5-2009

Class Numbers of Ray Class Fields of Imaginary Quadratic Fields

Omer Kucuksakalli
University of Massachusetts Amherst, komer@metu.edu.tr

CLASS NUMBERS OF RAY CLASS FIELDS OF IMAGINARY QUADRATIC FIELDS

A Dissertation Presented

by

OMER KUCUKSAKALLI

Submitted to the Graduate School of the
University of Massachusetts Amherst in partial fulfillment
of the requirements for the degree of

DOCTOR OF PHILOSOPHY

May 2009

Department of Mathematics and Statistics

CLASS NUMBERS OF RAY CLASS FIELDS OF IMAGINARY QUADRATIC FIELDS

A Dissertation Presented

by

OMER KUCUKSAKALLI

Approved as to style and content by:

Siman Wong, Chair

Farshid Hajir, Member

Tom Weston, Member

Robert Moll, Member

George Avrunin, Department Head
Mathematics and Statistics

ACKNOWLEDGMENTS

First and foremost, I would like to thank my advisor Siman Wong, without whom this thesis would not have been possible.

I would like to thank Farshid Hajir, Tom Weston and Robert Moll for being on my thesis committee. Special thanks to Farshid and Tom who have been responsible for large portions of my graduate education.

The Mathematics Department has been very kind and supportive of me throughout my years here, both financially and personally. I have received excellent advice and help from faculty and staff members.

Last but not least, I thank my family, whose love and support have accompanied me throughout my life.

ABSTRACT

CLASS NUMBERS OF RAY CLASS FIELDS OF IMAGINARY QUADRATIC FIELDS

MAY 2009

OMER KUCUKSAKALLI

B.S., MIDDLE EAST TECHNICAL UNIVERSITY

M.S., UNIVERSITY OF MASSACHUSETTS AMHERST

Ph.D., UNIVERSITY OF MASSACHUSETTS AMHERST

Directed by: Professor Siman Wong

Let K be an imaginary quadratic field with class number one and let $\mathfrak{p} \subset \mathcal{O}_K$ be a degree one prime ideal of norm p not dividing $6d_K$. In this thesis we generalize an algorithm of Schoof to compute the class number of ray class fields $K_{\mathfrak{p}}$ heuristically. We achieve this by using elliptic units analytically constructed by Stark and the Galois action on them given by Shimura's reciprocity law. We have discovered a very interesting phenomena where p divides the class number of $K_{\mathfrak{p}}$. This is a counterexample to the elliptic analogue of a well-known conjecture, namely the Vandiver's conjecture.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Computation of the class number of a number field is one of the most classical problems in number theory. The class number is a powerful invariant which can be used to investigate the integer solutions of polynomials. A well-known example is Fermat's Last Theorem which states that the equation $x^p + y^p = z^p$ does not have any non-trivial solution for any odd prime p. In 1847, Kummer proved this famous theorem for primes p not dividing the class number of $\mathbf{Q}(\zeta_p)$, the pth cyclotomic field.

A number field L is a finite field extension of rational numbers which has two invariants measuring its complexity, the degree $[L : \mathbf{Q}]$ and the discriminant d_L of the extension. The class number h_L can be computed for extensions with small degree and discriminant; however the running time of general algorithms grows rapidly with the degree and the discriminant of the number field. One of the simplest and most important example of a number field is the pth cyclotomic field $\mathbf{Q}(\zeta_p)$, and its class number is not known for any prime p bigger than 113.

The number field $\mathbf{Q}(\zeta_p)$ can be obtained by adjoining to $\mathbf{Q}$, the coordinates of p-division points on the unit circle. Similarly, the ray class fields $K_{\mathfrak{p}}$ of imaginary quadratic fields K can be constructed from the coordinates of $\mathfrak{p}$-division points on an elliptic curve (see Theorem 2.4). Using analytical properties of modular

functions, Stark constructs elliptic units in $K_{\mathfrak{p}}$ and shows that these units generate a subgroup of the full unit group of index precisely the class number of $K_{\mathfrak{p}}$ [8]. This is an analogue of a well-known theorem for real cyclotomic fields $\mathbf{Q}_{(p)} = \mathbf{Q}(\zeta_p) \cap \mathbf{R}$ which was used by Schoof to heuristically compute their class numbers [7].

In our thesis, we extend Schoof's algorithm to investigate the class number of ray class fields $K_{\mathfrak{p}}$. We achieve this by using the elliptic units given by Stark and the explicit Galois action on these elliptic units given by Shimura's reciprocity law. We work with imaginary quadratic fields K with class number one and with degree one prime ideals $\mathfrak{p} \subset K$ of norm p less than 700; their corresponding ray class fields $K_{\mathfrak{p}}$ have degree as big as $p-1$ over $\mathbf{Q}$. The class number computation of such fields using general-purpose algorithm is far beyond the capacity of any current computer software.

1.1 Statement of the Main Results

Let K be an imaginary quadratic field with class number one and let $\mathfrak{p} \subset \mathcal{O}_K$ be a degree one prime ideal not dividing $6d_K$. In general it is difficult to determine the full unit group of number fields. However, for ray class fields $K_{\mathfrak{p}}$ it is possible to give explicitly a group of units $\mathcal{E}$, namely the elliptic units. It is a well-known fact the quotient

$$B_{K_{\mathfrak{p}}} = \mathcal{O}_{K_{\mathfrak{p}}}^* / \mathcal{E}$$

is finite and its order is equal to the class number of $K_{\mathfrak{p}}$.

Let $G_{K_{\mathfrak{p}}}$ be the Galois group of the extension $K_{\mathfrak{p}}/K$. Both groups $\mathrm{Cl}(K_{\mathfrak{p}})$ and $B_{K_{\mathfrak{p}}}$ are finite $\mathbf{Z}[G_{K_{\mathfrak{p}}}]$-modules and hence admit Jordan-Hölder filtration with simple factors. It turns out that their submodules with Jordan-Hölder factors of

fixed order q have the same number of elements as well. This fact enables us to work with $B_{K_\mathfrak{p}}$ instead for the purpose of investigating the class number of $K_\mathfrak{p}$. In our thesis, we have found all simple Jordan-Hölder factors of $B_{K_\mathfrak{p}}$ with "small" order. More precisely, we have the following result.

Theorem 1.1 *For each K, we give a table involving all simple Jordan-Hölder factors of order $q < 2000$ of $B_{K_\mathfrak{p}}$ for $\mathfrak{p} \subset \mathcal{O}_K$ of norm $p < 700$. Our tables also contain the number $\tilde{h}_{K_\mathfrak{p}}$, the order of the largest submodule of $B_{K_\mathfrak{p}}$ (and therefore of $Cl(K_\mathfrak{p})$) all of whose Jordan-Hölder factors have order less than 2000.*

It easily follows that the numbers $\tilde{h}_{K_\mathfrak{p}}$ divide the class number of $K_\mathfrak{p}$ since it is the order of a subgroup. Moreover our computation implies that either

$$\#\mathrm{Cl}(K_\mathfrak{p}) = \tilde{h}_{K_\mathfrak{p}} \qquad \text{or} \qquad \#\mathrm{Cl}(K_\mathfrak{p}) > 2000 \cdot \tilde{h}_{K_\mathfrak{p}},$$

but we do not know for sure the class number of $K_\mathfrak{p}$ for any $\mathfrak{p}$ of norm $p > 40$. However, according to Cohen-Lenstra heuristics, the bigger the Jordan-Hölder factor, the lower its chance to appear in the filtration of $\mathrm{Cl}(K_\mathfrak{p})$. This allows us to show that (following Schoof) the number $\tilde{h}_{K_\mathfrak{p}}$ is actually the class number of $K_\mathfrak{p}$ heuristically.

We have discovered a very interesting phenomena where p divides the class number of $K_\mathfrak{p}$. This is a counterexample to the elliptic analogue of a well-known conjecture in the theory of cyclotomic number fields, namely the Vandiver's conjecture.

Counterexample 1.2 *Let K be the imaginary quadratic field $\mathbf{Q}(\sqrt{-163})$. The class number of $K_{\mathfrak{p}_{307}}$ is divisible by 307 where $\mathfrak{p}_{307} \subset \mathcal{O}_K$ is a degree one prime ideal of norm 307.*

We give a detailed explanation about the analogy between $\mathbf{Q}_{(p)}$ and $K_{\mathfrak{p}}$ in Section 2.2 and about the counterexample in Section 5.1.

1.2 Outline of the Thesis

In chapter 2, we provide the necessary background material for our thesis. We first describe finite Galois modules and their duals for a cyclic group. We also give a description of their Jordan-Hölder filtration. Secondly, we describe the ray class fields $\mathbf{Q}_{(p)}$ and $K_{\mathfrak{p}}$ and the analogy between them. In the last section we define modular functions $\phi(u, v, z)$ by infinite products and explain how to compute them with high accuracy. We also state the Shimura's reciprocity law which enables us to construct Stark's elliptic units.

In chapter 3, we give a summary of Schoof's algorithm for real cyclotomic fields. We reformulate Schoof's original steps so that the elliptic analogue will be easier to explain. The algorithm we give here is slower than the original since we do not make use of a property of cyclotomic units which is not available for the elliptic units.

In chapter 4, which is the key technical part of our thesis, we provide the elliptic analogue of Schoof's algorithm. In the first section, we construct elliptic units and give the Galois action on them using Shimura's reciprocity law. In the second section we explain how to reformulate the results in the cyclotomic case so that we obtain their elliptic analogues. In the third section we explain our algorithm and give an example. In the last section we apply Cohen-Lenstra heuristics to our case and argue that each table we give at the end is a table of class numbers with probability at least 96%.

In chapter 5, we explain the results based on the data we collect from our

algorithm. In the first section we give a counterexample to the elliptic analogue of Vandiver's conjecture. In the second section, we give a table for each K involving the order of the largest submodule of $B_{K_\mathfrak{p}}$ with Jordan-Hölder factors of order less than 2000. We explain how to obtain structure of $(B_{K_\mathfrak{p}})_\varphi$ for each Jordan-Hölder factor listed in the tables. We also give an example showing that $B_{K_\mathfrak{p}}$ and $\mathrm{Cl}(K_\mathfrak{p})$ are not isomorphic as Galois modules.

In the last chapter, we mention about two future projects which are natural generalizations of our thesis.

CHAPTER 2

BACKGROUND MATERIAL

In this chapter, we provide the necessary background material for our thesis. We first describe finite Galois modules and their duals for a cyclic group. We also give a description of their Jordan-Hölder filtration. Secondly we describe the ray class fields $\mathbf{Q}_{(p)}$ and $K_{\mathfrak{p}}$ and the analogy between them. In the last section we define modular functions $\phi(u, v, z)$ by infinite products and explain how to compute them with high accuracy. We also state the Shimura's reciprocity law which enables us to construct Stark's elliptic units.

2.1 Galois Modules

Let R be a finite commutative ring. For any R-module A, the additive groups

$$A^{\perp} := \mathrm{Hom}_R(A, R) \qquad A^{\mathrm{dual}} := \mathrm{Hom}_{\mathbf{Z}}(A, \mathbf{Q}/\mathbf{Z})$$

are R-modules via $(\lambda f)(a) = \lambda f(a) = f(\lambda a)$ for $\lambda \in R$ and $a \in A$. The ring R is called *Gorenstein* if the R-module R^{dual} is free of rank 1 over R.

Proposition 2.1 *Let R be a finite Gorenstein ring. Then*

1. *For every R-module A, the map*

$$A^{\perp} \longrightarrow A^{dual}$$

defined by $f \mapsto \chi \circ f$ *is an isomorphism of* R*-modules where* $\chi : R \longrightarrow \mathbf{Q}/\mathbf{Z}$ *is a generator of* R^{dual}.

2. *The functor* $A \mapsto A^{\perp}$ *from the category of finite* R*-modules to itself is exact. Moreover* $(A^{\perp})^{\perp} \cong A$.

Proof. See Schoof [7, Proposition 1.1]. ◇

Let G be a cyclic group then for any integer $M > 1$ the group ring $R = (\mathbf{Z}/M\mathbf{Z})[G]$ is Gorenstein, . For such rings we can make the isomorphism in Proposition 2.1 (1) more explicit by fixing a generator

$$\chi : \sum_{\sigma \in G} c_\sigma \sigma \longmapsto c_1$$

for the R-module R^{dual}. Here c_1 is the coefficient of the identity element $1 \in G$.

In order to apply Schoof's algorithm, we need to work with duals. The following proposition gives us the necessary connection between R-modules and their duals.

Proposition 2.2 *Let* R *be a finite Gorenstein ring and* $I \subset R$ *be an ideal. Then we have the following:*

1. *Any finite* R*-module is Jordan-Hölder isomorphic to its dual.*

2. *The modules* R/I *and* $(R/I)^{\perp}$ *are isomorphic* R*-modules if and only if* $Ann_R(I)$ *is principal.*

3. *If* R/I *has a Jordan-Hölder filtration of length at most 2, then* $(R/I)^{\perp} \cong R/I$.

4. *Suppose that there are an ideal* $J \subset R$ *and a surjection* $g : R/J \twoheadrightarrow I^{\perp}$ *with the property that* $Ann_R(J)$ *annihilates* R/I. *Then* $J = Ann_R(I)$ *and* g *is an isomorphism.*

Proof. See Schoof [7, Proposition 1.2]. ◇

Let G be a cyclic group of order n and let A be a finite $\mathbf{Z}[G]$-module. Now we give the Jordan-Hölder filtration of A using Schoof's description [7, Section 3]. We first decompose A as a product of its l-parts $A \otimes \mathbf{Z}_l$ where $\mathbf{Z}_l$ is the l-adic integers for prime l. Each l-part is a module over the ring $\mathbf{Z}_l[G]$, which is isomorphic to the polynomial ring $\mathbf{Z}_l[X]/(X^n - 1)$. Let us write $n = l^a m$ with the property $\gcd(m, l) = 1$ and decompose $X^m - 1$ in the polynomial ring $\mathbf{Z}_l[X]$. We have

$$X^m - 1 = \prod_{\varphi} \varphi(X)$$

where $\varphi(X) \in \mathbf{Z}_l[X]$ are irreducible polynomials. This gives rise to natural isomorphisms of $\mathbf{Z}_l$-algebras

$$\begin{aligned} \mathbf{Z}_l[G] &\cong \mathbf{Z}_l[X]/(X^{l^a m} - 1) \\ &\cong \prod_{\varphi} \mathbf{Z}_l[X]/\left(\varphi(X^{l^a})\right). \end{aligned}$$

This decomposition of the ring $\mathbf{Z}_l[G]$ enables us to make each l-part into smaller pieces. We have $A \otimes \mathbf{Z}_l = \prod_{\varphi} A_{\varphi}$ where

$$A_{\varphi} = (A \otimes \mathbf{Z}_l) \otimes_{\mathbf{Z}_l[G]} \left(\mathbf{Z}_l[X]/\left(\varphi(X^{l^a})\right)\right).$$

Therefore we have a filtration of the finite $\mathbf{Z}[G]$-module A given by

$$A = \prod_{l} \prod_{\varphi} A_{\varphi}$$

where each A_{φ} is a module over the corresponding $\mathbf{Z}_l[G]$-algebra $\mathbf{Z}_l[X]/\left(\varphi(X^{l^a})\right)$. The submodule A_{φ} admits a further filtration with simple subquotients, all of which are isomorphic to the residue field $\mathbf{F}_q = F_l[X]/(\varphi(X))$.

The residue fields of the ring $\mathbf{Z}[G]$ are precisely the residue fields of the various local rings $\mathbf{Z}_l[X]/(\varphi(X^{l^a}))$. Every finite $\mathbf{Z}[G]$-module A admits a Jordan-Hölder

filtration whose simple factors are one-dimensional vector spaces over these residue fields. The *order* of such a simple Jordan-Hölder factor is the order $q = l^f$ of the residue field and its *degree* d is the order of X modulo $\varphi(X)$. This implies that d divides n, the order of the cyclic group G. The order of l modulo d is equal to f. Therefore d divides $q-1$ as well. Combining these two facts we obtain

$$d | \gcd(n, q-1)$$

and this becomes useful in the first step of both Schoof's algorithm and its elliptic analogue (see Sections 3.3 and 4.3).

2.2 Ray Class Fields $\mathbf{Q}_{(p)}$ and $K_{\mathfrak{p}}$

Given a number field K, a *modulus* in K is a formal product $\mathfrak{m} = \prod \mathfrak{p}^{n_{\mathfrak{p}}}$ over all primes $\mathfrak{p}$, finite or infinite, of K. A modulus $\mathfrak{m}$ can be written as $\mathfrak{m}_0\mathfrak{m}_\infty$ where $\mathfrak{m}_0$ is an ideal of $\mathcal{O}_K$ and $\mathfrak{m}_\infty$ is a product of distinct real infinite primes of K. If K is an imaginary quadratic field, then there is no real infinite prime. Therefore it is enough to consider a modulus of an imaginary quadratic field K to be an ideal of $\mathcal{O}_K$.

Let $I_K(\mathfrak{m})$ be the group of all fractional $\mathcal{O}_K$-ideals relatively prime to $\mathfrak{m}$ and let $P_{K,1}(\mathfrak{m})$ be its subgroup generated by principal ideals (α) where $\alpha \in \mathcal{O}_K$ satisfies $\alpha \equiv 1 \bmod \mathfrak{m}_0$ and $\nu(\alpha) > 0$ for every $\nu | \mathfrak{m}_\infty$. A subgroup $H \subset I_K(\mathfrak{m})$ is called a *congruence subgroup* for $\mathfrak{m}$ if it satisfies $P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m})$ and the quotient $I_K(\mathfrak{m})/H$ is called a *generalized ideal class group* for $\mathfrak{m}$.

Class field theory gives us a connection between generalized ideal class groups and all Abelian extensions of K. The link between these two is provided by the Artin map. Let $\mathfrak{m}$ be a modulus divisible by all ramified primes of an Abelian

extension L/K. Given a prime $\mathfrak{q}$ not dividing $\mathfrak{m}$, we denote the *Artin symbol* by $\sigma_{\mathfrak{q}}$ which is the unique element in $\mathrm{Gal}(L/K)$ satisfying $\sigma_{\mathfrak{q}}(\alpha) \equiv \alpha^{N(\mathfrak{q})} \pmod{\mathfrak{q}}$ for all $\alpha \in \mathcal{O}_L$. The Artin symbol can be extended by multiplication to give a homomorphism which is called the *Artin map* of $K \subset L$ of modulus $\mathfrak{m}$.

Theorem 2.3 (Existence Theorem) *Let $\mathfrak{m}$ be a modulus of K, and let H be a congruence subgroup for $\mathfrak{m}$. Then there is a unique Abelian extension L of K, all of whose ramifies primes divide $\mathfrak{m}$ such that if*

$$\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow Gal(L/K)$$

is the Artin map of $K \subset L$, then $H = Ker(\Phi_{\mathfrak{m}})$

Proof. See Janusz [2, Chapter V, Theorem 9.16] ◇

Given any modulus $\mathfrak{m}$, the unique Abelian extension $K_{\mathfrak{m}}$ of K such that $P_{K,1}(\mathfrak{m}) = \mathrm{Ker}(\Phi_{\mathfrak{m}})$ is called the *ray class field* of conductor $\mathfrak{m}$. When $\mathfrak{m} = (1)$ the ray class field $K_{(1)}$ is the Hilbert class field, the maximal unramified Abelian extension of K.

Let us consider the ray class field $\mathbf{Q}_{(p)}$ of conductor $(p) \subset \mathbf{Z}$ where p is an odd prime. Since $\mathbf{Q}_{(p)}$ is an Abelian extension of $\mathbf{Q}$, there exists an integer n such that $L \subset \mathbf{Q}(\zeta_n)$, by the Kronecker-Weber Theorem [10, Theorem 14.1].

Let q be a rational prime different than p. The action of Artin symbol σ_q is given by $\sigma_q(\zeta_n) = \zeta_n^q$. We want the kernel of the Artin map to be $P_{\mathbf{Q},1}(p)$, which is the set of principal ideals generated by elements $\alpha \equiv 1 \pmod{p}$. This implies that n divides p and therefore $\mathbf{Q}_{(p)}$ is a subfield of the p-th cyclotomic field $\mathbf{Q}(\zeta_p)$.

