ABSTRACT

Title of dissertation: INVESTIGATIONS OF HIGHLY IRREGULAR PRIMES AND ASSOCIATED RAY CLASS FIELDS

Morgan Benjamin Stern,
Doctor of Philosophy, 2014

Dissertation directed by: Professor Lawrence Washington
Department of Mathematics

We investigate properties of the class number of certain ray class fields of prime conductor lying above imaginary quadratic fields. While most previous work in this area restricted to the case of imaginary quadratic fields of class number 1, we deal almost exclusively with class number 2. Our main results include finding 5 counterexamples to a generalization of the famous conjecture of Vandiver that the class number of the pth real cyclotomic field is never divisible by p. We give these counterexamples the name *highly irregular primes* due to the fact that any counterexample of classical Vandiver is an irregular prime. In addition we explore whether several consequences of Vandiver's conjecture still hold for these highly irregular primes, including the cyclicity of certain class groups.

INVESTIGATIONS OF HIGHLY IRREGULAR PRIMES AND ASSOCIATED RAY CLASS FIELDS

by

Morgan Benjamin Stern

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfilment
of the requirements for the degree of
Doctor of Philosophy
2014

Advisory Committee:
Professor Lawrence Washington, Chair/Advisor
Professor Thomas Haines
Professor Xuhua He
Professor Doron Levy
Professor William Gasarch

Acknowledgments

I'd like to first and foremost thank my advisor, Professor Larry Washington for working with me for these several years, and being infinitely understanding with the many delays that have gone on. Thanks for reviewing the many drafts of the dissertation, and particularly for help with the proofs of Theorem 3.1.3 and Section 5.2. I'd like to thank my committee, Professors Thomas Haines, Xuhua He, Doron Levy, and William Gasarch for their work.

I'd like to thank my wife, Elizabeth Petro, who has been endlessly patient and supportive through the last many years, making sure I never felt rushed. And I'd like to thank my mother, Heidi Markovitz, who continued to ask how my homework was coming along until I was 30.

This is dedicated to Poppy and Grandpa who blazed the trail of scholastic achievement before me.

Table of Contents

List of Abbreviations & Symbols

CRT	Chinese Remainder Theorem
ϵ	Generator of the elliptic units of $K_{\mathfrak{p}}$
$\mathcal{E}$	Group of elliptic units of $K_{\mathfrak{p}}$
f_ϵ	Minimal polynomial of ϵ over K
ϕ	Function defined in eq 3.1
gcd	Greatest common divisor
H_L	Hilbert class field of L
h_L	Class number of L
$\mathcal{I}$	An ideal in K
K	Imaginary quadratic number field
$K_{\mathcal{I}}$	Ray class field over K of conductor $\mathcal{I}$
L	Arbitrary number field
$N_{L'/L}$	Norm map from L' to L
$\mathcal{O}_L$	Ring of integers of L
p	Integral prime
$\mathfrak{p}$	Prime above p in $\mathcal{O}_K$
$\sigma_{\mathfrak{q}}$	Galois element corresponding to $\mathfrak{q}$ under the Artin map
ζ_n	Primitive nth root of unity

Chapter 1: Introduction

Let K be an imaginary quadratic field and p a prime that splits in $K/\mathbb{Q}$. This work considers the ray class field of conductor $\mathfrak{p}$ above p, $K_{\mathfrak{p}}$, and is principally concerned with whether its class number is divisible by p, as well as the consequences of this event. In order to do this we must perform large computations in several-hundred-degree extensions of K. Moreover, while previous work in this area often restricted computations to the simpler case where the base field has class number 1, we deal almost exclusively with class number 2, providing many ideas that can work in higher class numbers as well. This involves added complexity and requires reworking several well-known results that were not proven in sufficient generality.

Our main results include finding 5 counterexamples to a generalization of the famous Vandiver Conjecture that the class number of the pth real cyclotomic field is never divisible by p. We give these counterexamples the name *highly irregular primes* due to the fact that any counterexample of classical Vandiver is automatically an irregular prime.

Previous work by Kucuksakalli [5] found a single highly irregular prime, and it was computationally difficult to prove. We are able to provide a shorter proof that our 5 are indeed highly irregular primes, and confirm Kucuksakalli's is as well.

Moreover, we show a simple statistical argument in section 4 that this gives credence to the standard heuristic argument that there should be primes for which the classical Vandiver's conjecture fails.

Much of this work is concerned with computability and precision. Many of the constituent pieces of what we do have been described elsewhere in theoretical but not effective (practical and implementable) terms. As we are dealing with extensions of degree > 100, we are often dealing with degree 100 polynomials, each coefficient of which is several thousand digits. As we are multiplying these mathematical objects that take megabytes of storage in memory, the difference between storing a polynomial versus its square is the difference between feasible and infeasible. Even normally simple activities, such as taking a gcd between polynomials, have to be carefully optimized at this size. As a result, there are several algorithms throughout this text that appear to be performing easy tasks, but which are specifically written so that they will be quick in very large-degree extensions. When slight changes to an algorithm cause massive changes to the runtime it is noted in the text, most notably in sections 3.2, 3.3, and 3.4.

We give a description of a full-rank subgroup of the units for every cyclic ray class field of prime conductor in section 3.3, and numerically compute said subgroup for every prime with norm ≤ 307. While [5] used elliptic units when the base field had class number 1, the obvious generalization of those units often does not have full rank when the class number is not 1 (and we show a sufficient condition for this obvious generalization to have full rank in section 3.1).

Our unit group is a variant of elliptic units computed in previous works, in particular the work of Ramachandra [9], it is optimized so that the minimal polynomial of a generating set of the group is small. For example, while Ramachandra constructs elliptic units over base fields of any class number, he raises his generators to the $12p$th power in order to avoid keeping track of roots of unity. In constructing our new elliptic units we keep track of the roots of unity involved, allowing our computations to (often) use less than a hundredth the precision older elliptic units would require. The importance of actually being able to implement a theorem cannot be overstated, as this is exactly how we are able to prove that the generalized Vandiver's Conjecture fails for ray class fields, and indeed provide some new evidence that the famous conjecture may be false.

We use our units in a generalization of an algorithm by Kucuksakalli (which itself generalized an algorithm by Schoof [10]) in order to determine if the class number of the ray class field of prime conductor for a degree 1 prime is divisible by the norm of said prime. Specific implementation details of the algorithm are described in section 3.5.

In section 5.1 we create a new algorithm to determine when elements are singular primary. The algorithm, which involves the use of a linear recurrence relation and the p-adics, may be of more general interest in light of the fact that it involves taking a 1000-digit precision number, and efficiently raising it to a 1000-digit power. In particular, when naively trying to implement a test for singular primary elements, it would be difficult to run on a PC for primes larger than norm 5, while we do it for $\mathfrak{p}$ of norm 239 in minutes.

In looking for singular primary elements we find an interesting phenomenon in a highly irregular prime. Certain portions of the class group of cyclotomic fields can be shown to be cyclic assuming Vandiver's Conjecture and it is unclear what would happen if Vandiver failed. We demonstrate a highly irregular prime where the corresponding portions are cyclic in spite of the generalization of Vandiver not holding.

In section 5.3 we provide some numerical evidence that many of the techniques we use to investigate ray class fields of prime conductor will not easily extend to non-prime conductor.

The format of this paper is as follows: Chapter 2 goes over Vandiver's conjecture and basic facts about imaginary quadratic fields of class number 2. Chapter 3 represents the main body of the paper, going over how to construct our group of units, proving they are finite index, and explaining how to use them to compute divisibility by p. Chapter 4 contains the results of our calculations, the 5 highly irregular primes found, as well as statistical analysis that provides heuristic evidence to support a conjecture on the frequency of highly irregular primes. Chapter 5 contains the results of our attempts to construct an unramified abelian extension of $K_{\mathfrak{p}}(\zeta_p)$ of degree p and the consequences of these results.

Chapter 2: Background

In this section, we go over the basic background material necessary for future chapters.

2.1 Vandiver's Conjecture

Conjecture 2.1.1 (Vandiver)**.** *For any prime ideal $(p) \subset \mathbb{Z}$, the class number of $\mathbb{Q}_{(p)} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, the ray class field of conductor (p) is not divisible by p.*

A reasonable generalization of this is

Conjecture 2.1.2. *Let K be an imaginary quadratic field of class number h_K. For any degree one prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ such that $h_K \notin \mathfrak{p}$, the class number of $K_{\mathfrak{p}}$, the ray class field of conductor $\mathfrak{p}$, is not divisible by p.*

This conjecture turns out to be false. In [5] Kucuksakalli demonstrates a single counterexample, and in this work we find 5 others. As such, we will introduce a new definition:

Definition. Let K be an imaginary quadratic field of class number h_k and $\mathfrak{p} \subset \mathcal{O}_K$ a degree one prime ideal above p. We say $\mathfrak{p}$ is a *highly irregular prime* if $(h_K, p) = 1$ and $p | h_{K_{\mathfrak{p}}}$.

An *irregular prime* over $\mathbb{Q}$ has the property that $p|h_{\mathbb{Q}(\zeta_p)}$. It is well known ([13] theorem 4.11, for instance) that if a prime violates Vandiver's conjecture then it is also irregular (thus motivating our above definition).

2.2 The Basics of Class Number 2

Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field of class number 2 (d square-free). Let $\mathfrak{p}$ be an odd prime which lies above p in K and is relatively prime to $6d$. In general \mathfrak{} will be used to denote ideals in K. We use $K_{\mathfrak{p}}$ to denote the ray class field generated by $\mathfrak{p}$. In addition, for any field L the class number is denoted h_L, the Hilbert class field H_L, the number of roots of unity W_L, and the ring of integers $\mathcal{O}_L$.

Theorem 2.2.1. *Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field. K has class number 2 if and only if d is a square times one of the following integers:*

$$-5, -6, -10, -13, -15, -22, -35, -37, -51, -58, -91, -115, -123,$$
$$-187, -235, -267, -403, -427$$

Proof. See Stark [12] □

In this work, d will always be one of the above 18 integers. We denote the ring of integers of K by $\mathcal{O}_K = \mathbb{Z}[\omega]$. If $d \equiv 1 \bmod 4$ and is square-free then $\omega = \frac{1+\sqrt{d}}{2}$, otherwise $\omega = \sqrt{d}$. There are three ways to represent elements of $\mathcal{O}_K$ which we will use: First we can embed $\mathcal{O}_K$ into $\mathbb{C}$ by numerically computing $\sqrt{d}$ to some precision (we will pick the root with positive imaginary part). Second, we can embed $\mathcal{O}_K$ into

$\mathbb{Z}_r$ which similarly involves computing $\sqrt{d}$ to an r-adic precision, which in practice means we compute the root of the minimal polynomial in $\mathbb{Z}/r^n\mathbb{Z}$ for large n and saying our terms are correct within $O(r^n)$ (in this case typically the root with the "smallest" value mod r is picked). Last, we do not embed $\mathcal{O}_K$ anywhere, but think of it as $\mathbb{Z}[\omega]$ mod $\omega^2 - d$ (or $\omega^2 - \omega - \frac{d-1}{4}$) and never let a polynomial in ω have degree over 2. This last one has no precision limitations but has the potential to crash a computer without warning if the numbers get too large.

If a prime q splits into $\mathfrak{q}\bar{\mathfrak{q}}$ in K, then $\sqrt{d}$ must exist mod$q$. That is, we know $\mathcal{O}_K/\mathfrak{q} \simeq (\mathbb{Z}/q\mathbb{Z})$ so in this isomorphism $\sqrt{d}$ must go to something in $(\mathbb{Z}/q\mathbb{Z})$. We will make ω_q the smallest positive integer that ω is congruent to mod q. Thus, $\omega_q - \omega$ must be in the ideal $\mathfrak{q}$. Further, q must be in $\mathfrak{q}$ since the ideal divides (q). Finally, these two elements generate $\mathfrak{q}$ since clearly $(\mathbb{Z} \oplus \omega\mathbb{Z})/\langle q, \omega_q - \omega\rangle \simeq (\mathbb{Z}/q\mathbb{Z})$.

A similar argument works for any ideal in K: if we want to know the $\mathbb{Z}$-basis for a given product of ideals, we look at what the quotient space is. It is either cyclic or bicyclic. In the cyclic case we work out where ω is sent in the space to find one generator of the ideal, and throw in the order of the group for the other generator.

We use the following lemma to identify non-principal ideals:

Lemma 2.2.2. *Given $\mathcal{I} \subset \mathcal{O}_K$ principal, the smallest element of the ideal α (that is $|\alpha| \leq |z|$ for all non-zero $z \in \mathcal{I}$) must generate the ideal.*

Proof. All of the units in $\mathcal{O}_K$ are roots of unity and so have absolute value 1 under all embeddings. Assume $\mathcal{I}$ principal with generator α. If $z \in (\alpha) - \{0\}$ then $z = w\alpha$ and $Norm(z) = Norm(w) \cdot Norm(\alpha)$. Since $Norm(w) \in \mathbb{Z}^+$ and equals the square of its absolute value, we get $Norm(z) \geq Norm(\alpha)$ and the absolute value goes similarly. □

This gives us an easy way to tell if an ideal is principal. Given an integer basis for the ideal $\mathcal{I}$, we perform Gaussian reduction ([3], page 23, for example) to get α, the smallest element in $\mathcal{I}$. We then check if α divides both our initial basis elements for $\mathcal{I}$. If it does then $\mathcal{I} = (\alpha)$ and if not, we must have a non-principal ideal. In practice, because both basis elements start out within an order of magnitude of each other, if a and b form a basis the following algorithm suffices:

Algorithm 2.2.3. Finding the generator of an ideal from its $\mathbb{Z}$-basis (a, b) using Gaussian reduction

1. Replace b with the smallest of b, $a+b$, and $a-b$ (this is reversible, and so still gives a basis).

2. If $|a| > |b|$, relabel so that $|a| \leq |b|$.

3. If b has changed in the last two steps, go to step 1. If not, a is the smallest element.

4. If a divides b then a is the generator else the ideal is not principal.

We will make use of the following well-known theorem:

Theorem 2.2.4. *Let H_K be the Hilbert class field of K. An ideal $\mathcal{I} \subset K$ splits in H_K/K if and only if it is principal.*

Finally, genus theory easily characterizes possible H_K:

Theorem 2.2.5. *Given $K = \mathbb{Q}(\sqrt{d})$, an imaginary quadratic field of class number 2 with d as in Theorem 2.2.1, we have the following 4 cases:*

1. $H_K = \mathbb{Q}(\sqrt{-d}, i)$ *if d is prime.*
2. $H_K = \mathbb{Q}(\sqrt{2}, \sqrt{d/2})$ *if $d \equiv 6 \pmod 8$.*
3. $H_K = \mathbb{Q}(\sqrt{-d/2}, \sqrt{-2})$ *if $d \equiv 2 \pmod 8$.*
4. $H_K = \mathbb{Q}(\sqrt{d_1}, \sqrt{-d_2})$ *if $-d$ factors as primes $d_1, d_2 > 0$ and $d_1 \equiv 1 \pmod 4$.*

The fundamental unit δ of $\mathcal{O}_{H_K}$ is the fundamental unit of the maximal real subfield.

Proof. A simple check for each of the 18 possible d's. □

2.3 Constructing Ray Class Groups in Class Number 2

The ray class group over $\mathfrak{p}$ is defined to be the group of (fractional) ideals relatively prime to $\mathfrak{p}$ mod the group of (fractional) principal ideals with a generator congruent to 1 mod $\mathfrak{p}$. In this section, we show how to construct this group.

Given an odd prime p that splits in K, it is a simple matter to find the ideal $\mathfrak{p}$ lying above p. First, we solve the polynomial $x^2 - d \equiv 0 \bmod p$. We select one of the roots and declare that (lifted) root to be $\omega_\mathfrak{p}$ (or use $(1 + root)/2 \bmod p$ if $d \equiv 1 \bmod 4$). Finally we form our prime above p by defining it to be $\mathfrak{p} = \langle p, \omega_\mathfrak{p} - \omega \rangle$.

The above is a constructive version of the fact that odd p splits if and only if the Legendre symbol $\left(\frac{d}{p}\right) = 1$: if $x^2 - d = 0 \bmod p$ has no solution the construction would fail, and if it had one the construction leads to a ramified prime. Conversely p splitting implies $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_p \simeq (\mathbb{Z}/p\mathbb{Z})$, which implies $x^2 + d = 0$ has a solution mod$p$ since it does in $\mathcal{O}_K$. Further, this shows that p ramifies if and only if $p|d$, as this is the case when $x^2 - d \equiv 0 \bmod p$ has only one root (and therefore, one can construct only one prime above p).

We can use a similar fact to quickly see if $\mathfrak{p}$ is principal: All principal elements split in the Hilbert class field of K. One can take the norm of the prime above $\mathfrak{p}$ down to the maximal real subfield of H_K (given in Theorem 2.2.5) where it must equal a prime above p. So $\mathfrak{p}$ being principal requires p to split in the maximal real subfield of H_K, which can be checked with a different Legendre symbol. Similarly p splitting in both K and the maximal real subfield of H_K means it splits in their compositum, which is H_K, which means its factors must be principal in K.

Given the generator $a + b\omega$ of a principal ideal $\mathcal{I} \subset K$ it is easy to associate it to one of the ray classes containing $(1), (2), ..., (\frac{p-1}{2}) \bmod \mathfrak{p}$ by noting that we know $\omega \equiv \omega_{\mathfrak{p}} \bmod \mathfrak{p}$ and so $a + b\omega \equiv a + b\omega_{\mathfrak{p}}$, which is an integer. This integer can be taken mod p since $p \in \mathfrak{p}$. Finally, if this value is greater than $\frac{p-1}{2}$, then we can note $-a - b\omega$ generates the same ideal as $a + b\omega$ but is congruent to a smaller positive integer mod p. The fact that $W_K = 2$ for all our K means that there is no smaller integer generating an ideal in the ray class. This also shows that the ray class group contains a subgroup isomorphic to $\mathbb{F}_p^\times / \langle -1 \rangle$, which is cyclic because it is the quotient of a cyclic group.

Given a non-principal ideal $\mathcal{I}$, we know $\mathcal{I}^2$ is principal, and so we can use the above method to determine what element of the ray class group $\mathcal{I}^2$ is. This completely classifies all $p - 1$ elements of the ray class field in our case: they are either in the same class as one of $(1), (2), ..., (\frac{p-1}{2})$ or they are not but square to something that is.

Lemma 2.3.1. *Let $p-1 = 2^k m$ with m odd. Then the ray class group of conductor p is cyclic if and only if every non-principal ray classes has order divisible by 2^k.*

Proof. There are two cases, depending on $p \bmod 4$. If $p \equiv 3 \bmod 4$ then $\frac{p-1}{2}$ is odd and since we have a cyclic subgroup of order $\frac{p-1}{2}$ and a cyclic subgroup of the relatively prime order 2 (the class generated by the product of all non-principal ray classes), we know the group must be cyclic of order $p-1$.

When $p \equiv 1 \bmod 4$ the ray class group is cyclic, or alternatively it could be isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/\frac{p-1}{2}\mathbb{Z}$. Notice that the Sylow 2-subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$ is cyclic, and not cyclic in the other case, though in both cases it has 2^k elements. In the cyclic case $2^k/2$ elements of the Sylow 2-subgroup (out of 2^k of them) have order 2^k and zero do in the non-cyclic case. Moreover since the principal ray classes contain a subgroup of size $2^k/2$ (and so none of these is order 2^k), we know that all elements of order 2^k must be non-principal.

There are only $2^k/2$ non-principal elements in the Sylow 2-subgroup, so all of these must be order 2^k if the ray class group is cyclic. Since the class number is 2, any non-principal element differs from any other by a principal element. Thus when the ray class group is cyclic every non-principal ray class differs from a non-principal ray class of order 2^k by a principal element whose order is not divisible by 2^k.

