does not divide h_L.*

Rank Theorem 6.5 (Cor. 2.15 of [51]). *Let L/K be a cyclic extension of degree n. Let p be a prime that does not divide h_E for all intermediate fields E with $K \subseteq E \subset L$. If p divides h_L, then p^f divides h_L, where f is the order of p modulo n.*

6.2 A Variant of Miller's Approach For Unconditional h^+ Computation

We present a new approach for unconditional h^+ computation that is very similar to Miller's unconditional h^+ computation approach. The main difference between our approach and Miller's approach lies in the search process for finding prime integers which split completely into principal ideals of $\mathbb{Q}(\zeta_m)^+$. We use Algorithm 8 to find the prime integers which split completely into principal ideals. More precisely, we start from the smallest prime integer p which split completely in $\mathbb{Q}(\zeta_m)^+$ and check whether any ideal above p is principal by using Algorithm 8. If any ideal above p is principal, then p should split completely into principal ideals and we can include p into the set S of Theorem 6.1. We continue this strategy to the next split prime until we find enough prime integers in S, that can give a sufficient upper bound for the class number. Once we get the class number upper bound we use the same divisibility arguments used by Miller to obtain the exact class number. The

main computational task of our approach is PIP computation. But the norm relation-based PIP of [43] helps us to tackle this issue. We use Algorithm 10 to find the prime integers that split completely into principal ideals. We summarize our results with the following theorem.

Theorem 6.6. *The class number of* $\mathbb{Q}(\zeta_m)^+$ *is one for* $m = 285, 540, 372, 396, 308, 231, 462$.

Input : Integer $k > 0$, number field K, and a norm relation $d = \sum_i a_i N_{H_i} b_i$
Output: A list L_{primes} of prime integers which split completely into principal ideals in K

```
Initialize empty lists L and L_primes ;
L ← First k prime integers which splits completely in K;
for p in L do
    Choose any prime ideal 𝔭 above p in K;
    Solve PIP for the prime ideal 𝔭 by using Algorithm 8;
    if 𝔭 is principal then
        Find α of K such that 𝔭 = α𝒪_K;
        if N_{K/ℚ}(α)=p then
            Store p in L_primes;
        end
    end
end
Consider L_primes as S and compute B by using Equation (6.2);
if B > 0 then
    return: L_primes
else
    k ← 2k and go to step 1
end
```

Algorithm 10: Primes search algorithm

The significance of our approach Miller [54, 55] computed h^+ for cyclotomic fields of composite conductor up to degree 116 without assuming GRH. Generally, when the degree of the cyclotomic field $\mathbb{Q}(\zeta_m)$ increases, the root discriminant of the maximal real subfield $\mathbb{Q}(\zeta_m)^+$ also increases and we need a large contribution from the prime summation term in Equation (6.2) to obtain a positive B and an upper bound for h^+. As mentioned in the previous section, to find prime integers which split completely into principal ideals of $\mathbb{Q}(\zeta_m)^+$ Miller searches "sparse" vectors with respect to an integral basis of $\mathbb{Q}(\zeta_m)^+$ and

tries to find algebraic integers of prime norm. Usually, the prime integers we obtain by this approach are very large. So, we need a large number of prime integers to obtain a positive B in Equation (6.2). This makes h^+ computation very difficult when the degree of the cyclotomic field goes beyond 116. The primes we collect in our approach are smaller by construction, and each of these smaller primes has a high contribution to the prime sum term in Equation 6.2. Hence, we need a smaller number of primes to establish an unconditional upper bound for the class number compared to Miller's approach. As we mentioned in Section 3.3, Biasse, Fieker, Hofmann, and Page [20] introduced a recursive strategy for the computation of class groups by leveraging the information from subfields by using norm relation. In Table 1 and Table 2 of [20], Biasse, Fieker, Hofmann and Page present a list of cyclotomic fields with their unconditional h^+ values. Biasse et al. [20] used GRH-conditional computations in subfields for the class group computations [20, Sec. 4.5]. Then they performed unconditional certification in subfields by using PARI/GP *bnfcertify* function [80] and thus obtained unconditional h^+ values. So, the class groups are correct only if the class groups of subfields are correct. For all the number fields $\mathbb{Q}(\zeta_m)^+$ we consider in this chapter, the norm relation involves cyclic subfields with large discriminants. Therefore, the norm relation-based class group computation as in [20] is not applicable for these cyclic subfields, and we have to rely on classical methods. However, these cyclic subfields have large Minkowski bounds, making the classical class group computation infeasible. Consequently, the unconditional certification approach of [20] will not work for the number fields $\mathbb{Q}(\zeta_m)^+$ we consider in this chapter.

6.2.1 The Proof of $h^+_{285} = 1$

Consider the cyclotomic field $\mathbb{Q}(\zeta_{285})$ of degree 144. We compute the class number h^+_{285} of the maximal real subfield $\mathbb{Q}(\zeta_{285})^+$. If we use Miller's approach to establish a good unconditional class number upper bound, we might need more than 10^{12} primes which split completely into principal ideals and it becomes extremely computationally challenging. The

norm relation of $\mathbb{Q}(\zeta_{285})^+$ involves a subfield of degree 36 with cyclic Galois group. The class group computation with norm relation as in [20] is not applicable for this degree 36 subfield and we have to depend on classical methods. But the Minkowski bound for this degree 36 subfield is around 10^{20} and it is not computationally feasible. So, the unconditional certification as in [20] is not applicable for $\mathbb{Q}(\zeta_{285})^+$. But by implementing our approach, Algorithm 10, we get 6143 small prime integers which split completely into principal ideals in $\mathbb{Q}(\zeta_{285})^+$. We use these prime for the prime summation term in Equation (6.2) and obtain a positive B and thus an upper bound of 24 for h^+_{285}. Then we use the divisibility theorems to get the exact class number.

There are three subfields of degree 36 for $\mathbb{Q}(\zeta_{285})^+$. One of them is $\mathbb{Q}(\zeta_{95})^+$ the maximal real subfield of the cyclotomic field of conductor 95. Among the other two subfields of degree 36 one has cyclic Galois group over $\mathbb{Q}$. We denote this subfield as K_{36}. There are three degree 18 subfields for $\mathbb{Q}(\zeta_{285})^+$. One of them is $\mathbb{Q}(\zeta_{57})^+$ the maximal real subfield of the cyclotomic field of conductor 57. Among the other two subfields of degree 18 subfields one has root discriminant 62.48. We denote this subfield as $K_{18,1}$ and the remaining one as $K_{18,2}$.

2-part Consider the degree 18 subfield $\mathbb{Q}(\zeta_{57})^+$ of $\mathbb{Q}(\zeta_{285})^+$. Then the Galois extension $\mathbb{Q}(\zeta_{285})^+/\mathbb{Q}(\zeta_{57})^+$ has degree 4. The prime integer 5 is inert in $\mathbb{Q}(\zeta_{57})^+$. The prime ideal (5) is the only prime ideal of $\mathbb{Q}(\zeta_{57})^+$ that ramifies in the degree 4 extension $\mathbb{Q}(\zeta_{285})^+/\mathbb{Q}(\zeta_{57})^+$. Since $\mathbb{Q}(\zeta_{57})^+$, has class number 1, we can use the pushing down theorem to show that 2 does not divide h^+_{285}.

3-part We consider the extension $\mathbb{Q}(\zeta_{285})^+/\mathbb{Q}(\zeta_{19})^+$. We prove that 3 does not divide the class numbers of intermediate fields of $\mathbb{Q}(\zeta_{285})^+/\mathbb{Q}(\zeta_{19})^+$, those are cyclic over $\mathbb{Q}(\zeta_{19})^+$. Then we apply the Rank Theorem and obtain that 3 does not divide h^+_{285}.