Observe that any ideal class in the ray class group $I_{\mathbf{Q}}(p)/P_{\mathbf{Q},1}(p)$ can be represented by $[m\mathbf{Z}]$ where m is an integer relatively prime to p. Moreover two ideals classes $[m\mathbf{Z}]$ and $[m'\mathbf{Z}]$ are identical if only if $m \equiv \pm m' \pmod{p}$. This implies that

the ray class group, and therefore $\mathrm{Gal}(\mathbf{Q}_{(p)}/\mathbf{Q})$, has $(p-1)/2$ elements. Hence $\mathbf{Q}_{(p)}$ must be $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$, the p-th real cyclotomic field.

The main tool we use here to determine the ray class field $\mathbf{Q}_{(p)}$ is the Kronecker-Weber Theorem. This theorem enables us to analytically construct a generator for all Abelian extensions of $\mathbf{Q}$. In general it is not easy to do this for an arbitrary ground field. However in the case of imaginary quadratic fields we have the following theorem.

Theorem 2.4 *Let K be an imaginary quadratic field and let $\mathfrak{m}$ be a modulus in K. Then $K_{\mathfrak{m}} = K(j(\mathcal{O}_K), h((\mathbf{C}/\mathcal{O}_K)[\mathfrak{m}]))$ where $j(\mathcal{O}_K)$ is the j-invariant and h is the Weber function.*

Proof. See Lang [4, Chapter 10, Theorem 2]. ◇

Given an imaginary quadratic field K, we can consider $\mathcal{O}_K$ as a lattice embedded in complex numbers $\mathbf{C}$. The quotient $\mathbf{C}/\mathcal{O}_K$ is topologically a torus. The Weierstrass $\wp$-function gives a connection between $\mathbf{C}/\mathcal{O}_K$ and an elliptic curve E. We have

$$\begin{array}{ccc} \mathbf{C}/\mathcal{O}_K & \longrightarrow & E \\ z & \longmapsto & [\wp(z), \wp'(z)]. \end{array}$$

The curve E is given by the equation

$$y^2 = 4x^3 + g_2 x + g_3$$

where g_2 and g_3 are invariants of the lattice $\mathcal{O}_K$. The division points $(\mathbf{C}/\mathcal{O}_K)[\mathfrak{m}] = \{z \in \mathbf{C} : z\mathfrak{m} \subset \mathcal{O}_K\}$ can be mapped to E under this map. However these values are not invariant enough. By a suitable normalization, one can define the Weber function $h(z)$ which is closely related to the x-coordinate projection. In the generic case (i.e. when $d_K \neq -3, -4$) it is given by

$$h(z) = \frac{g_2 g_3}{\Delta} \wp(z)$$

where the discriminant Δ is equal to $g_2^3 - 27g_3^2$.

Suppose that K is an imaginary quadratic field with class number one. Then the j-invariant of $\mathcal{O}_K$ is rational. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a degree one prime ideal not dividing $6d_K$. Theorem 2.4 implies that

$$K_{\mathfrak{p}} = K(h((C/\mathcal{O}_K)[\mathfrak{p}]))$$

and this reminds us the geometric construction of real cyclotomic fields. Similar to the quotient $\mathbf{C}/\mathcal{O}_K$, consider the quotient $\mathbf{R}/\mathbf{Z}$ where $\mathbf{Z}$ is the ring of integers of $\mathbf{Q}$. It is topologically a circle and the cosine function, together with its derivative, gives a connection between $\mathbf{R}/\mathbf{Z}$ and the unit circle as follows.

$$\begin{array}{ccc} \mathbf{R}/\mathbf{Z} & \longrightarrow & C \\ t & \longmapsto & [\cos(2\pi t), -\sin(2\pi t)] \end{array}$$

Here the cosine function is in the same role of Weierstrass $\wp$-function. Observe that the real cyclotomic field $\mathbf{Q}_{(p)}$ is obtained by adjoining

$$\zeta_p + \zeta_p^{-1} = 2\cos(2\pi/p)$$

to the ground field $\mathbf{Q}$. In other words $\mathbf{Q}_{(p)}$ is obtained by adjoining the x-coordinate of the image of a p-division point in $(\mathbf{R}/\mathbf{Z})[p]$.

The ray class field $K_{\mathfrak{p}}$ is constructed from a CM elliptic curve in the same way the real cyclotomic field is constructed from a circle. Therefore we refer $K_{\mathfrak{p}}$ as the elliptic analogue of real cyclotomic fields.

2.3 Modular Functions

The computation of Stark's elliptic units (see Section 4.1) relies on the family of modular functions defined by

$$\phi(u,v,z) := -ie^{\pi iz/6}e^{\pi iu\gamma}(e^{\pi i\gamma}-e^{-\pi i\gamma})\prod_{m=1}^{\infty}(1-e^{2\pi i(mz+\gamma)})(1-e^{2\pi i(mz-\gamma)}),$$

where $\gamma = uz+v$ and z is an element in the upper half plane.

Proposition 2.5 *The function $\phi(u,v,z)$ satisfies the following transformation properties.*

1. $\phi(u,v+1,z) = -e^{\pi iu}\phi(u,v,z)$
2. $\phi(u+1,v,z) = -e^{-\pi iv}\phi(u,v,z)$
3. $\phi(u,v,z+1) = e^{\pi i/6}\phi(u,u+v,z)$
4. $\phi(u,v,-1/z) = e^{-\pi i/2}\phi(v,-u,z)$

Proof. These properties follow from Kronecker's second limit formula. See Stark [8, p. 205-208] for details. ◇

The group $\Gamma = SL_2(\mathbf{Z})/\{\pm I\}$ is called the *modular group* and it is generated by matrices $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. If $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is an element in Γ then it acts on the upper half plane by

$$Az = \frac{az+b}{cz+d}.$$

Let $n > 1$ be a fixed integer and let r, s be integers such that $\gcd(r,s,n) = 1$. Observe that the function $\phi(r/n, s/n, z)$ is invariant under the action of $A \in \Gamma$ if $A \equiv \pm I \pmod{12n^2}$. By definition $\phi(r/n, s/n, z)$ is a modular function(in z) of level $N = 12n^2$.

Let $\mathcal{F}_N$ be the field of all modular functions of level N whose q_z-expansions, where $q_z = e^{2\pi iz/N}$, have coefficients in $\mathbf{Q}(\zeta_N)$. The field $\mathcal{F}_N$ is a Galois extension of $\mathcal{F}_1 = \mathbf{Q}(j)$ with Galois group isomorphic to $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})/\{\pm I\}$. Given

$$f(z) = \sum_{m=m_0}^{\infty} \alpha_m q_z^m \in \mathcal{F}_N,$$

there are two basic rules for calculating $f \circ A$. If $A \in \Gamma$, then

$$(f \circ A)(z) = f(Az) = \sum_{m=m_0}^{\infty} \alpha_m q_{Az}^m$$

and if $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$, then

$$(f \circ A)(z) = (f \circ \sigma_d)(z) = \sum_{m=m_0}^{\infty} \alpha_m^{\sigma_d} q_z^m.$$

where σ_d is the automorphism of $\mathbf{Q}(\zeta_N)/\mathbf{Q}$ given by $\zeta_N^{\sigma_d} = \zeta_N^d$. Now we give the reciprocity law.

Theorem 2.6 (Shimura's Reciprocity Law) *Let K be an imaginary quadratic field and let $f(z) \in \mathcal{F}_N$ be a modular function of level N. Suppose q is a rational prime not dividing Nd_K such that $q\mathcal{O}_K = \mathfrak{q}\bar{\mathfrak{q}}$. Suppose that $\mathfrak{a} = [\mu, \nu]$ is a fractional ideal of K with $\theta = \mu/\nu$ in the upper half plane and let $B\binom{\mu}{\nu} = \binom{\mu'}{\nu'}$ be a basis for $\bar{\mathfrak{q}}\mathfrak{a}$. Then $f(\theta)$ is in the ray class field $K_{(N)}$ and*

$$f(\theta)^{\sigma_{\mathfrak{q}}} = [f \circ (qB^{-1})](\theta')$$

where $\theta' = \mu'/\nu'$.

Proof. See Stark [8, Theorem 3]. ◇

In order to compute Stark's elliptic units (see Section 4.1), we need to compute $\phi(u, v, z)$ with high precision for values $z = \theta$ given by Shimura's reciprocity law.

It turns out that it is possible to pick $v = 0$ in order to compute generators of the group of elliptic units $\mathcal{E}$ (see lemma 4.3). We have

$$\phi(u, 0, \theta) = -i\tau^{\frac{6u^2-6u+1}{12}}(1-\tau^u)\prod_{m=1}^{\infty}(1-\tau^{m+u})(1-\tau^{m-u})$$

where $\tau = e^{2\pi i\theta}$. One can obtain an approximation of $\phi(u, 0, \theta)$ by using the first M terms of the infinite product above. We want to determine the value of M to assure a certain level of accuracy.

Proposition 2.7 *We have the following bounds*

$$e^{B(M)} > \left|\prod_{m=M+1}^{\infty}(1-\tau^m)\right| > e^{-B(M)}$$

where

$$B(M) = \frac{|\tau|^{M+1}}{(1-|\tau|)(1-|\tau|^{M+1})}.$$

Proof. We start by taking the logarithm

$$\log\left|\prod_{m=M+1}^{\infty}(1-\tau^m)\right| = \sum_{m=M+1}^{\infty}\log|1-\tau^m|.$$

Then we use the inequality $|1-\tau^m| > 1-|\tau|^m$ and the Taylor series expansion $\log(1-x) = -\sum\frac{x^n}{n}$ to get

$$\begin{aligned}\sum_{m=M+1}^{\infty}\log|1-\tau^m| &> \sum_{m=M+1}^{\infty}\log(1-|\tau|^m)\\ &= -\sum_{m=M+1}^{\infty}\sum_{n=1}^{\infty}\frac{|\tau|^{mn}}{n}.\end{aligned}$$

Rearranging the terms and applying the summation formula for geometric series twice, we obtain

$$\begin{aligned}-\sum_{m=M+1}^{\infty}\sum_{n=1}^{\infty}\frac{|\tau|^{mn}}{n} &= -\sum_{n=1}^{\infty}\frac{1}{n}\sum_{m=M+1}^{\infty}|\tau|^{nm}\\ &= -\sum_{n=1}^{\infty}\frac{1}{n}\frac{|\tau|^{n(M+1)}}{1-|\tau|^n}\\ &> -\sum_{n=1}^{\infty}\frac{|\tau|^{n(M+1)}}{1-|\tau|} = -B(M).\end{aligned}$$

This finishes the proof of the bound on the right hand side. The proof for the other side is similar. $\diamond$

We should use θ with imaginary part as big as possible so that our approximation is better with the same number of terms. Let $A \in \Gamma$ such that $A\theta$ is in the fundamental domain $D = \{z \in \mathbf{C} : \mathrm{Im}(z) > 0, |z| \geq 1, |\mathrm{Re}(z)| \leq 1/2\}$. The transformation properties (3) and (4) given in Proposition 2.5 implies that

$$\phi(u, v, \theta) = \omega(A)\phi((u, v)A^{-1}, A\theta)$$

where $\omega(A)$ is a 12-th root of unity which can be obtained from the decomposition of A in terms of the generators $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ of Γ.

Without loss of generality, we assume that θ is in the fundamental domain D. This implies that the imaginary part of θ is bigger than $\sqrt{3}/2$ and therefore

$$|\tau| < e^{-\pi\sqrt{3}} \approx 0.00433342.$$

The second property given in Proposition 2.5 implies that $\phi(u+2, 0, \theta) = \phi(u, 0, \theta)$, hence we pick u with the property $0 < u < 2$. We use the first M terms in the infinite product to approximate $\phi(u, 0, \theta)$ and the corresponding error is

$$E(M) = \left| \prod_{m=M+1}^{\infty} (1 - \tau^{m+u})(1 - \tau^{m-u}) \right|.$$

Proposition 2.7 implies that

$$e^{2B(M-2)} > E(M) > e^{-2B(M-2)}.$$

In our computations, we want to work with values of $\phi(u, 0, \theta)$ which are accurate at least 500 decimal places. If we pick $M = 220$ then

$$E(M) \approx 1$$

with error less than 10^{-500}. Therefore it is enough to use the first 220 terms for the required precision.

CHAPTER 3

SCHOOF'S ALGORITHM

In this chapter, we give a summary of the algorithm which was used by Schoof to heuristically compute class numbers of real cyclotomic fields [7]. We state and rewrite all necessary steps in Schoof's paper in such a way that the elliptic curve analogue will be easy to explain. The algorithm we give here is slower than the original since we disregard a nice property of cyclotomic units which is not available for the elliptic units.

3.1 Cyclotomic Units

Let p be an odd prime then the p-th real cyclotomic field is given by $\mathbf{Q}(\zeta_p+\zeta_p^{-1})$. As we have shown in Section 2.2, it is the ray class field of $\mathbf{Q}$ for the modulus $(p) = p\mathbf{Z}$. Therefore we have $\mathbf{Q}_{(p)} = \mathbf{Q}(\zeta_p + \zeta_p^{-1})$ with Galois group

$$G_{\mathbf{Q}_{(p)}} \cong I_{\mathbf{Q}}(p)/P_{\mathbf{Q},1}(p)$$

by the class field theory. Observe that any ideal class in this quotient can be represented by $[m\mathbf{Z}]$ where m is an integer relatively prime to p. Moreover two ideals classes $[m\mathbf{Z}]$ and $[m'\mathbf{Z}]$ are identical if only if $m \equiv \pm m' \pmod{p}$. This implies that

$$G_{\mathbf{Q}_{(p)}} \cong (\mathbf{Z}/p\mathbf{Z})^*/\{\pm 1\}$$

which is cyclic of order $(p-1)/2$. Let m be an element of $(\mathbf{Z}/p\mathbf{Z})^*/\{\pm 1\}$. The action of the corresponding element in the Galois group is given by

$$\zeta_p + \zeta_p^{-1} \longmapsto \zeta_p^m + \zeta_p^{-m}$$

due to Artin map. Let g be a primitive root modulo p. Then the corresponding element σ_g in the Galois group generates the cyclic group $G_{\mathbf{Q}_{(p)}}$. Now we are ready to define cyclotomic units. The *group of cyclotomic units*, denoted by $\mathcal{C}$, is the multiplicative $\mathbf{Z}[G_{\mathbf{Q}_{(p)}}]$-module generated by the unit

$$\eta_g = \frac{\zeta_p^g - \zeta_p^{-g}}{\zeta_p - \zeta_p^{-1}}$$

where g is a primitive root modulo p. Observe that the group $\mathcal{C}$ does not depend on the choice g.

Lemma 3.1 *The group of cylotomic units $\mathcal{C}$ contains $\mu_{\mathbf{Q}} = \{\pm 1\}$, and we have an isomorphism*

$$\mathbf{Z}[G_{\mathbf{Q}_{(p)}}]/(N_{G_{\mathbf{Q}_{(p)}}}) \cong \mathcal{C}/\mu_{\mathbf{Q}}$$

where the $G_{\mathbf{Q}_{(p)}}$-norm map is defined by

$$N_{G_{\mathbf{Q}_{(p)}}} := \sum_{\sigma \in G_{\mathbf{Q}_{(p)}}} \sigma \in \mathbf{Z}[G_{\mathbf{Q}_{(p)}}].$$

Proof. Let g be a primitive root modulo p. The Galois group $G_{\mathbf{Q}_{(p)}}$ is cyclic of order $n = (p-1)/2$ and it is generated by the Artin symbol σ_g. The $G_{\mathbf{Q}_{(p)}}$-norm of η_g is given by

$$N_{G_{\mathbf{Q}_{(p)}}}(\eta_g) = \prod_{n=0}^{n-1} \sigma_g^i(\eta_g) = \prod_{n=0}^{n-1} \frac{\zeta_p^{g^{(i+1)}} - \zeta_p^{-g^{(i+1)}}}{\zeta_p^{g^i} - \zeta_p^{-g^i}}$$

and we obtain

$$N_{G_{\mathbf{Q}_{(p)}}}(\eta_g) = \frac{\zeta_p^{g^n} - \zeta_p^{-g^n}}{\zeta_p - \zeta_p^{-1}}$$

by cancelling the repeating terms. Since g is a primitive root modulo p, we have $g^n \equiv -1 \pmod{p}$. It follows that $N_{G_{\mathbf{Q}_{(p)}}}(\eta_g) = -1$ is a cyclotomic unit.

Now let us consider the $G_{\mathbf{Q}_{(p)}}$-homomorphism

$$\mathbf{Z}[G_{\mathbf{Q}_{(p)}}] \longrightarrow \mathcal{C}/\mu_{\mathbf{Q}}$$

given by $\varphi \mapsto \eta_g^{\varphi}$. The element φ is in the kernel of this map if only if it is a multiple of $N_{G_{\mathbf{Q}_{(p)}}}$. Therefore

$$\mathbf{Z}[G_{\mathbf{Q}_{(p)}}]/(N_{G_{\mathbf{Q}_{(p)}}}) \cong \mathcal{C}/\mu_{\mathbf{Q}}$$

as we have expected. ◇

Let us define the quotient group

$$B_{\mathbf{Q}_{(p)}} := \mathcal{O}^*_{\mathbf{Q}_{(p)}}/\mathcal{C} \tag{3.1}$$

which is a multiplicative $\mathbf{Z}[\mathbf{Q}_{(p)}]$-module. It is a well-known fact that the order of $B_{\mathbf{Q}_{(p)}}$ is equal to the class number of $\mathbf{Q}_{(p)}$. In fact we have something stronger.

Theorem 3.2 *Let H be a subgroup of $G_{\mathbf{Q}_{(p)}}$. Then we have*

$$\#Cl(\mathbf{Q}_{(p)}^H) = [(\mathcal{O}^*_{\mathbf{Q}_{(p)}})^H : \mathcal{C}^H].$$

Proof. A classical proof of this fact for $H = \{1\}$ can be found in [10, Theorem 8.2]. The more general result will follow, if the real cyclotomic field in the theorem is changed with $\mathbf{Q}_{(p)}^H$. However we follow Stark and give an alternative proof using the class number formula for $s = 0$. Our purpose is to give a motivation for the analogue of this theorem in the elliptic case.