If the ray class group isn't cyclic then no ray class has order 2^k (stronger than the converse of the "only if") and so we have proven the lemma. □

This gives us our next algorithm:

Algorithm 2.3.2. Determining whether a ray class group of conductor $\mathfrak{p}$ is cyclic

1. Find a prime $q \neq p$.

2. Use Legendre symbols to verify q splits non-principally as $\mathfrak{q}\bar{\mathfrak{q}}$.

3. Compute a basis of $\mathfrak{q}^2$ as above then use Algorithm 2.2.3 to find a principal generator of the ideal $\alpha = a + b\omega$.

4. Embed the class containing α into $\mathbb{F}_p$ with our map $\omega \mapsto \omega_{\mathfrak{p}}$. Call the result $c = a + b\omega_{\mathfrak{p}}$. Note that (c) is in the same ray class as $\mathfrak{q}^2$.

5. Compute $c^{\frac{p-1}{4}}$ mod p. If this equals ±1 then $\mathfrak{q}^{2*\frac{p-1}{4}}$ is in the same ray class as (± 1); the order of the class of $\mathfrak{q}$ divides $2\frac{p-1}{4} = m2^{k-1}$.

6. If $c^{\frac{p-1}{4}} \equiv \pm 1$ mod p then return "non-cyclic" else "cyclic."

Because p is small in practice, it is simple to just keep checking different q until we find $\mathfrak{q}$ that generates the group, and from then on, just define the group in terms of powers of $\mathfrak{q}$. For convenience in later computations, we make sure that $\mathfrak{q}$ generates the ray class group and will tend to refer to ray classes as $\mathfrak{q}^j$.

Lastly, we will often need to compute a basis of $\mathfrak{q}^n$ (as we did in the above algorithm); this is polynomial time in n. Since $\mathfrak{q}$ is prime, we obtained its basis by considering what ω was congruent to in $\mathcal{O}_K/\mathfrak{q}$. Similarly, since $\mathfrak{q}$ is a degree 1 prime, $\mathcal{O}_K/\mathfrak{q}^n \simeq (\mathbb{Z}/q^n\mathbb{Z})$.

We know $\mathfrak{q}$ contains q^n and we know ω must go to something which is consistent with the ω_q we defined earlier. But that is exactly what Hensel's Lemma [1] gives

[1] Mechanically, in PARI this is accomplished by taking $f_\omega(x)$, the minimal polynomial for ω and

us: a lift of ω_q to a unique consistent value mod q^n which we will call ω_{q^n}. Since these two elements of $\mathfrak{q}^n$ enable us to define a homomorphism $\mathcal{O}_K \twoheadrightarrow \mathcal{O}_K/\mathfrak{q}^n$, they must generate the ideal, and we have $\mathfrak{q}^n = \langle q^n, \omega_{q^n} - \omega \rangle$. It is worth noting that the matrix formed by thinking of the elements of this basis as integer sums of 1 and ω is in rational canonical form.

If we want to compute a basis of a product of prime ideals, we do that by the Chinese remainder theorem (CRT). In particular, let us consider the ideal $\mathfrak{pq}$ (which will show up in later computations). We know by CRT

$$\mathcal{O}_K/\mathfrak{pq} \simeq (\mathcal{O}_K/\mathfrak{p}) \oplus (\mathcal{O}_K/\mathfrak{q}) \simeq \mathbb{F}_p \oplus \mathbb{F}_q \simeq \mathbb{Z}/pq\mathbb{Z}.$$

We know further that pq maps to 0 and that ω maps to $(\omega_\mathfrak{p}, \omega_\mathfrak{q})$ in the left isomorphism (essentially by definition). But, the CRT tells us exactly[2] what that is mapped to in the right isomorphism and we will call this $\omega_{\mathfrak{pq}}$.

factoring it using the function polrootspadic(f, q^n) which gives the roots of a polynomial f mod q^n. We then pick the root which equals $\omega_\mathfrak{q}$ mod q

[2] In PARI the command would be chinese(Mod$(\omega_\mathfrak{p}, p)$,Mod$(\omega_\mathfrak{q}, q)$).

Chapter 3: Constructing Highly Irregular Primes Using Elliptic Units

In [5] Kucuksakalli generalized a method used to compute (approximations of) class numbers of real cyclotomic fields to instead compute (approximations of) class numbers of ray class fields of prime conductor lying over imaginary quadratic fields of class number 1. In doing this, he discovered the first highly irregular prime, $\mathfrak{p} = (13 - 2\omega) \subset \mathbb{Z}[\frac{1+\sqrt{-163}}{2}]$. The method involved exploiting the class number formula and generalizing a method of Schoof to demonstrate that the class number of $K_{\mathfrak{p}}$ is equal to the index of a group of elliptic units inside of the full unit group (see section 3.5 for details).

We extend the method to imaginary quadratic fields of class number 2 and find five further highly irregular primes. Our methods are able to determine if the class number of $K_{\mathfrak{p}}$ is divisible by p, though some care would have to be taken if one wanted to adapt it to look for divisibility by primes smaller than p. We restricted our search to ray class fields with cyclic Galois groups, but the techniques are easily modified to bicyclic Galois groups. Unless otherwise noted, all numerical calculations for class number 2 were done on a 1.6 GHz Intel Core i5-4200U CPU with 6 GB of DDR3 memory using PARI/GP Calculator version 2.5.5, 32-bit version.

3.1 Elliptic Units and Their Galois Action in $\mathbb{C}$

Our goal is to construct a finite index subgroup of the unit group whose index encodes the class number of our field. In this section we will lay out the theoretical basis for such a subgroup, leaving the actual method of computation for section 3.3. In [11] Stark introduces elliptic units with this property. Unfortunately, he only defines them in extensions of fields of class number 1. We will follow his approach, point out where it breaks down for higher class numbers and introduce a generalization. As in Stark, we make extensive use of the function ϕ defined by

$$\begin{aligned}\phi(x,y,z) =& 2\sin(\pi(xz+y))\exp(\pi i(x^2z+ay+z/6))\cdot \\ &\prod_{j=1}^{\infty}(1-\exp(2\pi i(y+z(x+j))))(1-\exp(-2\pi i(y+z(x-j))))\end{aligned} \tag{3.1}$$

The function ϕ satisfies several transformation properties (see page 208 of [11]), most notably:

$$\phi(x,y,z) = -e^{-\pi iy}\phi(x-1,y,z) \tag{3.2}$$

$$= -e^{\pi ix}\phi(x,y-1,z) \tag{3.3}$$

$$= -e^{\pi i/6}\phi(x,y+x,z-1) \tag{3.4}$$

$$= e^{-\pi i/2}\phi(y,-x,-1/z) \tag{3.5}$$

We will assign to each ideal $\mathcal{I}$ a particular $x_\mathcal{I}, y_\mathcal{I}, z_\mathcal{I}$ and from this we will have a function $\phi_\mathfrak{p}(\mathcal{I}) = \phi(x_\mathcal{I}, y_\mathcal{I}, z_\mathcal{I})^{12p}$. The selection of $x_\mathcal{I}, y_\mathcal{I}, z_\mathcal{I}$ will depend on choices made in their construction but $\phi_\mathfrak{p}(\mathcal{I})$ will be well-defined.

Definition. We say a triple $x_\mathcal{I}, y_\mathcal{I}, z_\mathcal{I}$ is a *proper* $\phi_\mathfrak{p}(\mathcal{I})$ *triple* or (proper triple for short) if it can be produced according to the following method.

1. Select $\mathfrak{a}$ so that $\mathfrak{a}\mathcal{I}$ is principal and generated by α.

2. As a $\mathbb{Z}$-module $\mathfrak{p}\mathfrak{a} = \mu\mathbb{Z} \oplus \nu\mathbb{Z}$ where $\mathrm{Im}(\mu/\nu) > 0$

3. Take $u, v \in \mathbb{Q}$ so that $u\mu + v\nu = \alpha$.

4. Set $x_{\mathcal{I}} = u$, $y_{\mathcal{I}} = v$, and $z_{\mathcal{I}} = \mu/\nu$.

Stark proves several properties of $\phi_{\mathfrak{p}}(\mathcal{I})$ summarized as

Theorem 3.1.1. *Given $\mathfrak{p}$ a degree one prime ideal in a quadratic imaginary number field K then the following holds:*

1. *$\phi_{\mathfrak{p}}(\mathcal{I}) = \phi_{\mathfrak{p}}(\mathcal{J})$ if and only if $\mathcal{I}$ and $\mathcal{J}$ lie in the same class of the ray class group of $\mathfrak{p}$.*

2. *A $12p/W_{H_K}$ root of $\phi_{\mathfrak{p}}(\mathcal{I})$, which we shall call $\pi(\mathcal{I})$, lies in the field $K_{\mathfrak{p}}$, where W_{H_K} is also the number of roots of unity lying in $K_{\mathfrak{p}}$.*

3. *$\pi(\mathcal{I})$ generates an ideal $\mathcal{O}_{K_{\mathfrak{p}}}$ with $N_{K_{\mathfrak{p}}/K}(\pi(\mathcal{I})) = \mathfrak{p}^{\frac{h_K W_{H_K}}{W_K}}$.*

4. *For a prime $q \in \mathbb{Z}$ relatively prime to $12p$, if q splits as $\mathfrak{q}\bar{\mathfrak{q}}$ then*
$$\left(\frac{\pi(\mathfrak{q})}{\pi(\mathcal{O}_K)^q}\right)^{1/W_{H_K}} \in \mathcal{O}_{K_{\mathfrak{p}}} \text{ or else } \left(\frac{\pi((q))}{\pi(\mathcal{O}_K)^{q^2}}\right)^{1/W_{H_K}} \in \mathcal{O}_{K_{\mathfrak{p}}}.$$

5. *Finally, the Galois action is given by $\phi_{\mathfrak{p}}(\mathcal{I})^{\sigma_{\mathfrak{q}}} = \phi_{\mathfrak{p}}(\mathcal{I}\bar{\mathfrak{q}})$.*

Proof. See [11], Lemma 7, 9 for proofs of items 1, 2, 3, 5, and a weak form of 4 (note he calls $\phi_{\mathfrak{p}}(\mathcal{I})$ by $E(\mathfrak{c})$). Item 4 is given in equation 37 (bottom of page 32) of Deuring [4]. □

From these properties we can deduce another interesting feature with particular application in our class number 2 case.

Corollary 3.1.2. *The following are units in $\mathcal{O}_{K_\mathfrak{p}}$:*

1. *If $\mathfrak{p}$ is not principal then $(\pi(\mathcal{I})/\pi(\mathcal{J}))^{1/2}$.*

2. *If $\mathcal{I}$ and $\mathcal{J}$ lie in the same class mod principal ideals then $\frac{\pi(\mathcal{I})}{\pi(\mathcal{J})}^{1/W_{H_K}}$.*

Proof. We shall proceed in two steps: First we show that $(\pi(\mathcal{I})/\pi(\mathcal{J}))^{1/W_{H_K}} \in K_\mathfrak{p}$ for all ideals in the same principal ideal class (and the square root is always in the field). Then we show that $\pi(\mathcal{I})/\pi(\mathcal{J})$ is a unit given the conditions of the theorem.

We know that

$$N_{K/\mathbb{Q}}(\pi(\mathcal{I})) = N_{K/\mathbb{Q}(\zeta_{W_{H_K}})}\left(N_{\mathbb{Q}(\zeta_{W_{H_K}})/\mathbb{Q}}(\pi(\mathcal{I}))\right)$$

and that $N_{\mathbb{Q}(\zeta_{W_{H_K}})/\mathbb{Q}}(\pi(\mathcal{I})) \equiv 1 \bmod W_{H_K}$ if $\pi(\mathcal{I})$ is relatively prime to W_{H_K}. Thus $N_{K/\mathbb{Q}}(\pi(\mathcal{I})) \equiv 1 \bmod W_{H_K}$. Further, we know from Theorem 3.1.1.3 that $\pi(\mathcal{I})$ is relatively prime to W_{H_K}. The same holds for $\pi(\mathcal{J})$. Thus

$$W_{H_K} | \left(N_{K/\mathbb{Q}}(\mathcal{J}) - N_{K/\mathbb{Q}}(\mathcal{I})\right).$$

On the other hand, Theorem 3.1.1 says

$$\left(\frac{\frac{\pi(\mathcal{I})}{\pi(\mathcal{O}_K)^{N_{K/\mathbb{Q}}(\mathcal{I}))}}}{\frac{\pi(\mathcal{J})}{\pi(\mathcal{O}_K)^{N_{K/\mathbb{Q}}(\mathcal{J}))}}}\right)^{1/W_{H_K}} \in K_\mathfrak{p}$$

since both the numerator and denominator are in $\mathcal{O}_{K_\mathfrak{p}}$. But this simplifies to

$$\frac{1}{\pi(\mathcal{O}_K)^{\frac{1}{W_{H_K}}(N_{K/\mathbb{Q}}(\mathcal{I}) - N_{K/\mathbb{Q}}(\mathcal{J}))}}\left(\frac{\pi(\mathcal{I})}{\pi(\mathcal{J})}\right)^{1/W_{H_K}} \in K_\mathfrak{p}$$

and multiplying by $\pi(\mathcal{O}_K) \in \mathcal{O}_{K_\mathfrak{p}}$ several times we get $\left(\frac{\pi(\mathcal{I})}{\pi(\mathcal{J})}\right)^{1/W_{H_K}} \in K_\mathfrak{p}$.

If $\mathcal{I}$ is principal but $\mathcal{J}$ is not, then we know $2|(N_{K/\mathbb{Q}}(\mathcal{I}) - N_{K/\mathbb{Q}}(\mathcal{J}))$ and we get the weaker $\left(\frac{\pi(\mathcal{I})}{\pi(\mathcal{J})}\right)^{1/2} \in K_\mathfrak{p}$.

We will now show that these elements are units (and thus in $\mathcal{O}_{K_\mathfrak{p}}$).

If $\mathfrak{p}$ is not principal then $\mathfrak{p}H_K$ is prime. By class field theory, $\mathfrak{p}$ ramifies in $K_\mathfrak{p}$ with degree $(p-1)/2$. If $\mathfrak{P} \subset \mathcal{O}_{K_\mathfrak{p}}$ lies above $\mathfrak{p}$ then we have $\mathfrak{P}^{\frac{p-1}{2}} = \mathfrak{p}K_\mathfrak{p}$. Thus, $N_{K_\mathfrak{p}/H_K}(\mathfrak{P}) = \mathfrak{p}$, so $N_{K_\mathfrak{p}/K}(\mathfrak{P}) = \mathfrak{p}^2$. Due to the ramification, $\mathfrak{P}$ is the only ideal in $\mathcal{O}_{K_\mathfrak{p}}$ with norm $\mathfrak{p}^{h_K}$. But we also have $N_{K_\mathfrak{p}/K}(\pi(\mathcal{I})) = \mathfrak{p}^{W_{H_K}}$, so $(\pi(\mathcal{I})) = \mathfrak{P}^{\frac{W_{H_K}}{2}}$ for all $\mathcal{I}$. As a result, $\pi(\mathcal{I})$ and $\pi(\mathcal{J})$ generate the same ideal, so their ratio must be a unit.

Similar to the above, if $\mathcal{I}$ and $\mathcal{J}$ lie in the same principal ideal class, consider $\sigma_{\mathcal{I}^{-1}\mathcal{J}} \in Gal(K_\mathfrak{p}/K)$. By construction $\mathcal{I}^{-1}\mathcal{J}$ is principal, so let us say $(\alpha) = \mathcal{I}^{-1}\mathcal{J}$. As a result, $\sigma_{\mathcal{I}^{-1}\mathcal{J}} \in Gal(K_\mathfrak{p}/H_K)$ so it must send any prime above $\mathfrak{p}$ in H_K to itself and therefore $(\pi(\mathcal{I})) = (\pi(\mathcal{I}))^{\sigma_{\bar{\alpha}}} = (\pi(\mathcal{J}))$ meaning $\pi(\mathcal{J})/\pi(\mathcal{I})$ must be a unit. □

In the similar case when $h_K = 1$, the units from Corollary 3.1.2 form the basis for what Stark calls *elliptic units* and one can show they have index in the full units proportional to the class number of $K_\mathfrak{p}$. In our experience, they are also full rank for $h_K = 2$ and $\mathfrak{p}$ non-principal, but for principal $\mathfrak{p}$ they are never full rank as $N_{K_\mathfrak{p}/H_K}(\pi(\mathcal{I})/\pi(\mathcal{J})) = 1$.

In order to guarantee full-rank for our elliptic units we instead define them as follows

Definition. A group of elliptic units $\mathcal{E}$ is defined as the multiplicative group generated by the Galois conjugates of

$$\epsilon = \left(\frac{\pi(\mathfrak{q}^2)}{\pi(\mathcal{O}_K)} \right)^{1/W_{H_K}} \delta \in \mathcal{O}_{K_\mathfrak{p}}$$

where $\mathfrak{q}$ generates the ray class group of conductor $\mathfrak{p}$ and δ is the fundamental unit of H_K greater than 1 in the embedding of $K_\mathfrak{p}$ implicitly computed with $\phi()$.

These elliptic units look just like those of Stark from part 2 of Corollary 3.1.2, but with a power of δ being multiplied in. They have a distinct advantage of being full rank.

Theorem 3.1.3. *The elliptic units $\mathcal{E}$ are full-rank. Moreover $[\mathcal{O}_{K_\mathfrak{p}}^\times : \mathcal{E}] = ch_{K_\mathfrak{p}}$ for some c divisible only by primes less than p.*

Proof. Let R_L be the regulator of a field L, let $G = Gal(K_\mathfrak{p}/K)$ (which is $\langle \sigma_\mathfrak{q} \rangle$ since G cyclic) and $G' = Gal(K_\mathfrak{p}/H_K)$. Equation 46 of Stark [11] reads

$$\prod_{\substack{\chi \neq 1 \\ \chi(G')=1}} L'(0,\chi) = \prod_{\substack{\chi \neq 1 \\ \chi(G')=1}} \left(-\frac{1}{6p} \sum_{\mathcal{I}} \chi(\mathcal{I}) \ln(|\phi_\mathfrak{p}(\mathcal{I})|) \right).$$

Stark then goes on to say that using primitive χ yields

$$\prod_{\chi \neq 1} L'(0,\chi) = \frac{h_{K_\mathfrak{p}} R_{K_\mathfrak{p}} / W_{K_\mathfrak{p}}}{h_K / W_K}$$

which is $\frac{h_{K_\mathfrak{p}} R_{K_\mathfrak{p}}}{W_{K_\mathfrak{p}}}$ because $h_K = 2$. Every non-trivial character of G is primitive except for the nontrivial character ψ of $Gal(H_K/K)$. So we get

$$L'(0,\psi) = \frac{h_{H_K} R_{H_K}}{W_{H_K}} = 2\frac{h_{H_K}}{W_{H_K}} \ln(\delta).$$

Similarly, for the primitive characters we get

$$L'(0,\chi) = -\frac{1}{6p} \sum_{\mathcal{I}} \chi(\mathcal{I}) \ln|\phi_\mathfrak{p}(\mathcal{I})| = -2 \sum_{j=0}^{p-1} \chi(\mathfrak{q}^j) \ln|\phi(x_{\mathfrak{q}^j}, y_{\mathfrak{q}^j}, z_{\mathfrak{q}^j})|.$$

There are $p-1$ characters of G: 1, ψ, and the remaining $p-3$. This gives

$$\frac{h_{K_\mathfrak{p}} R_{K_\mathfrak{p}}}{W_{K_\mathfrak{p}}} = 2\frac{h_{H_K}}{W_{H_K}} \ln(\delta) \prod_{\chi \neq 1, \psi} \left(-2 \sum_{j=0}^{p-1} \chi(\mathfrak{q}^j) \ln |\phi(x_{\mathfrak{q}^j}, y_{\mathfrak{q}^j}, z_{\mathfrak{q}^j})| \right)$$

which in turn gives us

$$h_{K_\mathfrak{p}} = \frac{c}{R_{K_\mathfrak{p}}} \ln(\delta) \prod_{\chi \neq 1, \psi} \left(\sum_{j=0}^{p-1} \chi(\mathfrak{q}^j) \ln |\phi(x_{\mathfrak{q}^j}, y_{\mathfrak{q}^j}, z_{\mathfrak{q}^j})| \right), \tag{3.6}$$

where c is a number only divisible by primes[1] less than p.