The maximal real subfield of the cyclotomic field of conductor 19, $\mathbb{Q}(\zeta_{19})^+$ has degree 9 and it is a subfield of $\mathbb{Q}(\zeta_{285})^+$. $\mathbb{Q}(\zeta_{19})^+$ has class number 1. $\mathbb{Q}(\zeta_{285})^+/\mathbb{Q}(\zeta_{19})^+$ is an abelian extension of degree 8. The extension $\mathbb{Q}(\zeta_{285})^+/\mathbb{Q}(\zeta_{19})^+$ is not cyclic. Three degree

18 subfields $K_{18,1}$, $K_{18,2}$ and $\mathbb{Q}(\zeta_{57})^+$ are cyclic over $\mathbb{Q}(\zeta_{19})^+$. Also, the degree 36 subfields $\mathbb{Q}(\zeta_{95})^+$ and K_{36} are cyclic over $\mathbb{Q}(\zeta_{19})^+$. These are the nontrivial intermediate fields of $\mathbb{Q}(\zeta_{285})^+/\mathbb{Q}(\zeta_{19})^+$, those are cyclic over $\mathbb{Q}(\zeta_{19})^+$. We want to check the divisibility of 3 for the class numbers of these degree 18 and 36 intermediate fields.

We start with degree 18 intermediate fields of $\mathbb{Q}(\zeta_{285})^+/\mathbb{Q}(\zeta_{19})^+$. The $\mathbb{Q}(\zeta_{57})^+$, has class number 1. So, 3 does not divide the class number of $\mathbb{Q}(\zeta_{57})^+$. Now let's check, whether 3 divides the class number of $K_{18,1}$. Consider the quadratic field defined by the polynomial $x^2 + x - 71$. Let's denote this field as K and it has class number 2. Consider the degree 9 extension $K_{18,1}/K$. Then the prime integer 19 factors as $(19) = P^2$ in K for a prime ideal P. The prime P is the only prime of K that ramifies in $K_{18,1}$. Since the class number of K is 2, by using the Pushing Down Theorem we can show that 3 does not divide the class number of $K_{18,1}$. For the subfield $K_{18,2}$, we can choose a pair $(45.037, 15.201)$ from Odlyzko's table of unconditional bounds for discriminants [61] to get a class number upper bound of 2. So, 3 does not divide the class number of $K_{18,2}$.

Now let's check the divisibility of 3 for degree 36 intermediate fields of $\mathbb{Q}(\zeta_{285})^+/\mathbb{Q}(\zeta_{19})^+$. The subfield $\mathbb{Q}(\zeta_{95})^+$, has class number 1. For K_{36}, consider the degree 4 cyclic extension $K_{36}/\mathbb{Q}(\zeta_{19})^+$. There is only one intermediate field $K_{18,2}$ for the extension $K_{36}/\mathbb{Q}(\zeta_{19})^+$. We have a class number upper bound of 2 for $K_{18,2}$. By using Miller's approach and by using an LLL reduced basis of the ring of integers, we can get a class number upper bound 8 for K_{36}. Thus, by the Rank Theorem, we obtain that 3 does not divide the class number of K_{36}.

So far, we have shown that 3 does not divide the class number of all the intermediate fields of $\mathbb{Q}(\zeta_{285})^+/\mathbb{Q}(\zeta_{19})^+$, those are cyclic over $\mathbb{Q}(\zeta_{19})^+$. So, by The Rank Theorem, we can show that 3 does not divide the class number of $\mathbb{Q}(\zeta_{285})^+$.

5-part 285 is the least common multiple of 5 and the conductor 285. From Washington's table [84], we find that 5 does not divide the relative class number h^-_{285}. Thus, by using the Reflection Theorem we obtain 5 does not divide h^+_{285}.

p-part $7 \leq p \leq 23$. We prove that p does not divide the class numbers of intermediate fields of $\mathbb{Q}(\zeta_{285})^+/\mathbb{Q}(\zeta_{19})^+$, which are cyclic over $\mathbb{Q}(\zeta_{19})^+$. Then we apply the Rank Theorem and obtain that p does not divide h^+_{285}. The only intermediate fields of $\mathbb{Q}(\zeta_{285})^+/\mathbb{Q}(\zeta_{19})^+$, that are cyclic over $\mathbb{Q}(\zeta_{19})^+$ are degree 18 intermediate fields $\mathbb{Q}(\zeta_{57})^+$, $K_{18,1}$,$K_{18,2}$ and degree 36 intermediate fields $\mathbb{Q}(\zeta_{95})^+$ and K_{36}.

Let's start with degree 18 intermediate fields of $\mathbb{Q}(\zeta_{285})^+/\mathbb{Q}(\zeta_{19})^+$. The degree 18 intermediate field $\mathbb{Q}(\zeta_{57})^+$ has class number one. So, p does not divide the class number of $\mathbb{Q}(\zeta_{57})^+$. We have already shown that the class number of the degree 18 intermediate field $K_{18,2}$ has an upper bound of 2. So, p does not divide the class number of $K_{18,2}$. For the degree 18 intermediate field $K_{18,1}$, we consider the degree 9 cyclic extension $K_{18,1}/K$ as we constructed earlier. We can not use the Push Down Theorem as we used for prime 3. The only nontrivial intermediate field for this extension is the degree 6 field defined by the polynomial $x^6 + x^5 - 74x^4 + 68x^3 + 607x^2 - 603x - 449$. This subfield has class number 2. By using Miller's approach as in Section 6.1, we can get a class number upper bound of 11 for $K_{18,1}$. So, by using the Rank Theorem we can show that p does not divide the class number of $K_{18,1}$.

Now, let's consider degree 36 intermediate fields of $\mathbb{Q}(\zeta_{285})^+/\mathbb{Q}(\zeta_{19})^+$. The degree 36 intermediate field $\mathbb{Q}(\zeta_{95})^+$ has class number 1. For K_{36}, we can use the same degree 4 cyclic extension $K_{36}/\mathbb{Q}(\zeta_{19})^+$ as we used for prime 3. There is only one intermediate field $K_{18,2}$ for the extension $K_{36}/\mathbb{Q}(\zeta_{19})^+$. We already have a class number upper bound of 2 for $K_{18,2}$ and a class number upper bound of 8 for K_{36}. Thus, by Rank Theorem we obtain that p does not divide the class number of K_{36}.

Since p does not divide the class number of all the intermediate fields of $\mathbb{Q}(\zeta_{285})^+/\mathbb{Q}(\zeta_{19})^+$, those are cyclic over $\mathbb{Q}(\zeta_{19})^+$, by using the Rank theorem, we can show that p does not divide the class number of $\mathbb{Q}(\zeta_{285})^+$.

So by using the upper bound $h^+_{285} \leq 24$, we can conclude that the class number $h^+_{285} = 1$.

6.2.2 The Proof of $h^+_{540} = 1$

Consider the cyclotomic field $\mathbb{Q}(\zeta_{540})$ of degree 144. We compute the class number h^+_{540} of its maximal real subfield $\mathbb{Q}(\zeta_{540})^+$. If we use Miller's approach to establish a good unconditional class number upper bound we might need more than 10^{12} primes which split completely into principal ideals and it becomes computationally almost impossible. The norm relation of $\mathbb{Q}(\zeta_{540})^+$ involves a subfield of degree 36 with cyclic Galois group. So, class group computation with norm relation as in [20] is not applicable for this degree 36 subfield and we have to depend on classical methods. But the Minkowski bound for this degree 36 subfield is around 10^{22} and it is not computationally feasible. So, unconditional certification as in [20] is not applicable for $\mathbb{Q}(\zeta_{540})^+$. But, by using our approach we can get a class number upper bound of 31 for h^+_{540}. Then we use the divisibility theorems to obtain the exact class number.