For the field $\mathbf{Q}_{(p)}^H$, the class number formula [8, p. 200] reads

$$\#\mathrm{Cl}(\mathbf{Q}_{(p)}^H)\mathrm{Reg}\left((\mathcal{O}^*_{\mathbf{Q}_{(p)}})^H\right) = \prod_{\chi \neq 1} L'(0,\chi)$$

where the product runs over nontrivial characters of $\mathrm{Gal}(\mathbf{Q}_{(p)}^H/\mathbf{Q})$. Let e be the order of the subgroup H and suppose that $\#G_{\mathbf{Q}_{(p)}} = (p-1)/2 = e\tilde{e}$. The Galois group $\mathrm{Gal}(\mathbf{Q}_{(p)}^H/\mathbf{Q})$ is isomorphic to $G_{\mathbf{Q}_{(p)}}/H$ and it has order $\tilde{e}$. Indeed we have

$$\mathrm{Gal}(\mathbf{Q}_{(p)}^H/\mathbf{Q}) = \{\sigma_g^i|_{\mathbf{Q}_{(p)}^H} : 0 \leq i \leq \tilde{e}-1\}$$

which is obtained by restricting elements of $G_{\mathbf{Q}_{(p)}}$ to the subfield $\mathbf{Q}_{(p)}^H$. Each nontrivial character has conductor p and therefore is primitive. By [8, Theorem 2], we have

$$L'(0,\chi) = -\frac{1}{2}\sum_{i=1}^{\tilde{e}-1}\chi(\sigma_g^i)\log|N_H(\xi(i))|$$

where $N_H = \sum_{\tau\in H}\tau$ is the H-norm and

$$\xi(i) = (1-\zeta_p^{g^i})(1-\zeta_p^{-g^i})$$

is an element in $\mathbf{Q}_{(p)}$. Observe that $\log|\xi(i)| = 2\log|1-\zeta_p^{g^i}|$. We want to use the theory of group determinants. For this purpose, let us define

$$f : \sigma_g^i \longmapsto \log|N_H(1-\zeta_p^{g^i}))|$$

a function of $\mathrm{Gal}(\mathbf{Q}_{(p)}^H/\mathbf{Q})$. Now we have

$$\begin{aligned}
\#\mathrm{Cl}(\mathbf{Q}_{(p)}^H)\mathrm{Reg}\left((\mathcal{O}_{\mathbf{Q}_{(p)}}^*)^H\right) &= \prod_{\chi\neq 1}L'(0,\chi)\\
&= \pm\prod_{\chi\neq 1}\sum_{i=1}^{\tilde{e}-1}\chi(\sigma_g^i)f(\sigma^i)\\
&= \pm\det\left[f(\sigma_g^{i-j}) - f(\sigma_g^i)\right]_{i,j\neq 0}
\end{aligned}$$

where the last equality follows from [10, Lemma 5.26]. It is easy to see that

$$f(\sigma_g^{i-j}) - f(\sigma_g^i) = \log\left|N_H\left(\frac{1-\zeta_p^{g^{i-j}}}{1-\zeta_p^{g^i}}\right)\right|$$

and therefore the above determinant is equal to $\mathrm{Reg}(\mathcal{C}^H)$, the regulator of cyclotomic units in $\mathbf{Q}_{(p)}^H$. We have

$$\#\mathrm{Cl}(\mathbf{Q}_{(p)}^H)\mathrm{Reg}\left((\mathcal{O}_{\mathbf{Q}_{(p)}}^*)^H\right) = \mathrm{Reg}(\mathcal{C}^H)$$

and it follows that $\mathcal{C}^H$ is of finite index in the full unit group $\mathbf{Q}_{(p)}^H$ and this index is exactly the class number of $\mathbf{Q}_{(p)}^H$. ◇

3.2 Galois Module $B_{\mathbf{Q}_{(p)}}$

Both groups $B_{\mathbf{Q}_{(p)}}$ and $\mathrm{Cl}(\mathbf{Q}_{(p)})$ are finite $\mathbf{Z}[G_{\mathbf{Q}_{(p)}}]$-modules and hence admit Jordan-Hölder filtration with simple factors. Let B and C be the submodules of $B_{\mathbf{Q}_{(p)}}$ and $\mathrm{Cl}(\mathbf{Q}_{(p)})$, respectively, all of whose simple Jordan-Hölder factors have some fixed order $q = l^f$. It turns out that they have the same number of elements as well. I thank René Schoof for his useful remark for this fact. Before giving his explanation, we need to state the following result.

Proposition 3.3 *Let H be a subgroup of $G_{\mathbf{Q}_{(p)}}$. Then the sequence of H-invariants*

$$0 \longrightarrow \mathcal{C}^H \longrightarrow {\mathcal{O}_{\mathbf{Q}_{(p)}}^*}^H \longrightarrow B_{\mathbf{Q}_{(p)}}^H \longrightarrow 0$$

is exact. In particular $B_{\mathbf{Q}_{(p)}}^G = 0$.

Proof. See Schoof [7, Proposition 5.1 (i)]. ◇

Each submodule B or C is the product of the Jordan-Hölder factors of degree d, where d runs over the divisors of $(p-1)/2$ for which q is the smallest power of l that is congruent to 1 modulo d. Combining Theorem 3.2 with Proposition 3.3, we obtain

$$\#\mathrm{Cl}(\mathbf{Q}_{(p)}^H) = \#B_{\mathbf{Q}_{(p)}}^H.$$

The statement $\#B = \#C$ now follows from the fact that the degree d part of $\mathrm{Cl}(\mathbf{Q}_{(p)})$ (or $B_{\mathbf{Q}_{(p)}}$) is precisely the part that appears in the subfield of degree

$$d = \#\mathrm{Gal}(\mathbf{Q}_{(p)}^H/\mathbf{Q}),$$

but not in any proper subfield. This enables us to work with $B_{\mathbf{Q}_{(p)}}$ instead of $\mathrm{Cl}(\mathbf{Q}_{(p)})$ in order to investigate the class number of $\mathbf{Q}_{(p)}$.

It is difficult in general to predict which simple Jordan-Hölder factors the module $B_{\mathbf{Q}_{(p)}}$ admit. However we have the following general result.

Proposition 3.4 *Let $p > 2$ be a prime. The module $B_{\mathbf{Q}_{(p)}}$ does not admit any simple Jordan-Hölder factors of degree $d = 1$. In particular, it does not admit any such factors of order $q = 2$.*

Proof. By Proposition 3.3, the $G_{\mathbf{Q}_{(p)}}$-invariants of $B_{\mathbf{Q}_{(p)}}$ and hence of its l-part $B_{\mathbf{Q}_{(p)}} \otimes \mathbf{Z}_l$ is zero. This implies that $(B_{\mathbf{Q}_{(p)}} \otimes \mathbf{Z}_l)/(X-1)(B_{\mathbf{Q}_{(p)}} \otimes \mathbf{Z}_l)$ is zero and by Nakayama's Lemma the module

$$(B_{\mathbf{Q}_{(p)}} \otimes \mathbf{Z}_l)/(X^{l^a}-1)(B_{\mathbf{Q}_{(p)}} \otimes \mathbf{Z}_l)$$

is also zero. In other words $B_\varphi = 0$ for $\varphi = X - 1$.

The degree d of a simple Jordan-Hölder factor divides $q - 1$. This implies that if q is equal to 2 then d must be 1. Hence $B_{\mathbf{Q}_{(p)}}$ does not admit any Jordan-Hölder factor of order $q = 2$. ◇

The advantage of working with the module $B_{\mathbf{Q}_{(p)}}$ instead of $\mathrm{Cl}(\mathbf{Q}_{(p)})$ is that we can understand Jordan-Hölder factors of $B_{\mathbf{Q}_{(p)}}$ in an easier fashion. Before giving the main tool to investigate these factors, we first prove a lemma.

Lemma 3.5 *Let M be a power of a prime l and $F = \mathbf{Q}_{(p)}(\zeta_{2M})$. The kernel of the map*

$$\mathcal{O}^*_{\mathbf{Q}_{(p)}}/(\mathcal{O}^*_{\mathbf{Q}_{(p)}})^M \longrightarrow F^*/(F^*)^M$$

is trivial if l is odd. It has order 2 and is generated by -1 if $l = 2$

Proof. Let $\Delta = \mathrm{Gal}(F/\mathbf{Q}_{(p)})$ and $\tau \in \Delta$ given by

$$\tau : \zeta_{2M} \longrightarrow \zeta_{2M}^{-1}.$$

It is easy to see that τ corresponds to the complex conjugation. Suppose x is in the kernel of the map in the lemma. Then $x = y^M$ for some $y \in \mathcal{O}_F^*$. Without loss of generality we can assume that y is real. In other words, we have

$$\tau(y) = y.$$

Let σ be an arbitrary element of Δ. Since σ fixes elements in $\mathbf{Q}_{(p)}$, we have $\sigma(x) = x$ and therefore $\sigma(y)^M = y^M$. This implies that $\sigma(y)/y$ is an M-th root of unity and we have $\sigma(y) = y\zeta_M^i$ for some integer i. Applying $\sigma\tau$ and $\tau\sigma$ to the element y we obtain

$$\sigma\tau(y) = \sigma(y) = y\zeta_M^i$$

and

$$\tau\sigma(y) = \tau(y\zeta_M^i) = y\zeta_M^{-i}$$

respectively. The Galois group Δ is Abelian by class field theory so τ and σ commute with each other and it follows that $[\sigma\tau(y)]^2 = y^2$. Now we have

$$\sigma(y^2) = y^2$$

since $\sigma\tau(y) = \sigma(y)$. The unit y^2 belongs to $\mathbf{Q}_{(p)}$ since it is invariant under Δ. If M is odd then using the facts that $y^M, y^2 \in \mathcal{O}_{\mathbf{Q}_{(p)}}^*$, we get $y \in \mathcal{O}_{\mathbf{Q}_{(p)}}^*$. Therefore the kernel of the map in the lemma is trivial.

If M is even, then y generates a quadratic extension of $\mathbf{Q}_{(p)}$ lying in $F = \mathbf{Q}_{(p)}(\zeta_{2M})$. Such an extension correspond to a quadratic extensions of $\mathbf{Q}$ lying in

$\mathbf{Q}(\zeta_{2M})$. There are three such fields, namely $\mathbf{Q}(\sqrt{2}), \mathbf{Q}(\sqrt{i})$ and $\mathbf{Q}(\sqrt{-2})$. This implies that

$$y^2 \in \langle -1, 2 \rangle {\mathbf{Q}^*_{(p)}}^2$$

by Kummer theory. Since y is a unit, this implies that $y^2 = \pm u^2$ for some $u \in \mathcal{O}^*_{\mathbf{Q}_{(p)}}$. We have $x = y^M = u^M$ unless $x = -1$. On the other hand -1 is the M-th power of ζ_{2M} but it is not even a square in the real cyclotomic field $\mathbf{Q}_{(p)}$. Therefore it is the only non-trivial element in the kernel of the map in the lemma. This finishes the proof. $\diamond$

This lemma enables us to identify the group $\mathcal{O}^*_{\mathbf{Q}_{(p)}}/\mu_{\mathbf{Q}}(\mathcal{O}^*_{\mathbf{Q}_{(p)}})^M$ with a subgroup of $F^*/(F^*)^M$. The field $F = \mathbf{Q}_{(p)}(\zeta_{2M})$ contains the M-th roots of unity. Therefore we have

$$\mathrm{Gal}\left(F\left(\sqrt[M]{\mathcal{O}^*_{\mathbf{Q}_{(p)}}}\right)/F\right) \cong \mathrm{Hom}_Z\left(\frac{\mathcal{O}^*_{\mathbf{Q}_{(p)}}}{\mu_{\mathbf{Q}}}, \mu_M\right) \tag{3.2}$$

by Kummer theory. Given an Artin symbol $\tau_{\mathfrak{R}}$ in this Galois group for a degree one prime ideal $\mathfrak{R}$ of F , let us denote the corresponding $\mathbf{Z}$-homomorphism by $f_{\mathfrak{R}}$. Let u be an element of $\mathcal{O}^*_{\mathbf{Q}_{(p)}}$. Then we have

$$f_{\mathfrak{R}}(u) = \frac{\tau_{\mathfrak{R}}(\sqrt[M]{u})}{\sqrt[M]{u}} \in \mu_M$$

by Kummer theory.

Now we are ready to give the main tool to investigate the Jordan-Hölder factors of $B_{\mathbf{Q}_{(p)}}$. Let R be the group ring $(\mathbf{Z}/M\mathbf{Z})[G_{\mathbf{Q}_{(p)}}]$. By definition $B_{\mathbf{Q}_{(p)}} = \mathcal{O}^*_{\mathbf{Q}_{(p)}}/\mathcal{C}$ where the group of cyclotomic units $\mathcal{C}$ is generated by the unit $\eta_g = (\zeta_p - \zeta_p^{-1})^{\sigma_g - 1}$ as a multiplicative $(\mathbf{Z}/M\mathbf{Z})[G_{\mathbf{Q}_{(p)}}]$-module.

Theorem 3.6 *Let $M > 1$ be a power of a prime l and let I denote the augmentation ideal of the ring $R = (\mathbf{Z}/M\mathbf{Z})[G_{\mathbf{Q}_{(p)}}]$. There is a natural isomorphism of*

$G_{K_\mathfrak{p}}$-modules

$$B_{\mathbf{Q}_{(p)}}[M]^\perp = I/\{f_\mathfrak{R}(\eta_g) : \mathfrak{R} \in S\}$$

where S denotes the set of unramified prime ideals $\mathfrak{R}$ of $F = \mathbf{Q}_{(p)}(\zeta_{2M})$ of degree one.

Proof. In order to understand the structure of $B_{\mathbf{Q}_{(p)}}[M]^\perp$ we start with the exact sequence

$$0 \longrightarrow \mathcal{C}/\mu_\mathbf{Q} \longrightarrow \mathcal{O}^*_{\mathbf{Q}_{(p)}}/\mu_\mathbf{Q} \longrightarrow B_{\mathbf{Q}_{(p)}} \longrightarrow 0$$

which is obtained by the definition of $B_{\mathbf{Q}_{(p)}}$ together with the fact that $\mathcal{C}$ contains $\mu_\mathbf{Q} = \{\pm 1\}$. Let us consider two copies of this sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{C}/\mu_\mathbf{Q} & \longrightarrow & \mathcal{O}^*_{\mathbf{Q}_{(p)}}/\mu_\mathbf{Q} & \longrightarrow & B_{\mathbf{Q}_{(p)}} & \longrightarrow & 0 \\ & & \downarrow M & & \downarrow M & & \downarrow M & & \\ 0 & \longrightarrow & \mathcal{C}/\mu_\mathbf{Q} & \longrightarrow & \mathcal{O}^*_{\mathbf{Q}_{(p)}}/\mu_\mathbf{Q} & \longrightarrow & B_{\mathbf{Q}_{(p)}} & \longrightarrow & 0 \end{array}$$

where the vertical maps are given by M-power map. Applying the snake lemma gives us the exact sequence

$$0 \longrightarrow B_{\mathbf{Q}_{(p)}}[M] \longrightarrow \frac{\mathcal{C}}{\mu_\mathbf{Q}\mathcal{C}^M} \longrightarrow \frac{\mathcal{O}^*_{\mathbf{Q}_{(p)}}}{\mu_\mathbf{Q}(\mathcal{O}^*_{\mathbf{Q}_{(p)}})^M}.$$

Let A be a fintie R-module. The dual $A^\perp$ is equal to $\mathrm{Hom}_R(A, R)$ by definition and the functor $\perp$ is exact by Proposition 2.1 (2). Applying this functor to the above sequence we obtain

$$\left(\frac{\mathcal{O}^*_{\mathbf{Q}_{(p)}}}{\mu_\mathbf{Q}(\mathcal{O}^*_{\mathbf{Q}_{(p)}})^M}\right)^\perp \longrightarrow \left(\frac{\mathcal{C}}{\mu_\mathbf{Q}\mathcal{C}^M}\right)^\perp \longrightarrow \left(B_{\mathbf{Q}_{(p)}}[M]\right)^\perp \longrightarrow 0. \tag{3.3}$$

Consider the R-homomorphism from $\left(\mathcal{C}/\mu_\mathbf{Q}\mathcal{C}^M\right)^\perp$ to R given by $f \mapsto f(\eta_g)$. The image of this map lies in the augmentation ideal I of R since $f(\eta_g)$ is annihilated by the $N_{G_{\mathbf{Q}_{(p)}}}$. The unit η_g generates $\mathcal{C}$ and $f(\eta_g) = 0$ only if f is trivial. This implies that the above map is injective. It follows that

$$\left(\frac{\mathcal{C}}{\mu_\mathbf{Q}\mathcal{C}^M}\right)^\perp \cong I$$

since the orders of these two groups are equal. Therefore the exact sequence (3.3) gives us

$$B_{\mathbf{Q}_{(p)}}[M]^{\perp} = I/\left\{f(\eta_g) : f \in D^{\perp}\right\} \quad \text{where} \quad D = \frac{\mathcal{O}^*_{\mathbf{Q}_{(p)}}}{\mu_{\mathbf{Q}}(\mathcal{O}^*_{\mathbf{Q}_{(p)}})^M}.$$

Now we explain the correspondence between $D^{\perp}$ and the Galois group of the Kummer extension given by (3.2). It is by definition $D^{\mathrm{dual}} = \mathrm{Hom}_{\mathbf{Z}}(D, \mathbf{Q}/\mathbf{Z})$ and Proposition 2.1 (1) gives us an explicit isomorphism between $D^{\perp}$ and D^{dual}. We have further isomorphisms as follows:

$$\begin{aligned} D^{\mathrm{dual}} = \mathrm{Hom}_{\mathbf{Z}}\left(\frac{\mathcal{O}^*_{\mathbf{Q}_{(p)}}}{\mu_{\mathbf{Q}}(\mathcal{O}^*_{\mathbf{Q}_{(p)}})^M}, \mathbf{Q}/\mathbf{Z}\right) &\cong \mathrm{Hom}_{\mathbf{Z}}\left(\frac{\mathcal{O}^*_{\mathbf{Q}_{(p)}}}{\mu_{\mathbf{Q}}}, \mathbf{Z}/M\mathbf{Z}\right) \\ &\cong \mathrm{Hom}_{\mathbf{Z}}\left(\frac{\mathcal{O}^*_{\mathbf{Q}_{(p)}}}{\mu_{\mathbf{Q}}}, \mu_M\right) \\ &\cong \mathrm{Gal}\left(F\left(\sqrt[M]{\mathcal{O}^*_{\mathbf{Q}_{(p)}}}\right)/F\right) \end{aligned}$$

Here the first isomorphism is natural and the second one depends on a choice of M-th root of unity. The last isomorphism is given by (3.2). Every element in the Galois group of this Kummer extension is equal to $\tau_{\mathfrak{R}}$, the Artin symbol of an unramified prime ideal $\mathfrak{R} \subset F$ of degree one. Let us denote the corresponding element in $D^{\perp}$ by $f_{\mathfrak{R}}$. Therefore we have

$$B_{\mathbf{Q}_{(p)}}[M]^{\perp} = I/\{f_{\mathfrak{R}}(\eta_g) : \mathfrak{R} \in S\}$$

as we have stated in the theorem. ◇

Now we give the construction of elements

$$f_{\mathfrak{R}}(\eta_g) = \sum_{\sigma \in G_{\mathbf{Q}_{(p)}}} c_\sigma \sigma \in I$$

explicitly. In order to do this we need to determine the coefficients $c_\sigma \in \mathbf{Z}/M\mathbf{Z}$. Suppose that $f_{\mathfrak{R}}$ and $\tau_{\mathfrak{R}}$ correspond to each other under the identification of The-

orem 3.6. We have

$$\left(\sqrt[M]{\sigma(\eta_g)}\right)^{\tau_{\mathfrak{R}}} \equiv \left(\sqrt[M]{\sigma(\eta_g)}\right)^{r} \pmod{\mathfrak{R}}$$

by definition of the Artin symbol. On the other hand, Kummer theory implies that

$$f_{\mathfrak{R}}\left(\sqrt[M]{\sigma(\eta_g)}\right) = \left(\sqrt[M]{\sigma(\eta_g)}\right)^{\tau_{\mathfrak{R}}-1}$$

and it is an M-th root of unity in $F = K_{\mathfrak{p}}(\zeta_{2M})$. Combining these two fact, we see that

$$\left(\sqrt[M]{\sigma(\eta_g)}\right)^{\tau_{\mathfrak{R}}-1} \equiv \left(\sqrt[M]{\sigma(\eta_g)}\right)^{(r-1)} \equiv \sigma(\eta_g)^{(r-1)/M} \pmod{\mathfrak{R}}$$

and it is an M-th root of unity in $\mathbf{Z}/r\mathbf{Z}$. Let us fix a primitive M-th root of unity ζ_M in $F = K_{\mathfrak{p}}(\zeta_{2M})$. The coefficients c_σ can be uniquely determined from the equation

$$\sigma(\eta_g)^{(r-1)/M} \equiv \zeta_M^{c_\sigma} \pmod{\mathfrak{R}}.$$

3.3 Schoof's Algorithm

The elements $f_{\mathfrak{R}}(\eta_g)$ given in the previous section can be computed easily due to two reasons. First we can easily obtain degree one prime ideals $\mathfrak{R}$ of F by using conditions from class field theory, namely $r \equiv 1 \pmod{2M}$ and $r \equiv \pm 1 \pmod{\mathfrak{p}}$. Secondly we have an algebraic expression for η_g which enables us to find

$$\sigma(\eta_g) \pmod{\mathfrak{R}}$$

easily for any $\sigma \in G_{\mathbf{Q}_{(p)}}$.