We now appeal to a technical lemma ([13], Lemma 5.26(c)):

Lemma 3.1.4. *Let G be a finite abelian group and let $f : G \to \mathbb{C}$. If $\sum_{\sigma \in G} f(\sigma) = 0$ then*

$$\det(f(\sigma\tau^{-1}))_{\sigma,\tau \neq 1} = \frac{1}{|G|} \prod_{\chi \neq 1} \left(\sum_{\sigma \in G} \chi(\sigma) f(\sigma) \right),$$

where χ runs through the non-trivial characters of G.

Let $\epsilon_0 = \left(\frac{\pi(\mathcal{O}_K)^{\sigma_\mathfrak{q}^2}}{\pi(\mathcal{O}_K)} \right)^{1/W_{H_K}}$, thus $|N_{K_\mathfrak{p}/H_K}(\epsilon_0)| = 1$. Because $\sigma_\mathfrak{q} \notin G_{H_K}$, note that $G = Gal(K_\mathfrak{p}/H_K) \cup \sigma_\mathfrak{q} Gal(K_\mathfrak{p}/H_K) = G_{H_K} \cup \sigma_\mathfrak{q} G_{H_K}$. Also $|\delta^{\sigma_\mathfrak{q}}| = |\delta^{-1}|$ and $|\delta^\sigma| = |\delta|$ for $\sigma \in G_{H_K}$. Applying the lemma we have

$$\det(\ln |(\epsilon_0\delta)^{\sigma\tau^{-1}}|)_{\sigma,\tau \neq 1} = \frac{1}{p-1} \prod_{\chi \neq 1} \left(\sum_{\sigma \in G} \chi(\sigma) \ln |(\epsilon_0\delta)^\sigma| \right).$$

[1] The number c is of the form 2^i3^j except for $d = 235$ when $h_{H_K} = 5$ so c is 2^i3^j5. However, since 5 ramifies in K in this case, we will have $p > 5$.

When $\chi = \psi$ the nontrivial character of G_{H_K} so that $\psi(\sigma_\mathfrak{q}) = -1$ we have

$$\begin{aligned}
\sum_{\sigma \in G} \psi(\sigma) \ln |(\epsilon_0 \delta)^\sigma| &= \sum_{\sigma \in G} \psi(\sigma) \left(\ln |\delta^\sigma| + \ln |\epsilon_0^\sigma| \right) \\
&= \sum_{\sigma \in G_{H_K}} \psi(\sigma) \left(\ln |\delta| + \ln |\epsilon_0^\sigma| \right) + \sum_{\sigma \in G_{H_K}} \psi(\sigma_\mathfrak{q}) \psi(\sigma) \left(\ln |\delta_\mathfrak{q}^\sigma| + \ln |\epsilon_0^{\sigma_\mathfrak{q} \sigma}| \right) \\
&= \sum_{\sigma \in G_{H_K}} \left(\ln |\delta| + \ln |\epsilon_0^\sigma| \right) - \sum_{\sigma \in G_{H_K}} \left(- \ln |\delta| + \ln |\epsilon_0^{\sigma_\mathfrak{q} \sigma}| \right) \\
&= 2 \sum_{\sigma \in G_{H_K}} \ln |\delta| - \sum_{\sigma \in G_{H_K}} \left(\ln |\epsilon_0^\sigma| + \ln |(\epsilon_0^\sigma)^{\sigma_\mathfrak{q}}| \right) \\
&= |G| \ln |\delta| - \ln |N_{K_\mathfrak{p}/H_K}(\epsilon_0)| + \ln |N_{K_\mathfrak{p}/H_K}(\epsilon_0)^{\sigma_\mathfrak{q}}| \\
&= |G| \ln |\delta|.
\end{aligned}$$

Now assume $\chi \neq \psi, 1$. Then

$$\begin{aligned}
\sum_{\sigma \in G} \chi(\sigma) \ln |(\epsilon_0 \delta)^\sigma| &= \sum_{\sigma \in G} \chi(\sigma) \left(\ln |\epsilon_0^\sigma| + \ln |\delta^\sigma| \right) \\
&= \sum_{\sigma \in G_{H_K}} \chi(\sigma) \left(\ln |\epsilon_0^\sigma| + \ln |\delta| \right) + \sum_{\sigma \in G_{H_K}} \chi(\sigma_\mathfrak{q}) \chi(\sigma) \left(\ln |(\epsilon_0^\sigma)^{\sigma_\mathfrak{q}}| - \ln |\delta| \right) \\
&= \sum_{\sigma \in G} \chi(\sigma) \ln |\epsilon_0^\sigma| + \left(\sum_{\sigma \in G_{H_K}} \chi(\sigma) \right) (1 - \chi(\sigma_\mathfrak{q})) \ln |\delta|.
\end{aligned}$$

Note that $\left(\sum_{\sigma \in G_{H_K}} \chi(\sigma) \right) = 0$ because (by assumption) χ is not trivial when restricted to G_{H_K}. Thus we have that if $\chi \neq \psi, 1$ then

$$\sum_{\sigma \in G} \chi(\sigma) \ln |(\epsilon_0 \delta)^\sigma| = \sum_{\sigma \in G} \chi(\sigma) \ln |\epsilon_0^\sigma|.$$

It follows that the regulator of the group generated by the Galois conjugates of $\epsilon_0 \delta$

is

$$\begin{aligned} R_{\epsilon_0\delta} &= \det(2\ln|(\epsilon_0\delta)^{\sigma\tau^{-1}}|)_{\sigma,\tau\neq 1} \\ &= c\ln|\delta| \prod_{\chi\neq\psi,1}\left(\sum_{\sigma\in G}\chi(\sigma)\ln|\epsilon_0^{\sigma}|\right) \end{aligned}$$

for c a power of 2.

But, by the definition of ϵ_0 this is

$$\begin{aligned} R_{\epsilon_0\delta} &= c\ln|\delta| \prod_{\chi\neq\psi,1}\left(\sum_{\sigma\in G}\chi(\sigma)\ln|\epsilon_0^{\sigma}|\right) \\ &= c\ln|\delta| \prod_{\chi\neq\psi,1}\left(\sum_{j=0}^{p-2}\chi(\sigma_{\mathsf{q}}^{j})\left(\ln|\phi(x_{\mathsf{q}^{j+2}},y_{\mathsf{q}^{j+2}},z_{\mathsf{q}^{j+2}})|-\ln|\phi(x_{\mathsf{q}^{j}},y_{\mathsf{q}^{j}},z_{\mathsf{q}^{j}})|\right)\right) \\ &= c\ln|\delta| \prod_{\chi\neq\psi,1}(\chi(\sigma_{\mathsf{q}}^{2})^{-1}-1)\left(\sum_{j=0}^{p-2}\chi(\sigma_{\mathsf{q}}^{j})\ln|\phi(x_{\mathsf{q}^{j}},y_{\mathsf{q}^{j}},z_{\mathsf{q}^{j}})|\right) \\ &= c\ln|\delta| \left(\prod_{\chi\neq\psi,1}(\chi(\sigma_{\mathsf{q}}^{2})^{-1}-1)\right)\prod_{\chi\neq\psi,1}\left(\sum_{j=0}^{p-2}\chi(\sigma_{\mathsf{q}}^{j})\ln|\phi(x_{\mathsf{q}^{j}},y_{\mathsf{q}^{j}},z_{\mathsf{q}^{j}})|\right). \end{aligned}$$

Finally, we note that since $\chi(\sigma_{\mathsf{q}}^{2})$ is a $(p-1)/2$ root of unity, we have

$$\prod_{\chi\neq\psi,1}(\chi(\sigma_{\mathsf{q}}^{2})^{-1}-1) = \prod_{j=1}^{p-1}(\zeta_{\frac{p-1}{2}}^{j}-1)^2 = \left(\frac{p-1}{2}\right)^2$$

with the final equality being the well-known identity $\prod_{j=1}^{n-1}(\zeta_n^j-1)=n$. Plugging this back into the regulator calculation, we get

$$\begin{aligned} R_{\epsilon_0\delta} &= c\ln|\delta|\left(\frac{p-1}{2}\right)^2 \prod_{\chi\neq\psi,1}\left(\sum_{j=0}^{p-2}\chi(\sigma_{\mathsf{q}}^{j})\ln|\phi(x_{\mathsf{q}^{j}},y_{\mathsf{q}^{j}},z_{\mathsf{q}^{j}})|\right) \\ &= c\ln(\delta) \prod_{\chi\neq\psi,1}\left(\sum_{j=0}^{p-2}\chi(\sigma_{\mathsf{q}}^{j})\ln|\phi(x_{\mathsf{q}^{j}},y_{\mathsf{q}^{j}},z_{\mathsf{q}^{j}})|\right), \qquad (3.7) \end{aligned}$$

absorbing the $p-1$ into c which remains divisible only by primes less than p and noting δ is positive.

It is a well-known fact (see [13] Lemma 4.15, for instance) that a ratio of regulators gives a group index:

$$\frac{R_{\epsilon_0\delta}}{R_{K_\mathfrak{p}}} = [\mathcal{O}_{K_\mathfrak{p}}^\times : \pm\langle(\epsilon_0\delta)^\sigma\rangle_{\sigma\in G}].$$

Combining equation 3.6 with equation 3.7, using the above relation (and noting that removing ±1 only changes an index by a factor of 2), we get

$$h_{K_\mathfrak{p}} = c[\mathcal{O}_{K_\mathfrak{p}}^\times : \langle(\epsilon_0\delta)^\sigma\rangle_{\sigma\in G}],$$

where c has once again absorbed all primes less than p. Since $\mathcal{E}$ is defined as being generated by conjugates of $\epsilon = \epsilon_0\delta$ we are done. □

3.2 Calculating Elliptic Units: Computing ϕ

It is worth here repeating the transformation properties of ϕ laid out in equations 3.2-3.5:

$$\begin{aligned}\phi(x, y, z) &= -e^{-\pi i y}\phi(x-1, y, z)\\ &= -e^{\pi i x}\phi(x, y-1, z)\\ &= -e^{\pi i/6}\phi(x, y+x, z-1)\\ &= e^{-\pi i/2}\phi(y, -x, -1/z)\end{aligned}$$

When computing the function ϕ, there are several trade-offs between numerical stability and speed. For instance, the dummy variable j in the infinite product of equation 3.1 only shows up multiplying the z term, but not the x or y. Thus, we can separate that out, obtaining $(1 - c_1c_2^j)(1 - \bar{c}_1c_2^j)$ where $c_1 = \exp(2\pi i(y + zx))$

and $c_2 = \exp(-2\pi i z)$. Writing this way it is clear that c_2 and thus the imaginary part of z is the variable that most controls the speed of convergence. As a result, if one wants to compute ϕ more quickly with no cost to precision, a simple trick is to use transformation properties of the function to maximize the imaginary part. Moreover, if we are using the transformation properties to decrease the size of x and y or increase the imaginary size of z, we should do all our transformations, and then simplify. If we do not then $\phi_{\mathfrak{p}}(\mathcal{I})$ will paradoxically have less precision than $\phi_{\mathfrak{p}}(\mathcal{I}^p)$ even though they are the same (and in fact, $\phi_{\mathfrak{p}}(\mathcal{I}^{p-1})$ will have enough less precision that our computations will go poorly later on).

Lemma 3.2.1. *If* $\operatorname{Im}(z) < 1/2$ *then using equation 3.4 to reduce to* $|\operatorname{Re}(z)| \leq 1/2$ *followed by equation 3.4 causes* $\operatorname{Im}(z)$ *to increase by at least a factor of 2. That is, this procedure causes* $\operatorname{Im}(z)$ *to increase to greater than 1/2 exponentially fast.*

Proof. Assume $z = a + bi$ with $|a| \leq 1/2$. Then we have

$$\operatorname{Im}\frac{-1}{z} = \operatorname{Im}\frac{-1}{a+bi} = \frac{b}{a^2+b^2} > \frac{b}{1/4+1/4} = 2b.$$

Note that if $b \ll a$ then $|z|^2 \approx a^2$ so that $\operatorname{Im}\frac{-1}{z} \approx a^{-2}b$. In other words, the increase can be super-exponential for very small a. □

While hypothetically it can take an arbitrarily long time to get to the largest possible value of $\operatorname{Im}(z)$ (the unique value for which it is $\geq \sqrt{3}/2$), in practice it occurs within one iteration of when the above transformation lemma causes $\operatorname{Im}(z) > 1/2$.

In our calculations $\operatorname{Im}(z)$ starts off being proportional to either $1/p$ or $1/(12p^2)$ for $p \leq 300$, so this alternation between the third and fourth transformation rules never needs to be done more than 20 times to get $\mathrm{Im}(z) \geq 1/2$ (and hits the maximum within 5 typically). Moreover, as both rules cause us to multiply ϕ by a 12th root of unity, there is not need for us to actually multiply until the end, when we know exactly which 12th root of unity it is.

Once we have the optimal z, we reduce x using a first transformation law and then reduce y using the second so that both have absolute value less than 1. Because x and y started out as fractions with denominator p, this step only ever introduces a pth root of unity, and we can just compute which one and multiply by that rather than computing $e^{\pi i x}$ for a mammoth x (x will often be around 10^{p-1} in our computations).

For example, let us say we are computing $\phi_{\mathfrak{p}}(\langle 2, \sqrt{-6}\rangle^8) = \phi_{\mathfrak{p}}(\langle 16\rangle)$ for $\mathfrak{p} = \langle 59, 17 - \sqrt{-6}\rangle$, which lies above 59. We have the following:

$$\phi_{\mathfrak{p}}(\langle 2, \sqrt{-6}\rangle^8) = \phi\left(\frac{16}{59}, \frac{0}{59}, \frac{59}{17-\sqrt{-6}}\right)^{12p}$$

But the real part of $\frac{59}{17-\sqrt{-6}} = \frac{17+\sqrt{-6}}{5}$ is 3.4 and the imaginary around .49. So, we start modifying it by alternately reducing the real part and inverting:

$$\begin{aligned}\phi\left(\frac{16}{59}, \frac{0}{59}, \frac{59}{17-\sqrt{-6}}\right) &= -e^{\pi i 3/6}\phi\left(\frac{16}{59}, \frac{48}{59}, \frac{3+\sqrt{-6}}{5}\right)\\ = -e^{\pi i 3/6}e^{-\pi i/2}\phi\left(\frac{48}{59}, \frac{-16}{59}, \frac{5}{-3-\sqrt{-6}}\right) &= -\phi\left(\frac{48}{59}, \frac{-16}{59}, \frac{-3+\sqrt{-6}}{3}\right)\\ = e^{\pi i/6}\phi\left(\frac{48}{59}, \frac{-64}{59}, \frac{\sqrt{-6}}{3}\right) &= e^{\pi i/6}\phi\left(\frac{48}{59}, \frac{-64}{59}, \frac{\sqrt{-2}}{\sqrt{3}}\right)\\ = e^{\pi i/6}e^{-\pi i/2}\phi\left(\frac{-64}{59}, \frac{-48}{59}, \frac{\sqrt{-3}}{\sqrt{2}}\right) &= e^{-\pi i/3}\phi\left(\frac{-64}{59}, \frac{-48}{59}, \frac{\sqrt{-3}}{\sqrt{2}}\right)\end{aligned}$$

which has imaginary part around 1.22, well above the .86 that defines the maximum.

Now, we shrink the first two arguments to ease the computation:

$$\phi\left(\frac{16}{59},\frac{0}{59},\frac{59}{17-\sqrt{-6}}\right)=e^{-\pi i/3}\phi\left(\frac{-64}{59},\frac{-48}{59},\frac{\sqrt{-3}}{\sqrt{2}}\right)$$
$$=e^{-\pi i/3}e^{\pi i(-48/59)}\phi\left(\frac{-5}{59},\frac{-48}{59},\frac{\sqrt{-3}}{\sqrt{2}}\right)=$$
$$=e^{-\frac{\pi i}{3}}e^{\pi i\frac{-48}{59}}e^{-\pi i\frac{-5}{59}}\phi\left(\frac{-5}{59},\frac{11}{59},\frac{\sqrt{-3}}{\sqrt{2}}\right)=e^{\pi i\frac{166}{177}}\phi\left(\frac{-5}{59},\frac{11}{59},\frac{\sqrt{-3}}{\sqrt{2}}\right).$$

Thus we are left with a function that both converges much faster, and with higher precision.

Further, by thinking of the infinite product in equation 3.1 as being

$$\prod_{j=1}^{\infty}(1-c_1c_2^j)(1-\bar{c}_1c_2^j),$$

we only need to compute c_1, c_2 once. We can view our infinite product as a geometrically decreasing sequence, rather than recomputing the exponential function many times. Doing this causes the computation to speed up by several orders of magnitude. The one potential issue with this that if we don't recompute c_2^j regularly we might worry about the loss in precision (that is, computing the same number of terms will have slightly less precision with this method than recomputing the exponential function each time). On the other hand, the precision being lost to multiplication (around half a bit) is minimal compared with the decrease in magnitude of c_2 so long as $|c_2| < 1/2$ (and after applying transformation rules $|\exp(2\pi i c_2)| < 0.12$). In other words, in practice it is faster (and/or more precise) to compute the c_1, c_2 to a higher precision once and do the product than to compute exp() to a lower precision every time we want another term in the product.

3.3 Computing Elliptic Units in $\mathbb{C}$

In this section we are concerned with showing that the "correct" way to compute our elliptic units involves the following algorithm:

Algorithm 3.3.1. Computing values of ϕ which are nearly Galois conjugate

1. Select the smallest $q \equiv 1 \bmod \frac{24p}{W_{H_K}}$ such that $q = \mathfrak{q}\bar{\mathfrak{q}}$ and $\mathfrak{q} = \langle q, \omega_{\mathfrak{q}} - \omega \rangle$ generates the ray class group
2. Compute α, the principal generator of $\mathfrak{q}^2$
3. For every $j \leq \frac{p-1}{2}$ write α^j as $a_j + b_j\omega$
4. Set $z_{\mathfrak{q}^k} = p/(\omega_{\mathfrak{p}} - \omega)$ if $k = 2j$ and $z_{\mathfrak{q}^k} = pq/(\omega_{\mathfrak{q}\mathfrak{p}} - \omega)$ if $k = 2j+1$
5. Set $y_{\mathfrak{q}^k} = -b_j$
6. Set $x_{\mathfrak{q}^k} = (a_j + b_j\omega_{\mathfrak{q}})/pq$
7. Compute $\phi(x_{\mathfrak{q}^k}, y_{\mathfrak{q}^k}, z_{\mathfrak{q}^k})$ for every $0 \leq k \leq p$

While the unit $\frac{\pi(\mathcal{I})}{\pi(\mathcal{O}_K)}\delta$ may generate a subgroup of the exact index we want, it is not completely clear how to get π from the function ϕ. Stark's function $\phi_{\mathfrak{p}}(\mathcal{I})$ is a power of $\pi(\mathcal{I})$, and only one root lies in $K_{\mathfrak{p}}$. Unfortunately identifying which root is the correct one is not easy.