2-part h^-_{396} is odd. So, by the Parity Check Theorem, h^-_{540} is odd.

3-part Consider the degree 24 field $\mathbb{Q}(\zeta_{180})^+$. It is a subfield of $\mathbb{Q}(\zeta_{540})^+$. Consider the degree 3 extension $\mathbb{Q}(\zeta_{540})^+/\mathbb{Q}(\zeta_{180})^+$. Then the prime integer 3 factors as P^6 in $\mathbb{Q}(\zeta_{180})^+$ for a prime ideal P of $\mathbb{Q}(\zeta_{180})^+$. P is the only prime ideal of $\mathbb{Q}(\zeta_{180})^+$ that ramifies in $\mathbb{Q}(\zeta_{540})^+$. Since the class number of $\mathbb{Q}(\zeta_{180})^+$ is one, by using the Push Down Theorem we obtain that 3 does not divide h^+_{540}.

p-part $p = 5, 7, 11, 13, 17, 23, 29, 31$. Consider the degree 9 extension $\mathbb{Q}(\zeta_{540})^+/\mathbb{Q}(\zeta_{60})^+$. The class number of $\mathbb{Q}(\zeta_{60})^+$ is one. The only intermediate field which is cyclic over $\mathbb{Q}(\zeta_{60})^+$ is $\mathbb{Q}(\zeta_{180})^+$. The class number of $\mathbb{Q}(\zeta_{180})^+$ is one. Since p^f, where f is the order of p modulo n is greater than 31, by using the Rank Theorem we conclude that p does not divide h^+_{540}.

19-part Consider the degree 4 extension $\mathbb{Q}(\zeta_{540})^+/\mathbb{Q}(\zeta_{108})^+$. The class number of $\mathbb{Q}(\zeta_{108})^+$ is one. There is only one intermediate field which is cyclic over $\mathbb{Q}(\zeta_{108})^+$. That is a degree 36 subfield and let's denote it by K_{20}. By using the PARI/GP [80] we can get the class number of K_{20} as one. The PARI/GP *bnfcertify* unconditional certification for this class number of

K_{20} took just a few seconds. Since the order of 19 modulo 4 is 2, by using the Rank Theorem we obtain that 19 does not divide h^+_{540}.

Then by using the class number upper bound of 31 and the above divisibility arguments, we can conclude that the class number $h^+_{540} = 1$.

6.2.3 The Proof of $h^+_{396} = 1$

Consider $\mathbb{Q}(\zeta_{396})$ is of degree 120. We compute the class number of its maximal real subfield $\mathbb{Q}(\zeta_{396})^+$. The norm relation of $\mathbb{Q}(\zeta_{396})^+$ involves a degree 30 subfield with cyclic Galois group. The Minkowski bound for this degree 30 subfield is around 10^{16}. So, the unconditional certification approach of [20] is not applicable for h^+_{396} computation. By using the Algorithm 10, we get 2448 small prime integers which split completely into principal ideals in $\mathbb{Q}(\zeta_{396})^+$. Then Equation 6.2 provides us a positive B and thus an upper bound of 20 for h^+_{396}.

2-part The relative class number of the cyclotomic field of conductor 396 is odd. So by the Parity Check Theorem h^+_{396} is odd.

3-part The field $\mathbb{Q}(\zeta_{132})^+$ of degree 20 is a subfield of $\mathbb{Q}(\zeta_{396})^+$. Consider the degree 3 extension $\mathbb{Q}(\zeta_{396})^+/\mathbb{Q}(\zeta_{132})^+$. The prime integer 3 factors as P^2 in $\mathbb{Q}(\zeta_{132})^+$. This is the only prime of $\mathbb{Q}(\zeta_{132})^+$ that ramifies in $\mathbb{Q}(\zeta_{396})^+$. Since the class number of $\mathbb{Q}(\zeta_{132})^+$ is one, using the Pushing Down Theorem we obtain that 3 does not divide h^+_{396}.

5-part The field $\mathbb{Q}(\zeta_{33})^+$ of degree 10 is a subfield of $\mathbb{Q}(\zeta_{396})^+$. Its class number is one. Consider the degree 6 extension $\mathbb{Q}(\zeta_{396})^+/\mathbb{Q}(\zeta_{33})^+$. There is an intermediate field of degree 30 which is cyclic over $\mathbb{Q}(\zeta_{33})^+$ with root discriminant 44.97. We can choose a pair $(45.037, 15.201)$ from Odlyzko's table of unconditional bounds for discriminants [61] to get a class number upper bound of 4 for this degree 30 intermediate field. The field $\mathbb{Q}(\zeta_{132})^+$ is also an intermediate field for the extension $\mathbb{Q}(\zeta_{396})^+/\mathbb{Q}(\zeta_{33})^+$. $\mathbb{Q}(\zeta_{132})^+$ is cyclic over $\mathbb{Q}(\zeta_{33})^+$. The class number of $\mathbb{Q}(\zeta_{132})^+$ is one. The order of 5 modulo 6 is 2. So if 5 divides h^+_{396}, then

by the Rank Theorem, 25 must divide h^+_{396}. Since we have the class number upper bound of 20 for h^+_{396}, 5 does not divide h^+_{396}.

7-part There is a unique degree 12 subfield for $\mathbb{Q}(\zeta_{396})^+$. Let's denote this subfield as K_{12}. Consider the degree 5 extension $\mathbb{Q}(\zeta_{396})^+/K_{12}$. There are no intermediate fields for this extension. The root discriminant of K_{12} is 34.47. We can choose a pair $(55.509, 29.867)$ from Odlyzko's table of unconditional bounds for discriminants to get a class number upper bound of 5 for K_{12}. The order of 7 modulo 5 is 4. So, by using the Rank Theorem we can find that 7 does not divide h^+_{396}.

11-part Here we can use the degree 6 extension $\mathbb{Q}(\zeta_{396})^+/\mathbb{Q}(\zeta_{33})^+$ as we used for $p = 5$. Since the order of 11 modulo 6 is 2, by using the Rank Theorem we get 11 does not divide h^+_{396}.

p-part $13 \leq p \leq 19$. Here we can use the degree 7 extension $\mathbb{Q}(\zeta_{396})^+/K_{12}$ as we did for p=7. Since the order of p modulo 5 is greater than one, by using the Rank Theorem we obtain that p does not divide h^+_{396}.

So, by using the class number upper bound $h^+_{396} \leq 20$, we obtain that $h^+_{396} = 1$.

6.2.4 The Proof of $h^+_{372} = 1$

Consider $\mathbb{Q}(\zeta_{372})$ of degree 120. We compute the class number h^+_{372} of its maximal real subfield $\mathbb{Q}(\zeta_{372})^+$. The norm relation of $\mathbb{Q}(\zeta_{372})^+$ involves a degree 30 subfield with cyclic Galois group. The Minkowski bound for this degree 30 subfield is around 10^{17}. So, the unconditional certification approach of [20] is not applicable for h^+_{372} computation. By using the Algorithm 10, we get 6871 small prime integers which split completely into principal ideals in $\mathbb{Q}(\zeta_{372})^+$. We use these prime for the prime summation term in Equation (6.2) and obtain a positive B and thus an upper bound of 15 for h^+_{372}.

2-part There is a unique degree 12 subfield for $\mathbb{Q}(\zeta_{372})^+$. Let's denote it by K_{12}. Consider the degree 5 extension $\mathbb{Q}(\zeta_{372})^+/K_{12}$. There are no intermediate fields for this extension. By using PARI/GP [80] we find that the conditional class number of K_{12} is one. The

unconditional certification for this class number by using PARI/GP *bnfcertify* function [80] took just a few seconds. The order 2 modulo 5 is 4. So, if 2 divides the h^+_{372}, then by the Rank Theorem, 16 should divide h^+_{372}. Since we have a class number upper bound of 11 for $\mathbb{Q}(\zeta_{372})^+$, 2 does not divide h^+_{372}.