Let $\mathfrak{R}$ be an unramified prime ideal of $F = \mathbf{Q}_{(p)}(\zeta_{2M})$ of degree one with underlying primes $\mathfrak{r} \subset \mathbf{Q}_{(p)}$ and $r \subset \mathbf{Q}$. In order to compute $f_{\mathfrak{R}}(\eta_g)$ we need to make

choices for elements η_g and ζ_M modulo $\mathfrak{R}$. Consider the following diagram:

$$\begin{array}{cc} F & \mathfrak{R} \\ | & \\ \mathbf{Q}_{(p)} & \mathfrak{r} \\ | & \\ \mathbf{Q} & r \end{array}$$

If we change $\mathfrak{R}$ lying above $\mathfrak{r}$, then it corresponds to a different choice of ζ_M. Therefore the elements $f_{\mathfrak{R}}(\eta_g)$ differ from each other by a unit of $\mathbf{Z}/M\mathbf{Z}$ for a different choice of $\mathfrak{R}$ over a fixed $\mathfrak{r}$. Changing $\mathfrak{r}$ over r is equivalent to change η_g with one of its conjugates. Such a change corresponds to multiplying $f_{\mathfrak{R}}(\eta_g)$ with a power of σ_g, a unit in $(\mathbf{Z}/M\mathbf{Z})[G_{\mathbf{Q}_{(p)}}]$. Therefore the ideal generated by elements $f_{\mathfrak{R}}(\eta_g)$ only depend on the rational prime r. Now we formulate previous results in terms of polynomials. We have an isomorphism

$$(\mathbf{Z}/M\mathbf{Z})[G_{\mathbf{Q}_{(p)}}] \cong (\mathbf{Z}/M\mathbf{Z})[X]/(X^{(p-1)/2} - 1)$$

obtained by $\sigma_g \mapsto X$. Let $f_r(X)$ denote the image of $f_{\mathfrak{R}}(\eta_g)$ under this isomorphism which is well-defined up to a unit. We denote the augmentation ideal of both rings by I.

Theorem 3.7 *Using the notation above, we have that*

$$B_{\mathbf{Q}_{(p)}}[M]^{\perp} = I/\langle f_r(X) : r \in S_M \rangle$$

where S_M is the set of primes satisfying $r \equiv \pm 1 \pmod{p}$ and $r \equiv 1 \pmod{2M}$.

Proof. This easily follows from Theorem 3.6. ◇

Now we are ready to determine if $B_{\mathbf{Q}_{(p)}}$ admits a Jordan-Hölder factor of order $q = l^f$ or not. Any finite R-module is Jordan-Hölder isomorphic to its dual and we

have

$$B^{\perp}_{\mathbf{Q}_{(p)}} = \prod_{l} \prod_{\varphi} (B^{\perp}_{\mathbf{Q}_{(p)}})_{\varphi}$$

by the Jordan-Hölder filtration given in Section 2.1. The irreducible polynomials φ are obtained by factoring $X^m - 1$ in l-adic polynomial ring $\mathbf{Z}_l[X]$ where m is given by $(p-1)/2 = l^a m$ with $\gcd(m, l) = 1$.

3.3.1 Step 1

In the first step we check if $B^{\perp}_{\mathbf{Q}_{(p)}}$ admits any Jordan-Hölder factors of order q at all. Fix p and $q = l^f$. The possible degree d of these factors all divide

$$\delta = \gcd\left((p-1)/2, q-1\right).$$

Proposition 3.4 implies that the first step is trivial if $\delta = 1$. Otherwise we compute

$$f_r(X) \pmod{X^{\delta} - 1} \tag{3.4}$$

for several primes r with $M = l$.

Computing the greatest common divisors of these elements recursively, we look for a common divisor $\varphi \neq X - 1$ of degree exactly f. If we guarantee that there is no such factor, we stop. Then using Theorem 3.7, we conclude that

$$\frac{B_{\mathbf{Q}_{(p)}}[l]^{\perp}}{\varphi B_{\mathbf{Q}_{(p)}}[l]^{\perp}}$$

is zero for all $\varphi \neq X - 1$ of degree f. This follows that $B^{\perp}_{\mathbf{Q}_{(p)}}$, and therefore $B_{\mathbf{Q}_{(p)}}$, does not admit any Jordan-Hölder factors of order q.

If there is a repeating factor $\varphi | \frac{X^{\delta}-1}{X-1}$ with $\deg(\varphi) = f$ (possibly more than one) then we believe that $B_{\mathbf{Q}_{(p)}}$ admits a non-trivial Jordan-Hölder factor of order q and we proceed to the second step of the algorithm.

3.3.2 Step 2

In this step we determine what the structure of $(B^{\perp}_{\mathbf{Q}_{(p)}})_{\varphi}$ could be for each φ from Step 1. We first find a lift of φ, denoted by φ_M, to an irreducible divisor of $X^{q-1}-1 \in (\mathbf{Z}/M\mathbf{Z})[X]$ for $M \in \{l, l^2, l^3, ...\}$. Theorem 3.7 gives us

$$(B_{\mathbf{Q}_{(p)}}[M]^{\perp})_{\varphi} \cong R/\langle \varphi_M(X^{l^a}), f_r(X) : r \in S_M \rangle$$

since φ-part of the augmentation ideal I is isomorphic to the φ-part of the ring $R = (\mathbf{Z}/M\mathbf{Z})[G]$ itself. We compute

$$f_r(X) \pmod{\varphi_M(X^{l^a})}$$

for several values of $r \in S_M$. For each M, we heuristically find the ideal $\mathcal{I}^{(M)} = \langle f_r(X) : r \in S_M \rangle$ by adding more generators until it stabilizes. Observe that Chebotarev's density theorem implies that the ideal $\mathcal{I}^{(M)}$ is obtained after finitely many steps. For M big enough the orders of the quotients $R/\mathcal{I}^{(M)}$ must stabilize since $(B^{\perp}_{\mathbf{Q}_{(p)}})_{\varphi}$ is finite. Suppose M_0 is such a number, i.e. $\left|R/\mathcal{I}^{(M_0)}\right| = \left|R/\mathcal{I}^{(lM_0)}\right|$. Then M_0 annihilates

$$\left(B_{\mathbf{Q}_{(p)}}[lM_0]^{\perp}\right)_{\varphi} = \frac{(\mathbf{Z}/lM_0\mathbf{Z})[X]}{((\varphi(X^{l^a}) + \mathcal{I}^{(lM_0)})}$$

and by Nakayama's Lemma, M_0 annihilates $(B^{\perp}_{\mathbf{Q}_{(p)}})_{\varphi}$. We have an explicit ideal $\mathcal{I}^{(M_0)} \subset R$ and a surjective homomorphism

$$R/\mathcal{I}^{(M_0)} \twoheadrightarrow (B^{\perp}_{\mathbf{Q}_{(p)}})_{\varphi}$$

and in the last step we attempt to prove that this map is an isomorphism.

3.3.3 Step 3

Let φ be as in Step 2. Let $M = M_0$ be the power of l that annihilates $(B^{\perp}_{\mathbf{Q}_{(p)}})_{\varphi}$ from Step 2. Proposition 2.2 (1) implies that $(B_{\mathbf{Q}_{(p)}})_{\varphi}$ is Jordan-Hölder isomorphic

to its dual and therefore it is annihilated by M as well. Observe that φ part of the ring $R = (\mathbf{Z}/M\mathbf{Z})[G]$ is given by

$$R_\varphi = (\mathbf{Z}/M\mathbf{Z})[X]/(\varphi_M(X^{l^a})).$$

Consider the exact sequence

$$0 \longrightarrow B_{\mathbf{Q}_{(p)}}[M] \longrightarrow \frac{\mathcal{C}}{\mu_{\mathbf{Q}}\mathcal{C}^M} \longrightarrow \frac{\mathcal{C}}{\mu_{\mathbf{Q}}\left(\mathcal{O}^*_{\mathbf{Q}_{(p)}}\right)^M} \longrightarrow 0$$

where the first homomorphism is given by $u \mapsto u^M$. Recall that the term in the middle is isomorphic to the augmentation ideal I of R. The φ-part of I is equal to the φ-part of the ring R itself since $\varphi \neq X - 1$. Since M annihilates $(B_{\mathbf{Q}_{(p)}})_\varphi$, we obtain the exact sequence

$$0 \longrightarrow (B_{\mathbf{Q}_{(p)}})_\varphi \longrightarrow R_\varphi \longrightarrow C_\varphi \longrightarrow 0$$

of $R\varphi$-modules where $C = \mathcal{C}/\mu_{\mathbf{Q}}(\mathcal{O}^*_{\mathbf{Q}_{(p)}})^M$.

We use Proposition 2.2 (4) with $J = \mathcal{I}^{(M)}$. By Step 2, the first condition is already satisfied. Now we must show that $\mathrm{Ann}_R(J)$ annihilates C_φ. It is easy to see that this happens if and only if

$$\frac{X^{(p-1)/2} - 1}{\varphi_M(X^{l^a})}\mathrm{Ann}_R(J)$$

annihilates C. In order to check this, we first find a finite set of generators $z(X)$ of $\mathrm{Ann}_R(J)$. For each $z(X)$, we compute the cyclotomic unit

$$\eta_z := \eta_g^{\left(\frac{X^{(p-1)/2}-1}{\varphi_M(X^{l^a})}z(X)\right)} \tag{3.5}$$

and show that it is an M-th power of a unit $u \in \mathcal{O}^*_{\mathbf{Q}_{(p)}}$. Observe that the norm map $(X^{(p-1)/2} - 1)/(X^{dl^a} - 1)$ divides the power of η_g in equation (3.5). It follows that the unit η_z is an element in the unique subextension L of $\mathbf{Q}_{(p)}$ which has degree dl^a over $\mathbf{Q}$.

Let us denote by u_i the embedding of units $\sigma_g^i(\eta_z)$ for $1 \leq i \leq dl^a$ into $\mathbf{R}$ with high accuracy. Suppose that M is odd so that taking M-th root is well-defined in $\mathbf{R}$. Then we compute the polynomial

$$G(t) = \prod_{i=1}^{dl^a} (t - \sqrt[M]{u_i})$$

and check if its coefficients are very close to integers. For M even, there are sign ambiguities since square root of an element is not well-defined in $\mathbf{R}$. By switching between $\pm u_i$, we find $G(t)$ with almost integer coefficients. If the approximations are sufficiently accurate, this proves that η_z is an M-th power in $\mathbf{Q}_{(p)}$. Therefore the surjection given at the end of Step 2 is actually an isomorphism. The structure of $(B^{\perp}_{\mathbf{Q}_{(p)}})_{\varphi}$, and therefore its order, can be obtained explicitly by using this isomorphism.

3.3.4 A Note on Schoof's Original Algorithm

The algorithm we give here is slower than the original one since we disregard a nice property of cyclotomic units. The most time consuming part of the algorithm is to find polynomials $f_r(X) \pmod{X^{\delta} - 1}$ in Step 1. In the original algorithm, Schoof computes such polynomials by using the expression

$$\sum_{i=0}^{\delta-1} \log_r \left(\prod_{k \equiv j \pmod{\delta}} (\zeta^{g^k} - \zeta^{-g^k}) \right) \cdot X^j$$

where $\log_r(x)$ denotes the element $i \in \mathbf{Z}/M\mathbf{Z}$ for which $\zeta_M^i \equiv x^{(r-1)/M} \pmod{\mathfrak{R}}$.

The advantage of doing this is that we can first compute the products inside and their logarithms afterwards. This is much faster than computing

$$f_r(X) = \sum_{\sigma \in G_{\mathbf{Q}_{(p)}}} c_{\sigma} \sigma$$

by finding each coefficient $c_\sigma \in G_{\mathbf{Q}_{(p)}}$ separately and then reducing the polynomial modulo $X^\delta - 1$. We disregard this property in our summary of Schoof's algorithm since we can not generalize it to the elliptic case, due to the lack of algebraic expressions for elliptic units.

3.4 Heuristics for the Cyclotomic Case

In this section, we estimate the behavior of Jordan-Hölder factors of the ideal class group $\mathrm{Cl}(\mathbf{Q}_{(p)})$ that have very large order. A simple Jordan-Hölder factor of the group ring $\mathbf{Z}[G_{\mathbf{Q}_{(p)}}]$ of order $q = l^f$ and degree $d > 1$ is a residue field of the unique quotient ring of $\mathbf{Z}[G_{\mathbf{Q}_{(p)}}]$ that is isomorphic to $\mathbf{Z}[X]/(X^d - 1)$. The ring $\mathbf{Z}[X]/(X^d - 1)$ admits $\phi(d)/f$ residue fields of order q. Here ϕ is the Euler's phi-function. The number of residue fields of order q of the ring $\mathbf{Z}[G_{\mathbf{Q}_{(p)}}]$ is obtained by

$$n_{p,q} = \sum_d \frac{\phi(d)}{f}$$

where $d \neq 1$ runs through divisors of $\delta = \gcd((p-1)/2, q-1)$ for which the order of p modulo d is f. According to Cohen-Lenstra Heuristics, the probability that the class group of $\mathbf{Q}_{(p)}$ does not admit any simple Jordan-Hölder factor of order q at all is at least

$$H_{\mathbf{Q}_{(p)}}(p, q) = \left(\prod_{k \geq 2} 1 - q^{-k} \right)^{n_{p,q}}.$$

Schoof's main table contains the numbers $\tilde{h}_{\mathbf{Q}_{(p)}}$, the order of the subgroup of $\mathrm{Cl}(\mathbf{Q}_{(p)})$ that admit only Jordan-Hölder factors of order $q < Q = 80,000$, for $p < P = 10,000$. The numbers $\tilde{h}_{\mathbf{Q}_{(p)}}$ are all equal to the class numbers of the

corresponding fields with probability at least

$$\mathcal{P}_{\mathbf{Q}} = \prod_{p<P} \prod_{q>Q} H_{\mathbf{Q}_{(p)}}(p,q).$$

The calculations of Schoof show that $-\log(\mathcal{P}_{\mathbf{Q}_{(p)}}) < \frac{c\pi(P)}{Q}$ where $c = 1.295730...$ is a constant and $\pi(P) = 1228$ is the number of odd primes less than P [7, Section 6]. Therefore

$$\mathcal{P}_{\mathbf{Q}} > 0.980307...$$

which implies that the table of $\tilde{h}_{\mathbf{Q}_{(p)}}$ is a table of class numbers with probability at least 98%.

3.5 Results

In this section we give a summary of Schoof's results [7]. Recall that we denote by $\tilde{h}_{\mathbf{Q}_{(p)}}$, the order of the largest submodule of $B_{\mathbf{Q}_{(p)}}$ that admits a Jordan-Hölder factor filtration with simple factors of order $q < 80,000$. There are 1228 odd primes p less than $10,000$. For 925 of these, Schoof shows that $\tilde{h}_{\mathbf{Q}_{(p)}} = 1$. The remaining 303 primes p are listed in the main table, at the end of Schoof's paper. This table gives $\tilde{h}_{\mathbf{Q}_{(p)}}$ as a product of orders q of the contributing simple Jordan-Hölder factors together with the degree d of each factor.

It is not difficult to derive the Galois module structure of $B_{\mathbf{Q}_{(p)}}$ from the tables. Most of the simple Jordan-Hölder factors of $B_{\mathbf{Q}_{(p)}}$ occur with multiplicity 1 in which case the structure of $(B_{\mathbf{Q}_{(p)}})_{\varphi}$ is obvious. There are extra tables for the exceptional cases where the multiplicity is non-trivial. By Proposition 2.2 (3), the module $(B_{\mathbf{Q}_{(p)}})_{\varphi}$ is isomorphic to $(B^{\perp}_{\mathbf{Q}_{(p)}})_{\varphi}$ if the length of $(B^{\perp}_{\mathbf{Q}_{(p)}})_{\varphi}$ is at most two. For those factors with the length bigger than 2, there are 6 such cases, Schoof gives the structure of $(B_{\mathbf{Q}_{(p)}})_{\varphi}$ separately.

Even though $\mathrm{Cl}(\mathbf{Q}_{(p)})$ and $B_{\mathbf{Q}_{(p)}}$ have the same number of elements, it is not true in general that they are isomorphic as Galois modules. Indeed for $p = 7687$ and $\varphi = X^2 + X + 1 \in \mathbf{Z}_2[X]$, the φ-part of the $\mathrm{Cl}(\mathbf{Q}_{(p)})$ is annihilated by 2, whereas φ-part of $B_{\mathbf{Q}_{(p)}}$ is not. However, cohomology groups of $\mathrm{Cl}(\mathbf{Q}_{(p)})$ and $B_{\mathbf{Q}_{(p)}}$ are isomorphic.

Proposition 3.8 *Let H be a subgroup of $G_{\mathbf{Q}_{(p)}}$. Then there are canonical isomorphisms $\widehat{H}^i(H, Cl(\mathbf{Q}_{(p)})) \cong \widehat{H}^{i+2}(H, B_{\mathbf{Q}_{(p)}})$ for each $i \in \mathbf{Z}$. In particular, for each choice of a generator of H there are natural isomorphisms $\widehat{H}^i(H, Cl(\mathbf{Q}_{(p)})) \cong \widehat{H}^i(H, B_{\mathbf{Q}_{(p)}})$ for each $i \in \mathbf{Z}$.*

Proof. See Schoof [7, Proposition 5.1 (*ii*)]. ◇

CHAPTER 4

ELLIPTIC ANALOGUE OF SCHOOF'S ALGORITHM

In this chapter, we describe the analogue of Schoof's algorithm for ray class fields $K_{\mathfrak{p}}$ of imaginary quadratic fields. We call it *elliptic analogue* since $K_{\mathfrak{p}}$ is related to a CM elliptic curve, in the same way $\mathbf{Q}_{(p)}$ is related to a circle. This relation is explained in Section 2.2.

In the first section, we construct elliptic units, and give the Galois action on them using Shimura's reciprocity law. In the second section we explain how to reformulate the results in the cyclotomic case so that we obtain their elliptic analogues. In the third section we explain our algorithm and give an example. In the last section we apply Cohen-Lenstra heuristics to our case and argue that each table we give in Chapter 5 is a table of class numbers with probability at least 96%.

4.1 Elliptic Units

Let K be an imaginary quadratic field with class number one and $\mathfrak{p} \subset \mathcal{O}_K$ be a degree one prime ideal of norm p not dividing $6d_K$. In this section, we first give the structure of the Galois group $G_{K_{\mathfrak{p}}} = \mathrm{Gal}(K_{\mathfrak{p}}/K)$. In the second part, we explain how to compute Stark's elliptic units by extracting the $12p$-th root of unity. At the

end, we define the group of elliptic units $\mathcal{E}$ and show that its index in the full unit group of $K_{\mathfrak{p}}$ is equal to the class number of $K_{\mathfrak{p}}$.

We start with the complete list of imaginary quadratic fields with class number one.

Theorem 4.1 *There are only 9 imaginary quadratic fields with class number one. The discriminant d_K of these fields are given by*

$$\{-3, -4, -7, -8, -11, -19, -43, -67, -163\}.$$

Proof. See Stark [9]. ◇

We fix some notation first. Define

$$w := \begin{cases} \sqrt{d_K}/2 & \text{if } d_K = -4, -8 \\ (\sqrt{d_K}+1)/2 & \text{otherwise} \end{cases}$$

so that $\mathcal{O}_K = \mathbf{Z}[w]$ for each K. Also define $w_{\mathfrak{p}}$ to be the smallest non-negative integer which satisfies the congruence

$$w \equiv w_{\mathfrak{p}} \pmod{\mathfrak{p}}.$$

It is easy to see that $0 \leq w_{\mathfrak{p}} \leq p-1$. We fix a basis $[p, w_{\mathfrak{p}} - w]$ for $\mathfrak{p}$ where p is the rational prime lying under $\mathfrak{p}$. Observe that the imaginary part of the quotient $p/(w_{\mathfrak{p}} - w)$ is positive. This fact will be useful later when we apply Shimura's reciprocity law.