Kucuksakalli takes a slightly different approach in [5], which we follow and generalize here. In particular, rather than deal with $\phi_{\mathfrak{p}}(\mathcal{I}) = \phi(x_{\mathcal{I}}, y_{\mathcal{I}}, z_{\mathcal{I}})^{12p}$, which is well-defined for each ray class, we pick a particular $x_{\mathcal{I}}, y_{\mathcal{I}}, z_{\mathcal{I}}$ and compute $\phi(x_{\mathcal{I}}, y_{\mathcal{I}}, z_{\mathcal{I}})$

$\in K_{(12p^2)}$. This is not well-defined but depends on our choices. However, Kucuksakalli takes advantage of the Shimura reciprocity law to come up with a good choice of $x_{\mathfrak{q}\mathcal{I}}, y_{\mathfrak{q}\mathcal{I}}, z_{\mathfrak{q}\mathcal{I}}$ given $x_{\mathcal{I}}, y_{\mathcal{I}}, z_{\mathcal{I}}$. Here we rewrite the reciprocity law (which is a general statement about values of level-N modular functions) to more specifically apply to values of ϕ.

Theorem 3.3.2 (Shimura Reciprocity)**.** *Take $\mathfrak{q}\bar{\mathfrak{q}} = q$ prime with $gcd(q, 12dp) = 1$. Take $x_{\mathcal{I}}, y_{\mathcal{I}}, z_{\mathcal{I}}$ a proper triple. In particular $z_{\mathcal{I}} = \mu/\nu$ where $\mu\mathbb{Z} \oplus \nu\mathbb{Z}$ is an ideal of K divisible by $\mathfrak{p}$ with $\operatorname{Im}(\mu/\nu) > 0$ (and $(x_{\mathcal{I}}\mu + y_{\mathcal{I}}\nu)$ is divisible by $\mathcal{I}$). Take $B \in \mathrm{GL}_2(\mathbb{Z})$ so that $\det(B) = q$ and $B\binom{\mu}{\nu}$ is a basis for the ideal $\langle \mu, \nu \rangle \bar{\mathfrak{q}}$ and the ratio of the first basis element to the second has positive imaginary part. Then*

$$\phi(x_{\mathcal{I}}, y_{\mathcal{I}}, z_{\mathcal{I}})^{\sigma_{\mathfrak{q}}} = \phi\left((x_{\mathcal{I}}, y_{\mathcal{I}})qB^{-1}, B(z_{\mathcal{I}})\right) \in K_{(12p^2)}.$$

In the above B^{-1} is acting as a matrix and B as a fractional linear transformation.

Proof. See Theorem 3 in [11]. □

It should be noted that it appears that B depends entirely on $\mathfrak{q}$ and $z_{\mathcal{I}}$ and is independent of x, y (except in that they are selected along with z). We will later show this more formally.

In class number 1, one can pick the same z for all $\mathcal{I}$ by carefully selecting the basis of $\mathfrak{q}$ (as Kucuksakalli does) thus reusing the same B and getting a compact closed form for the orbit of an element. In higher class numbers, we can not.

Lemma 3.3.3. *If $\mathcal{I}$ and $\mathcal{J}$ are in the same principal ideal class, then the ratio of every basis of $\mathcal{I}$ can be realized as the ratio of a basis in $\mathcal{J}$. If they are not in the same ideal class, then no ratio of a basis of $\mathcal{I}$ can be realized from a basis of $\mathcal{J}$.*

Proof. If $\mathcal{I}$ and $\mathcal{J}$ are in the same principal ideal class there exists a (fractional) principal ideal (α) such that $(\alpha)\mathcal{I} = \mathcal{J}$. Take μ, ν as an integer basis for $\mathcal{I}$ and call their ratio $z = \mu/\nu$. Clearly $\alpha\mu$, $\alpha\nu$ is an integer basis for $\mathcal{J}$ and $(\alpha\mu)/(\alpha\nu) = z$.

By way of the contrapositive, assume there exists μ, ν an integer basis of $\mathcal{I}$ and μ', ν' an integer basis of $\mathcal{J}$ with $\mu/\nu = \mu'/\nu'$. We promptly get $\mu = \frac{\nu}{\nu'}\mu'$ and we define $\alpha = \frac{\nu}{\nu'}$. We immediately get that $(\alpha\mu')/\nu = \mu'/\nu'$ and so $\nu = \alpha\nu'$ implying $\mathcal{I} = (\alpha)\mathcal{J}$ and the two are in the same principal class. □

Thus, the minimum number of z values one will have (and correspondingly the minimum number of matrices B one will have to keep track of) is the class number of K; we will attempt to limit z to two values.

We select $(x_{\mathcal{O}_K}, y_{\mathcal{O}_K}, z_{\mathcal{O}_K}) = (1/p, 0, p/(\omega_{\mathfrak{p}} - \omega))$. That is, $(1)\mathcal{O}_K$ is principal and generated by 1, and $(1)\mathfrak{p} = p\mathbb{Z} \oplus (\omega_{\mathfrak{p}} - \omega)\mathbb{Z}$. Then

$$1 = (x_{\mathcal{O}_K} p) + (y_{\mathcal{O}_K}(\omega_{\mathfrak{p}} - \omega)).$$

Take $\mathfrak{q}$ a prime whose ray class generates the ray class group. Let us compute $\phi(1/p, 0, p/(\omega_{\mathfrak{p}} - \omega))^{\sigma_{\mathfrak{q}}}$ using Shimura Reciprocity. As discussed in section 2.3 a basis of $\mathfrak{q}$ is q, $\omega_{\mathfrak{q}} - \omega$ so a basis of $\bar{\mathfrak{q}}$ is q, $\omega_{\bar{\mathfrak{q}}} - \omega$ (where $\omega_{\bar{\mathfrak{q}}} = 1 - \omega_{\mathfrak{q}} \bmod q$ if $d = 1 \bmod 4$ and $-\omega_{\mathfrak{q}} \bmod q$ otherwise). We need a basis of $\mathfrak{p}\bar{\mathfrak{q}}$.

Using the Chinese Remainder Theorem, we can easily compute $\omega_{\mathfrak{p}\bar{\mathfrak{q}}}$, the smallest positive integer congruent to ω mod $\mathfrak{p}\bar{\mathfrak{q}}$. Since we had previously computed $\omega_{\mathfrak{p}}$ and $\omega_{\bar{\mathfrak{q}}}$, it can be easily validated that we get

$$\omega_{\mathfrak{p}\bar{\mathfrak{q}}} = [q(q^{-1} \bmod p)\omega_{\mathfrak{p}} + p(p^{-1} \bmod q)\omega_{\bar{\mathfrak{q}}}] \bmod pq.$$

Thus a $\mathbb{Z}$-basis for our ideal $\mathfrak{p}\bar{\mathfrak{q}}$ is pq, $\omega_{\mathfrak{p}\bar{\mathfrak{q}}} - \omega$. We want B_0 satisfying

$$B_0 \binom{p}{\omega_\mathfrak{p} - \omega} = \binom{pq}{\omega_{\mathfrak{p}\bar{\mathfrak{q}}} - \omega} = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \binom{p}{\omega_\mathfrak{p} - \omega}.$$

We get $s = 0$ since pq is real so $r = q$. This then lets us solve for t and u:

$$B_0 = \begin{bmatrix} q & 0 \\ \frac{\omega_{\mathfrak{p}\bar{\mathfrak{q}}} - \omega_\mathfrak{p}}{p} & 1 \end{bmatrix}.$$

Note that $\omega_{\mathfrak{p}\bar{\mathfrak{q}}} = \omega_\mathfrak{p} \bmod p$ by construction so the fraction is an integer. Also note that $\det(B_0) = q$ as required. We put it all together to get

$$\phi\left(\frac{1}{p}, 0, \frac{p}{\omega_\mathfrak{p} - \omega}\right)^{\sigma_\mathfrak{q}} = \phi\left(\frac{1}{p}, 0, \frac{pq}{\omega_{\mathfrak{p}\bar{\mathfrak{q}}} - \omega}\right).$$

Now we might want to compute

$$\phi\left(\frac{1}{p}, 0, \frac{p}{\omega_\mathfrak{p} - \omega}\right)^{\sigma_\mathfrak{q}^2} = \phi\left(\frac{1}{p}, 0, \frac{pq}{\omega_{\mathfrak{p}\bar{\mathfrak{q}}} - \omega}\right)^{\sigma_\mathfrak{q}}.$$

Reiterating our previous argument, we have encoded in the third argument a basis of $\mathfrak{p}\bar{\mathfrak{q}}$ and we will need to get a basis of $\mathfrak{p}\bar{\mathfrak{q}}^2$. But $\bar{\mathfrak{q}}^2$ is principal since $h_K = 2$ so if $(a + b\omega) = \bar{\mathfrak{q}}^2$ then a perfectly fine basis of $\mathfrak{p}\bar{\mathfrak{q}}^2$ is $(a + b\omega)p$, $(a + b\omega)(\omega_\mathfrak{p} - \omega)$. Better still, the ratio of these two basis elements is $p/(\omega_\mathfrak{p} - \omega)$ so this is a convenient basis. We will let $B_1 \in \mathrm{GL}_2(\mathbb{Z})$ be the matrix that accomplishes this change of basis.

$$\begin{aligned} B_1 \binom{pq}{\omega_{\mathfrak{p}\bar{\mathfrak{q}}} - \omega} &= \binom{ap + bp\omega}{(a + b\omega)(\omega_\mathfrak{p} - \omega)} \\ &= \begin{cases} \binom{ap+bp\omega}{(a\omega_\mathfrak{p} - \frac{d-1}{4}b) + (b(\omega_\mathfrak{p} - 1) - a)\omega} & \text{if } d = 1 \bmod 4 \\ \binom{ap+bp\omega}{(a\omega_\mathfrak{p} - db) + (b\omega_\mathfrak{p} - a)\omega} & \text{otherwise.} \end{cases} \end{aligned}$$

As before, we have 4 linear equations and 4 unknowns when looking at the real and imaginary parts of the two components of the right-hand side. In fact we use the same trick as in B_0 to first solve for the right components of B_1 since the imaginary part of the target vector cannot come from pq. Solving we obtain (the somewhat cumbersome)

$$B_1 = \begin{cases} \begin{bmatrix} \dfrac{a + b\omega_{\mathfrak{p}\bar{\mathfrak{q}}}}{q} & -bp \\ \dfrac{a\omega_{\mathfrak{p}} - \dfrac{d-1}{4}b + (b(\omega_{\mathfrak{p}} - 1) - a)\omega_{\mathfrak{p}\bar{\mathfrak{q}}}}{pq} & a - b(\omega_{\mathfrak{p}} - 1) \end{bmatrix} & \text{if } d = 1 \bmod 4 \\ \\ \begin{bmatrix} \dfrac{a + b\omega_{\mathfrak{p}\bar{\mathfrak{q}}}}{q} & -bp \\ \dfrac{a\omega_{\mathfrak{p}} - db + (b\omega_{\mathfrak{p}} - a)\omega_{\mathfrak{p}\bar{\mathfrak{q}}}}{pq} & a - b\omega_{\mathfrak{p}} \end{bmatrix} & \text{otherwise.} \end{cases}$$

Taking determinants, we get (after fully expanding and cancelling)

$$\det(B_1) = \begin{cases} \frac{a^2+ab+b^2\frac{d-1}{4}}{q} = \frac{Norm(\bar{\mathfrak{q}}^2)}{q} = q & \text{if } d = 1 \bmod 4 \\ \\ \frac{a^2-b^2d}{q} = \frac{Norm(\bar{\mathfrak{q}}^2)}{q} = q & \text{otherwise} \end{cases}$$

and so B_1 satisfies the requirements of Shimura reciprocity. We compute qB_1^{-1} and we have

$$\phi\left(\frac{1}{p}, 0, \frac{p}{\omega_{\mathfrak{p}} - \omega}\right)^{\sigma_{\mathfrak{q}}^2} = \begin{cases} \phi\left(\frac{a+b-b\omega_{\mathfrak{p}}}{p}, -bp, \frac{p}{\omega_{\mathfrak{p}}-\omega}\right) & \text{if } d = 1 \bmod 4 \\ \\ \phi\left(\frac{a-b\omega_{\mathfrak{p}}}{p}, -bp, \frac{p}{\omega_{\mathfrak{p}}-\omega}\right) & \text{otherwise.} \end{cases} \tag{3.8}$$

As we now have $p/(\omega_{\mathfrak{p}} - \omega)$ in the third argument again, we are potentially back to the action of $\sigma_{\mathfrak{q}}$ being accomplished with B_0. At this point we invoke the fact that B_0 and B_1 are $\mathbb{C}$-linear (and so $B_0\binom{\mu}{\nu} = \binom{\mu'}{\nu'}$ implies $B_0\binom{\alpha\mu}{\alpha\nu} = \binom{\alpha\mu'}{\alpha\nu'}$ for all $\alpha \in \mathbb{C}$).

The result is that B_0 and B_1 will effect $\sigma_{\mathfrak{q}}$ according to Shimura reciprocity so long as $z_{\mathcal{I}}$ is either $\frac{p}{\omega_{\mathfrak{p}}-\omega}$ or $\frac{pq}{\omega_{\mathfrak{p}\bar{\mathfrak{q}}}-\omega}$ respectively.

This brings us to the following Theorem, which is what we actually use to compute ϕ:

Theorem 3.3.4. *Let $\mathfrak{q}$ be a degree 1 prime ideal that generates the ray class group of conductor $\mathfrak{p}$ in K, with $h_K = 2$. Let α be the generator of $\bar{\mathfrak{q}}^2$ with positive imaginary part. If $\alpha^i = u + v\omega$, then let*

$$\begin{aligned} x_{\bar{\mathfrak{q}}^{2i-1}} &= \frac{u + v\omega_{\mathfrak{p}\bar{\mathfrak{q}}}}{pq} \\ y_{\bar{\mathfrak{q}}^{2i-1}} &= -v \\ z_{\bar{\mathfrak{q}}^{2i-1}} &= \frac{pq}{\omega_{\mathfrak{p}\bar{\mathfrak{q}}} - \omega} \end{aligned}$$

and let

$$\begin{aligned} x_{\bar{\mathfrak{q}}^{2i}} &= \frac{u + v\omega_{\mathfrak{p}}}{p} \\ y_{\bar{\mathfrak{q}}^{2i}} &= -v \\ z_{\bar{\mathfrak{q}}^{2i}} &= \frac{p}{\omega_{\mathfrak{p}} - \omega}. \end{aligned}$$

Then for all $j, k \geq 0$ we have

$$\phi\left(x_{\bar{\mathfrak{q}}^j}, y_{\bar{\mathfrak{q}}^j}, z_{\bar{\mathfrak{q}}^j}\right)^{\sigma_{\mathfrak{q}}^{k-j}} = \phi\left(x_{\bar{\mathfrak{q}}^k}, y_{\bar{\mathfrak{q}}^k}, z_{\bar{\mathfrak{q}}^k}\right).$$

Proof. After the above lemma and examples, it is enough to show $x_{\bar{\mathfrak{q}}^j}, y_{\bar{\mathfrak{q}}^j}, z_{\bar{\mathfrak{q}}^j}$ is a proper $\phi_{\mathfrak{p}}(\bar{\mathfrak{q}}^j)$ triple for all j and demonstrate that both

$$(\frac{1}{p}, 0)\left((qB_0^{-1})(qB_1^{-1})\right)^i = (x_{\bar{\mathfrak{q}}^{2i}}, y_{\bar{\mathfrak{q}}^{2i}})$$

and

$$(\frac{1}{p},0)(qB_0^{-1})\left((qB_1^{-1})(qB_0^{-1})\right)^i=(x_{\bar{\mathfrak{q}}^{2i+1}},y_{\bar{\mathfrak{q}}^{2i+1}}).$$

By construction, $z_{\bar{\mathfrak{q}}^j}=\mu/\nu$ with $\mu=p$ and $\nu=\omega_{\mathfrak{p}}-\omega$ or $\mu=pq$ and $\nu=\omega_{\mathfrak{p}\bar{\mathfrak{q}}}-\omega$. We can quickly verify that

$$\begin{aligned}(x_{\bar{\mathfrak{q}}^j},y_{\bar{\mathfrak{q}}^j})\begin{pmatrix}\mu\\ \nu\end{pmatrix}=&x_{\bar{\mathfrak{q}}^j}\mu+y_{\bar{\mathfrak{q}}^j}\nu\\ =&\frac{u+v\omega_{\mathfrak{p}}}{p}p+(-v)(\omega_{\mathfrak{p}}-\omega)\\ =&u+v\omega=\alpha^{\frac{j}{2}}\end{aligned}$$

if j even, while if j is odd we get

$$\begin{aligned}(x_{\bar{\mathfrak{q}}^j},y_{\bar{\mathfrak{q}}^j})\begin{pmatrix}\mu\\ \nu\end{pmatrix}=&\frac{u+v\omega_{\mathfrak{p}\bar{\mathfrak{q}}}}{pq}pq+(-v)(\omega_{\mathfrak{p}\bar{\mathfrak{q}}}-\omega)\\ =&u+v\omega=\alpha^{\frac{j+1}{2}}.\end{aligned}$$

As a result, it satisfies the requirements of a proper triple. On the other hand, we can show that Shimura Reciprocity sends proper triples to proper triples since

$$\begin{aligned}\left((x,y)(qB^{-1})\right)\cdot\left(B^T(\mu,\nu)\right)&=(x,y)\cdot\left((qB^{-1})^TB^T(\mu,\nu)\right)\\ &=q\left((x,y)\cdot(\mu,\nu)\right)\\ &=q(x\mu+y\nu)\end{aligned}$$

From this we get that if $x_{\mathcal{I}}\mu+y_{\mathcal{I}}\nu=\beta$ then $x_{\bar{\mathfrak{q}}^2\mathcal{I}}\mu'+y_{\bar{\mathfrak{q}}^2\mathcal{I}}\nu'=q^2\beta$ after applying the $\sigma_{\mathfrak{q}}$ transformation twice in a row. Starting at $x_{\mathcal{O}_K}p+y_{\mathcal{O}_K}(\omega_{\mathfrak{p}}-\omega)=1$ we get that for all i

$$x_{\bar{\mathfrak{q}}^{2i}}\alpha^ip+y_{\bar{\mathfrak{q}}^{2i}}\alpha^i(\omega_{\mathfrak{p}}-\omega)=q^{2i}$$

which, using the identity $\alpha^i\bar{\alpha}^i = q^{2i}$, means

$$\begin{aligned} x_{\bar{\mathfrak{q}}^{2i}}p + y_{\bar{\mathfrak{q}}^{2i}}(\omega_{\mathfrak{p}} - \omega) =& \bar{\alpha}^i \\ =& \begin{cases} u + v - v\omega & \text{if } d \equiv 1 \bmod 4 \\ \\ u - v\omega & \text{otherwise.} \end{cases} \end{aligned}$$

At this point we have two linear equations by looking at the real and imaginary parts, and given that we know $x_{\bar{\mathfrak{q}}^{2i}}, y_{\bar{\mathfrak{q}}^{2i}}$ are real, we have two unknowns. Solving yields the values given in the Theorem.