3-part Here we can use the same extension $\mathbb{Q}(\zeta_{372})^+/K_{12}$ as we used for $p = 2$. The order of 3 modulo 5 is 4. So, if 3 divides h^+_{372}, then by the Rank Theorem, 81 divides h^+_{372}. Since the class number upper bound for $\mathbb{Q}(\zeta_{372})^+$ is 11, 3 does not divide h^+_{372}.

5-part There is a unique degree 20 subfield. Let's denote it by K_{20}. Consider the degree 3 extension $\mathbb{Q}(\zeta_{372})^+/K_{20}$. There are no intermediate fields for this extension. By using PARI/GP [80] function we can get the class number of one for K_{20}. The PARI/GP *bnfcertify* unconditional certification took just a few seconds. The order of 5 modulo 3 is 2. If 5 divides h^+_{372}, then by the Rank Theorem 25 must divide h^+_{372}. Since the class number upper bound for $\mathbb{Q}(\zeta_{372})^+$ is 15, 5 does not divide h^+_{372}.

7-part Here we can use the same extension $\mathbb{Q}(\zeta_{372})^+/K_{12}$ as we used for $p = 2$. The order of 7 modulo 5 is 4. So, if 7 divides h^+_{372}, then by Rank Theorem 7^4 divides h^+_{372}. Since the class number upper bound for $\mathbb{Q}(\zeta_{372})^+$ is 15, 7 does not divide h^+_{372}.

11-part Here we can use the same extension $\mathbb{Q}(\zeta_{372})^+/K_{20}$ as we used for $p = 3$. The order of 11 modulo 3 is 2. So, if 11 divides h^+_{372}, then by Rank Theorem 11^2 divides h^+_{372}. Since the class number upper bound for $\mathbb{Q}(\zeta_{372})^+$ is 15 , 11 does not divide h^+_{372}.

13-part For p=13, consider the degree 5 extension $\mathbb{Q}(\zeta_{372})^+/K_{12}$ as we used for $p = 2$. The order of 13 modulo 5 is 4. So, by the Rank Theorem, 13 does not divide h^+_{372}.

6.2.5 The Proof of $h^+_{231} = 1$

Consider the maximal real subfield $\mathbb{Q}(\zeta_{231})^+$ of the cyclotomic field $\mathbb{Q}(\zeta_{231})$. We compute the class number h^+_{231} of $\mathbb{Q}(\zeta_{231})^+$. The norm relation of $\mathbb{Q}(\zeta_{231})^+$ involves a degree 30 subfield with cyclic Galois group. The Minkowski bound for this degree 30 subfield is around 10^{15}. So, the unconditional certification approach of [20] is not applicable for h^+_{231} computation.

By using Algorithm 10, we can obtain 1962 primes that split completely into principal ideals in $\mathbb{Q}(\zeta_{231})^+$, resulting in an upper bound of 10 for the class number h^+_{231}. We then use the following divisibility arguments to determine the exact class number.

2-part The degree 30 field $\mathbb{Q}(\zeta_{77})^+$ is subfield of $\mathbb{Q}(\zeta_{231})^+$. The prime integer 3 is inert in $\mathbb{Q}(\zeta_{77})^+$ and the prime ideal (3) is the only prime that ramifies in degree 2 extension $\mathbb{Q}(\zeta_{231})^+/\mathbb{Q}(\zeta_{77})^+$. The class number of $\mathbb{Q}(\zeta_{77})^+$ is one. So, the Pushing Down Theorem shows that h^+_{231} is odd.

3-part There is only one degree 20 subfield for $\mathbb{Q}(\zeta_{231})^+$. Let's denote it by K_{20}. Consider the degree 3 extension $\mathbb{Q}(\zeta_{231})^+/K_{20}$. Then the prime integer 3 factors as P^2 in K_{20} for a prime ideal P of K_{20}. P is the only prime ideal of K_{20} that ramifies in $\mathbb{Q}(\zeta_{231})^+$. The class number of K_{20} is one according to the PARI/GP *bnfcertify* function. So, by using the Push Down Theorem we obtain that 3 does not divide h^+_{231}.

5-part Consider the degree 3 extension $\mathbb{Q}(\zeta_{231})^+/K_{20}$. There are no subfields for this extension. The class number of K_{20} is one. The order of 5 modulo 3 is 2. Since we have a class number upper bound of 10 for $\mathbb{Q}(\zeta_{231})^+$, 5 does not divide h^+_{231} by the Rank Theorem.

7-part The least common multiple of 7 and 231 is 231. 7 does not divide h^-_{231} [84]. So, by the Reflection Theorem, 7 does not divide h^+_{231}.

By using the class number upper bound of 10 and above divisibility arguments we conclude that the class number $h^+_{231} = 1$.

6.2.6 The Proof of $h^+_{462} = 1$

Consider the maximal real subfield $\mathbb{Q}(\zeta_{462})^+$ of the cyclotomic field $\mathbb{Q}(\zeta_{462})$. We compute the class number h^+_{462} of $\mathbb{Q}(\zeta_{462})^+$. The norm relation of $\mathbb{Q}(\zeta_{462})^+$ involves a degree 30 subfield with cyclic Galois group. The Minkowski bound for this degree 30 subfield is around 10^{15}. So, the unconditional certification approach of [20] is not applicable for the computation of h^+_{396}. By using Algorithm 10, we can get 1962 primes that split completely into principal

ideals in $\mathbb{Q}(\zeta_{462})^+$ and thus class number upper bound of 10 for h^+_{462}. Then we use the following divisibility arguments to obtain an exact class number.

2-part The degree 30 field $\mathbb{Q}(\zeta_{77})^+$ is subfield of $\mathbb{Q}(\zeta_{462})^+$. The prime integer 3 is inert in $\mathbb{Q}(\zeta_{77})^+$ and the prime ideal (3) is the only prime that ramifies in degree 2 extension $\mathbb{Q}(\zeta_{462})^+/\mathbb{Q}(\zeta_{77})^+$. The class number of $\mathbb{Q}(\zeta_{77})^+$ is one. So, the Pushing Down Theorem shows that h^+_{462} is odd.

3-part There is only one degree 20 subfield for $\mathbb{Q}(\zeta_{462})^+$. Let's denote it by K_{20}. Consider the degree 3 extension $\mathbb{Q}(\zeta_{462})^+/K_{20}$. Then the prime integer 7 factors as P^2 in K_{20} for a prime ideal P of K_{20}. P is the only prime ideal of K_{20} that ramifies in $\mathbb{Q}(\zeta_{462})^+$. The class number of K_{20} is one by PARI/GP *bnfcertify* function. So, by using the Push Down Theorem we find that 3 does not divide h^+_{462}.

5-part There is only one degree 12 subfield for $\mathbb{Q}(\zeta_{462})^+$. Let's denote it by K_{12}. Consider the degree 5 extension $\mathbb{Q}(\zeta_{462})^+/K_{12}$. Then the prime integer 11 factors as P^2 in K_{12} for a prime ideal P of K_{12}. P is the only prime ideal of K_{12} that ramifies in $\mathbb{Q}(\zeta_{462})^+$. The class number of K_{12} is one. So, by using the Push Down Theorem we get 5 does not divide h^+_{462}.

7-part Consider the degree 7 extension $\mathbb{Q}(\zeta_{462})^+/K_{12}$. There are no subfields for this extension. The class number of K_{12} is one. The order of 7 modulo 5 is 4. Since we have a class number upper bound of 10 for $\mathbb{Q}(\zeta_{462})^+$, 7 does not divide h^+_{462} by the Rank Theorem.

So, by applying the class number upper bound of 10 and employing the aforementioned divisibility arguments, we conclude that $h^+_{462} = 1$.