4.1.1 The Galois Group of $K_{\mathfrak{p}}/K$

The ray class field $K_{\mathfrak{p}}$ is an Abelian extension of K with Galois group isomorphic to $I_K(\mathfrak{p})/P_{K,1}(\mathfrak{p})$ by class field theory. Set $G_{K_{\mathfrak{p}}} = \mathrm{Gal}(K_{\mathfrak{p}}/K)$. The map

$$\psi : xw + y \longmapsto xw_{\mathfrak{p}} + y$$

gives a surjective homomorphism from $\mathcal{O}_K$ onto $\mathbf{F}_p$ with $\mathrm{Ker}(\psi) = \mathfrak{p}$. The unit group of $\mathcal{O}_K$ is finite and consists of roots of unity μ_K. The number of elements in each μ_K is given by

$$W_K := \begin{cases} 6 & \text{if } d_K = -3 \\ 4 & \text{if } d_K = -4 \\ 2 & \text{otherwise.} \end{cases}$$

Since any ideal in $\mathcal{O}_K$ is principal, the group $I_K(\mathfrak{p})$ of all fractional $\mathcal{O}_K$-ideals relatively prime to $\mathfrak{p}$ is

$$I_K(\mathfrak{p}) = \{(\alpha) : \alpha \in K, \alpha \not\equiv 0 \pmod{\mathfrak{p}}\}.$$

Observe that two elements generate the same ideal only if they differ by a unit. Let ζ be a root of unity in $\mathcal{O}_K$ generating μ_K. We have $\zeta^{(W_K/2)} = -1$. It follows that

$$\psi : \mu_K \longrightarrow \mathbf{F}_p^*$$

is an injection and we can construct a well-defined map

$$\begin{aligned} \widehat{\psi} : \quad I_K(\mathfrak{p}) \quad &\longrightarrow \mathbf{F}_p^*/\psi(\mu_K) \\ (xw + y) \quad &\longmapsto xw_{\mathfrak{p}} + y \end{aligned}$$

It is easy to show that $\widehat{\psi}$ is a homomorphism and we have

$$\begin{aligned} \mathrm{Ker}\left(\widehat{\psi}\right) &= \{(\alpha) : \alpha \equiv \zeta \pmod{\mathfrak{p}}, \zeta \in \mu_K\} \\ &= \{(\alpha) : \alpha \equiv 1 \pmod{\mathfrak{p}}\} \\ &= P_{K,1}(\mathfrak{p}). \end{aligned}$$

Therefore the Galois group of $K_{\mathfrak{p}}/K$ is given by

$$G_{K_{\mathfrak{p}}} \cong \mathbf{F}_p^*/\psi(\mu_K)$$

which is cyclic and has order $(p-1)/W_K$. The degree of the extension $K_{\mathfrak{p}}/K$ is equal to $(p-1)/W_K$ as well, since it is equal to the order of the Galois group $G_{K_{\mathfrak{p}}}$. Let m be an integer relatively prime to p. Consider the class in $I_K(\mathfrak{p})/P_{K,1}(\mathfrak{p})$ involving the ideal $m\mathcal{O}_K$. We denote the corresponding element in $G_{K_{\mathfrak{p}}}$ by σ_m. Suppose that the ideal $\mathfrak{q}$ is generated by $\alpha \in \mathcal{O}_K$ and $\alpha \equiv m \pmod{\mathfrak{p}}$. Then we have $\sigma_{\mathfrak{q}} = \sigma_m$ where $\sigma_{\mathfrak{q}}$ is the Artin symbol.

4.1.2 Extracting $12p$-th Root of Unity

The ray class field $K_{\mathfrak{p}}/K$ is totally ramified above $\mathfrak{p}$ and there is a unique prime $\mathfrak{P} \subset \mathcal{O}_{K_{\mathfrak{p}}}$ lying above $\mathfrak{p}$. We use the basis $[p, w_{\mathfrak{p}} - w]$ for $\mathfrak{p}$ as in the previous section. Define

$$\theta := \frac{p}{w_{\mathfrak{p}} - p}$$

which is an element in the upper half plane. The modular function $\phi(u, v, z)$ is defined in Section 2.3.

Theorem 4.2 *Let a be an integer relatively prime to p. There exists $\pi(a) \in \mathcal{O}_{K_{\mathfrak{p}}}$ of norm p such that*

$$\left[\phi\left(\frac{a}{p}, 0, \theta\right)^{W_K}\right]^{12p} = \pi(a)^{12p}.$$

The element $\pi(m)$ generates the unique prime ideal $\mathfrak{P} \subset \mathcal{O}_{K_{\mathfrak{p}}}$ lying above $\mathfrak{p}$. The quotient $\frac{\pi(a)}{\pi(1)}$ is the W_K-th power of a unit in $\mathcal{O}_{K_{\mathfrak{p}}}$ and

$$\sigma_m\left(\frac{\pi(a)}{\pi(1)}\right) = \frac{\pi(ma)}{\pi(m)}$$

for all $\sigma_m \in G_{K_{\mathfrak{p}}}$.

Proof. See Stark [8, p. 226 and p. 229] ◇

In order to compute the units mentioned in this theorem, we start by applying Shimura's reciprocity law (Theorem 2.6) to the element $\phi(a/p, 0, \theta)$.

Let $\mathfrak{q} = (x_\mathfrak{q} w + y_\mathfrak{q})$ be a degree one prime ideal in $\mathcal{O}_K$ of norm q not dividing pd_K. We denote conjugate of this prime by $\bar{\mathfrak{q}} = (x_{\bar{\mathfrak{q}}} w + y_{\bar{\mathfrak{q}}})$ where we can take $x_{\bar{\mathfrak{q}}} = x_\mathfrak{q}$. This implies that

$$y_{\bar{\mathfrak{q}}} = \begin{cases} -y_\mathfrak{q} & \text{if } d_K = -4, -8 \\ -(x_\mathfrak{q} + y_\mathfrak{q}) & \text{otherwise.} \end{cases}$$

We take $(x_{\bar{\mathfrak{q}}} w + y_{\bar{\mathfrak{q}}})[p, w_\mathfrak{p} - w]$ as a basis for $\bar{\mathfrak{q}}\mathfrak{p}$ and so B is defined by

$$B \begin{pmatrix} p \\ w_\mathfrak{p} - w \end{pmatrix} = (x_{\bar{\mathfrak{q}}} w + y_{\bar{\mathfrak{q}}}) \begin{pmatrix} p \\ w_\mathfrak{p} - w \end{pmatrix}.$$

Comparing the coefficients of w, one can obtain

$$B = \begin{bmatrix} x_\mathfrak{q}\omega_\mathfrak{p} + y_{\bar{\mathfrak{q}}} & -px_\mathfrak{q} \\ * & -(x_\mathfrak{q} w_\mathfrak{p} + y_\mathfrak{q}) \end{bmatrix},$$

a matrix of determinant q, and then

$$qB^{-1} = \begin{bmatrix} -(x_\mathfrak{q} w_\mathfrak{p} + y_\mathfrak{q}) & px_\mathfrak{q} \\ * & x_\mathfrak{q} w_\mathfrak{p} + y_{\bar{\mathfrak{q}}} \end{bmatrix}.$$

We denote by $\sigma_\mathfrak{q}$, the Artin symbol of $\mathfrak{q}$ in the Galois group $\mathrm{Gal}(K_{(12p^2)}/K)$. The function $\phi(a/p, 0, z)$ is a modular function of level $12p^2$. Shimura's reciprocity law (Theorem 2.6) implies that $\phi\,(a/p, 0, \theta)$ is an element of the ray class field $K_{(12p^2)}$ and

$$\begin{aligned} \phi\left(\frac{a}{p}, 0, \theta\right)^{\sigma_\mathfrak{q}} &= \phi\left(\left(\frac{a}{p}, 0\right) qB^{-1}, \theta\right) \\ &= \phi\left(-\frac{a(x_\mathfrak{q} w_\mathfrak{p} + y_\mathfrak{q})}{p}, ax_\mathfrak{q}, \theta\right) \\ &= \phi\left(-\frac{a(x_\mathfrak{q} w_\mathfrak{p} + y_\mathfrak{q})}{p}, 0, \theta\right) \left(-e^{\pi i\left(-\frac{a(x_\mathfrak{q} w_\mathfrak{p} + y_\mathfrak{q})}{p}\right)}\right)^{ax_\mathfrak{q}} \\ &= \phi\left(-\frac{a(x_\mathfrak{q} w_\mathfrak{p} + y_\mathfrak{q})}{p}, 0, \theta\right) \left(\zeta_p^{-\frac{x_\mathfrak{q}(x_\mathfrak{q} w_\mathfrak{p} + y_\mathfrak{q})}{2}}\right)^{a^2} (-1)^{ax_\mathfrak{q}}. \quad (4.1) \end{aligned}$$

The action of $\sigma_{\mathfrak{q}}$ on the roots of unity is given by $\zeta^{\sigma_{\mathfrak{q}}} = \zeta^q$. Theorem 4.2 implies that $\phi\left(a/p, 0, \theta\right)^{W_K}$ is in $K_{\mathfrak{p}}$ up to a $12p$-th root of unity. Suppose that

$$q \equiv 1 \pmod{12p}.$$

This implies that $\sigma_{\mathfrak{q}}$ acts trivially on the $12p$-th root of unity part and

$$\frac{\left[\phi\left(\frac{a}{p}, 0, \theta\right)^{W_K}\right]^{\sigma_{\mathfrak{q}}}}{\phi\left(\frac{a}{p}, 0, \theta\right)^{W_K}} = \left[\frac{\phi\left(\frac{a}{p}, 0, \theta\right)^{\sigma_{\mathfrak{q}}}}{\phi\left(\frac{a}{p}, 0, \theta\right)}\right]^{W_K}$$

is in $K_{\mathfrak{p}}$. Moreover this element is the W_K-th power of a unit in the same field by Theorem 4.2. The field K contains the W_K-th roots of unity. This allows us to take W_K-th root of elements within the field $K_{\mathfrak{p}} \supset K$. Therefore

$$\frac{\phi\left(\frac{a}{p}, 0, \theta\right)^{\sigma_{\mathfrak{q}}}}{\phi\left(\frac{a}{p}, 0, \theta\right)} = \phi\left(\frac{a}{p}, 0, \theta\right)^{\sigma_{\mathfrak{q}}-1}$$

is in $\mathcal{O}_{K_{\mathfrak{p}}}^*$.

Let m be an integer relatively prime to p. We can pick a prime ideal $\mathfrak{q} = (x_{\mathfrak{q}} w + y_{\mathfrak{q}}) \subset \mathcal{O}_K$ of norm $q \equiv 1 \pmod{12p}$ so that $-(x_{\mathfrak{q}} w + y_{\mathfrak{q}}) \equiv m \pmod{\mathfrak{p}}$ by the Chebotarev's density theorem. The Artin symbol $\sigma_{\mathfrak{q}}$ of the prime ideal $\mathfrak{q}$ is an element in $\mathrm{Gal}(K_{(12p^2)}/K)$ such that $\sigma_{\mathfrak{q}}|_{K(\zeta_{12p})}$ is the identity and $\sigma_{\mathfrak{q}}|_{K_{\mathfrak{p}}} = \sigma_m$. The last equality means that the ideals $\mathfrak{q}$ and $m\mathcal{O}_K$ are in the same class in the ray class group $I_K(\mathfrak{p})/P_{K,1}(\mathfrak{p})$. Using the equation (4.1) with the fact $\phi\left(a/p, 0, \theta\right)^{\sigma_{\mathfrak{q}}-1}$ is in $\mathcal{O}_{K_{\mathfrak{p}}}^*$, we find that

$$\phi\left(\frac{a}{p}, 0, \theta\right)^{\sigma_{\mathfrak{q}}-1} = \frac{\phi\left(\frac{am}{p}, 0, \theta\right)}{\phi\left(\frac{a}{p}, 0, \theta\right)} \left(\zeta_p{}^{k(m)}\right)^{a^2} (-1)^{a x_{\mathfrak{q}}} \tag{4.2}$$

is in $\mathcal{O}_{K_{\mathfrak{p}}}^*$ where

$$k(m) := x_{\mathfrak{q}} m/2 \pmod{p}.$$

The integer $k(m)$ modulo p is unique since $K_{\mathfrak{p}}$ does not contain p-th roots of unity. We define the elliptic unit

$$\epsilon_m := \frac{\phi\left(\frac{1}{p},0,\theta\right)^{\sigma_{\mathfrak{q}}-1}}{(-1)^{x_{\mathfrak{q}}}} = \frac{\phi\left(\frac{m}{p},0,\theta\right)}{\phi\left(\frac{1}{p},0,\theta\right)}{\zeta_p}^{k(m)} \in \mathcal{O}_{K_{\mathfrak{p}}}^*$$

by choosing $a = 1$ and dropping $(-1)^{x_{\mathfrak{q}}}$ in the equation (4.2).

Now we want to find the Galois conjugates of ϵ_m. Let g be a primitive root modulo p. Then the Galois group $G_{K_{\mathfrak{p}}} = \mathrm{Gal}(K_{\mathfrak{p}}/K)$ is generated by σ_g. The conjugate $\sigma_g^i(\epsilon_m)$ is equal to

$$\frac{\phi\left(\frac{g^i m}{p},0,\theta\right)}{\phi\left(\frac{g^i}{p},0,\theta\right)}$$

up to a root of unity by Theorem 4.2. Consider the elements $\phi\left(a/p,0,\theta\right)$ in the ray class field $K_{(12p^2)}$ which are conjugates of each other. Let τ_i be an element in $\mathrm{Gal}(K_{(12p^2)}/K)$ such that

$$\tau_i : \phi\left(\frac{1}{p},0,\theta\right) \longmapsto \phi\left(\frac{g^i}{p},0,\theta\right).$$

The automorphisms τ_i and $\sigma_{\mathfrak{q}}$ commute with each other and we have

$$\tau_i(\epsilon_m) \;=\; \frac{\phi\left(\frac{g^i}{p},0,\theta\right)^{\sigma_{\mathfrak{q}}-1}}{(-1)^{x_{\mathfrak{q}}}} = \frac{\phi\left(\frac{g^i m}{p},0,\theta\right)}{\phi\left(\frac{g^i}{p},0,\theta\right)}\left({\zeta_p}^{k(m)}\right)^{g^{2i}}(-1)^{(g^i-1)x_{\mathfrak{q}}}.$$

where the second equality follows from the equation (4.2). This shows that $\tau_i|_{K_{\mathfrak{p}}} = \sigma_g^i$ and

$$\sigma_g^i(\epsilon_m) = \frac{\phi\left(\frac{g^i m}{p},0,\theta\right)}{\phi\left(\frac{g^i}{p},0,\theta\right)}\left({\zeta_p}^{k(m)}\right)^{g^{2i}}(-1)^{(g^i-1)x_{\mathfrak{q}}}.$$

Observe that if we use an odd primitive root g modulo p, we can neglect the power of -1 since it becomes trivial for all values of i.

Lemma 4.3 *Let g be an odd primitive root modulo p. Let m be an integer relatively prime to p. Then*

$$\sigma_g^i(\epsilon_m) = \frac{\phi\left(\frac{g^i m}{p}, 0, \theta\right)}{\phi\left(\frac{g^i}{p}, 0, \theta\right)} \zeta_p^{\,k(m)g^{2i}}$$

for all i.

Now we give some nice properties of the function $k(m)$ which simplifies the computation of elliptic units.

Lemma 4.4 *Let g be an odd primitive root modulo p. Then*

$$k(g^a) = k(g)\left(1 + g^2 + ... + g^{2(a-1)}\right) \pmod{p}.$$

Proof. Observe that $\epsilon_{g^2} = \epsilon_g \sigma_g(\epsilon_g)$ by Lemma 4.3. Comparing the powers of the p-th root of unity, one gets $k(g^2) = k(g)(1 + g^2)$. The general result follows from the fact

$$\epsilon_{g^a} = \epsilon_g \sigma_g(\epsilon_g) \cdots \sigma_g^{a-1}(\epsilon_g).$$

$\diamond$

The following lemma gives us more freedom to compute $k(g)$ by relaxing the condition on the prime ideal $\mathfrak{q} \subset \mathcal{O}_K$.

Lemma 4.5 *Let g be an odd primitive root modulo p. Let $\mathfrak{q} = (x_\mathfrak{q} w + y_\mathfrak{q}) \subset \mathcal{O}_K$ be a degree one prime ideal of norm $q \equiv 1 \pmod{12p}$ such that $\sigma_\mathfrak{q}|_{K_\mathfrak{p}}$ is not trivial. Set $m \equiv -(x_\mathfrak{q} w + y_\mathfrak{q}) \pmod{\mathfrak{p}}$. Then*

$$k(g) = \frac{g^2 - 1}{m^2 - 1} k(m) \pmod{p}$$

where $k(m) = (x_\mathfrak{q} m)/2 \pmod{p}$.

Proof. Since g is a primitive root modulo p, there exists an integer a such that $m = g^a \pmod{p}$. By Lemma 4.4, we have

$$k(g) = \frac{k(m)}{(1 + g^2 + ... + g^{2(a-1)})} \pmod{p}.$$

Multiplying both numerator and denominator with $g^2 - 1$, we get

$$k(g) = \frac{g^2 - 1}{m^2 - 1} k(m) \pmod{p}.$$

$\diamond$

4.1.3 Stark's Elliptic Units

The *group of elliptic units*, denoted by $\mathcal{E}$, is the multiplicative $\mathbf{Z}[G_{K_\mathfrak{p}}]$-module generated by the unit

$$\epsilon_g = \frac{\phi\left(\frac{g}{p}, 0, \theta\right)}{\phi\left(\frac{1}{p}, 0, \theta\right)} {\zeta_p}^{k(g)} \tag{4.3}$$

where g is a primitive root modulo p. Observe that the group $\mathcal{E}$ does not depend on the choice of g.

Lemma 4.6 *The group of elliptic units $\mathcal{E}$ contains μ_K, the unit group of $\mathcal{O}_K$, and we have an isomorphism*

$$\mathbf{Z}[G_{K_\mathfrak{p}}]/(N_{G_{K_\mathfrak{p}}}) \cong \mathcal{E}/\mu_K$$

where the $G_{K_\mathfrak{p}}$-norm map is defined by

$$N_{G_{K_\mathfrak{p}}} := \sum_{\sigma \in G_{K_\mathfrak{p}}} \sigma \in \mathbf{Z}[G_{K_\mathfrak{p}}].$$

Proof. Let g be a primitive root modulo p. Without loss of generality let us assume that g is odd. Consider the product

$$\prod_{i=1}^{(p-1)/2} \sigma_g^i(\epsilon_g) = \prod_{i=1}^{(p-1)/2} \frac{\phi\left(\frac{g^{i+1}}{p}, 0, \theta\right)}{\phi\left(\frac{g^i}{p}, 0, \theta\right)} {\zeta_p}^{k(g)(i+1)^2}.$$

It is easy to see that this product involves $W_K/2$ copies of $N_{G_{K_\mathfrak{p}}}(\epsilon_g)$, the norm of ϵ_g. The sum of the powers of ζ_p appearing in the above product is given by

$$\sum_{i=0}^{(p-1)/2} k(g)(i+1)^2 = k(g)\frac{g^{p-1}-1}{g^2-1}$$

and it is congruent to zero modulo p. Therefore the power of the p-th root of unity in the product is zero. Cancelling the repeating terms we obtain

$$\prod_{i=0}^{(p-1)/2} \sigma_g^i(\epsilon_g) = \frac{\phi\left(\frac{g^{(p-1)/2}}{p}, 0, \theta\right)}{\phi\left(\frac{1}{p}, 0, \theta\right)}.$$

Since g is odd, it is a primitive root not only modulo p but also modulo $2p$. Therefore we have $g^{(p-1)/2} \equiv -1 \pmod{2p}$. Finally we obtain

$$\prod_{i=0}^{p-1} \sigma_g^i(\epsilon_g) = \frac{\phi\left(\frac{-1}{p}, 0, \theta\right)}{\phi\left(\frac{1}{p}, 0, \theta\right)} = -1,$$

using the fact that $\varphi(u+1, 0, \theta) = -\varphi(u, 0, \theta)$. It follows that $N_{G_{K_\mathfrak{p}}}(\epsilon_g)^{(W_K/2)} = -1$ and μ_K is generated by the $G_{K_\mathfrak{p}}$-norm of ϵ_g, an elliptic unit. This shows that $\mu_K \subset \mathcal{E}$.