Similarly, starting with $x_{\bar{\mathfrak{q}}}(pq) + y_{\bar{\mathfrak{q}}}(\omega_{\mathfrak{pq}} - \omega) = 1$ we get that

$$x_{\bar{\mathfrak{q}}^{2i+1}}\alpha^i(pq) + y_{\bar{\mathfrak{q}}^{2i+1}}\alpha^i(\omega_{\mathfrak{pq}} - \omega) = \bar{\alpha}^i.$$

We can once again solve and verify, which completes the proof. □

We know the 12pth power of $\phi(x_{\mathfrak{q}^j}, y_{\mathfrak{q}^j}, z_{\mathfrak{q}^j})$ is in $\mathcal{O}_{K_{\mathfrak{p}}}$ and that the W_{H_K} power equals $\pi(\mathfrak{q}^j)$ up to an appropriate root of unity ([11] lemma 9, which is slightly more technical than our Theorem 3.1.1). This implies

$$\phi(x_{\mathfrak{q}^j}, y_{\mathfrak{q}^j}, z_{\mathfrak{q}^j})^{W_{H_K}} = \pi(\mathfrak{q}^j)\zeta_{12p}^k \tag{3.9}$$

for some k. So $\phi(x_{\mathfrak{q}^j}, y_{\mathfrak{q}^j}, z_{\mathfrak{q}^j})^{W_{H_K}}$ is an element of $\mathcal{O}_{K_{\mathfrak{p}}}$ multiplied by a root of unity (which might not be in $K_{\mathfrak{p}}$). Applying $\sigma_{\mathfrak{q}}^r$ we get

$$\phi(x_{\mathfrak{q}^{j+r}}, y_{\mathfrak{q}^{j+r}}, z_{\mathfrak{q}^{j+r}})^{W_{H_K}} = \phi(x_{\mathfrak{q}^j}, y_{\mathfrak{q}^j}, z_{\mathfrak{q}^j})^{W_{H_K}\sigma_{\mathfrak{q}}^r} = \left(\pi(\mathfrak{q}^j)\zeta_{12p}^k\right)^{\sigma_{\mathfrak{q}}^r} = \pi(\mathfrak{q}^{j+r})\zeta_{12p}^{q^r k}.$$

If we could set $q \equiv 1 \bmod 12p$ then $\zeta_{12p}^{q^r k} = \zeta_{12p}^k$ and

$$\left(\frac{\phi(x_{\mathfrak{q}^j}, y_{\mathfrak{q}^j}, z_{\mathfrak{q}^j})}{\phi(x_{\mathfrak{q}^{j+r}}, y_{\mathfrak{q}^{j+r}}, z_{\mathfrak{q}^{j+r}})}\right)^{W_{H_K}} \in K_{\mathfrak{p}}.$$

By construction we know a W_{H_K}th root of this lies in $\mathcal{O}_{K_\mathfrak{p}}$ if r is divisible by h_K. But since the W_{H_K}th roots of unity lie in $\mathcal{O}_{K_\mathfrak{p}}$ all roots of the above ratio lie in $\mathcal{O}_{K_\mathfrak{p}}$, so that for r even and $q \equiv 1 \bmod 12p$ we have

$$\frac{\phi(x_{\mathfrak{q}^j}, y_{\mathfrak{q}^j}, z_{\mathfrak{q}^j})}{\phi(x_{\mathfrak{q}^{j+r}}, y_{\mathfrak{q}^{j+r}}, z_{\mathfrak{q}^{j+r}})} \in \mathcal{O}_{K_\mathfrak{p}}.$$

Having $q \equiv 1 \bmod 12p$ is not possible for every K, in particular, not when H_K has extra roots of unity. This is because $\mathfrak{q}$ must be non-principal if it generates the ray class field. Non-principaltiy means $\mathfrak{q}$ doesn't split in H_K, which means it does not split in the maximal real subfield of H_K. Referring back to Theorem 2.2.5 we get that if $3|d$ then $q \equiv 2 \bmod 3$ while if d prime then $q \equiv 3 \bmod 4$. If for instance $3|d$ and $q \equiv 1 \bmod 4p$ and $q \equiv 2 \bmod 3$ then

$$\left(\frac{\phi(x_{\mathfrak{q}^j}, y_{\mathfrak{q}^j}, z_{\mathfrak{q}^j})}{\phi(x_{\mathfrak{q}^{j+r}}, y_{\mathfrak{q}^{j+r}}, z_{\mathfrak{q}^{j+r}})}\right)^3 \zeta_3^{(q^r-1)k} \in \mathcal{O}_{K_\mathfrak{p}}.$$

But since $\zeta_3 \in \mathcal{O}_{K_\mathfrak{p}}$ the ratio of the two is in $\mathcal{O}_{K_\mathfrak{p}}$ as well. Thus we can redefine $\pi(\mathfrak{q})$ (which was only defined up to root of unity in $K_\mathfrak{p}$) so that $k \equiv 0 \bmod 3$. Similarly if d is prime and $q \equiv 1 \bmod 3p$ the ratio lies in $\mathcal{O}_{K_\mathfrak{p}}$. Thus we are able to compute our elliptic units of subsection 3.1 as

$$\epsilon^{\sigma_\mathfrak{q}^r} = \left(\left(\frac{\pi(\mathfrak{q}^2)}{\pi(K)}\delta\right)^{\frac{1}{W_{H_K}}}\right)^{\sigma_\mathfrak{q}^r} = \left(\frac{\phi(x_{\mathfrak{q}^j}, y_{\mathfrak{q}^j}, z_{\mathfrak{q}^j})}{\phi(x_{\mathfrak{q}^{j+r}}, y_{\mathfrak{q}^{j+r}}, z_{\mathfrak{q}^{j+r}})}\right)\delta^{(-1)^q}$$

where δ is the fundamental unit of H_K.

To summarize, to generate the elliptic units we perform the following process:

Algorithm 3.3.5. Constructing generators of elliptic units and their Galois action

1. Select primes $q = 1 + 12pj$ for increasing values of j ($1 + 4pj$ or $1 + 3pj$ for $3|d$ or d prime respectively).

2. Increment j until $\left(\frac{d}{q}\right) = 1$, ensuring q splits in K, and $\left(\frac{d_1}{q}\right) \neq 1$ (where d_1 is the discriminant of the maximal real subfield of H_K), so the factors of (q) are non-principal because they don't split in H_K.

3. Fix $\mathfrak{q}$ by factoring $f_\omega(x)$ mod q and selecting a root. Let $\omega_\mathfrak{q}$ be the lift of this root to $\mathbb{Z}$.

4. Compute α which generates $\mathfrak{q}^2$ by the methods of section 2.2.

5. Write α as $m + n\omega$ and check if $\frac{p-1}{2} | \text{Order}(m + n\omega_\mathfrak{p} \bmod p)$. If not, go back to step 1. Because $q \equiv 1 \bmod p$ is in the trivial class we know the ray class of $\bar{\mathfrak{q}}$ is the inverse of the class of $\mathfrak{q}$ and so also generates the group.

6. Compute $\phi(x_{\mathfrak{q}^j}, y_{\mathfrak{q}^j}, z_{\mathfrak{q}^j})$ for every $0 \leq j \leq p$ using Algorithm 3.3.1. Ensure $x_{\mathfrak{q}^j}, y_{\mathfrak{q}^j}$ are stored as rational numbers so they all have the same precision.

7. For every $0 \leq j < p - 1$ compute

$$\epsilon^{\sigma_\mathfrak{q}^j} = \left(\frac{\phi(x_{\mathfrak{q}^{j+2}}, y_{\mathfrak{q}^{j+2}}, z_{\mathfrak{q}^{j+2}})}{\phi(x_{\mathfrak{q}^j}, y_{\mathfrak{q}^j}, z_{\mathfrak{q}^j})} \right) \delta^{(-1)^q}.$$

While Theorem 3.1.3 showed the elliptic units are finite index, we can empirically verify this once we have computed the conjugates: We create the $(p-2) \times (p-2)$ matrix whose entry in position (i, j) is given by $\log(|\epsilon^{\sigma^{ij}}|)$. Since the group index is the ratio of the regulators, this has non-zero determinant exactly in the case where the group is finite index.

With all the Galois conjugates of ϵ in $K_\mathfrak{p}/K$ we can obtain the minimal polynomial by interpolation. That is,

$$f_\epsilon(x) = \prod_{i=1}^{p-1}(x - \epsilon^{\sigma^i}) \tag{3.10}$$

This polynomial lies over K making it a convenient way to check if our computations have gone correctly regardless of how we computed ϵ. We divide the imaginary part of every coefficient by the imaginary part of ω, check we have an integer, then subtract that integer multiple of ω from the coefficient to verify we have an integer. Moreover, after doing this step we can write $f_\epsilon = g(x) + h(x)\omega$ where $g, h \in \mathbb{Z}[x]$. This seemingly trivial fact bears repeating as it will be used extensively:

Algorithm 3.3.6. Creating a polynomial f independent of the embedding of $\mathcal{O}_K$ (or finding out your polynomial does not lie in the polynomial ring).

1. Take f.

2. Let $h = \lceil \mathrm{Im}(f)/\mathrm{Im}(\omega) \rfloor$ where $\lceil \cdot \rfloor$ rounds every coefficient to the nearest integer.

3. Let $g = \lceil f - h\omega \rfloor$.

4. If $\lceil f - g + h\omega \rfloor == 0$ then return $g, h \in \mathbb{Z}[x]$

5. Else recompute f with precision greater than the size of the absolute value largest coefficient, or $f \notin \mathcal{O}_K[x]$.

A simple first use of the algorithm allows us to easily compute ϵ to arbitrary precision over $\mathbb{C}$: first we compute ω to a high precision, next we recompute $f_\epsilon = g(x) + h(x)\omega$ with this new precision, then we apply a fast root-finding algorithm such as the Splitting Circle Method used in PARI [14] to evaluate the roots of f_ϵ numerically. While the product defining ϕ converges geometrically, meaning each extra term we multiply by gets us a fixed number more bits of precision, other methods converge faster so that each iteration of the algorithm gives more bits of precision than the last. For instance, computing ϕ to the precision necessary to perform the computations in section 3.6 took hours per value of ϕ (of which there were over a hundred) while interpolating the minimal polynomial at a lower precision then using the PARI command polroots() on this polynomial could find all the roots to the desired precision in a few hours.

Now that we have these units, we can easily recover $\pi(\mathfrak{q})$ and its conjugates. In fact we can often do better. Let $\zeta_j = \exp(2\pi i/j)$. If

$$\gamma = \phi(x_\mathfrak{q}, y_\mathfrak{q}, z_\mathfrak{q})^r \in \zeta_{12p}^k K_\mathfrak{p},$$

then so is $\phi(x_{\mathfrak{q}^j}, y_{\mathfrak{q}^j}, z_{\mathfrak{q}^j})^r$ for all j so long as we picked $\sigma_\mathfrak{q}$ so that it fixes all $12p$th roots of unity not in $K_\mathfrak{p}$ (which we can do since the fields $K_\mathfrak{p}$ and $K(\zeta_p)$ are disjoint). Without loss of generality, we may assume $k < 6p$ and $r < 12p$. If $q \equiv 1 \bmod \frac{24p}{W_{H_K}}$ then

$$\begin{aligned}\left(\phi(x_\mathfrak{q}, y_\mathfrak{q}, z_\mathfrak{q})^r \zeta_{12p}^{-k}\right)^{\sigma_\mathfrak{q}^{j-1}} =& \phi(x_{\mathfrak{q}^j}, y_{\mathfrak{q}^j}, z_{\mathfrak{q}^j})^r \zeta_{12p}^{-q^{j-1}k} \\ =& \phi(x_{\mathfrak{q}^j}, y_{\mathfrak{q}^j}, z_{\mathfrak{q}^j})^r \zeta_{\frac{24p}{W_{H_K}}}^{-k} \zeta_{W_{H_K}}^{-q^{j-1}k}.\end{aligned}$$

One guesses what $k \bmod \frac{24p}{W_{H_K}}$ is (call this guess g) and then interpolates the putative minimal polynomial of $\phi(x_\mathfrak{q}, y_\mathfrak{q}, z_\mathfrak{q})^r \zeta_{12p}^{-g}$ as

$$\tilde{f}_\gamma(x) = \prod_{i=1}^{p-1} \left(x - \zeta_{\frac{24p}{W_{H_K}}}^{-g} \zeta_{W_{H_K}}^{-q^{j-1}g} \phi(x_{\mathfrak{q}^j}, y_{\mathfrak{q}^j}, z_{\mathfrak{q}^j})^r \right).$$

Checking that this polynomial lies in $\mathcal{O}_K[x]$ then shows that we have chosen g correctly:

Lemma 3.3.7. *If the polynomial $\tilde{f}_\gamma(x)$ lies in $K[x]$ then $g = k$.*

Proof. Because $K_{(12p^2)}/K$ is an abelian extension we know $\tilde{f}_\gamma$ splits in a degree-$(p-1)$ extension. Because the roots of $\tilde{f}_\gamma$ only differ from the roots of f_γ by a root of unity, $f_{\gamma^{12p/r}}$ must split in a subfield of the splitting field of $\tilde{f}_\gamma$ and in $K_\mathfrak{p}$, the splitting field of f_γ. Thus verifying $f_{\gamma^{12p/r}}$ is irreducible shows by degree arguments that $K_\mathfrak{p}$ is the splitting field of $\tilde{f}_\gamma$. Assume $f_{\gamma^{12p/r}}$ factors into two polynomials h_1, h_2 over K. By construction there is a Galois element that moves any given root of $f_{\gamma^{12p/r}}$ to any other, thus there is an element that moves any given root of h_1 to a root of h_2. But since all the Galois conjugates of roots of h_1 are themselves roots of h_1 we have that $h_2 = h_1$. But this implies there is a Galois element τ with $\gamma^{\frac{12p}{r}} = \gamma^{\frac{12p}{r}\tau}$. Note that δ, the fundamental unit of H_K, is fixed by τ^2 since it lies in a degree-two extension of K. Thus τ induces a relation among the elliptic units, namely

$$\epsilon^{12p} = \frac{\gamma^{\frac{12p}{r}\sigma_\mathfrak{q}^2}}{\gamma^{\frac{12p}{r}}}\delta^{12p} = \left(\frac{\gamma^{\frac{12p}{r}\sigma_\mathfrak{q}^2}}{\gamma^{\frac{12p}{r}}}\delta^{12p}\right)^{\tau^2} = \epsilon^{12p\tau^2},$$

and both are elliptic units. As $N_{K_\mathfrak{p}/K}(\epsilon) = 1$ should be the only relation, we conclude $\tau^2 = 1$ so $\tau = \sigma_\mathfrak{q}^{\frac{p-1}{2}}$ in the splitting field. If $p \equiv 1 \bmod 4$ then $\frac{p-1}{2}$ is even so $\delta^\tau = \delta$, and we get the nontrivial relation

$$\frac{\gamma^{\frac{12p}{r}\sigma_\mathfrak{q}^2}}{\gamma^{\frac{12p}{r}}}\delta^{12p} = \left(\frac{\gamma^{\frac{12p}{r}\sigma_\mathfrak{q}^2}}{\gamma^{\frac{12p}{r}}}\right)^{\tau}\delta^{12p} = \left(\frac{\gamma^{\frac{12p}{r}\sigma_\mathfrak{q}^2}}{\gamma^{\frac{12p}{r}}}\delta^{12p}\right)^{\sigma_\mathfrak{q}^{\frac{p-1}{2}}}$$

which is impossible. Similarly, if $p \equiv 3 \bmod 4$ so that

$$\frac{\gamma^{\frac{12p}{r}\sigma_{\mathfrak{q}}^2}}{\gamma^{\frac{12p}{r}}}\delta^{12p} = \left(\frac{\gamma^{\frac{12p}{r}\sigma_{\mathfrak{q}}^2}}{\gamma^{\frac{12p}{r}}}\right)^{\sigma_{\mathfrak{q}}^{\frac{p-1}{2}}} \delta^{-12p}$$

we can take the norm down to H_K and as the left side should norm to positive powers of δ while the right should norm to negative powers, we have a contradiction. Thus we conclude $f_{\gamma^{12p/r}}$ irreducible and we are done. □

It should be noted here that the minimal polynomial of $\pi(\mathfrak{q})$ or any other γ is a larger polynomial typically than f_ϵ because it is not a unit (and generally has been raised to a power) therefore computation of $f_{\pi(\mathcal{O}_K)}$ would require at least twice the precision. Because interpolating at high precision takes time, one might instead look at

$$\left|\sum_{j=1}^{p-1} \zeta_{W_{H_K}}^{-q^j g}\phi(x_{\mathfrak{q}^j}, y_{\mathfrak{q}^j}, z_{\mathfrak{q}^j})^r\right|^2 .$$

When it is an integer, you have probably guessed part of k correctly (and you certainly have if only one does), at which point we can multiply the sum by powers of $\zeta_{\frac{24p}{W_{H_K}}}$ until it lies in K. This requires much less precision, and in practice always works (as in only one g satisfies the conditions), so one can recover k without needing enough precision to actually compute f_γ.

3.4 Constructing Elliptic Units and Their Galois Action Over $\mathbb{Z}_r$

We follow [5] in embedding ϵ and its conjugates into $\mathbb{Z}_r$. By splitting f_ϵ into $g(x) + h(x)\omega$ we can embed the polynomial into $\mathbb{Z}_r[x]$ so long as $\omega \in \mathbb{Z}_r$ (which in turn just requires $\left(\frac{d}{r}\right) = 1$). We then take the roots of this to obtain ϵ and its conjugates. Often the r we deal with are not congruent to 1 mod p, so $\mathcal{O}_{K_{(p)}}$ (which contains the pth roots of unity) does not embed in $\mathbb{Z}_r$. In this case there is only one way to embed f_ϵ into $\mathbb{Z}_r[x]$ and have it factor into linear terms. As usual we have $\mathcal{O}_{K_\mathfrak{p}} \subset \mathbb{Z}_r$ if and only if r splits in $\mathcal{O}_{K_\mathfrak{p}}$. Thus we construct r's that specifically split.

Algorithm 3.4.1. Generating r so that $\mathcal{O}_{K_\mathfrak{p}} \subset \mathbb{Z}_r$

1. Select $a, b \in \mathbb{Z}$
2. Set $j = \omega_\mathfrak{p}^{-1} \bmod p$ and $k = 0$
3. Let $\mathfrak{r} = ((ap + k + 1) - (bp + jk)\omega)$. Note that $\mathfrak{r}$ is in the trivial ray class mod$\mathfrak{p}$.
4. Set $r = N(\mathfrak{r})$.
5. If r is prime, then $\mathcal{O}_{K_\mathfrak{p}}$ embeds in $\mathbb{Z}_r$.
6. If r is not prime and $k < p$ then go to 2 and set $k = k + 1$.
7. If r is not prime and $k = p$ then go to 1 and set $a = a + 1$ if $|a + 1 + b\omega| < |a + (b + 1)\omega|$ or set $b = b + 1$ otherwise.

For speed purposes, we want to have step 3 before 4 because primality testing is the longest step (if still pretty short) and the probability of r being a prime is $1/\log(r)$ which is typically much larger than the probability of something being in the trivial ray class, $1/(p - 1)$. We increment the way we do in step 7 to keep r small and thus more likely to be prime. This mostly matters for p in the hundreds where finding an r may take seconds. If we want to add an additional condition, it is easy to do so. For instance, to ensure the pth roots of unity are in $\mathbb{Z}_r$ we just require $k = 0$; to cause no roots of unity to lie in $\mathbb{Z}_r$, we skip $k = 0$.

We continue following the methods of [5] in determining the Galois action on the roots of f_ϵ. For a cyclic Galois group, there is no canonical way to fix which root of f_ϵ in $\mathbb{Z}_r$ is ϵ; by declaring a root to be ϵ we have fixed an embedding. Now we need to figure out the Galois action. To do this, we encode the action of a Galois element in the minimal polynomial of an element of the unit group

$$f_{increment}(x) = \prod_{i=1}^{p-1}(x - \epsilon^{\sigma^i + \sigma^{i+1}}). \tag{3.11}$$

The roots of this polynomial are the product of input/output pairs of the σ function. We can compute this polynomial over $K[x] \in \mathbb{C}[x]$ using the techniques of the previous section. Since this polynomial is over $K[x]$ we can easily break it into two components $g(x) + h(x)\omega$ and embed it into $\mathbb{Z}_r[x]$. We can then use its roots, along with the roots of f_ϵ to find every input/output pair of σ in our embedding.