6.2.7 The Proof of $h^+_{308} = 1$

Consider $\mathbb{Q}(\zeta_{308})$ of degree 120. We compute the class number h^+_{308} of its maximal real subfield $\mathbb{Q}(\zeta_{308})^+$. The norm relation of $\mathbb{Q}(\zeta_{308})^+$ involves a degree 30 subfield with cyclic Galois group. The Minkowski bound for this degree 30 subfield is around 10^{16}. So, the unconditional certification approach of [20] is not applicable for h^+_{308} computation. By using Algorithm 10, we can get 3587 primes that split completely into principal ideals in $\mathbb{Q}(\zeta_{308})^+$.

So, we have an upper bound of 12 for h^+_{308}. Then we use the following divisibility arguments to get an exact class number.

2-part The degree 30 field $\mathbb{Q}(\zeta_{77})^+$ is a subfield of $\mathbb{Q}(\zeta_{308})^+$. The prime integer 2 is inert in $\mathbb{Q}(\zeta_{77})^+$ and the prime ideal (2) is the only prime that ramifies in degree 2 extension $\mathbb{Q}(\zeta_{308})^+/\mathbb{Q}(\zeta_{77})^+$. The class number of $\mathbb{Q}(\zeta_{77})^+$ is one. So, the Pushing Down Theorem shows that h^+_{308} is odd.

3-part There is only one degree 12 subfield for $\mathbb{Q}(\zeta_{308})^+$. Let's denote it by K_{12}. Consider the degree 5 cyclic extension $\mathbb{Q}(\zeta_{308})^+/K_{12}$. There are no subfields for this extension. By using the PARI/GP function we can get the conditional class number of K_{12} as one. The PARI/GP unconditional certification took just a few seconds. The order 3 modulo 5 is 4. So, if 3 divides h^+_{308} then by Rank Theorem 3^4 divides h^+_{308}. Since we have the class number upper bound of 12 for $\mathbb{Q}(\zeta_{308})^+$, 3 does not divide h^+_{308}.

5-part There is only one degree 20 subfield for $\mathbb{Q}(\zeta_{308})^+$. Let's denote it by K_{20}. By using the PARI/GP [80], we find that the class number of K_{20} is 1 unconditionally. The order of 5 modulo 3 is 2. Consider the degree 3 extension $\mathbb{Q}(\zeta_{308})^+/K_{20}$. There are no subfields for this extension. If 5 divides h^+_{308}, by using the Rank Theorem to the degree 3 extension $\mathbb{Q}(\zeta_{308})^+/K_{20}$, we obtain that 25 divides h^+_{308}. Since we have the class number upper bound of 12 for $\mathbb{Q}(\zeta_{308})^+$, 5 does not divide h^+_{308}.

7-part Consider the degree 5 extension $\mathbb{Q}(\zeta_{308})^+/K_{12}$ as we used for $p = 3$. The order of 7 modulo 5 is 4. So, by using the Rank Theorem we find that 7 does not divide h^+_{308}.

11-part Consider the degree 3 extension $\mathbb{Q}(\zeta_{308})^+/K_{20}$ as we used for $p = 5$. The order of 11 modulo 3 is 2. So, by using the Rank Theorem we obtain that 11 does not divide h^+_{308}.

Hence, by applying the class number upper bound of 12 and employing the aforementioned divisibility arguments, we conclude that $h^+_{308} = 1$.

CHAPTER 7

FUTURE WORKS

Our modified version of Hafner and McCurley algorithm introduced in Chapter 4 improves the asymptotic time complexity of class group computation of imaginary quadratic fields. The key component of our new approach is the improvement in the creation of the lattice of relations whose determinant is class number h. In 1990, Buchmann [23] generalized the Hafner and McCurley algorithm for class group computation of number fields of higher degree. Buchmann's algorithm computes the class group of infinite classes of number fields of fixed degree. Since the unit group is non-trivial in general number fields, Buchmann's method has to create a lattice L, whose determinant is hR, where R is the regulator of the number field. It will be interesting to investigate our new approach for relation collection as introduced in Chapter 4 can be applied to creating the lattice L and consequently improve the asymptotic run time of Buchmann's class group algorithm.

The existence of norm relation for a number field K with Galois group G implies the following equality of zeta functions [20, Prop. 3.8]:

$$\zeta_K(s)^{a_1} = \prod_{1 \neq H \leq G} \zeta_{K^H}(s)^{a_H} \tag{7.1}$$

where $a_H \in \mathbb{Z}$ and $a_1 > 0$. Equation (7.1) motivates us to investigate whether the class number upper bound for h^+ can be deduced from the class number upper bounds of the subfields involved in norm relation. Finding the class number upper bound for subfields of $\mathbb{Q}(\zeta_m)^+$ is comparatively easy because of its small degree and it may help us to find h^+ for cyclotomic fields of higher degree.

REFERENCES

[1] L. Adleman. "Factoring Numbers Using Singular Integers". In: *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, May 5-8, 1991, New Orleans, Louisiana, USA*. Ed. by Cris Koutsougeras and Jeffrey Scott Vitter. ACM, 1991, pp. 64–71. DOI: 10.1145/103418.103432. URL: https://doi.org/10.1145/103418.103432.

[2] S. Arnold and V. Strassen. "Schnelle Multiplikation großer Zahlen". In: *Computing* 7 (1971), pp. 281–292. URL: https://api.semanticscholar.org/CorpusID:9738629.

[3] E. Artin and J. Tate. *Class field theory*. Reprinted with corrections from the 1967 original. AMS Chelsea Publishing, Providence, RI, 2009, pp. viii+194. ISBN: 978-0-8218-4426-7.

[4] E. Bach. "Explicit bounds for primality testing and related problems". In: *Math. Comp.* 55.191 (1990), pp. 355–380.

[5] J. Bauch et al. "Short Generators Without Quantum Computers: The Case of Multiquadratics". In: *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part I*. Ed. by Jean-Sébastien Coron and Jesper Buus Nielsen. Vol. 10210. Lecture Notes in Computer Science. 2017, pp. 27–59. DOI: 10.1007/978-3-319-56620-7_2. URL: https://doi.org/10.1007/978-3-319-56620-7%5C_2.

[6] K. Belabas et al. *A note on the low order assumption in class group of an imaginary quadratic number fields*. Cryptology ePrint Archive, Report 2020/1310. https://eprint.iacr.org/2020/1310. 2020.

[7] D. Bernstein. “How to find smooth parts of integers”. In: (Jan. 2004).

[8] W. Beullens, T. Kleinjung, and F. Vercauteren. “CSI-FiSh: Efficient Isogeny Based Signatures Through Class Group Computations”. In: *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part I*. Ed. by Steven D. Galbraith and Shiho Moriai. Vol. 11921. Lecture Notes in Computer Science. Springer, 2019, pp. 227–247. DOI: 10.1007/978-3-030-34578-5_9. URL: https://doi.org/10.1007/978-3-030-34578-5%5C_9.

[9] C. Bian et al. “Unconditional computation of the class groups of real quadratic fields”. English. In: *LuCaNT: LMFDB, computation, and number theory*. Contemporary Mathematics. United States: American Mathematical Society, 2024. ISBN: 978-1-4704-7260-3. DOI: 10.1090/conm/796/15996.

[10] J.-F. Biasse. “An L(1/3) algorithm for ideal class group and regulator computation in certain number fields.” In: *Math. Comp.* 83.288 (2014), pp. 2005–2031.

[11] J.-F. Biasse. “Improvements in the computation of ideal class groups of imaginary quadratic number fields.” In: *Adv. in Math. of Comm.* 4.2 (2010), pp. 141–154.

[12] J.-F. Biasse. “Subexponential time relations in the class group of large degree number fields”. In: *Advances in Mathematics of Communications* 8.4 (2014), pp. 407–425. URL: http://aimsciences.org/journals/displayArticlesnew.jsp?paperID=10551.