Let us consider $G_{K_\mathfrak{p}}$-homomorphism

$$\mathbf{Z}[G_{K_\mathfrak{p}}] \longrightarrow \mathcal{E}/\mu_K$$

given by $\varphi \mapsto \epsilon_g^\varphi$. The element φ is in the kernel if only if it is a multiple of $N_{G_{K_\mathfrak{p}}}$. Therefore

$$\mathbf{Z}[G_{K_\mathfrak{p}}]/(N_{G_{K_\mathfrak{p}}}) \cong \mathcal{E}/\mu_K.$$

$\diamond$

Following the cyclotomic setup, see the equation (3.1), define

$$B_{K_\mathfrak{p}} := \mathcal{O}_{K_\mathfrak{p}}^*/\mathcal{E}$$

which is a multiplicative $\mathbf{Z}[G_{K_\mathfrak{p}}]$-module. It is a well-known fact that $B_{K_\mathfrak{p}}$ is finite and its order is equal to the class number of $K_\mathfrak{p}$. In fact we have something stronger.

Theorem 4.7 *Let H be a subgroup of $G_{K_\mathfrak{p}}$. Then we have*

$$\#Cl(K_\mathfrak{p}^H) = [(\mathcal{O}_{K_\mathfrak{p}}^*)^H : \mathcal{E}^H].$$

Proof. This is a generalization of the Stark's proof [8, p.229] for $H = \{1\}$. We start with the class number formula which gives us

$$\#\mathrm{Cl}(K_\mathfrak{p}^H)\mathrm{Reg}\left((\mathcal{O}_{K_\mathfrak{p}}^*)^H\right) = \prod_{\chi\neq 1} L'(0,\chi)$$

where the product runs over nontrivial characters of $\mathrm{Gal}(K_\mathfrak{p}^H/K)$. Let e be the order of the subgroup H and suppose that $\#G_{K_\mathfrak{p}} = (p-1)/W_K = e\tilde{e}$. The Galois group $\mathrm{Gal}(K_\mathfrak{p}^H/K)$ is isomorphic to $G_{K_\mathfrak{p}}/H$. In fact we have

$$\mathrm{Gal}(K_\mathfrak{p}^H/K) = \{\sigma_g^i|_{K_\mathfrak{p}^H} : 0 \leq i \leq \tilde{e}-1\}$$

where σ_g is a generator of $G_{K_\mathfrak{p}}$ for some primitive root g modulo p. Each nontrivial character χ has conductor p in the ray class group $I_K(\mathfrak{p})/P_{K,1}(\mathfrak{p})$, which is isomorphic to $(\mathbf{Z}/p\mathbf{Z})^*/\psi(\mu_K)$, and therefore primitive. By [8, Theorem 2], we have

$$L'(0,\chi) = -\frac{1}{W_K}\sum_{i=1}^{\tilde{e}-1}\chi(\sigma_g^i)\log\left(|N_H(\pi(g^i))|^2\right)$$

where $N_H = \sum_{\tau\in H}\tau$ is the H-norm and $\pi(g^i)$ is given by Theorem 4.2. In order to use the theory of group determinants, let us define

$$f : \sigma_g^i \longmapsto \log\left(|N_H(\pi(g^i))|^2\right)$$

a function of $\mathrm{Gal}(K_\mathfrak{p}^H/K)$. Now we have

$$\begin{aligned}
\#\mathrm{Cl}(K_\mathfrak{p}^H)\mathrm{Reg}\left((\mathcal{O}_{K_\mathfrak{p}}^*)^H\right) &= \prod_{\chi\neq 1} L'(0,\chi) \\
&= \pm\frac{1}{(W_K)^{\tilde{e}}}\prod_{\chi\neq 1}\sum_{i=1}^{\tilde{e}-1}\chi(\sigma_g^i)f(\sigma_g^i) \\
&= \pm\frac{1}{(W_K)^{\tilde{e}}}\det\left[f(\sigma_g^{i-j}) - f(\sigma_g^i)\right]_{i,j\neq 0}
\end{aligned}$$

by [10, Lemma 5.26]. It easy to see that

$$f(\sigma_g^{i-j}) - f(\sigma_g^i) = \log\left(\left|N_H\left(\frac{\pi(g^{i-j})}{\pi(g^i)}\right)\right|^2\right).$$

Both elements $\pi(g^{i-j}), \pi(g^i)$ are of norm p and their quotient is an elliptic unit. In fact we have

$$\frac{\pi(g^{i-j})}{\pi(g^i)} = \left[\sigma_g^i(\epsilon_{-j})\right]^{W_K}$$

by definition. Finally we obtain

$$\begin{aligned}\#\mathrm{Cl}(K_{\mathfrak{p}}^H)\mathrm{Reg}\left((\mathcal{O}_{K_{\mathfrak{p}}}^*)^H\right) &= \pm\det\left[2\log\left|N_H\left(\sigma^i(\epsilon_{-j})\right)\right|\right]_{i,j\neq 0} \\ &= \mathrm{Reg}\left(\mathcal{E}^H\right)\end{aligned}$$

and it follows that the index of $\mathcal{E}^H$ in the full unit group of $K_{\mathfrak{p}}^H$ is exactly the class number of $K_{\mathfrak{p}}^H$. ◇

4.2 Galois Module $B_{K_{\mathfrak{p}}}$

Similar to the real cyclotomic case, we want to work with $B_{K_{\mathfrak{p}}}$ in order to investigate the class number of $K_{\mathfrak{p}}$. We first give the analogue of Proposition 3.3 in the elliptic case.

Proposition 4.8 *Let H be a subgroup of $G_{K_{\mathfrak{p}}}$. Then the sequence of H-invariants*

$$0 \longrightarrow \mathcal{E}^H \longrightarrow {\mathcal{O}_{K_{\mathfrak{p}}}^*}^H \longrightarrow B_{K_{\mathfrak{p}}}^H \longrightarrow 0$$

is exact. In particular $B_{\mathbf{Q}_{(p)}}^G = 0$.

Proof. The proof is identical with Schoof's proof for real cyclotomic fields except one step. We need to show that ϵ_g, the generator of elliptic units, is congruent to a primitive root modulo $\mathfrak{P} \subset K_{\mathfrak{p}}$, the unique prime ideal lying above p. We have

already shown that $N_{G_{K_\mathfrak{p}}}(\epsilon_g)$ generates the roots of unity μ_K within the proof of Lemma 4.6. This gives us that

$$\left[N_{G_{K_\mathfrak{p}}}(\epsilon_g)\right]^{W_K/2} \equiv -1 \pmod{\mathfrak{P}}$$

and since we have $\sigma(\mathfrak{P}) = \mathfrak{P}$, it is easy to see that $\sigma(\epsilon_g) \equiv \epsilon_g \pmod{\mathfrak{P}}$ for all $\sigma \in G_{\mathbf{Q}_{(p)}}$. This implies that

$$\epsilon_g^{(p-1)/2} \equiv -1 \pmod{\mathfrak{P}}.$$

and finishes the proof. $\diamond$

Let B and C be the submodules of $B_{K_\mathfrak{p}}$ and $\mathrm{Cl}(K_\mathfrak{p})$, respectively, all of whose simple Jordan-Hölder factors have some fixed order $q = l^f$. Each submodule B or C is the product of the Jordan-Hölder factors of degree d, where d runs over the divisors of $(p-1)/W_K$ for which q is the smallest power of l that is congruent to 1 modulo d. Combining Theorem 4.7 with Proposition 4.8, we obtain

$$\#\mathrm{Cl}(K_\mathfrak{p}^H) = \#B_{K_\mathfrak{p}}^H.$$

It follows $\#B = \#C$ by the fact that the degree d part of $\mathrm{Cl}(K_\mathfrak{p})$ (or $B_{K_\mathfrak{p}}$) is precisely the part that appears in the subfield of degree

$$d = \#\mathrm{Gal}(K_\mathfrak{p}^H/K),$$

but not in any proper subfield.

The following fact is another consequence of Proposition 4.8 and it is used in the first step of our algorithm.

Proposition 4.9 *Let $p > 2$ be a prime. The module $B_{K_\mathfrak{p}}$ does not admit any simple Jordan-Hölder factors of degree $d = 1$. In particular, it does not admit any such factors of order $q = 2$.*

Proof. Change the field $\mathbf{Q}_{(p)}$ with its analogue $K_{\mathfrak{p}}$ in the proof of Proposition 3.4. The result follows easily. $\diamond$

Let F be the number field given by $K_{\mathfrak{p}}(\zeta_{2M})$ where $M > 1$ is a power of a prime l. We use a different notation for prime ideals in F for the elliptic case since we have one more level of field extensions. Given an unramified prime ideal $\mathcal{R} \subset F$ of degree one, we have the following diagram:

$$\begin{array}{cc} F & \mathcal{R} \\ | & \\ K_{\mathfrak{p}} & \mathfrak{R} \\ | & \\ K & \mathfrak{r} \\ | & \\ \mathbf{Q} & r \end{array}$$

In order to obtain the main tool for our algorithm, we need to construct a special Kummer extension of F, similar to the real cyclotomic case. We start with the following lemma.

Lemma 4.10 *Let M be a power of a prime l and $F = K_{\mathfrak{p}}(\zeta_{2M})$. The kernel of the map*

$$\psi : \mathcal{O}^*_{K_{\mathfrak{p}}}/(\mathcal{O}^*_{K_{\mathfrak{p}}})^M \longrightarrow \mathcal{O}^*_F/(\mathcal{O}^*_F)^M$$

is trivial if l is odd. It has order 2 and is generated by -1 if $l = 2$

Proof. Change $\mathbf{Q}_{(p)}$ with $K_{\mathfrak{p}}$ in the proof of Lemma 3.5. The automorphism $\tau \in \Delta = \mathrm{Gal}(F/K_{\mathfrak{p}})$, sending ζ_{2M} to its inverse, does not correspond to the complex conjugation anymore since the ground field $K_{\mathfrak{p}}$ is imaginary.

Suppose x is in the kernel of ψ. Then $x = y^M$ for some $y \in \mathcal{O}_F^*$. It is easy to see that $\tau(y) = y\zeta_M^i$ for some $i \in \mathbf{Z}$. Pick $\tilde{y} = y\zeta_{2M}^i$. It follows that

$$\tau(\tilde{y}) = \tau(y)\zeta_{2M}^{-i} = y\zeta_{2M}^i = \tilde{y}$$

and without loss of generality we can assume $\tau(y) = y$.

Observe that the field $F = K_{\mathfrak{p}}(\zeta_{2M})$ lies in the ray class field $K_{(2Mp)}$ and therefore it is an abelian extension of K. The rest of the proof follows easily from the proof of Lemma 3.5. ◇

This lemma enables us to identify the group $\mathcal{O}_{K_{\mathfrak{p}}}^*/\mu_K(\mathcal{O}_{K_{\mathfrak{p}}}^*)^M$ with a subgroup of $F^*/(F^*)^M$. The field $F = K_{\mathfrak{p}}(\zeta_{2M})$ contains the M-th roots of unity. Therefore we have

$$\mathrm{Gal}\left(F\left(\sqrt[M]{\mathcal{O}_{K_{\mathfrak{p}}}^*}\right)/F\right) \cong \mathrm{Hom}_Z\left(\frac{\mathcal{O}_{K_{\mathfrak{p}}}^*}{\mu_K}, \mu_M\right). \tag{4.4}$$

by Kummer theory. Now we are ready to give the main tool for our algorithm, the analogue of Theorem 3.6 in the elliptic case, and give the construction of elements $f_{\mathcal{R}}(\epsilon_g)$.

Theorem 4.11 *Let $M > 1$ be a power of a prime l and let I denote the augmentation ideal of the group ring $R = (\mathbf{Z}/M\mathbf{Z})[G_{K_{\mathfrak{p}}}]$. There is a natural isomorphism of $G_{K_{\mathfrak{p}}}$-modules*

$$B_{K_{\mathfrak{p}}}[M]^{\perp} \cong I/\langle f_{\mathcal{R}}(\epsilon_g) : \mathcal{R} \in S\rangle$$

where S denotes the set of unramified prime ideals $\mathcal{R}$ of $F = K_{\mathfrak{p}}(\zeta_{2M})$ of degree one.

Proof. Change $\mathbf{Q}, (p), \mathcal{C}, \eta_g, f_{\mathfrak{R}}(\eta_g)$ with $K, \mathfrak{p}, \mathcal{E}, \epsilon_g, f_{\mathcal{R}}(\epsilon_g)$ respectively in the proof of Theorem 3.6. The result follows easily. ◇

The construction of elements

$$f_{\mathcal{R}}(\epsilon_g) = \sum_{\sigma \in G_{K_\mathfrak{p}}} c_\sigma \sigma$$

is identical to the construction of $f_{\mathfrak{R}}(\eta_g)$ in the real cyclotomic case. In order to determine the coefficients $c_\sigma \in \mathbf{Z}/M\mathbf{Z}$, we use the relation

$$\sigma(\epsilon_g)^{(r-1)/M} \equiv \zeta_M^{c_\sigma} \pmod{\mathcal{R}}$$

where ζ_M is a primitive M-th root of unity in $F = K_\mathfrak{p}(\zeta_{2M})$.

4.3 The Algorithm

In order to construct elements $f_{\mathcal{R}}(\epsilon_g)$ given in the previous section, we need to determine several unramified degree one prime ideals $\mathcal{R}$ of $F = K_\mathfrak{p}(\zeta_{2M})$ and the integer values $\sigma(\epsilon_g) \pmod{\mathcal{R}}$ for any $\sigma \in G_{K_\mathfrak{p}}$.

Construction of the prime ideals $\mathcal{R}$ can be done using class field theory. We start with a degree one prime ideal $\mathfrak{r} \subset \mathcal{O}_K$ with norm $r \equiv 1 \pmod{2M}$ and check if its generator $\pi_\mathfrak{r}$ satisfies $(\pi_\mathfrak{r})^{W_K} \equiv 1 \pmod{\mathfrak{p}}$. This implies that $\mathfrak{r}$ totally splits in F.

Even tough we can easily obtain the prime ideals $\mathcal{R}$, it is not easy to find $\sigma(\epsilon_g) \pmod{\mathcal{R}}$ for any $\sigma \in G_{\mathbf{Q}_{(p)}}$. The main reason is that, unlike the cyclotomic case, we do not have an algebraic expression for ϵ_g.

Now we describe how to find $\sigma(\epsilon_g) \pmod{\mathcal{R}}$ for any $\sigma \in G_{\mathbf{Q}_{(p)}}$ by using r-adic numbers $\mathbf{Q}_r$. Let g be a primitive root modulo p, and let σ_g be the corresponding element generating the Galois group $G_{K_\mathfrak{p}}$. Given $\alpha \in \mathcal{O}_{K_\mathfrak{p}}$, define the polynomial

$$P_\alpha(x) := \prod_{i=0}^{n-1} (x - \sigma_g^i(\alpha)) \in \mathcal{O}_K[x]$$

where $n = (p-1)/W_K$ is the degree of the extension $K_{\mathfrak{p}}/K$. Since the prime ideal $\mathfrak{r} \subset \mathcal{O}_K$ splits totally in the extension $K_{\mathfrak{p}}/K$, we have an injection

$$K_{\mathfrak{p}} \hookrightarrow \mathbf{Q}_r$$

which is uniquely determined by the image of ϵ. Consider the factorization of the polynomial

$$P_{\epsilon_g}(x) = \prod_{i=0}^{n-1}(x - e_i)$$

in the ring $\mathbf{Q}_r[x]$. Let us fix an injection of $K_{\mathfrak{p}}$ into $\mathbf{Q}_r$ which maps ϵ_g to e_0. For a given element $\alpha \in K_{\mathfrak{p}}$, we denote the corresponding element in $\mathbf{Q}_r$ by $\tilde{\alpha}$. For each $0 \leq i \leq n-1$, there exists j_i such that

$$\sigma_g^i(\tilde{\epsilon_g}) = e_{j_i}.$$

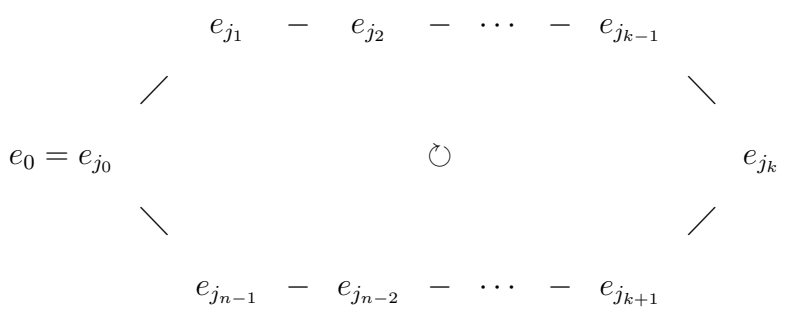
We already have $j_0 = 0$. In order to determine j_1, let us consider the factorization of the polynomial

$$P_{\epsilon_g \sigma_g(\epsilon_g)}(x) = \prod_{k=0}^{n-1}(x - h_k)$$

in the ring $\mathbf{Q}_r[x]$. We determine those $1 \leq i \leq n-1$ for which the product $e_0 e_i$ is equal to h_k for some $0 \leq k \leq n-1$. There are only two such values; one of them is for $\tilde{\epsilon_g}\sigma_g(\tilde{\epsilon_g})$ and the other one is for $\sigma_g^{-1}(\tilde{\epsilon_g}\sigma_g(\tilde{\epsilon_g}))$. We apply this algorithm until we obtain a cycle

connecting each e_i to those two values. Finally we need to determine if $\sigma^i(\tilde{\epsilon_g})$ is obtained by going clockwise or counterclockwise. We use the factorization of the

polynomial $P_{\epsilon_g\sigma_g(\epsilon_g)\sigma_g^3(\epsilon_g)}(x)$ in the ring $\mathbf{Q}_r[x]$ to check which direction is correct. Finally we obtain the cycle



with the property $\sigma_g^i(\tilde{\epsilon}_g) = e_{j_i}$.

The choice $\tilde{\epsilon_g} = e_0$ corresponds to a unique prime ideal $\mathcal{R} \subset K_\mathfrak{p}$ so that $\epsilon_g \pmod{\mathcal{R}^n}$ is given by $e_{j_i} \pmod{r^n}$ for all $n \geq 1$. Now it is easy to see that the integer value $\sigma_g^i(\epsilon_g) \pmod{\mathcal{R}}$ is given by $e_{j_i} \pmod{r}$ for all $0 \leq i \leq n-1$.

This is all we need, for the construction of $f_\mathcal{R}(\epsilon_g)$. Since we need to go through this process every time, our analogue of Schoof's algorithm is slower than the original. That's why our ranges for the norm of conductors and the size of Jordan-Hölder factors are rather small with respect to the ranges Schoof has used.

Let $\mathcal{R}$ be an unramified prime ideal of $F = K_\mathfrak{p}(\zeta_{2M})$ of degree one with underlying primes $\mathfrak{R} \subset K_\mathfrak{p}$ and $\mathfrak{r} \subset K$. In order to compute $f_\mathcal{R}(\epsilon_g)$ we need to make choices for elements ϵ_g and ζ_M modulo $\mathcal{R}$. Consider the following diagram:

$$\begin{array}{cc} F & \mathcal{R} \\ | & \\ K_\mathfrak{p} & \mathfrak{R} \\ | & \\ K & \mathfrak{r} \end{array}$$

If we change $\mathcal{R}$ lying above $\mathfrak{R}$, then it corresponds to a different choice of ζ_M. Therefore the elements $f_\mathcal{R}(\epsilon_g)$ differ from each other by a unit of $\mathbf{Z}/M\mathbf{Z}$ for a

different choice of $\mathcal{R}$ over a fixed $\mathfrak{R}$. Changing $\mathfrak{R}$ over $\mathfrak{r}$ is equivalent to change ϵ_g with one of its conjugates. Such a change corresponds to multiplying $f_{\mathcal{R}}(\epsilon_g)$ with a power of σ_g, a unit in $(\mathbf{Z}/M\mathbf{Z})[G_{\mathbf{Q}_{(p)}}]$. Therefore the ideal generated by elements $f_{\mathcal{R}}(\epsilon_g)$ only depend on the prime ideals $\mathfrak{r}$ in the ground field K.