Unfortunately, we do not know which element of the pair is input and which is output. By starting at a pair that included ϵ and claiming this pair uses ϵ as the input, we can work our way through all the pairs and construct a function. But, we won't know if we guessed correctly in the first pair we picked (in which case we reconstructed σ) or not (meaning we reconstructed σ^{-1}). So we employ one final polynomial

$$f_{direction}(x) = \prod_{i=1}^{p-1}(x - \epsilon^{\sigma^i + \sigma^{i+1} + \sigma^{i+3}}). \tag{3.12}$$

We once again embed this in $\mathbb{Z}_r[x]$ and take roots. We then check whether the root of $f_{increment}$ that we thought corresponded to $\epsilon^{1+\sigma}$ actually is, by multiplying it by the purported ϵ^{σ^3} and seeing if it is a root of $f_{direction}$.

An example will hopefully clear things up. Let $\mathfrak{p} = (1+\omega) \subset \mathcal{O}_K$ with $K = \mathbb{Q}(\sqrt{-6})$, so $p = 7$. Using the methods of the previous section we can get

$$\begin{aligned} f_\epsilon =& x^6 + (-2+3\omega)x^5 + (-12+6\omega)x^4 + (-22+9\omega)x^3 + (25-3w)x^2 + 22x + 1 \\ =&(x^6 - 2x^5 - 12x^4 - 22x^3 + 25x^2 + 22x + 1) \\ &+ (3x^5 + 6x^4 + 9x^3 - 3x^2)\omega. \end{aligned}$$

We can verify that a $\mathcal{R}$ lying above $r = 26209$ has the r-adic properties we want. So, in $\mathbb{Z}_r$ we get $\omega = 627 + O(r)$ and

$$\begin{aligned} f_\epsilon =& x^6 + (1879 + O(r))x^5 + (3750 + O(r))x^4 + (5621 + O(r))x^3 \\ &- (1856 + O(r))x^2 + 22x + 1 \\ =&(x - 4521 + O(r))(x - 12045 + O(r))(x - 15266 + O(r)) \\ &(x - 21500 + O(r))(x - 24368 + O(r))(x - 25257 + O(r)). \end{aligned}$$

Finding the roots above was a simple polynomial-time algorithm (polrootspadic() in PARI for instance). We fix an embedding by declaring $\epsilon = 4521 + O(r)$ (the first root). There is only one way now to consistently assign names to the other roots. We have

$$\begin{aligned} f_{increment} =&(x^6 - 14x^5 + 101x^4 - 138x^3 - 668x^2 - 16x + 1) \\ &+ (-6x^5 + 75x^4 - 309x^3 - 228x^2 + 3x)\omega \\ =&(x - 3693 + O(r))(x - 9289 + O(r))(x - 11301 + O(r)) \\ &(x - 12702 + O(r))(x - 22580 + O(r))(x - 22838 + O(r)). \end{aligned}$$

We see that the ratio of the 2nd root of $f_{increment}$ to the 3rd of f_ϵ is $4521 + O(r)$ (our ϵ), as is the ratio of the 3rd root of $f_{increment}$ to the 5rd root of f_ϵ. Thus either $\epsilon^\sigma = 15266 + O(r)$ and $\epsilon^{\sigma^5} = 24368 + O(r)$, or vice versa.

Let's assume for the moment $\epsilon^\sigma = 15266 + O(r)$. Dividing all the roots of $f_{increment}$ by $15266+O(r)$, only the first and second quotients are on the list of roots of f_ϵ. Since we know the second root of $f_{increment}$ corresponds to $\epsilon\epsilon^\sigma$, the first must be $\epsilon^\sigma\epsilon^{\sigma^2}$ and $\epsilon^{\sigma^2} = 21500 + O(r)$.

Dividing the roots of $f_{increment}$ by $21500 + O(r)$, we see the fifth quotient is a root of f_ϵ so $\epsilon^{\sigma^3} = 12045 + O(r)$. The one remaining root of f_ϵ is $25257 + O(r)$, so this must be ϵ^{σ^4}.

In order to see if our guess was correct, we compute $\epsilon\epsilon^\sigma\epsilon^{\sigma^3} = 25993 + O(r)$, then we stick it into

$$\begin{aligned} f_{direction} =& (x^6 + 16x^5 - 78x^4 + 122x^3 - 29x^2 - 10x + 1) \\ &+ (6x^5 + 51x^4 + 54x^3 + 9x^2 - 3x)\omega \end{aligned}$$

which yields $0 + O(r)$, so we must have made the correct guess for the value of ϵ^σ. We have now well-defined an embedding of $K_\mathfrak{p}$ into $\mathbb{Z}_r$ since we have stated where a K-linear basis gets sent.

From here on, one should think of $\epsilon^{\sigma_\mathfrak{q}^j}$ in the r-adics as being an ordered $p-1$ long vector where each entry is an integer mod r^k for some k.

As our algorithms below will involve embedding in many different r-adics, lining up roots with $f_{increment}$ can easily become a bottleneck in the code. As a result, we here state the standard trick to find pairs of roots of f_ϵ whose product is a root of $f_{increment}$.

The naive method would be to multiply every root of f_ϵ by every other (which will take at least $p^2/2$ operations) and then comparing each of these to the list of roots of $f_{increment}$ (another factor of p for a total of $p^3/2$).

A standard speed-up is to sort the list of roots. Sorting a list of length n takes approximately $n \log_2(n)$ operations, and most standard programming languages will have this functionality built in (vecsort() in PARI for instance). First we multiply every root of f_ϵ by a particular root, say ϵ_0 and make a list of tuples $(\epsilon_0\tau, \tau)$. Next, we add a tuple $(\gamma, 0)$ to the list for every root γ of $f_{increment}$. We sort (say, based on the value of the roots when lifted naively to the integers). We now need only compare the first component of every element on our list to those immediately before and after it. If $\epsilon_0\tau$ is a root of $f_{increment}$ then $(\epsilon_0\tau, 0)$ will be on the list right before $(\epsilon_0\tau, \tau)$. The work is therefore $\approx 2p\log_2(2p)$ for each root of f_ϵ or $\approx 2p^2\log_2(2p)$ total.

3.5 Schoof's Method

Schoof's method computes a factor of the class number of a field (likely the whole thing) by finding relations in a group of the same size as the class group. If we are unable to find relations after a small number of attempts, the remaining (potentially nontrivial) elements in the group give us a guide for where to look to prove the existence of a nontrivial element of the class group. While Schoof only used his method on real cyclotomic fields [10], Kucuksakalli generalized this method [5] to ray class fields over imaginary quadratics of class number 1. These methods, however, carry over in a straightforward way to any cyclic ray class field of an imaginary quadratic as long as we have a unit whose Galois conjugates generate a finite index subgroup.

In particular, if E is the group of units and $\mathcal{E}$ is our above defined group of elliptic units, then let $B = E/\mathcal{E}$ and $R = (\mathbb{Z}/p\mathbb{Z})G$ where $G = Gal(K_{\mathfrak{p}}/K)$. We can see that $B[p]$ is an R-module in a natural way. That is to say, elements of G stabilize the group $\mathcal{E}$ by construction and p-torsion always can be acted upon by $\mathbb{Z}/p\mathbb{Z}$. Our goal is to probe whether this is a trivial module or not. If $B[p]$ has a non-trivial element then $p|[E : \mathcal{E}]$ and so $p|h_{K_{\mathfrak{p}}}$.

Definition. A finite ring R is Gorenstein if the module $R^{dual} = \hom_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$ is free of rank 1 over R.

It is simple to see that our R is finite Gorenstein. Finite Gorenstein rings have several useful properties (as proved in, for instance [10] or [1]). Most notable for us are the following:

Theorem 3.5.1. *Let R be a finite Gorenstein ring. Then the following hold:*

1. *Given an R-module A we have $A^{\perp} = \hom_R(A, R) \cong A^{dual}$ by the map $f \mapsto \chi \circ f$ where χ generates R^{dual}.*

2. *Any finite A is Jordan-Hölder equivalent to A^{dual}.*

3. *Given I, J ideals of R and a surjection $g : R/J \to I^{\perp}$ with the property that $Ann_R(J)$ annihilates R/I. Then g is an isomorphism.*

Thanks to Theorem 3.1.3 we know that $\mathcal{E}$ is a free R-module generated by ϵ. Because R is a finite Gorenstein ring, we have that $B[p]$ is Jordan-Hölder equivalent to $B[p]^{\perp} = \hom_R(B[p], R)$. Among other things, this implies they are the same size. In Schoof's original method (which concerns itself with $\mathbb{Q}_{(p)}$), he uses an identity on $B[p]^{\perp}$ to demonstrate it is isomorphic to I, the augmentation ideal of R quotiented out by the ideal generated by the group ring elements that correspond to unramified prime ideals in $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. Kucuksakalli shows in Theorem 4.11 of [5] that this same process works for $K_{\mathfrak{p}}(\zeta_p)/K$. We present a simplified version below:

Theorem 3.5.2 (Kucuksakalli)**.** *Let $I = \langle \sigma_{\mathfrak{q}} - 1 \rangle$ denote the augmentation ideal of the group ring R. There is a natural isomorphism of R modules*

$$B[p]^{\perp} \cong I / \langle F_{\mathcal{R}}(\sigma_{\mathfrak{q}}) : \mathcal{R} \in \mathcal{S} \rangle,$$

where $\mathcal{S}$ is the set of degree-1 unramified prime ideals in $K_{\mathfrak{p}}(\zeta_p)/K$ and the group ring elements $F_{\mathcal{R}}(\sigma_{\mathfrak{q}})$ are defined by

$$F_{\mathcal{R}}(\epsilon) = \sum_{j=0}^{p-1} c_j \sigma_{\mathfrak{q}}^j,$$

where

$$(\epsilon^{\sigma^j})^{\frac{r-1}{p}} \equiv \zeta_p^{c_j} \bmod \mathcal{R},$$

and ϵ generates the elliptic units.

Our goal therefore, is to find these group ring elements $F_{\mathcal{R}}$. To do this, we need to simultaneously see how the Galois action effects both the pth roots of unity and our units ϵ. Over $\mathbb{Q}$ Schoof is able to use algebraic properties of the cyclotomic units that we lack. Instead, Kucuksakalli embeds $\mathcal{O}_{K_{\mathfrak{p}}(\zeta_p)}$ into $\mathbb{Z}_r$ where $r = |N_{K_{\mathfrak{p}}(\zeta_p)/K}(\mathcal{R})|^2$.

Given an embedding of $\mathcal{O}_{K_{\mathfrak{p}}(\zeta_p)}$ into $\mathbb{Z}_r$ there is an obvious homomorphism $\psi : \mathcal{O}_{K_{\mathfrak{p}}(\zeta_p)} \to \mathbb{F}_r$. That is, given $x = \sum_{j=0}^{\infty} x_j r^j$ then $\psi(x) = x_0 \bmod r$. The kernel of this homomorphism must be a prime ideal lying above r (since quotienting by the kernel yields a field) which we will call $\mathcal{R}$. Thus, by selecting an embedding we immediately select a degree-1 prime which is "easy" to compute with. We have found an $\mathcal{R}$ for which computations $\bmod \mathcal{R}$ are actually computations $\bmod r$ in the r-adics.

In order to ease the notational confusion of having polynomials in values that are usually considered known, we will denote $F_{\mathcal{R}}$ as polynomials in X (instead of σ) for the remainder of this section.

The first step is to find some $\mathcal{R}$'s, which really reduces to finding r's.

We need $r \equiv 1 \bmod p$ so the roots of unity are in $\mathbb{Z}_r$, which means we perform Algorithm 3.4.1 with the slight change that we skip step 6 so that we only produce r satisfying the congruence. This causes us to take slightly longer than the basic algorithm (since the r's are bigger they are less likely to be prime).

Given this r, we raise ϵ to $(r-1)/p$, and then we observe which root of unity it is congruent to $\bmod r$. This is repeated for every conjugate, yielding all the coefficients of $f_{\mathcal{R}}$.

Because r is typically much larger than p^2, we are able to do all our computation mod r. That is, $f_\epsilon(x)(x^p - 1)$ is typically square-free mod r so there is no ambiguity in our computation. We take a root of $x^p - 1 \bmod r$ and call it a. We take each ϵ^{σ^i}, raise it to the $\frac{r-1}{p}$ power and see which power of a it is. As there are only p powers, doing this by exhaustion[2] is much less work than embedding into $\mathbb{Z}_r$.

Algorithm 3.5.3. Computing $F_{\mathcal{R}}$ for some $\mathcal{R} \in K_{\mathfrak{p}}(\zeta_p)$ above r.

1. Find $a \neq 1$ such that $a^p \equiv 1 \bmod r$
2. Set $j = 0$ and initialize $F_{\mathcal{R}} = 0$.
3. Take $\epsilon^{\sigma_{\mathfrak{q}}^j} \equiv n \bmod r$ as computed by section 3.4
4. Compute $b = n^{\frac{r-1}{p}} \bmod r$
5. Take the discrete log of b (which is a pth root of unity) with respect to a which generates them, calling this c.
6. Add cX^j to $F_{\mathcal{R}}$, and if $j < p-1$, increment j and go to step 3.

This process involved two arbitrary choices: which root of $f_\epsilon(x)$ you declare is ϵ (from section 3.4) and which root of $x^p - 1$ you declare is a. As a result, whatever element of the ideal you get is only unique up to multiplication by X^j (if the root you call ϵ used to be called ϵ^{σ^j}) and multiplication by a scalar k (if the root called a used to be called a^k). Since both non-zero scalars and powers of X are units in R, the ideal $F_{\mathcal{R}}$ generates is independent of these choices.

We are trying to find the ideal generated by these $F_{\mathcal{R}}(X)$, so we will employ the above algorithm for many different r. Moreover, when we get an $F_{\mathcal{R}}(X)$ we want to figure out how it limits what could be in the ideal.

[2] Although we did it using the PARI command znlog($\epsilon^{\frac{r-1}{p}\sigma_{\mathfrak{q}}^j}$,$a$,[$p$,Mat([$p$,1])]) which is faster for larger p

Consider a single polynomial in our ideal $F_{\mathcal{R}}(X) = \sum_{j=1}^{p-1} c_j X^j$ defined by

$$\epsilon^{\frac{r-1}{p}\sigma^j} \equiv \zeta_p^{c_j} (\text{mod} \mathcal{R}).$$

We appeal to the following lemma concerning what generates our ideal.

Lemma 3.5.4. *Fix $\mathcal{R}$ and take $\mathcal{I} = \langle F_{\mathcal{R}}(X) \rangle$, and F the lowest degree lift of $F_{\mathcal{R}}$ to $\mathbb{F}_p[x]$. If g is the product of all linear polynomials dividing F, then $\mathcal{I} = \langle g \bmod X^{p-1} - 1 \rangle$.*

Proof. Since $g \cdot (F/g) \bmod X^{p-1} - 1 = F_{\mathcal{R}}$, clearly $\mathcal{I} \subset \langle g \bmod X^{p-1} - 1 \rangle$.

Notice that $g | (X^{p-1} - 1)$ since $X^{p-1} - 1$ is divisible by every linear polynomial. On the other hand, F and $X^{p-1} - 1$ can share no other factors since $X^{p-1} - 1$ is not divisible by any irreducible polynomials of degree > 1. Thus, there exists $a, b \in \mathbb{F}_p[x]$ with $aF + b(X^{p-1} - 1) = g$. And so $aF_{\mathcal{R}} = g \bmod X^{p-1} - 1 \in \langle F_{\mathcal{R}}(X) \rangle$. □

We are trying to get a handle on the ideal generated by all the $F_{\mathcal{R}}$. So, we compute several $F_{\mathcal{R}}$ for different r, look at common zeroes among them, and conclude the ideal generated by all $F_{\mathcal{R}}$ must contain the ideal generated by the product of these common linear divisors.

Naively, if we believe $F_{\mathcal{R}}$ is a random element of our ring, then it would have a $1/p$ chance of being divisible by a particular linear term not in our ideal. That is, $F_{\mathcal{R}}(j)$ has a $1/p$ chance of being zero, and is independent of the other terms j' unless the ideal forces it to be 0. As such, if our ideal were the whole ring, a single $F_{\mathcal{R}}(X)$ would be expected to have $(p-1)/p$ many zeroes, two polynomials would be expected to share $(p-1)/p^2$ many zeroes and more generally, we expect

$(p-1)/p^k$ shared zeroes from k polynomials with the odds of observing none being $(1-\frac{1}{p^k})^{p-1} \approx 1-\frac{p-1}{p^k}$. In other words, observing three $F_{\mathcal{R}}$ makes the odds of thinking there is a nontrivial ideal when there is not (a Type 1 error) less than one in a hundred (heuristically); we did it for a least 10 primes (or until the gcd was $X-1$ and so we knew the $F_{\mathcal{R}}$ generated the entire augmentation ideal I).

If there is a common factor g amongst the $F_{\mathcal{R}}$ then it is possible that

$$B[p]^{\perp} \cong I/\langle g \rangle.$$

Since $X-1$ generates I and $F_{\mathcal{R}} \in I$, it is always in the ideal; we will only obtain a degree p element if there is another linear factor.

3.6 Following the Trail of Bread Crumbs

Once we have a putative non-trivial element of the ring $B[p]^{\perp}$, we can use this to track down a proof. Since we are asserting there is a non-trivial element of a group, we must find said element. In this case, the group is units modulo the elliptic units, so we must find an elliptic unit which has a pth root in the field which is not an elliptic unit. Such a root would then be in the non-trivial coset.

Our strategy is to take a potential non-trivial element of $B[p]^{\perp}$, then lift this to $g(\sigma) \in \mathbb{Z}[Gal(K_{\mathfrak{p}}/K)]$.

The lift is quite simple, since $B[p]^{\perp} = I/\langle F_{\mathcal{R}} : \mathcal{S}\rangle$ if $\langle F_{\mathcal{R}} : \mathcal{S}\rangle = \langle F \rangle$ then, going back through the isomorphisms we get

$$\tilde{g}(\sigma_{\mathfrak{q}}) = \prod_{F(j)\neq 0} (\sigma_{\mathfrak{q}} - j) \in B[p]^{\perp}.$$

This in turn implies that $\epsilon^{g(\sigma_{\mathfrak{q}})}$ is a nontrivial element of $B[p]$ where $g(\sigma_{\mathfrak{q}})$ is any lift of $\tilde{g}$ from R to $\mathbb{Z}G$. For ease of computation, every coefficient of g will lie between $-(p-1)/2$ and $(p-1)/2$.

We apply this element to a generator of the elliptic units (embedded in $\mathbb{C}$), getting $\eta = \epsilon^{g(\sigma_{\mathfrak{q}})}$ and its Galois conjugates $\epsilon^{\sigma_{\mathfrak{q}}^j g(\sigma_{\mathfrak{q}})}$. It bears thinking for a moment how to do this:

Algorithm 3.6.1. Computing $\epsilon^{\sigma_{\mathfrak{q}}^j g(\sigma_{\mathfrak{q}})}$ given ϵ and its conjugates

1. Use Algorithm 3.3.5 to generate the list $(\epsilon, \epsilon^{\sigma_{\mathfrak{q}}}, \epsilon^{\sigma_{\mathfrak{q}}^2}, ...)$
2. Defining $\eta = \epsilon^{\sigma_{\mathfrak{q}}^j g(\sigma_{\mathfrak{q}})}$, set
$$\eta^{\sigma_{\mathfrak{q}}^j} = \prod_{k=0}^{p-2} (\epsilon^{\sigma_{\mathfrak{q}}^k})^{\mathit{coefficient}_{k-j \bmod p-1}(g(X))}$$
3. Return the list $(\eta, \eta^{\sigma_{\mathfrak{q}}}, \eta^{\sigma_{\mathfrak{q}}^2}, ...)$.