[13] J.-F. Biasse and M. Erukulangara. “A proof of the conjectured run time of the Hafner-McCurley class group algorithm”. In: *Advances in Mathematics of Communications* 17 (Jan. 2021). DOI: 10.3934/amc.2021055.

[14] J.-F. Biasse and C. Fieker. “Subexponential class group and unit group computation in large degree number fields”. In: *LMS Journal of Computation and Mathematics* 17 (Special Issue A Jan. 2014), pp. 385–403. ISSN: 1461-1570. DOI: 10.1112/S1461157014000345. URL: http://journals.cambridge.org/article_S1461157014000345.

[15] J.-F. Biasse, C. Fieker, and M. Jacobson. “Fast heuristic algorithms for computing relations in the class group of a quadratic order, with applications to isogeny evaluation”. In: *LMS Journal of Computation and Mathematics* 19 (Jan. 2016), pp. 371–390. DOI: 10.1112/S1461157016000358.

[16] J.-F. Biasse and M. Jacobson. “Practical Improvements to Class Group and Regulator Computation of Real Quadratic Fields”. In: *Algorithmic Number Theory, 9th International Symposium, ANTS-IX, Nancy, France, July 19-23, 2010. Proceedings*. Ed. by Guillaume Hanrot, François Morain, and Emmanuel Thomé. Vol. 6197. Lecture Notes in Computer Science. Springer, 2010, pp. 50–65. DOI: 10.1007/978-3-642-14518-6_8. URL: https://doi.org/10.1007/978-3-642-14518-6%5C_8.

[17] J.-F. Biasse, M. Jacobson, and A. Silvester. “Security Estimates for Quadratic Field Based Cryptosystems”. In: *Information Security and Privacy - 15th Australasian Conference, ACISP 2010, Sydney, Australia, July 5-7, 2010. Proceedings*. Ed. by Ron Steinfeld and Philip Hawkes. Vol. 6168. Lecture Notes in Computer Science. Springer, 2010, pp. 233–247. DOI: 10.1007/978-3-642-14081-5_15. URL: https://doi.org/10.1007/978-3-642-14081-5%5C_15.

[18] J.-F. Biasse and C. van Vredendaal. “Fast multiquadratic S-unit computation and application to the calculation of class groups”. In: *Proceedings of ANTS XIII*. 2019, pp. 103–118.

[19] J.-F. Biasse et al. “Mildly Short Vectors in Ideals of Cyclotomic Fields Without Quantum Computers”. In: *Mathematical Cryptology* 2.1 (Nov. 2022), pp. 84–107. URL: https://journals.flvc.org/mathcryptology/article/view/132573.

[20] J.-F. Biasse et al. “Norm relations and computational problems in number fields”. In: *Journal of the London Mathematical Society* 105 (2020). URL: https://api.semanticscholar.org/CorpusID:211532705.

[21] S. Birmpilis, G. Labahn, and A. Storjohann. "A Las Vegas algorithm for computing the smith form of a nonsingular integer matrix". In: *ISSAC '20: International Symposium on Symbolic and Algebraic Computation, Kalamata, Greece, July 20-23, 2020*. Ed. by I. Emiris and L. Zhi. ACM, 2020, pp. 38–45. DOI: 10.1145/3373207.3404022. URL: https://doi.org/10.1145/3373207.3404022.

[22] R. Brauer. "Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers. Herrn Professor Dr. Erhard Schmidt in dankbarer Verehrung zum 75. Geburtstag". In: *Mathematische Nachrichten* 4 (1950), pp. 158–174. URL: https://api.semanticscholar.org/CorpusID:123474215.

[23] J. Buchmann. "A subexponential algorithm for the determination of class groups and regulators of algebraic number fields". In: 1990, pp. 27–41.

[24] J. Buchmann, M. Jacobson, and E. Teske. "On some computational problems in finite abelian groups". In: *Math. Comput.* 66 (1997), pp. 1663–1687. URL: https://api.semanticscholar.org/CorpusID:1888350.

[25] J. Buchmann and A. Schmidt. "Computing the structure of a finite abelian group". In: *Math. Comput.* 74 (2005), pp. 2017–2026. URL: https://api.semanticscholar.org/CorpusID:18339459.

[26] J. Buchmann and H. Williams. "A Key Exchange System Based on Real Quadratic Fields". In: *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*. Ed. by Gilles Brassard. Vol. 435. Lecture Notes in Computer Science. Springer, 1989, pp. 335–343. DOI: 10.1007/0-387-34805-0_31. URL: https://doi.org/10.1007/0-387-34805-0%5C_31.

[27] J. Buchmann and H. Williams. "A Key-Exchange System Based on Imaginary Quadratic Fields." In: *J. Cryptology* 1 (June 1988), pp. 107–118. DOI: 10.1007/BF02351719.

[28] D. Buell. “Small class numbers and extreme values of L-functions of quadratic fields”. In: *Mathematics of Computation* 31 (1977), pp. 786–796. URL: https://api.semanticscholar.org/CorpusID:120279937.

[29] H. Cohen. “A course in computational algebraic number theory”. In: *Graduate texts in Math.* 138 (1993), p. 88. URL: https://ci.nii.ac.jp/naid/10006515766/en/.

[30] H. Cohen, F. Diaz Y Diaz, and M. Olivier. “Subexponential Algorithms for Class Group and Unit Computations”. In: *Journal of Symbolic Computation* 24.3 (1997), pp. 433–441. ISSN: 0747-7171. DOI: http://dx.doi.org/10.1006/jsco.1996.0143. URL: http://www.sciencedirect.com/science/article/pii/S0747717196901431.

[31] R. Cramer, L. Ducas, and B. Wesolowski. “Mildly Short Vectors in Cyclotomic Ideal Lattices in Quantum Polynomial Time”. In: *Journal of the ACM* 68 (Jan. 2021), pp. 1–26. DOI: 10.1145/3431725.

[32] R. Cramer, L. Ducas, and B. Wesolowski. “Short Stickelberger Class Relations and Application to Ideal-SVP”. In: *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part I*. Ed. by Jean-Sébastien Coron and Jesper Buus Nielsen. Vol. 10210. Lecture Notes in Computer Science. 2017, pp. 324–348. DOI: 10.1007/978-3-319-56620-7_12. URL: https://doi.org/10.1007/978-3-319-56620-7%5C_12.

[33] R. Cramer et al. “Recovering Short Generators of Principal Ideals in Cyclotomic Rings”. In: *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II*. Ed. by Marc Fischlin and Jean-Sébastien Coron. Vol. 9666. Lecture Notes in Computer Science. Springer, 2016, pp. 559–585. DOI: 10.1007/978-3-662-49896-5_20. URL: https://doi.org/10.1007/978-3-662-49896-5%5C_20.

[34] G. Dirichlet. “Recherches sur les formes quadratiques à coëfficients et à indéterminées complexes. Première partie.” In: *Journal für die reine und angewandte Mathematik (Crelles Journal)* 1842 (), pp. 291–371. URL: https://api.semanticscholar.org/CorpusID:122293169.

[35] P. Dirichlet and R. Dedekind. *Vorlesungen über Zahlentheorie*. v. 2. F. Vieweg und sohn, 1894. URL: https://books.google.com/books?id=WZIKAAAAYAAJ.

[36] W. Duke and Y. Tschinkel. *Analytic Number Theory: A Tribute to Gauss and Dirichlet*. Clay mathematics proceedings. American Mathematical Society, 2007. ISBN: 9780821843079. URL: https://books.google.com/books?id=tqaWlHIsZXAC.