Now we reformulate our previous results in terms of polynomials. It is easy to see that we have an isomorphism

$$(\mathbf{Z}/M\mathbf{Z})[G_{K_\mathfrak{p}}] \cong (\mathbf{Z}/M\mathbf{Z})[X]/(X^{(p-1)/W_K} - 1)$$

obtained by $\sigma_g \mapsto X$. Let $f_\mathfrak{r}(X)$ denote the image of $f_{\mathcal{R}}(\epsilon_g)$ under this isomorphism which is well-defined up to a unit. We denote the augmentation ideal of both rings by I.

Theorem 4.12 *Using the notation above, we have that*

$$B_{K_\mathfrak{p}}[M]^\perp = I/\langle f_\mathfrak{r}(X) : \mathfrak{r} \in S_M \rangle$$

where S_M is the set of prime ideals $\mathfrak{r} = (\pi_\mathfrak{r})$ in $\mathcal{O}_K$ of norm r satisfying $(\pi_\mathfrak{r})^{W_K} \equiv 1 \pmod{\mathfrak{p}}$ and $r \equiv 1 \pmod{2M}$.

Proof. This easily follows from Theorem 4.11. ◇

Now we are ready to determine if $B_{K_\mathfrak{p}}$ admits a Jordan-Hölder factor of order $q = l^f$ or not. Any finite R-module is Jordan-Hölder isomorphic to its dual and we have

$$B_{K_\mathfrak{p}}^\perp = \prod_l \prod_\varphi (B_{K_\mathfrak{p}}^\perp)_\varphi$$

by the Jordan-Hölder filtration given in Section 2.1. The irreducible polynomials φ are obtained by factoring $X^m - 1$ in l-adic polynomial ring $\mathbf{Z}_l[X]$ where m is given by $(p-1)/W_K = l^a m$ with $\gcd(m, l) = 1$.

4.3.1 Step 1

This step is very similar to the Step 1 of Schoof's algorithm and we check if $B_{K_\mathfrak{p}}^{\perp}$ admits any Jordan-Hölder factors of order q at all. Fix p and $q = l^f$. The possible degree d of these factors all divide

$$\delta = \gcd\left((p-1)/W_K, q-1\right).$$

Proposition 4.9 implies that the first step is trivial if $\delta = 1$. Otherwise we compute

$$f_\mathfrak{r}(X) \pmod{X^\delta - 1}$$

for several prime ideals $\mathfrak{r} \in S_M$ with $M = l$.

Computing the greatest common divisors of these elements recursively, we look for a common divisor $\varphi \neq X - 1$ of degree exactly f. If we guarantee that there is no such factor, we stop. Then using Theorem 4.12, we conclude that

$$\frac{B_{K_\mathfrak{p}}[l]^{\perp}}{\varphi B_{K_\mathfrak{p}}[l]^{\perp}}$$

is zero for all $\varphi \neq X - 1$ of degree f. This follows that $B_{K_\mathfrak{p}}^{\perp}$, and therefore $B_{K_\mathfrak{p}}$, does not admit any Jordan-Hölder factors of order q.

If there is a repeating factor $\varphi | \frac{X^\delta - 1}{X-1}$ with $\deg(\varphi) = f$ (possibly more than one) then we believe that $B_{K_\mathfrak{p}}$ admits a non-trivial Jordan-Hölder factor of order q and we proceed to the second step of the algorithm.

4.3.2 Step 2

This step is identical to the Step 2 of Schoof's algorithm. At the end, we obtain an explicit ideal $\mathcal{I}^{(M)} \subset R$ and a surjective homomorphism

$$R/\mathcal{I}^{(M)} \twoheadrightarrow (B_{K_\mathfrak{p}}^{\perp})_\varphi$$

which is likely to be an isomorphism.

4.3.3 Step 3

Except one essential point, this step is also identical to the corresponding step of Schoof's algorithm. Let M be the power of a prime l from Step 2. In his algorithm, Schoof relies on computing Mth roots of real numbers which can be easily done for real cyclotomic fields. In our case we have to work with imaginary fields $K_{\mathfrak{p}}$ in which the correct Mth root of an element is not obvious. Instead of complex numbers, we embed our number field $K_{\mathfrak{p}}$ into $\mathbf{Q}_r$, r-adic rational numbers, for some special prime $r \in \mathbf{Z}$. The rational prime r must split totally in $K_{\mathfrak{p}}$ so that embedding is possible. We also require that $r \not\equiv 1 \pmod{l}$ which makes taking Mth root unique in $\mathbf{Q}_r$.

4.3.4 Example

Let $K = \mathbf{Q}(w)$ be the imaginary quadratic field with $w = (\sqrt{-67}+1)/2$. Let $\mathfrak{p}_{421} \subset \mathcal{O}_K$ be the degree one prime ideal of norm $p = 421$ with $w_{\mathfrak{p}} = 85$. We fix a basis $[421, 85 - w]$ for $\mathfrak{p}$ so that the number $\theta = 421/(85 - w)$ is in the upper half plane. The Galois group $\mathrm{Gal}(K_{\mathfrak{p}_{421}}/K)$ is isomorphic to $(\mathbf{Z}/421\mathbf{Z})^*/\{\pm 1\}$. Let $g = 23$ be an odd primitive root modulo 421. By definition

$$\epsilon_g = \frac{\phi\left(\frac{g}{p}, 0, \theta\right)}{\phi\left(\frac{1}{p}, 0, \theta\right)} \zeta_p{}^{k(g)}$$

and we will use Lemma 4.5 to find $k(g)$. It is easy to find a split prime $\mathfrak{q} = (8w - 175)$ of norm $q = 30313$ with the properties $q \equiv 1 \pmod{12p}$ and the Artin symbol $\sigma_{\mathfrak{q}}$ is non-trivial in $\mathrm{Gal}(K_{\mathfrak{p}}/K)$. Here $x_{\mathfrak{q}} = 8$ and $y_{\mathfrak{q}} = -175$. Set $m = 337$ since $-(x_{\mathfrak{q}} w + y_{\mathfrak{q}}) \equiv 337 \pmod{\mathfrak{p}}$. Finally we obtain

$$k(g) = \frac{g^2 - 1}{m^2 - 1} k(m) \pmod{p}$$

where $k(m) = x_{\mathfrak{q}}m/2 \pmod{p}$ by Lemma 4.5. Moreover we can compute all Galois conjugates $\sigma_g^i(\epsilon_g)$ using Lemma 4.3.

Applying Step 1 with $\delta = 2 = \gcd((421-1)/2, 3-1)$ for several primes $\mathfrak{r} \subset \mathcal{O}_K$ we see that the non-trivial factor $\varphi = X+1$ appears every time. We start to believe that $(B_{K_{\mathfrak{p}_{421}}})_\varphi$ is non-trivial. We write the degree of the extension 210 as a product $l^a m$ where m is coprime to $l = 3$. This gives us $a = 1$ and $(B_{K_{\mathfrak{p}_{421}}})_\varphi$ is a module over the ring $\mathbf{Z}_3[X]/(\varphi(X^3)) \cong \mathbf{Z}_3[X]/(X^3+1)$.

Following Schoof, we introduce a new variable for simpler computations. Observe that X has order 6 in the local ring $\mathbf{Z}_3[X]/(X^3+1)$. We pick $1+T = X^2$ as in Iwasawa theory so that the maximal ideal of the local ring

$$\mathbf{Z}_3[T]/((1+T)^3 - 1) \cong \mathbf{Z}_3[X]/(X^3+1)$$

is of the form $(T, 3)$. Now we perform Step 2 for $M \in \{3, 9, 27, ...\}$ and compute elements in $(\mathbf{Z}/M\mathbf{Z})[T]/((1+T)^3 - 1)$.

$\mathfrak{r} = (r, w - w_{\mathfrak{r}})$	$M = 3$	$M = 9$	$M = 27$
$(248509, w - 14797)$	T^2	$T^2 + 6T$	$10T^2 + 24T$
$(297757, w - 78203)$	0	$6T^2 + 6$	$15T^2 + 18T + 15$
$(306991, w - 59125)$	0	$3T^2$	$3T^2$
$(317197, w - 24608)$	T^2	$T^2 + 6T + 3$	$T^2 + 24T + 3$
$(354727, w - 104164)$	0	$3T^2 + 3T + 3$	$12T^2 + 3T + 12$
$(458569, w - 272363)$	$2T^2$	$2T^2 + 3T + 6$	$20T^2 + 12T + 15$

For $M = 3$, we compute $\mathcal{I}^{(3)}$ generated by $f_{\mathfrak{r}}$ in the corresponding column. After several tries, we believe that $\mathcal{I}^{(3)}$ is generated by T^2. We have a surjective map

$$(\mathbf{Z}/3\mathbf{Z})[T]/(T^2) \twoheadrightarrow \left((B_{K_{\mathfrak{p}_{421}}})_\varphi[3]\right)^\perp \tag{4.5}$$

which we believe to be an isomorphism.

For $M = 9$, the ideal $\mathcal{I}^{(9)}$ is generated by T^2 and 3. The module $(\mathbf{Z}/9\mathbf{Z})[T]/(T^2, 3)$ is isomorphic to the previous one and this concludes Step 2.

We suspect that $(B_{K_{\mathfrak{p}_{421}}})_\varphi$ is isomorphic to $\mathbf{Z}_3[T]/(T^2, 3)$. In order to verify this we apply step 3. We use the surjective map above with Proposition 2.2 (4). We have $R = (\mathbf{Z}/3\mathbf{Z})[T]/((1+T)^3 - 1)$ and $J = (T^2)$ so that $\mathrm{Ann}_R(J) = (T)$. Since $1 + T = X^2$, we have $T = X^2 - 1$. Let

$$h_\varphi(X) = \frac{X^{210} - 1}{X^3 + 1}(X^2 - 1)$$

in $(Z/3\mathbf{Z})[X]/(X^{210} - 1)$. We define an elliptic unit $\epsilon_\varphi := \epsilon_g^{h_\varphi(\sigma)}$ and we want to show that it is a third power of another unit in $K_\mathfrak{p}$. Let K_6 be the unique subfield of $K_\mathfrak{p}$ such that $[K_6 : K] = 6$. Observe that $X^3 + 1$ divides $X^6 - 1$. This implies that the norm map from $K_\mathfrak{p}$ to K_6, divides $h_\varphi(X)$ and therefore $\epsilon_\varphi \in K_6$. In fact the minimal polynomial of ϵ_φ is given by

$$\begin{aligned} F(t) = t^6 \quad & +(25552848w + 62631721)t^5 \\ & +(63659755470266w - 10490555538824)t^4 \\ & +(825954922943743w - 12797162812861606)t^3 \\ & +(-4136459180619w - 1293163421150)t^2 \\ & +(23197957w - 46562185)t + 1. \end{aligned}$$

Now we compute $G(t) = \prod_{i=1}^{6} \sqrt[3]{t - \sigma_g^i(\epsilon_\varphi)}$. We obtain the correct third roots of ϵ_φ using r-adic integers $\mathbf{Q}_r$ with r totally split in the extension $K_\mathfrak{p}/\mathbf{Q}$ and $r \not\equiv 1 \pmod 3$. We have

$$\begin{aligned} G(t) = t^6 \quad & +(-96w - 140)t^5 + (7630w + 53784)t^4 \\ & +(6920w - 233277)t^3 + (-3819w - 23252)t^2 \\ & +(-127w + 144)t + 1. \end{aligned}$$

This shows that $\epsilon_\varphi = u^3$ for some $u \in K_6 \subset K_{\mathfrak{p}}$. We conclude that the module $(B^{\perp}_{K_{\mathfrak{p}421}})_\varphi$ is actually isomorphic to $\mathbf{Z}_3[T]/(T^2, 3)$.

4.4 Heuristics for the Elliptic Case

In this section, we estimate the behavior of Jordan-Hölder factors of the ideal class group $\mathrm{Cl}(K_{\mathfrak{p}})$ that have very large order by using the ideas given in Section 3.4. We can use Schoof's results since we work with cyclic extensions of number fields in the elliptic case as well. According to Cohen-Lenstra heuristics, the probability that the class group of $K_{\mathfrak{p}}$ does not admit any simple Jordan-Hölder factor of order q at all is at least

$$H_{K_{\mathfrak{p}}}(p,q) = \left(\prod_{k \geq 2} 1 - q^{-k} \right)^{n_{p,q}}.$$

Observe that not all the primes p leads to extensions $K_{\mathfrak{p}}/K$. If the rational prime p is inert in the extension $K/\mathbf{Q}$ then we define $H_{K_{\mathfrak{p}}}(p,q)$ to be 1. Now it is easy to see that

$$H_{K_{\mathfrak{p}}}(p,q) \geq H_{\mathbf{Q}_{(p)}}(p,q).$$

for all values of p and q. The tables in Section 5.2 contain the numbers $\tilde{h}_{K_{\mathfrak{p}}}$, the order of the subgroup of $\mathrm{Cl}(K_{\mathfrak{p}})$ that admit only Jordan-Hölder factors of order $q < Q = 2000$, for $\mathfrak{p}$ of norm $p < P = 700$. The numbers $\tilde{h}_{K_{\mathfrak{p}}}$ are all equal to the class numbers of the corresponding fields with probability at least

$$\mathcal{P}_K = \prod_{p<P} \prod_{q>Q} H_{K_{\mathfrak{p}}}(p,q).$$

The calculations given in [7, p. 933-934] is suitable for our purpose and we have

$$-\log(\mathcal{P}_K) < c\frac{\pi_K(700)}{2000}$$

where $c = 1.29573095...$ and $\pi(n)$ is the number of odd primes which split in K less than n. The number $\pi(n)$ corresponds to the number of extension $K_{\mathfrak{p}}$ for each K. The largest set of $K_{\mathfrak{p}}$ appears for $d_K = -67$ and there are 63 ray class fields $K_{\mathfrak{p}}$ with conductor $\mathfrak{p}$ of norm less than 700. Therefore we have

$$\mathcal{P}_K > 0.96000621...$$

for each ground field K.

CHAPTER 5

RESULTS

In this chapter we explain the results based on the data we collect from our algorithm. In the first section we give a counterexample to the elliptic analogue of Vandiver's conjecture. In the second section, we give a table for each K involving the order of the largest submodule of $B_{K_\mathfrak{p}}$ with Jordan-Hölder factors of order less than 2000. We explain how to obtain the structure of $(B_{K_\mathfrak{p}})_\varphi$ for each Jordan-Hölder factor listed in the tables. We also give an example showing that $B_{K_\mathfrak{p}}$ and $\mathrm{Cl}(K_\mathfrak{p})$ are not isomorphic as Galois modules.

5.1 Counterexample

Let K be the imaginary quadratic field $\mathbf{Q}(\sqrt{-163})$ and let $\mathfrak{p}_{307}$ be a degree one prime ideal in $\mathcal{O}_K$ of norm 307. Computing $f_\mathcal{R}(\epsilon_g)$ for several primes, we observe that the factor $\varphi = X + 92$ appears every time. As it is described in the third step of the algorithm, we first find the generators for $\mathrm{Ann}(\varphi)$, the annihilator of the ideal generated by φ. It is easy to see that the ideal $\mathrm{Ann}(\varphi)$ is principal since $(\mathbf{Z}/307\mathbf{Z})[X]/(X^{153} - 1)$ is a principal ideal domain. A generator for $\mathrm{Ann}(\varphi)$ is given by

$$\psi = \frac{X^{153} - 1}{X + 92} \in (\mathbf{Z}/307\mathbf{Z})[X]/(X^{153} - 1).$$

and we define

$$\epsilon_\varphi := \epsilon_g^\psi$$

which is an elliptic unit in $K_\mathfrak{p}$. In order to show that the class number of $K_\mathfrak{p}$ is divisible by 307, we need to verify that ϵ_φ is a 307th power of a unit u in the same field. The unit u will be automatically non-elliptic since there is no polynomial $f \in \mathbf{Z}[X]$ such that $\psi = 307f$.

We can obtain ϵ_φ with accuracy as high as we want as an imaginary number. However the correct 307-th root of ϵ_φ in $\mathbf{C}$ is not obvious. Therefore we work with $\mathbf{Q}_r$, r-adic rational numbers, for some special prime $r \in \mathbf{Z}$. The rational prime r must split totally in $K_\mathfrak{p}$ so that embedding is possible. We also require that $r \not\equiv 1 \pmod{307}$ which makes taking 307th root in $\mathbf{Q}_r$ unique. For example, $r = 25801$ is such a prime for $\mathfrak{p} = [307, 148 - w]$ where $w = (\sqrt{-163} + 1)/2$.

Factorizing the minimal polynomial of $\epsilon_g \in K_\mathfrak{p}$ in the polynomial ring $\mathbf{Z}_r[x]$ with 1000 digit r-adic precision, we obtain ϵ_g and all its conjugates r-adically. Then we compute

$$G(x) = \prod_{i=1}^{153} \left(x - \sqrt[307]{\sigma_g^i(\epsilon_\varphi)} \right)$$

which has r-adic coefficients. It turns out that each coefficient is an element of $\mathcal{O}_K$ which was verified with the help of the command `algdep` in PARI. We have also verified that the resulting polynomial $G(x) \in \mathcal{O}_K[x]$ generates the extension $K_\mathfrak{p}$ using Chebotarev's density theorem with 5000 primes. We conclude that $\epsilon_\varphi = u^{307}$ for some non-elliptic unit u in $\mathcal{O}^*_{K_{\mathfrak{p}_{307}}}$.

Recall that $B_{K_\mathfrak{p}} = \mathcal{O}^*_{K_\mathfrak{p}}/\mathcal{E}$ for all $K_\mathfrak{p}$. The unit u is a non-trivial element of this quotient group and order of u is equal to 307, a prime number. This implies that 307 divides the order of $B_{K_\mathfrak{p}}$ and finally we obtain

$$307 | \#\mathrm{Cl}(K_{\mathfrak{p}_{307}})$$

using the fact that $B_{K_\mathfrak{p}}$ and $\mathrm{Cl}(K_\mathfrak{p})$ have the same number of elements.

There are interesting family of numbers, namely Bernoulli and Hurwitz numbers, for fields $\mathbf{Q}_{(p)}$ and $K_\mathfrak{p}$ respectively. These numbers are related to the p-divisibility of the class number of the corresponding field. The Herbrand's Theorem states that if p divides the class number of p-th cyclotomic field $\mathbf{Q}(\zeta_p)$ then it divides the numerator of a Bernoulli number with even index less than $p-1$. It is a well-known fact the class group of the real cyclotomic field $\mathbf{Q}_{(p)}$ injects into the class group of $\mathbf{Q}(\zeta_p)$. Therefore we easily obtain the following result.

Corollary 5.1 *Let p be a prime dividing the class number of $\mathbf{Q}_{(p)}$ then p divides the numerator of a Bernoulli number with even index less than $p-1$.*

In order to illustrate the situation in the elliptic case, we first give the definition of Hurwitz numbers following Robert [5]. Let K be an imaginary quadratic field and let $\mathcal{O}_K$ be its ring of integers considered as a lattice in complex numbers. The Hurwitz numbers attached to $\mathcal{O}_K$ are the numbers

$$G_k(\mathcal{O}_K) = \sum_{\substack{\lambda \in \mathcal{O}_K \\ \lambda \neq 0}} \frac{1}{\lambda^k}$$

given by the Eisenstein series of $\mathcal{O}_K$ of weight $k > 2$. It can be shown that these numbers are closely related to the coefficients of the Laurent series expansion of the Weierstrass $\wp$-function. In fact we have

$$\wp(z; \mathcal{O}_K) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2}(\mathcal{O}_K) z^{2k}.$$

Observe that the odd terms do not appear since the Weierstrass $\wp$-function is even. Now we give the analogue of Corollary 5.1 in the elliptic case.