At this point we should check that these η conjugates form a finite index subgroup of the unit group to verify they are not lying in a subfield. If they do lie in a subfield, then we can change our arguments below slightly to take place in said subfield of $K_{\mathfrak{p}}$, but this never happened in practice.

We interpolate all the conjugates of η to get the minimal polynomial $f_\eta(x) \in K[x]$.

Our element η is obviously in the group of elliptic units, but since $g(\sigma)$ is not divisible by p by construction, and the elliptic units are freely generated by ϵ, we know the pth roots of the roots of η are definitely not elliptic. What remains is to verify that there is some root $\eta^{1/p} \in K_{\mathfrak{p}}$.

We will try to show $\eta^{1/p} \in K_{\mathfrak{p}}$ by constructing the minimal polynomial of $\eta^{1/p}$. If $f_\eta(x^p)$ factors over $K[x]$ and one of the factors f' is degree $p-1$, then we know the roots of f' are in $K_{\mathfrak{p}}$ by the following lemma:

Lemma 3.6.2. *Take $f \in K[x]$ irreducible with one root of f generating its splitting field. Take $g, h \in K[x]$ so that $g | f(h(x))$ with g irreducible and of the same degree as f. Then the roots of g lie in the same field as the roots of f.*

Proof. Take α so that $g(\alpha) = 0$. Then $h(\alpha)$ is a zero of f and so the splitting field of f is contained in $K(\alpha)$. But as the degree of f is the degree of g, they are the same field. $\square$

Given that the coefficients of $f_\eta(x)$ are very large, often with absolute value over 10^{1000}, factoring $f_\eta(x^p)$ over $K[x]$ is not a trivial task. One can take the norm of the polynomial down to $\mathbb{Z}[x]$, factor there, then if there are factors of degree $2(p-1)$, take the gcd of those factors with $f_\eta(x)$ (to get back to $K[x]$) and verify it is degree $p-1$. The issue with this method is that the algorithms for factoring polynomials in computer algebra packages require a large amount of memory. The polynomial itself is in the megabytes.

One might ask why we didn't take the pth roots of η^{σ^j} directly and save the polynomial factoring step. The issue is that there are p many pth roots for each element, and, because $\zeta_p \notin K_{\mathfrak{p}}$, at most one of these roots lies in $K_{\mathfrak{p}}$. Our only reasonable test for membership in $K_{\mathfrak{p}}$ involves computing the minimal polynomial, and so we would have to correctly guess the pth root of all $p-1$ units at once, a $p^{-(p-1)}$ event, or infeasible if $p > 11$.

Kucuksakalli [5] has a method for finding unique pth roots in a field which uses memory proportional to the amount required to store the polynomial, and so is preferable to factoring for p larger than, say, 50.

He notes that if $r \neq 1(\text{mod} p)$ then unique pth roots can be taken in $\mathbb{Z}_r$. So, one merely finds an r such that r completely splits in $K_\mathfrak{p}$, implying $\mathcal{O}_{K_\mathfrak{p}} \subset \mathbb{Z}_r$ and one can take roots in $\mathcal{O}_{K_\mathfrak{p}}$. In this setup, we embed ϵ and its conjugates into $\mathbb{Z}_r$ as in the previous section by embedding its minimal polynomial, as well as the polynomials that let us define the Galois action.[3] We then directly compute the $\epsilon^{\sigma^j \frac{g(\sigma)}{p}}$ and get their minimal polynomial $f_{\eta^{1/p}}(x)$ over $\mathbb{Z}_r[x]$. If this is actually the minimal polynomial of a unit in $K_\mathfrak{p}$ then the polynomial $f_{\eta^{1/p}}(x)$ lies in $K[x]$.

Finally, we lift $f_{\eta^{1/p}}(x)$ up to $(\mathbb{Z} \oplus \omega\mathbb{Z})[x]$, as described below. There is a little subtlety to the lifting. Kucuksakalli applied the PARI command algdep() to each coefficient, which uses the LLL algorithm to find a polynomial of a stated degree with "small" coefficients that evaluates to zero at the input (a putative minimal polynomial). One can then factor the polynomial one gets out of algdep() and verify it splits over K. This leaves one with two roots that we could lift the coefficient to. To be consistent, we should write the roots as $a + b\omega$ and $a + b\bar{\omega}$. We still know which embedding of ω into $\mathbb{Z}_r$ we used, so we verify which of the two roots maps to our coefficient under this embedding. Another subtlety to this is that algdep() as coded into PARI does not know we are lifting to a polynomial whose leading coefficient is 1 (see Appendix). As such, it is using a 3-dimensional lattice, when

[3] One interesting new wrinkle is that $\mathcal{O}_{K_\mathfrak{p}}$ can be embedded, but typically not $\mathcal{O}_{K_{\bar{\mathfrak{p}}}}$. This means that one putative embedding of $f_\epsilon \in \mathbb{Z}_r[x]$ will split (the actual embedding) and the other won't (the embedding to $\bar{f}_\epsilon$).

really a 2-dimensional lattice would do, slowing down the computation substantially, and in practice requiring 50% more precision to our numbers (vastly slowing down the process).

Algorithm 3.6.3. Determining if $f(x) \in \mathbb{Z}_r[x]$ likely lies in $\mathcal{O}_K[x]$ and finding the most likely polynomial.

1. Take $f(x) \in \mathbb{Z}_r[x]$ to $O(r^k)$ precision. Take $f_i \in \mathbb{Z}_r$ its ith coefficient.

2. Set $\gamma \in \mathbb{Z}_r$ as your favorite root of $x^2 - d$ to $O(r^k)$ precision.

3. Set $i = 1$, $f_{real}(x) = 0$ and $f_{imag}(x) = 0$.

4. Find a small polynomial $g_i(x) = a_i x^2 + b_i x + c_i \in \mathbb{Z}[x]$ which f_i is almost a root of (see Appendix for details).

5. If $a_i = 0$ verify $b_i = \pm 1$ and $f_i = -b_i c_i + O(r^k)$. If yes, set $f_{real} + = -b_i c_i x^i$ (where += means set the left-hand side to its current value plus the right-hand side) and go to step 4 with $i+ = 1$, otherwise $f \notin \mathcal{O}_K[x]$.

6. Verify $a_i | b_i, c_i$ and $(b_i^2 - 4a_i c_i)/d$ is a square. If not, return $f \notin \mathcal{O}_K[x]$.

7. If

   $$f_i = \frac{-b_i \pm \sqrt{(b_i^2 - 4a_i c_i)/d}\gamma}{2a_i} + O(r^k)$$

   then $f_{real} + = \frac{-b_i}{2a_i} x^i$ and $f_{imag} + = \pm \frac{\sqrt{(b_i^2 - 4a_i c_i)/d}}{2a_i} x^i$ and go to step 4 with $i+ = 1$, otherwise $f \notin \mathcal{O}_K[x]$.

8. If i =degree(f) then if $d \equiv 1 \bmod 4$ set $f_{imag} = f_{imag}/2$ and $f_{real} - = f_{imag}$. If $f_{real}, f_{imag} \in \mathbb{Z}[x]$ and $f_{real} + \gamma f_{imag} = f(x)$ up to $O(r^k)$ we are done, otherwise $f \notin \mathcal{O}_K[x]$.

A theoretical (though not practical) weakness of this r-adic embedding method is that if the lifting to $\mathcal{O}_K[x]$ fails, we do not know whether it is due to a lack of r-adic precision or because $f_{\eta^{1/p}}(x) \notin \mathcal{O}_K[x]$; the class number may not really be divisible by p and we will never find a polynomial of the sort we want. This is not a practical weakness since Schoof's method, while probabilistic, is heuristically giving an astronomically small chance of being wrong, so if $f_{\eta^{1/p}}$ doesn't lift one can assume one has not used enough precision. Second, given the size of the elliptic units over $\mathbb{C}$ one can come up with an upper bound on the minimal amount of precision needed if one wanted to prove one was using enough precision. In our work, we never encountered a putative $f_{\eta^{1/p}}$ which didn't lift.

Upon lifting $f_{\eta^{1/p}}(x)$ up to $(\mathbb{Z} \oplus \omega\mathbb{Z})[x]$ we can verify that $f_\eta(x^p) \bmod f_{\eta^{1/p}}(x) = 0$ and invoke Lemma 3.6.2 to prove the lifted $f_{\eta^{1/p}}$ was in fact the correct polynomial.[4] Note, we always know that f_η has the correct value since it was computed from ϵ and its conjugates directly.

Algorithm 3.6.4. Verifying $f|g$ when $f, g \in (\mathbb{Z} \oplus \omega\mathbb{Z})[x]$.

1. Take $d_f = f_{real} + \omega f_{imag}$ and $d_g = g_{real} + \omega g_{imag}$.

2. While degree of $f = a >$ degree of $g = b$, let $c = n + m\omega$ be the leading

[4] One might claim that the ability to find such a lift is ample heuristic proof that it is true as the likelihood of algdep() lifting even a single coefficient to K that doesn't belong there is on the order of $10^{-precision}$. If the pth root isn't in $\mathcal{O}_K$ it must be in an extension, so at least one of the coefficients doesn't live in K.

coefficient of f and

$$f_{real} - = \begin{cases} x^{d_f - d_g}(ng_{real} + m\frac{d-1}{4}g_{imag}) & \text{if } d \equiv 1 \bmod 4 \\ x^{d_f - d_g}(ng_{real} + mdg_{imag}) & \text{otherwise} \end{cases}$$

$$f_{imag} - = \begin{cases} x^{d_f - d_g}m(g_{real} + g_{imag}) & \text{if } d \equiv 1 \bmod 4 \\ x^{d_f - d_g}mg_{real} & \text{otherwise} \end{cases}$$

3. $f \bmod g = f_{real} + f_{imag}\omega$ at the end.

While this method takes some time (we do it as above so we do not need to worry about precision issues), it is very little compared with the rest of the Kucuksakalli/Schoof process and it is very elegant (requiring all of 4 lines of code). But it appears to have not been used in [5], who relies on an argument using Chebotarev's density theorem and class field theory to show his putative minimal polynomial gives the same field extension as $K_{\mathfrak{p}}$. Kucuksakalli provides few details of his calculations so we are unable to reproduce them. However, we have independently verified that his highly irregular prime $\mathfrak{p} = (13 - 2\omega) \subset \mathbb{Z}[\frac{1+\sqrt{-163}}{2}]$ is highly irregular using Algorithm 3.6.4.

Chapter 4: Highly Irregular Primes

We used the above methods to see whether any class numbers were divisible by the prime conductor of the field. We exhausted over every imaginary quadratic field of class number 2 and every prime ≤ 307 which split and gave a cyclic ray class group for a given field. This came out to 462 many (pairs of conjugate) ray class fields (83 of 545 primes did not have cyclic class groups). This yielded the following result:

Theorem 4.0.5. *There are exactly 5 pairs of ray class fields $K_{\mathfrak{p}}/K$ where K is an imaginary quadratic field of class number 2 and $K_{\mathfrak{p}}$ has a degree 1 prime conductor $\mathfrak{p}$ with $Norm(\mathfrak{p}) \leq 307$ and for which $p|h_{K_{\mathfrak{p}}}$. These are given by*

Quadratic Field	p
$\mathbb{Q}(\sqrt{-267})$	*41*
$\mathbb{Q}(\sqrt{-10})$	*103*
$\mathbb{Q}(\sqrt{-235})$	*113*
$\mathbb{Q}(\sqrt{-22})$	*211*
$\mathbb{Q}(\sqrt{-427})$	*239*

While we may be able to show p larger than 307 are not highly irregular using

Schoof, our methods would not work on any that are. This is because the minimal polynomial of the unit which would correspond to a class group element of order p, when not embedded into a larger field, has a largest term whose size is expected to grow cubically in p. We need enough precision to be able to find the nearest element of $\mathcal{O}_K$ for each coefficient of a minimal polynomial. The $p = 239$ example required over 15,000 digits of precision to do Schoof's method alone. Moreover, completing the proof necessitates computing a polynomial f_η which typically requires precision quartic in p. The largest coefficient of f_η required over 108,000 digits of precision for the $p = 239$ case. This was actually too large for PARI's native root finding algorithm to be run on a machine with a 32-bit RAM architecture. Instead we ran this portion of the computation on compute1, a 48 GB RAM machine with a 64-bit architecture at the University of Maryland running PARI version 4.7.1. The root-finding took somewhat under 6 hours and appeared to use around 5 GB of RAM.

Given the number of observed fields, we can compare this with the "expected" number from some heuristic. In section 8.3 of [13] Washington argues that the number of highly irregular primes in $\mathbb{Q}$ less than n grows as $\log(\log(n))/2$, and therefore if a counterexample to Vandiver's Conjecture existed, we would not necessarily expect it to appear at the sizes we have heretofore looked at. These results provide more evidence for these arguments.

Washington argues that we would expect the numerator of a Bernoulli number to be random mod p, and that as a result it is a $1/p$ chance that the numerator of the jth Bernoulli number is divisible by p. We know that the class number of

$\mathbb{Q}(\zeta_p + \bar{\zeta}_p)$ is divisible by p only if the jth Bernoulli number's numerator is divisible by p for some j less than $p-1$ (with each number corresponding to an eigenspace of the class group). Washington further argues that if the numerator of the jth Bernoulli number is divisible by p, then and only then should we assume there is a 1 in p chance that the portion of the class group corresponding to said Bernoulli number has a 1 in p chance of being divisible by p. Since all odd-indexed Bernoulli numbers are 0, this works out to a $\frac{p-3}{2p^2} \approx \frac{1}{2p}$ probability that a given prime is highly irregular.[1] Invoking the prime number theorem, the expected number of counterexamples to Vandiver for $p \leq n$ is $\log(\log(n))/2$. Vandiver's conjecture is only verified for $p \leq 163,577,356$ (see [2]). By the Bernoulli number argument, we expect around 1.0 primes to be highly irregular (obtained from summing over all $p < 163,577,356$ and not the prime number theorem approximation). Assuming the above argument is valid, the likelihood we still observed zero counterexamples so far is close to $e^{-1.0} \approx 35\%$, which is reasonable.

We adapt this argument to our present case. For $h_K = 1$ there are Hurwitz numbers associated to each imaginary quadratic field defined as

$$H_j(\mathcal{O}_K) = \sum_{z \in \mathcal{O}_K/\{0\}} \frac{1}{z^j} \tag{4.1}$$

for $j \in \mathbb{Z}^+$. It was proven by Robert [7] that if p divides the class number of $K_\mathfrak{p}$ then there exists a nonzero Hurwitz number whose numerator is divisible by p and whose index is less than $p-1$, with each numerator corresponding to a different

[1] Actually, if each Bernoulli number is thought of as independent (which is reasonable as each corresponds to a different part of the class group) then $\frac{p-3}{2p^2}$ is the expected number of parts of the class group divisible by p and $1-(1-p^{-2})^{\frac{p-3}{2}}$ is the probability the class number is divisible by p. These are nearly the same value, especially as p grows, so we will not give more than 2 significant digits for any number in this section

eigenspace of the class group. Hurwitz numbers are zero for any index j not divisible by the W_K, the number of roots of unity in the field[2]. So following the argument as before (when $W_K = 2$ and slightly altered when not), if the jth Hurwitz number has probability $1/p$ of being divisible by p, we might expect a $(p-3)/2$ in p^2 chance[3] that the class number of $K_{\mathfrak{p}}$ is divisible by p. So, overall, there would be a $\frac{p-3}{2p^2}$ chance that a particular $h_{K_{\mathfrak{p}}}$ is divisible by p. On the other hand, $p|h_{K_{\mathfrak{p}}}$ if and only if $p|h_{K_{\bar{\mathfrak{p}}}}$ (that is, these events are perfectly correlated).

But, there is no reason why this argument should be limited to the case where Hurwitz or Bernoulli numbers have historically been defined. The argument is essentially that there is a $1/p^2$ chance that a non-trivial eigenspace of the class group of $K_{\mathfrak{p}}$ is divisible by p. We can apply this logic to any $K_{\mathfrak{p}}$.

We only checked those $\mathfrak{p}$ for which the ray class group was cyclic, of which there were 462. Computing the expected number of counterexamples we get

$$\sum_{\mathfrak{p}\text{ that we checked}} \frac{p-3}{2p^2} \approx 3.0 \tag{4.2}$$

As there were 462 theoretically independent Bernoulli trials (of varying probabilities of success) that went into the above summation, it is reasonable to approximate this as a Poisson distribution. Given this, there is an 10% chance that there are 5 highly irregular primes (and 19% chance of at least 5), so this is just as we expect.

[2] If $\mathcal{O}_K$ contains the kth roots of unity, then $\zeta_k \mathcal{O}_K = \mathcal{O}_K$ so

$$\sum_{z\in\mathcal{O}_K/\{0\}} z^{-j} = \sum_{z\in\mathcal{O}_K/\{0\}} \left(\zeta_k^\ell z\right)^{-j}.$$

Thus, $kH_j(\mathcal{O}_K) = \sum_{\ell=1}^{k} \zeta_k^{j\ell} H_j(\mathcal{O}_K)$ which is clearly zero unless $k|j$.

[3] see earlier footnote

Moreover, we can include Kucuksakalli's experiments in out data: he performed a similar computation for all degree 1 primes lying above $p < 700$ for quadratic imaginary fields of class number 1. He found a single pair of highly irregular primes ($\mathfrak{p}|307$ in $\mathbb{Q}(\sqrt{-163})$) out of the 537 primes he checked. We compute that 1.7 is the expected number of pairs he would have found.[4] Adding his results to our own gives an expected number of highly irregular primes equal to 4.7 of the 999 primes checked, while 6 were found. This gives a probability of 14% that there were exactly 6 (34% that there was more than 5), which is an even more likely. This leads to the following conjecture:

Conjecture 4.0.6. *Take K equal to $\mathbb{Q}$ or an imaginary quadratic field. Let $D_K(n)$ be the number of highly irregular primes $\mathfrak{p} \in K$ with $Norm(\mathfrak{p}) < n$. Then*

$$\lim_{n\to\infty} \frac{D_K(n)}{\log(\log(n))} = h_K \frac{[K:\mathbb{Q}]}{W_K}$$

Given that we know $D_{\mathbb{Q}}(163, 577, 356) = 0$, the conjecture puts it at roughly even odds that there is a prime of at most 32 digits that violates Vandiver's conjecture and 99% chance of a prime with at most 80,000 digits. Both are outside the realm of possibility for exhaustion for the foreseeable future.

[4] Kucuksakalli's expected number of highly irregular primes is much lower than ours because in class number 1, p can only split into a principal ideal whose generator has a norm of p. As a result, p doesn't split if $p < |\omega|^2$. But these are the exact p that give the majority of the weight to our expected value. This is the reason we haven't found highly irregular rational primes: there are many fewer small primes for it to occur at than in quadratic fields. Further, because $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$ have 4 and 6 roots of unity respectively, the ray class fields in those cases have fewer non-zero Hurwitz numbers.