[37] A. Enge, P. Gaudry, and E. Thomé. “An L(1/3) Discrete Logarithm Algorithm for Low Degree Curves”. In: *Journal of Cryptology* 24 (2009), pp. 24–41. URL: https://api.semanticscholar.org/CorpusID:8898480.

[38] T. Funakura. “On Artin theorem of induced characters”. In: *Comment. Math. Univ. St. Paul.* 27.1 (1978), pp. 51–58. ISSN: 0010-258X.

[39] C. Gentry. “A fully homomorphic encryption scheme”. crypto.stanford.edu/craig. PhD thesis. Stanford University, 2009.

[40] C. Gentry. “Fully Homomorphic Encryption Using Ideal Lattices”. In: vol. 9. May 2009, pp. 169–178. DOI: 10.1145/1536414.1536440.

[41] J. Hafner and K. McCurley. “A rigorous subexponential algorithm for computation of class groups”. In: *Journal of the American Mathematical Society* 2 (1989), pp. 837–850.

[42] W. Hart, G. Tornaría, and M. Watkins. “Congruent Number Theta Coefficients to 10^{12}”. In: *Algorithmic Number Theory, 9th International Symposium, ANTS-IX, Nancy, France, July 19-23, 2010. Proceedings*. Vol. 6197. Lecture Notes in Computer Science. Springer, 2010, pp. 186–200.

[43] C. Fieker J.-F. Biasse, T. Hofmann, and W. Youmans. “An algorithm for solving the principal ideal problem with subfields”. In: *Advances in Mathematics of Communications* (Jan. 2023). DOI: 10.3934/amc.2023021.

[44] M. Jacobson. “Applying sieving to the computation of quadratic class groups”. In: *Math. Comput.* 68.226 (1999), pp. 859–867. DOI: 10.1090/S0025-5718-99-01003-0. URL: https://doi.org/10.1090/S0025-5718-99-01003-0.

[45] M. Jacobson, S. Ramachandran, and H. Williams. “Numerical Results on Class Groups of Imaginary Quadratic Fields”. In: *Algorithmic Number Theory, 7th International Symposium, ANTS-VII, Berlin, Germany, July 23-28, 2006, Proceedings*. Ed. by Florian Hess, Sebastian Pauli, and Michael E. Pohst. Vol. 4076. Lecture Notes in Computer Science. Springer, 2006, pp. 87–101. DOI: 10.1007/11792086_7. URL: https://doi.org/10.1007/11792086%5C_7.

[46] D. Jao, S. Miller, and R. Venkatesan. “Expander graphs based on GRH with an application to elliptic curve cryptography”. In: *J. Number Theory* 129.6 (2009), pp. 1491–1504. ISSN: 0022-314X. DOI: 10.1016/j.jnt.2008.11.006. URL: http://dx.doi.org/10.1016/j.jnt.2008.11.006.

[47] S. Kuroda. “Über die Klassenzahlen algebraischer Zahlkörper”. In: *Nagoya Mathematical Journal* 1.none (1950), pp. 1–10.

[48] H. Lenstra. “On the calculation of regulators and class numbers of quadratic fields”. In: *Journées arithmétiques*. Cambridge Univ. Press, 1982, pp. 123–150.

[49] F. van der Linden. “Class number computations of real abelian number fields”. In: *Mathematics of Computation* 39 (1982), pp. 693–707. URL: https://api.semanticscholar.org/CorpusID:119353702.

[50] V. Lyubashevsky, C. Peikert, and O. Regev. “On Ideal Lattices and Learning with Errors over Rings”. In: *J. ACM* 60.6 (Nov. 2013). ISSN: 0004-5411. DOI: 10.1145/2535925. URL: https://doi.org/10.1145/2535925.

[51] J. Masley. “Class numbers of real cyclic number fields with small conductor”. In: *Compositio Mathematica* 37 (1978), pp. 297–319. URL: https://api.semanticscholar.org/CorpusID:55120258.

[52] J. Matoušek. “Lattices and Minkowski’s Theorem”. In: *Lectures on Discrete Geometry*. Ed. by Jiří Matoušek. New York, NY: Springer New York, 2002, pp. 17–28. ISBN: 978-1-4613-0039-7. DOI: 10.1007/978-1-4613-0039-7_2. URL: https://doi.org/10.1007/978-1-4613-0039-7_2.

[53] K. McCurley. “Cryptographic key distribution and computation in class groups”. In: *Number theory and applications (Banff, AB, 1988)*. Vol. 265. NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci. Kluwer Acad. Publ., Dordrecht, 1989, pp. 459–479.

[54] J. Miller. “Class numbers of real cyclotomic fields of composite conductor”. In: *Lms Journal of Computation and Mathematics* 17 (2014), pp. 404–417. URL: https://api.semanticscholar.org/CorpusID:123869613.

[55] J. Miller. “Class numbers of totally real number fields”. https://api.semanticscholar.org/CorpusID:124386620. PhD thesis. Rutgers University, 2015.

[56] J. Miller. “Real cyclotomic fields of prime conductor and their class numbers”. In: *Math. Comput.* 84 (2014), pp. 2459–2469. URL: https://api.semanticscholar.org/CorpusID:20347318.

[57] A. Mosunov and M. Jacobson. “Unconditional class group tabulation of imaginary quadratic fields to $|\Delta| < 240$”. In: *Mathematics of Computation* 85.300 (2016), pp. 1983–2009. ISSN: 00255718, 10886842. URL: https://www.jstor.org/stable/mathcomp.85.300.1983 (visited on 03/21/2024).

[58] J. Neukirch. *Algebraic number theory*. Comprehensive Studies in Mathematics. ISBN 3-540-65399-6. Springer-Verlag, 1999.

[59] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*. Second. Vol. 323. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 2008, pp. xvi+825. ISBN: 978-3-540-37888-4. DOI: 10.1007/978-3-540-37889-1. URL: https://doi.org/10.1007/978-3-540-37889-1.

[60] A. Odlyzko. "Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions : a survey of recent results". eng. In: *Journal de théorie des nombres de Bordeaux* 2.1 (1990), pp. 119–141. URL: http://eudml.org/doc/93506.

[61] A. Odlyzko. *Unconditional bounds for discriminants*. https://www-users.cse.umn.edu/~odlyzko/unpublished/discr.bound.table4. 1976.

[62] M. Pohst and H. Zassenhaus. *Algorithmic algebraic number theory*. Vol. 30. Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, 1989, pp. xiv+465. ISBN: 0-521-33060-2. DOI: 10.1017/CBO9780511661952. URL: https://doi.org/10.1017/CBO9780511661952.

[63] G. Poitou. "Sur les petits discriminants". fr. In: *Séminaire Delange-Pisot-Poitou. Théorie des nombres* 18.1 (1977). talk:6, pp. 1–17. URL: http://www.numdam.org/item/SDPP_1976-1977__18_1_A6_0/.

[64] S. Ramachandran. *Numerical results on class groups of imaginary quadratic fields*. Master's thesis. Calgary, Canada, 2006.

[65] O. Regev and N. Stephens-Davidowitz. "A reverse Minkowski theorem". In: *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*. Ed. by Hamed Hatami, Pierre McKenzie, and Valerie King. ACM, 2017, pp. 941–953. DOI: 10.1145/3055399.3055434. URL: https://doi.org/10.1145/3055399.3055434.

[66] B. Riemann. “Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse”. In: *Bernard Riemann’s gesammelte mathematische Werke und wissenschaftlicher Nachlass*. Ed. by Richard Dedekind and Heinrich MartinEditors Weber. Cambridge Library Collection - Mathematics. Cambridge University Press, 2013, pp. 136–144.

[67] RobHar. *Discriminant49CubicFieldFundamentalDomain.png*. 2010. URL: https://commons.wikimedia.org/wiki/File:Discriminant49CubicFieldFundamentalDomain.png#.