Theorem 5.2 *Let K be an imaginary quadratic field and let $\mathfrak{p} \subset \mathcal{O}_K$ be a degree one prime ideal of norm p not dividing $6d_K$. If p divides the class number of $K_\mathfrak{p}$ then p divides the numerator of $G_k(\mathcal{O}_K)$ for some k divisible by W_K with $0 < k < p-1$.*

Proof. This is a result of Robert's work [5]. A proof, specialized to the case where K has class number one, can be found in [3]. $\diamond$

Now we focus on our counterexample. Let K be the imaginary quadratic field $\mathbf{Q}(\sqrt{-163})$ and let $\mathfrak{p} \subset \mathcal{O}_K$ be a degree one prime ideal of norm 307. The minimal Weierstrass equation of the elliptic curve $E \cong \mathbf{C}/\mathcal{O}_K$ over $\mathbf{Q}$ is given by

$$E : y^2 + y = x^3 - 2174420x + 1234136692.$$

We have used the PARI command `ellwp(E,z)` in order to obtain the Laurent series

$$\wp(z; \mathcal{O}_K) = z^{-2} + 434884z^2 - \frac{705220967}{4}z^4 + \cdots$$

and therefore the Hurwitz numbers $G_k(\mathcal{O}_K)$. We have shown that 307 divides the class number of $K_\mathfrak{p}$. Theorem 5.2 implies that 307 divides the numerator of $G_k(\mathcal{O}_K)$ for some even k between 0 and 306. It turns out that 307 divides the numerator $G_{94}(\mathcal{O}_K)$.

5.2 Tables

Our analogue of Schoof's algorithm gives us the largest submodule of $B_{K_\mathfrak{p}}$ with Jordan-Hölder factors of order less than 2000. We denote the order of this submodule by $\tilde{h}_{K_\mathfrak{p}}$. The observation we make after Proposition 4.8 implies that the number $\tilde{h}_{K_\mathfrak{p}}$ is equal to the largest submodule $\mathrm{Cl}(K_\mathfrak{p})$ with Jordan-Hölder factors of order less than 2000.

There are 9 imaginary quadratic fields with class number one. The discriminant d_K of these fields are given by

$$\{-3, -4, -7, -8, -11, -19, -43, -67, -163\}.$$

For each ground field K, we have worked with degree one prime ideals $\mathfrak{p} \subset K$ of norm p less than 700 and not dividing $6d_K$. In total there are 535 ray class fields $K_\mathfrak{p}$. For 455 of these, we have found that $\tilde{h}_{K_\mathfrak{p}} = 1$. The remaining 80 are given in the tables at the end of this chapter.

In our tables, we use the same format of the main table in Schoof's paper. The numbers $\tilde{h}_{K_\mathfrak{p}}$ are given as a product of the orders of their simple Jordan-Hölder factors. The degree d of each factor is indicated in the third column respectively. If a simple Jordan-Hölder factor $\mathbf{F}_p[X]/(\varphi(X))$ of order q occurs with multiplicity greater than 1, we write $\tilde{h}_{K_\mathfrak{p}}$ as a product $q^{s_0}q^{s_1}\cdots q^{s_n}$ with respective degrees $d, dl, ..., dl^n$ to indicate the orders of $(B_{K_\mathfrak{p}}^{\perp})_\varphi$ modulo $\varphi(X^{l^i})$ are $q^{s_0+\cdots+s_i}$ for $0 \leq i \leq n$.

If $(B_{K_\mathfrak{p}})_\varphi$ has a Jordan-Hölder filtration of length 1, then it is isomorphic to $(Z/lZ)[X]/(\varphi(X))$ as a Galois module. In such a case, $(B_{K_\mathfrak{p}})_\varphi$ has f copies of $\mathbf{Z}/l\mathbf{Z}$ as an abelian group where f is the degree of the irreducible polynomial $\varphi \in \mathbf{Z}_l[X]$. There are 6 cases in which $(B_{K_\mathfrak{p}})_\varphi$ has a Jordan-Hölder filtration of length bigger than 1. We list them in the table below together with the structure of $(B_{K_\mathfrak{p}}^{\perp})_\varphi$. The use of parameter T is explained on page 57.

d_K	p	q	d	length	$(B_{K_\mathfrak{p}}^{\perp})_\varphi$
19	271	4	3	2	$\mathbf{Z}_2[\zeta_3]/4\mathbf{Z}_2[\zeta_3]$
43	397	3	2	2	$\mathbf{Z}_3[T]/(T+3,9)$
67	421	3	2	2	$\mathbf{Z}_3[T]/(T^2,3)$
67	457	3	2	2	$\mathbf{Z}_3[T]/(T-3,9)$
67	461	4	2	2	$\mathbf{Z}/9\mathbf{Z}$
163	641	5	4	3	$\mathbf{Z}/125\mathbf{Z}$

In order to obtain the structure of $(B_{K_\mathfrak{p}})_\varphi$ for these cases, one can use Propo-

sition 2.2 (3) which implies that $(B_{K_\mathfrak{p}})_\varphi \cong (B^\perp_{K_\mathfrak{p}})_\varphi$ whenever the length of $(B^\perp_{K_\mathfrak{p}})_\varphi$ is at most 2. There is only one case with Jordan-Hölder filtration of length bigger than 2, namely $d_K = 163, p = 641, l = 5$. In this case, the annihilator of the module $(B^\perp_{K_\mathfrak{p}})_\varphi$ is principal and we still have $(B_{K_\mathfrak{p}})_\varphi \cong (B^\perp_{K_\mathfrak{p}})_\varphi$ by Proposition 2.2 (2).

It is not true in general that $B_{K_\mathfrak{p}}$ and $\mathrm{Cl}(K_\mathfrak{p})$ are isomorphic as Galois modules. A counterexample for real cyclotomic fields is given by a degree 3 extension of $\mathbf{Q}$ lying in $\mathbf{Q}_{(p)}$. We have looked for a similar example in the elliptic case and in fact we have found one. Let $K = \mathbf{Q}(\sqrt{-163})$ and let $\mathfrak{p}_{2659} \subset \mathcal{O}_K$ be a prime ideal of norm 2659. The ray class field $K_{\mathfrak{p}_{2659}}$ has a unique subfield K_3 such that $[K_3 : K] = 3$. Starting with a generator of elliptic units and then taking its trace from $K_{\mathfrak{p}_{2659}}$ to K_3, we obtain the minimal polynomial of this extension $K_3/\mathbf{Q}$ as follows.

$$\begin{aligned} f_{K_3/\mathbf{Q}} \quad &= x^6 \quad +389x^5 + 18196x^4 - 7076416x^3 \\ &\qquad -488496804x^2 + 48339551084x + 3971404926677. \end{aligned}$$

The software PARI gives us

$$\mathrm{Cl}(K_3) \cong (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z}).$$

as an Abelian group. Let $\varphi = X^2 + X + 1 \in \mathbf{Z}_2[X]$. Since φ is the only irreducible polynomial dividing $\frac{X^3-1}{X-1}$, the Galois module $(\mathrm{Cl}(K_{\mathfrak{p}_{2659}}))_\varphi$ is isomorphic to $\mathrm{Cl}(K_3)$ and it is annihilated by 2. On the other hand $(B_{K_{\mathfrak{p}_{2659}}})_\varphi$ has 16 elements and is a subset of $(\mathbf{Z}/16\mathbf{Z})[X]/(X^2 + X + 1)$. It is clear that $(B_{K_{\mathfrak{p}_{2659}}})_\varphi$ is not annihilated by 2. Therefore $B_{K_\mathfrak{p}}$ and $\mathrm{Cl}(K_\mathfrak{p})$ are not isomorphic as Galois modules in general. However, they have isomorphic Galois cohomology groups.

Proposition 5.3 *There are canonical isomorphisms*

$$\widehat{H}^i(H, Cl(K_\mathfrak{p})) \xrightarrow{\cong} \widehat{H}^{i+2}(H, B_{K_\mathfrak{p}})$$

for each $i \in \mathbf{Z}$. In particular, for each choice of a generator of H there are natural isomorphisms $\widehat{H}^i(H, Cl(K_\mathfrak{p})) \cong \widehat{H}^i(H, B_{K_\mathfrak{p}})$ for each $i \in \mathbf{Z}$.

Proof. The prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ is totally and tamely ramified in the extension $K_\mathfrak{p}/K$. The proof of this proposition can be adapted from its cyclotomic analogue [7, Proposition 5.1 (ii)]. $\diamond$

	p	$\tilde{h}_{K_\mathfrak{p}}$	d	p	$\tilde{h}_{K_\mathfrak{p}}$	d
$d_K = -3$	337	5	4	601	5	4
	433	3	2	613	3	2

	p	$\tilde{h}_{K_\mathfrak{p}}$	d	p	$\tilde{h}_{K_\mathfrak{p}}$	d
$d_K = -4$	281	11	10	521	11	5
	353	3	2	541	4	3
	421	4	3	577	$17 \cdot 37$	$16, 36$

	p	$\tilde{h}_{K_\mathfrak{p}}$	d	p	$\tilde{h}_{K_\mathfrak{p}}$	d
$d_K = -7$	317	3	2	487	4	3
	379	4	3	613	4	3
	463	4	3	631	43	21

	p	$\tilde{h}_{K_\mathfrak{p}}$	d	p	$\tilde{h}_{K_\mathfrak{p}}$	d
$d_K = -8$	281	3	2	601	5	4
	577	$5 \cdot 19$	$4, 9$	643	4	3
	593	5	2	673	5	2

	p	$\tilde{h}_{K_\mathfrak{p}}$	d	p	$\tilde{h}_{K_\mathfrak{p}}$	d
$d_K = -11$	257	5	4	421	$7 \cdot 211$	$3, 35$
	317	3	2	449	$5 \cdot 9$	$4, 8$
	353	67	22	521	11	5

	p	$\tilde{h}_{K_\mathfrak{p}}$	d	p	$\tilde{h}_{K_\mathfrak{p}}$	d
$d_K = -19$	61	7	6	389	3	2
	131	16	5	577	$4 \cdot 97$	$3, 96$
	137	5	4	593	5	4
	163	4	3	617	$3 \cdot 5$	$2, 4$
	229	4	3	619	7	3
	271	$4^2 \cdot 11$	$3, 5$	691	4	3

	p	$\tilde{h}_{K_\mathfrak{p}}$	d	p	$\tilde{h}_{K_\mathfrak{p}}$	d
$d_K = -43$	41	$5 \cdot 11$	$4, 5$	397	$3 \cdot 3$	$2, 6$
	53	3	2	401	$5 \cdot 9$	$4, 4$
	229	13	6	431	31	5
	269	3	2	557	5	2
	307	4	3	613	307	102
	337	$3 \cdot 5$	$2, 4$	661	$3 \cdot 67$	$2, 11$
	353	$5 \cdot 49$	$4, 8$			

	p	$\tilde{h}_{K_\mathfrak{p}}$	d	p	$\tilde{h}_{K_\mathfrak{p}}$	d
$d_K = -67$	17	5	4	421	$3 \cdot 3$	$2, 6$
	37	4	3	449	61	4
	151	11	5	457	$3 \cdot 3$	$2, 6$
	173	5	2	461	3^2	2
	193	49	48	613	19	3
	389	3	2	617	67	11

	p	$\tilde{h}_{K_\mathfrak{p}}$	d	p	$\tilde{h}_{K_\mathfrak{p}}$	d
$d_K = -163$	97	7	3	373	7	3
	113	3	2	409	7	6
	151	61	5	421	$4 \cdot 7$	$3, 6$
	173	3	2	439	13	3
	223	7	3	457	$5 \cdot 419$	$2, 19$
	281	5	4	641	5^3	4
	307	307	153	661	7	3
	367	37	3			

CHAPTER 6

FUTURE WORK

A primary objective of our future work is to continue the investigation of class numbers which is one of the most classical problems in number theory. Another classical problem of great interest is the determination of explicit subgroups of the full unit group of number fields. It is also possible to consider the function field analogue of a problem in number fields. This perspective not only results in an interesting results but also gives insight about the original problem.

In this chapter, we give several projects that could be investigated after our thesis problem. We explain why these problems are interesting and how we are planning to solve them.

6.1 General Imaginary Quadratic Ground Field

In this thesis we focus on imaginary quadratic fields with class number one for which there are nine of them. A natural generalization of our thesis problem would be working with an arbitrary imaginary quadratic field. We can still use Stark's results on the ray class fields $K_{\mathfrak{p}}$ and explicit Galois action given by Shimura's reciprocity.

The main idea in constructing the cyclotomic or elliptic units is to compare the different generators of the unique prime ideals $\mathfrak{P}$ and $\mathcal{P}$ in the ray class fields $\mathbf{Q}_{(p)}$ and $K_{\mathfrak{p}}$ respectively. Let L be the Hilbert class field of K, the maximal unramified Abelian extension. The degree $[L : K]$ is equal to h_K, the class number of K. If we work with an imaginary quadratic field K with non-trivial class number, then the extension L/K will be non-trivial as well. This implies that there could be several primes $\mathcal{P}_i \subset \mathcal{O}_{K_{\mathfrak{p}}}$ lying above $\mathfrak{p} \subset \mathcal{O}_K$.

$$
\begin{array}{ccccc}
K_{\mathfrak{p}} & \mathcal{P}_1 & \cdots & \mathcal{P}_r \\
| & | & & | \\
L & \mathfrak{P}_1 & \cdots & \mathfrak{P}_r \\
| & \diagdown & & \diagup \\
K & & \mathfrak{p} &
\end{array}
$$

In order to resolve this we can compare the generators of primes $\mathcal{P}_i$ for each i separately. In order to generate elements similar to $f_{\mathcal{R}}(\epsilon_g)$, we can work with principal primes ideals $\mathfrak{r} \subset \mathcal{O}_K$ of degree one which totally splits in the extension $K_{\mathfrak{p}}/K$. Such primes can be found by class field theory and there are infinitely many with norm $r \equiv 1 \pmod{2M}$ by Chebotarev's Density Theorem.

6.2 Cyclotomic Function Fields

Algebraic number theory arises from algebraic extensions of the rational numbers $\mathbf{Q}$. Similarly we can consider finite algebraic extensions of rational functions and such extensions are called algebraic function fields. It would be interesting to generalize Schoof's algorithm to its function field analogue, namely cyclotomic function fields. They are finite algebraic extensions of $k = \mathbf{F}_q(T)$ satisfying properties very similar to the cyclotomic number fields.

In order to construct the p-th cyclotomic number field $\mathbf{Q}_{(p)}$, we start with a prime ideal (p) in the ground field and use class field theory to generate the maximal Abelian extension which ramify only above (p) and the prime at infinity. In the function field case, similarly we start with a place P, corresponding to a monic irreducible polynomial, and construct an extension k_P which ramifies only P and the place at infinity. Let k_P^+ be the maximal real subextension of the cyclotomic function field k_P. In other words the extension k_P^+/k is ramified only above P. It turns out that the fields $\mathbf{Q}_{(p)}$ and k_P^+ have many properties in common. For example, we have

$$h_{k_P^+} = \left[\mathcal{O}_{k_P^+}^* : \mathcal{E}_P\right]$$

where h_{k_P} is the class number of the real cyclotomic function field k_P^+ and $\mathcal{E}_P$ is the group of cyclotomic units [6, p. 295].

In order to generalize Schoof's algorithm to compute the class number of cyclotomic function fields, we need to construct analogues of the elements

$$f_{\mathfrak{R}}(\eta_g) = \sum_{\sigma \in G} c_\sigma \sigma$$

that we used for investigating class number of $\mathbf{Q}_{(p)}$. A nice property of the Galois group $\mathrm{Gal}(k_{(P)}/k) \cong (\mathbf{F}_q[T]/(P))^*$ is that it is cyclic and its action is well-understood. However we still need to construct special extensions of k_P similar to the extension $\mathbf{Q}_{(p)}(\zeta_{2M})$ in the cyclotomic number field case. We hope to achieve this by using the explicit class theory for rational function fields [1].

A P P E N D I X

FREQUENTLY USED NOTATION

Given a number field L, we use the following notation:

d_L	discriminant of L
$\mathcal{O}_L$	ring of integers of L
$\mathcal{O}_L^*$	group of units in the ring $\mathcal{O}_L$
μ_L	roots of unity in L
$\mathrm{Cl}(L)$	class group of L
h_L	class number of L
$\mathrm{Reg}(U)$	regulator of $U \subset \mathcal{O}_L^*$
$\mathfrak{m}$	a modulus in L
$I_L(\mathfrak{m})$	fractional $\mathcal{O}_L$-ideals coprime to $\mathfrak{m}$
$P_{L,1}(\mathfrak{m})$	principal $\mathcal{O}_L$-ideals generated by $\alpha \equiv 1 \pmod{\mathfrak{m}}$
$L_\mathfrak{m}$	ray class field of conductor $\mathfrak{m}$
$G_{L_\mathfrak{m}}$	Galois group $\mathrm{Gal}(L_\mathfrak{m}/L)$
$\sigma_\mathfrak{p}$	Artin symbol of the ideal $\mathfrak{p} \subset \mathcal{O}_L$

Let G be a cylic group and let $H \subset G$ be a subgroup. Given a finite $\mathbf{Z}[G]$-module A, we use the following notation:

$A^{\perp}$	$\mathrm{Hom}_R(A, R)$
A^{dual}	$\mathrm{Hom}_{\mathbf{Z}}(A, \mathbf{Q}/\mathbf{Z})$
A_{φ}	φ-part of A (page 8)
$A[M]$	$\{a \in A : Ma = 0\}$
A^H	$\{a \in A : a^{\sigma} = a \text{ for all } \sigma \in H\}$
N_H	$\sum_{\sigma \in H} \sigma$

The ray class field $\mathbf{Q}_{(p)}$ is the p-th real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. We use the following notation:

$\mathcal{C}$	group of cyclotomic units in $\mathcal{O}^*_{\mathbf{Q}_{(p)}}$ (page 18)
η_g	a generator of cyclotomic units $\mathcal{C}$ (page 18)
$B_{\mathbf{Q}_{(p)}}$	the quotient group $\mathcal{O}^*_{\mathbf{Q}_{(p)}}/\mathcal{C}$ (page 19)
$\tilde{h}_{\mathbf{Q}_{(p)}}$	a special integer dividing $h_{\mathbf{Q}_{(p)}}$ (page 33)

Let K be an imaginary quadratic field. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a degree one prime ideal of norm p. We use the following notation:

w	a special element such that $\mathcal{O}_K = \mathbf{Z}[w]$ (page 37)
$w_{\mathfrak{p}}$	smallest non-negative integer satisfying $w \equiv w_{\mathfrak{p}} \pmod{\mathfrak{p}}$ (page 37)
W_K	number of roots of unity in K (page 38)
$\mathcal{E}$	group of elliptic units in $\mathcal{O}^*_{K_{\mathfrak{p}}}$ (page 44)
ϵ_g	a generator of elliptic units $\mathcal{E}$ (page 44)
$B_{K_{\mathfrak{p}}}$	the quotient group $\mathcal{O}^*_{K_{\mathfrak{p}}}/\mathcal{E}$ (page 45)
$\tilde{h}_{K_{\mathfrak{p}}}$	a special integer dividing $h_{K_{\mathfrak{p}}}$ (page 3)

BIBLIOGRAPHY

[1] D. R. Hayes, *Explicit class field theory for rational function fields.* Trans. Amer. Math. Soc. 189 (1974), 77–91.

[2] G. Janusz, *Algebraic Number Fields*. Academic Press, New York, 1973.

[3] Á. Lozano-Robledo, *Bernoulli numbers, Hurwitz numbers, p-adic L-functions and Kummer's criterion.* RACSAM Rev. R. Acad. Cienc. Exactas Fs. Nat. Ser. A Mat. 101 (2007), no. 1, 1–32.

[4] S. Lang, *Elliptic Functions; second edition*. Graduate Texts in Math. 112, Springer-Verlag, New York Berlin Heidelberg 1987.

[5] G. Robert, *Nombres de Hurwitz et Unités Elliptiques*. Ann. scient. Éc. Norm. Sup. (1978), 4^e série, 11, 297-389.

[6] M. Rosen, *Number Theory in Function Fields*. Graduate Texts in Math. 210, Springer-Verlag, Berlin Heidelberg New York 2002.

[7] R. Schoof, *Class numbers of real cyclotomic fields of prime conductor*. Math. Comp. 72 (2003), no. 242, 913–937

[8] H. M. Stark, *L-Functions at s=1. IV. First Derivatives at s=0*. Adv. in Math. 35 (1980), no. 3, 197–235.

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

[10] L. C. Washington, *Introduction to Cyclotomic Fields; second edition*. Graduate Texts in Math. 83, Springer-Verlag, Berlin Heidelberg New York 1997.

[11] PARI/GP, version `2.3.2`, `http://pari.math.u-bordeaux.fr/`, Bordeaux, 2006.