[68] C. Schnorr. “A Hierarchy of Polynomial Time Lattice Basis Reduction Algorithms”. In: *Theor. Comput. Sci.* 53 (1987), pp. 201–224. URL: https://api.semanticscholar.org/CorpusID:205092716.

[69] R. Schoof. “Class numbers of real cyclotomic fields of prime conductor”. In: *Math. Comput.* 72 (2003), pp. 913–937.

[70] R. Schoof. *Quadratic fields and factorization*. 1982.

[71] R. Schoof and M. van der Vlugt. “Hecke operators and the weight distributions of certain codes”. In: *J. Comb. Theory, Ser. A* 57 (1991), pp. 163–186. URL: https://api.semanticscholar.org/CorpusID:16047318.

[72] M. Seysen. “A probabilistic factorization algorithm with quadratic forms of negative discriminant”. In: *Mathematics of Computation* 48 (1987), pp. 757–780.

[73] D. Shanks. “Class number, a theory of factorization, and genera”. In: *Proceedings of Symposia in Pure Mathematics*. Ed. by W. J. LeVeque and E. G. Straus. Vol. 20. American Mathematical Society, 1969, pp. 415–440.

[74] D. Shanks. “The infrastructure of a real quadratic field and its applications”. In: *Proceedings of the 1972 Number Theory Conference*. Boulder: University of Colorado: American Mathematical Society, 1972, pp. 217–224.

[75] D. Simon. “Équations dans les Corps de Nombres et Discriminants Minimaux,thése”. PhD thesis. University of Bordeaux, 1998.

[76] D. Simon. “Solving norm equations in relative number fields using S-units”. In: *Math. Comput.* 71 (July 2002), pp. 1287–1305. DOI: 10.1090/S0025-5718-02-01309-1.

[77] N. Smart and F. Vercauteren. “Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes”. In: *Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010. Proceedings*. Ed. by Phong Q. Nguyen and David Pointcheval. Vol. 6056. Lecture Notes in Computer Science. Springer, 2010, pp. 420–443. DOI: 10.1007/978-3-642-13013-7_25. URL: https://doi.org/10.1007/978-3-642-13013-7%5C_25.

[78] A. Srinivasan. “Computations of Class Numbers of Real Quadratic Fields”. In: *Mathematics of Computation* 67.223 (1998), pp. 1285–1308. ISSN: 00255718, 10886842. (Visited on 03/21/2024).

[79] A. Storjohann. “The shifted number system for fast linear algebra on integer matrices”. In: *J. Complex.* 21.4 (2005), pp. 609–650. DOI: 10.1016/j.jco.2005.04.002.

[80] The PARI Group. *PARI/GP*. Version 2.13.1. 2021. URL: https://pari.math.u-bordeaux.fr/.

[81] U. Vollmer. “An Accelerated Buchmann Algorithm for Regulator Computation in Real Quadratic Fields”. In: *Algorithmic Number Theory, 5th International Symposium, ANTS-V, Sydney, Australia, July 7-12, 2002, Proceedings*. Ed. by Claus Fieker and David R. Kohel. Vol. 2369. Lecture Notes in Computer Science. Springer, 2002, pp. 148–162. DOI: 10.1007/3-540-45455-1_12. URL: https://doi.org/10.1007/3-540-45455-1%5C_12.

[82] U. Vollmer. “Asymptotically Fast Discrete Logarithms in Quadratic Number Fields”. In: *Algorithmic Number Theory, 4th International Symposium, ANTS-IV, Leiden, The Netherlands, July 2-7, 2000, Proceedings*. Ed. by Wieb Bosma. Vol. 1838. Lecture Notes in Computer Science. Springer, 2000, pp. 581–594. DOI: 10.1007/10722028_39. URL: https://doi.org/10.1007/10722028%5C_39.

[83] C. Walter. “Kuroda’s class number relation”. eng. In: *Acta Arithmetica* 35.1 (1979), pp. 41–51. URL: http://eudml.org/doc/205624.

[84] L. Washington. *Introduction to Cyclotomic Fields*. Graduate Texts in Mathematics. Springer New York, 1997. ISBN: 9780387947624. URL: https://books.google.com/books?id=qea_OXafBFoC.

[85] F. White. “Disquisitiones Arithmeticae. By Carl Friedrich Gauss. Translated by A. A. Clarke, S. J. Pp. xx, 472. £4. 10s. 1966. (Yale University Press.)” In: *The Mathematical Gazette* 51.375 (1967), pp. 89–89. DOI: 10.2307/3613672.

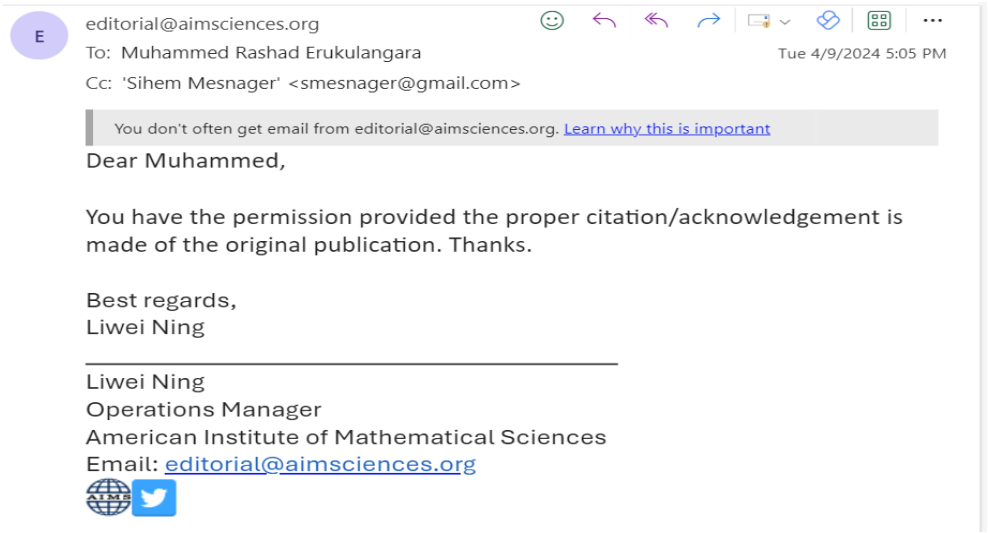
APPENDIX A

AMC LICENSE

Chapter 4 and some part of Section 3.2 are based on collaborative research with Jean-François Biasse, published in Advances in Mathematics of Communications (AMC) [13].

Jean-François Biasse and Muhammed Rashad Erukulangara. "A proof of the conjectured run time of the Hafner-McCurley class group algorithm." In: Advances in Mathematics of Communications (AMC) 17 (Jan. 2021). DOI: https://doi.org/10.3934/amc.2021055.

The following is the permission I received from AMC to include the published paper [13] in this dissertation.



E

editorial@aimsciences.org

To: Muhammed Rashad Erukulangara

Tue 4/9/2024 5:05 PM

Cc: 'Sihem Mesnager' <smesnager@gmail.com>

You don't often get email from editorial@aimsciences.org. Learn why this is important

Dear Muhammed,

You have the permission provided the proper citation/acknowledgement is made of the original publication. Thanks.

Best regards,
Liwei Ning

Liwei Ning
Operations Manager
American Institute of Mathematical Sciences
Email: editorial@aimsciences.org

APPENDIX B

MC LICENSE

The content of Chapter 5 is based on collaborative work with Jean-François Biasse, William Youmans, Claus Fieker, Tommy Hofmann, and myself, which was published in Mathematical Cryptology(MC) [19].

Jean-François Biasse et al. "Mildly Short Vectors in Ideals of Cyclotomic Fields Without Quantum Computers". In: Mathematical Cryptology 2.1 (Nov. 2022), pp. 84–107. url: https://journals.flvc.org/mathcryptology/article/view/132573