Chapter 5: Constructing Unramified Abelian Extensions of Ray Class Fields

We numerically explore some consequences of when Vandiver fails. One classic result is that when Vandiver's conjecture holds for an irregular prime p, we can construct an unramified abelian extension of $\mathbb{Q}_{(\zeta_p)} = \mathbb{Q}^+(\zeta_p)$ by adjoining the pth root of a cyclotomic unit in the field. Similarly, in a ray class field, when the generalization of Vandiver holds and a certain part of the class number of $K_\mathfrak{p}(\zeta_p)$ is a multiple of p, one can construct a unramified abelian extension of $K_\mathfrak{p}(\zeta_p) = K_{(p)}$ by adjoining the pth root of an elliptic unit.

However, one might ask what happens for highly irregular primes? For reasons we describe below, one might assume that taking the pth root of the unit which causes the counterexample would give an abelian extension; however, we show that for none of the counterexamples does this generate such an extension.

5.1 Searching for Singular Primary Elements

From the techniques of previous sections, we have identified a non-elliptic unit whose pth power is elliptic. For this section, we will call said unit α.

We will follow exercise 9.3 of [13] in constructing unramified abelian extensions of a field by taking the roots of singular primary elements. Let $\varpi = 1 - \zeta_p$, an ideal lying above p. We say an element is *singular primary* if $x^p - \alpha \bmod \varpi^p$ has a root in our field and $(\alpha) = \mathcal{I}^p$ for some ideal. Since α is a unit in field (and so $(\alpha)^p = (\alpha)$) the later is always true, though verifying the former takes a little more work. However, as [13] points out, if α is singular primary after being embedded into a field with the pth roots of unity, then $\alpha^{1/p}$ root will generate an unramified extension. A lemma will help us find a suitable field:

Lemma 5.1.1. *If p does not ramify in K then $\zeta_p \in K_{(p)}$ and further $K_{\mathfrak{p}}(\zeta_p) = K_{(p)}$.*

Proof. The prime (p) is the only prime of $\mathbb{Q}$ that ramifies in $\mathbb{Q}(\zeta_p)$ and so the only ideals that ramify in $K(\zeta_p)/K$ are $\mathfrak{p}$ and $\bar{\mathfrak{p}}$. Thus, since $K(\zeta_p)$ is an abelian extension, by class field theory there exists j with $K(\zeta_p) \subset K_{(p)^j}$. On the other hand, we know for $k > 0$

$$[Gal(K_{(p)^{k+1}}/K) : Gal(K_{(p)^k}/K)] = p^2.$$

Since $Gal(K(\zeta_p)/K)$ has an element of order $p-1$ (the one sending ζ_p to ζ_p^2) we know $K(\zeta_p) \subset K_{(p)^{k+1}}$ only if $K(\zeta_p) \subset K_{(p)^k}$. Thus $K(\zeta_p) \subset K_{(p)}$.

The field $K_{\mathfrak{p}}/K$ does not ramify at $\bar{\mathfrak{p}}$ while in $K(\zeta_p)/K$ the prime has ramification index $p-1$ (which equals the degree of the extension). Thus $K_{\mathfrak{p}} \cap K(\zeta_p) = K$ and we see their compositum must have degree equal to the product of their degrees, $(p-1)^2$. On the other hand $K_{(p)}/K$ is a degree $(p-1)^2$ extension, so we get $K_{\mathfrak{p}}(\zeta_p) = K_{(p)}$ as desired. □

It should be noted (and will be used in a subsequent section) that the above lemma actually works for any imaginary quadratic extension, not just those of class number 2, with the proof just involving the obvious modifications.

To check the existence of the pth root of α in $K_{(p)} = K_{\mathfrak{p}}(\zeta_p)$ we will employ the same method we have been using, embedding the elliptic units in an r-adic field where the ideal is easily defined. In this case, it will be $\mathbb{Z}_p$ which contains the ring[1] $\mathcal{O}_K$. Unfortunately, it cannot contain $K_{\mathfrak{p}}$ since p ramifies, but we shall see this is not necessary.

Without loss of generality, we can replace α with any power of itself not divisible by p. As a result, we replace α with $\alpha^{p^{p-1}-1}$. This operation puts α in the Sylow p-subgroup of $(\mathcal{O}_{K_{(p)}}/(\varpi)^p)^\times$ (which has exponent p) because every prime lying above p in $K_{(p)}$ has inertia degree dividing[2] $p-1$. Thus, either $x^p - \alpha \bmod \varpi^p$ has no roots or $\alpha = 1 \bmod \varpi^p$ (and its roots are all the pth roots of unity).

Now we are asking the question of whether we can tell if an element of $K_{(p)}$ is congruent to $1 \bmod \varpi^p$, and this only requires its minimal polynomial to be embedded in $\mathbb{Z}_p$. So, first we embed f_α into $\mathbb{Z}_p$ which can be done since the ring contains $\mathcal{O}_K$. However, we do not know the congruence of this α we have embedded. However, with f_α it is easy to compute f_{α^j} in time polynomial in the size of j. In fact we prove the following statement:

Theorem 5.1.2. *Given an element $\alpha \in L/M$ with minimal polynomial $f_\alpha \in \mathbb{Z}_r$ and a polynomial $g(x) \in \mathbb{Z}[x]$ there exists a algorithm for computing $f_{g(\alpha)}$ which is*

[1] Because K can be embedded two different ways, we will have to repeat all our computations twice in case we chose the "wrong" embedding

[2] The prime $\mathfrak{p}$ has ramification index $p-1$ in $K(\zeta_p)/K$ leaving it to have inertia at most $p-1$ in $K_{(p)}/K(\zeta_p)$. Similarly for $\bar{\mathfrak{p}}$.

polynomial in the degree of f, the number of terms of g, and the size of the degree of g.

Proof. In order to prove the theorem we will need to appeal to two identities by Newton relating two bases of the symmetric polynomials over n variables: the elementary symmetric polynomials e_k and the power sum polynomials s_k. We define the elementary symmetric polynomials as

$$e_k(x_1, ..., x_n) = \sum_{1 \le j_1 < j_2 < ... < j_k \le n} x_{j_1} x_{j_2} ... x_{j_k}$$

for $k \le n$ and 0 otherwise. We define the power sum polynomials as

$$s_k(x_1, ..., x_n) = \sum_{j=1}^{n} x_j^k$$

with $s_0 = 1$.

Both of these form a basis for the symmetric polynomials over n variables with the change of basis being given by (for $k > 0$)

$$s_k = (-1)^{k-1} k e_k + \sum_{j=1}^{k-1} (-1)^{j-1} e_j s_{k-j}$$

and

$$e_k = \frac{1}{k} \sum_{j=1}^{k-1} (-1)^{j-1} e_{k-j} s_j.$$

Because $f_\alpha = \prod_{\sigma \in Gal(L/M)} (x - \alpha^\sigma)$ the coefficients of f_α are the elementary symmetric polynomials evaluated at the Galois conjugates of α. Thus, by using the above change of basis, we are able to evaluate the s_k at the Galois conjugates of α.

However, given $s_k(\{\alpha^\sigma\})$ for $k < n$, we can easily compute this for n. This is because $f_\alpha(\alpha^\sigma) = 0$ so

$$\alpha^{n\sigma} = -\sum_{j=0}^{n-1} f_{\alpha_j}\alpha^{j\sigma}. \tag{5.1}$$

Summing the above equation over all the conjugates yields

$$\begin{aligned}\sum_{\sigma\in Gal(L/M)} \alpha^{n\sigma} &= -\sum_{\sigma\in Gal(L/M)}\sum_{j=0}^{n-1} f_{\alpha_j}\alpha^{j\sigma} \\ &= -\sum_{j=0}^{n-1} f_{\alpha_j}\sum_{\sigma\in Gal(L/M)}\alpha^{j\sigma} \\ = s_n(\{\alpha^{n\sigma}\}) &= -\sum_{j=0}^{n-1} f_{\alpha_j} p_n(\{\alpha^{n\sigma}\})\end{aligned}$$

In essence, α and its conjugates satisfy a linear recurrence relationship, and we will use this to quickly compute high powers of them. So, similar to the above calculation, we can easily compute $s_{2n}(\{\alpha^\sigma\})$. Given equation 5.1, we can square both sides and collect like terms among the n^2 coefficients to get

$$\alpha^{2n\sigma} = (\sum_{j=0}^{n-1} f_{\alpha_j}\alpha^{j\sigma})^2$$

which is $(x^n - f_\alpha(x))^2 \bmod f_\alpha(x)$ evaluated at $x = \alpha^\sigma$.

Then we sum both sides over all $\sigma \in Gal(L/M)$ to obtain

$$s_{2n}(\{\alpha^\sigma\}) = \sum_{j=0}^{n-1} s_j(\{\alpha^\sigma\})\text{coefficient}_j\left((x^n - f_\alpha(x))^2 \bmod f_\alpha(x)\right).$$

Any polynomial of α^σ we would like to compute is treated similarly:

$$\begin{aligned}&g(\alpha)^\sigma \\ &= g(\alpha^\sigma) = g(x) \bmod f_\alpha(x)|_{x=\alpha^\sigma} \\ \Rightarrow s_1(\{g(\alpha)^\sigma\}) &= \sum_{j=0}^{n-1} s_j(\{\alpha^\sigma\})\cdot\text{coefficient}_j\left(g(x) \bmod f_\alpha(x)\right).\end{aligned}$$

Every monomial $x^j \bmod f_\alpha(x)$ is easy to compute via square-and-multiply methods (with roughly n^2 scalar multiplies required for every polynomial square or multiply), so if $g(x)$ is the sum (or product) of relatively few easy to compute terms, finding $s_1(\{g(\alpha)^\sigma\})$ takes a number of multiplies in the coefficient ring which is polynomial in the degree and number of non-zero coefficients. Since $s_k(\{g(\alpha)^\sigma\}) = s_1(\{(g(\alpha)^k)^\sigma\})$, we can compute $s_k(\{g(\alpha)^\sigma\})$ for all $k < n$. At this point one changes the basis back to the elementary symmetric polynomials, and we have $e_k(\{g(\alpha)^\sigma\})$, the coefficients of $f_{g(\alpha)}$.

While this technique works with f_α embedded in any polynomial ring, embedding in a nonarchimedean ring like $\mathbb{Z}_r$ ensures the precision of $f_{g(\alpha)}$ is the same as we started with, and causes the algorithm to take polynomial time. For instance, if performed over $\mathbb{Z}$ one would expect the coefficient size to increase proportionally to the degree of g, and so the multiplication of these coefficients would take time at least proportionate to the degree of g and the computations would be at best polynomial time in the degree of g (instead of the size of the degree). $\square$

The theorem gives us the remarkable fact: although we struggled to get enough precision to initially compute α in section 3.6, often needing thousands of digits of precision in each calculation and going to great lengths in section 3.3 to compute ϵ instead of the ϵ^{W_k} that Stark uses, we are now able to compute α raised to a hundred digit number with no problem at all! The number is for instance, far too big to lift out of $\mathbb{Z}_p$ using Algorithm 3.6.4.

Since α lies in $K_\mathfrak{p}$, we know the prime above p in $K_\mathfrak{p}$ is ramified at most $p-1$

times, and thus α gets mapped to an element in the finite field of order p^{p-1} when $\mathcal{O}_{K_{\mathfrak{p}}}$ is modded out by said prime. With the above theorem in place we can use any f_α in the p-adics to compute a new polynomial $f_{\alpha^{p^{p-1}-1}}$ of the same precision, but its roots lie in the Sylow p-subgroup of $((O)_{K_{(p)}}/(\varpi)^p)^\times$. So, without loss of generality, we assume α lies in the Sylow p-subgroup. Given such a polynomial, we can easily construct $f_{\alpha-1}(x)$ (even without the theorem, it equals $f_\alpha(x+1)$). Our goal now is to show every root of $f_{\alpha-1}(x)$ simultaneously is (or is not) congruent to 0 mod ϖ^p. Since $(\varpi)^{p-1} = (p)$, the p-adic valuation of the roots is intimately tied to the ϖ-adic valuation.

We will show that σ (the Galois element that sends α to its conjugates) fixes the ideal (ϖ) and so every element of $K_{(p)}$ has the same p-adic valuation as its conjugates and in particular, all the roots of $f_{\alpha-1}$ must be equally divisible by ϖ. This occurs because σ must send ζ_p to ζ_p^j for some j, which means $\varpi^\sigma = 1 - \zeta_p^j$. But, this only differs from ϖ by the cyclotomic unit

$$\frac{1-\zeta_p^j}{1-\zeta_p} = \sum_{m=0}^{j-1} \zeta_p^m,$$

so σ fixes the ideal (ϖ). Since $(\varpi)^{p-1} = (p)$, the ϖ-adic valuation of a single conjugate must equal the p-adic valuation of the product of all $p-1$ conjugates. But the product is just the constant term of $f_{\alpha-1}$. If its valuation is at least p, then we know $\alpha \equiv 1 \bmod \varpi^p$ and α's pth roots generate the extension. If not, then $\alpha^{1/p}$ does generate a ramified extension of $K_{(p)}$.

For all 5 discovered highly irregular primes and for Kucuksakalli's highly irregular prime[3], the prime above 307 in $\mathbb{Q}(\sqrt{-163})$, this did not get the desired extension. In particular it always resulted in a valuations of 2 and $p-1$, one for each embedding of f_α into $\mathbb{Z}_p$. This leaves an open question of whether it is feasible to construct an unramified abelian extension of $K_{(p)}$, even when its existence is guaranteed.

5.2 Consequences due to α not being singular primary

The above calculations demonstrating that α is not singular primary actually allow us to conclude that a part of the class group of $K_{\mathfrak{p}}(\zeta_p)$ is cyclic for Kucuksakalli's highly irregular prime. We will make use of arguments very similar to those used in cyclotomic fields. This is interesting as in cyclotomic fields one typically uses Vandiver's conjecture to show that part of the class group of $\mathbb{Q}(\zeta_p)$ is cyclic. It is therefore unknown whether the class group of $\mathbb{Q}(\zeta_p)$ always has cyclic parts even if the conjecture fails. One would generally suspect that the class group is cyclic anyway due to the Cohen-Lenstra Heuristics (see, for instance [3]), but there is no proof. We will demonstrate that at least one known highly irregular prime has the corresponding effect in an imaginary quadratic field, suggesting that the heuristics should apply when Vandiver doesn't hold. In this, we follow very closely to Washington's arguments concerning the Reflection Theorems in chapter 10.2 of [13].

For the remainder of this subsection, we shall assume K is an imaginary quadratic field of class number k and p factors into unramified degree-1 primes

[3] We made the obvious modifications in the above for the degree-$(p-1)/2$ extension

and $p \nmid k$.

Let $L = K_{(p)} = K_{\mathfrak{p}}(\zeta_p)$. Lemma 5.1.1 will also apply in these circumstances with minimal changes to the proof. Let $G_1 = \mathrm{Gal}(K_{\mathfrak{p}}/K) \simeq \mathrm{Gal}(L/K(\zeta_p))$. Let $G_2 = \mathrm{Gal}(K(\zeta_p)/K) \simeq \mathrm{Gal}(L/K_{\mathfrak{p}})$. Because $K_{\mathfrak{p}} \cap K(\zeta_p) = K$ we have $\mathrm{Gal}(L/K) = G_1 \times G_2$. Let χ be a character of G_1 and let ψ generate the characters of G_2. Since $\psi^{p-1} = \chi^{p-1} = 1$ we can regard them as being mod$p$-valued. Let

$$\gamma_{\chi\psi^a} = \frac{1}{(p-1)^2} \sum_{(g_1,g_2)} \chi(g_1)\psi(g_2)^a g_1^{-1} g_2^{-1} \in \mathbb{F}[G_1 \times G_2].$$

If $\gamma_{\chi\psi^a}$ acts on $y \in {K_{\mathfrak{p}}}^{\times}/({K_{\mathfrak{p}}}^{\times})^p$ we have

$$\begin{aligned} \gamma_{\chi\psi^a}(y) =& \frac{1}{(p-1)^2} \sum_{g_1} \chi(g_1) \left(\sum_{g_2} \psi(g_2)^a \right) y \\ =& \begin{cases} \frac{1}{p-1} \sum_{g_1} \chi(g_1) g_1^{-1}(y) & \text{if } a = 1 \bmod p \\ \\ 1 & \text{if } a \neq 0 \bmod p. \end{cases} \end{aligned}$$

Let $h_\chi = \frac{1}{p-1} \sum_{g_1} \chi(g_1) g_1^{-1}(y) \in \mathbb{F}[G_1]$. The above says that $\gamma_{\chi\psi^a}$ restricts to h_χ on ${K_{\mathfrak{p}}}^{\times}$. Let $U = \mathcal{O}_L^{\times}$.

Lemma 5.2.1. *For all known highly irregular primes, $\gamma_\chi(U/U^p)$ has $\mathbb{F}_p$-dimension of at most 1.*

Proof. Take $u \in U$. We have

$$\begin{aligned} \gamma_\chi(u) &\equiv \frac{1}{(p-1)^2} \sum_{g_1} \chi(g_1) g_1^{-1} \sum_{g_2} g_2^{-1}(u) \\ &\equiv \sum_{g_1} \chi(g_1) g_1^{-1} \left(N_{L/K_{\mathfrak{p}}}(u) \right). \end{aligned}$$

If $v = N_{L/K_{\mathfrak{p}}}(u) \in \mathcal{O}_{K_{\mathfrak{p}}}^{\times}$ then $\gamma_{\chi}(u) \equiv h_{\chi}(v)^{-1} \bmod U^p$. Therefore we have a surjection

$$h_{\chi}\left(\mathcal{O}_{K_{\mathfrak{p}}}^{\times}/(\mathcal{O}_{K_{\mathfrak{p}}}^{\times})^p\right) \twoheadrightarrow \gamma_{\chi}(U/U^p).$$

Since $h_{\chi}\left(\mathcal{O}_{K_{\mathfrak{p}}}^{\times}/(\mathcal{O}_{K_{\mathfrak{p}}}^{\times})^p\right)$ has dimension ≤ 1 for all known highly irregular primes, this proves the lemma. □

Take $\alpha \in \gamma_{\chi}(U/U^p)$ and suppose it has been shown that $L(\alpha^{1/p})/L$ ramifies (as we did in the previous section for our highly irregular primes). Since $\dim_{\mathbb{F}_p} \gamma_{\chi}(U/U^p) \leq 1$ this implies no element of $\gamma_{\chi}(U/U^p)$ is a Kummer generator for a non-trivial unramified p-extension of L.

As in section 10.2 of [13] we define L' as the maximal unramified elementary p extension of L, and $H = \mathrm{Gal}(L'/L)$, and A the Sylow p-subgroup of the class group of L. One can show that $H \simeq A/A^p$ as $(G_1 \times G_2)$-modules, and there exists a subset B of $L^{\times}/(L^{\times})^p$ so that $L' = L(\sqrt[p]{B})$.

The Kummer pairing is a non-degenerate, bilinear pairing from $H \times B$ onto the pth roots of unity, μ_p. As in [13] there is also a $(G_1 \times G_2)$-linear map $\varphi : B \to A[p]$ that induces an exact sequence

$$\gamma_{\chi}(\ker \varphi) \to \gamma_{\chi} B \to \gamma A[p].$$

We know $\gamma_{\chi}(\ker \varphi)$ only contains 1 since it is contained in $\gamma_{\chi}(U/U^p) \cap B$ and by assumption $\gamma_{\chi}(U/U^p)$ has none of the Kummer generators. Thus $\gamma_{\chi} B$ is mapped injectively into $\gamma_{\chi} A[p]$ so that $|\gamma_{\chi} B| \leq |\gamma_{\chi} A[p]|$. Therefore

$$|\gamma_{\chi^{-1}\psi}(A/A^p)| = |\gamma_{\chi^{-1}\psi}(H)| = \gamma_{\chi} B| \leq |\gamma_{\chi} A[p]|. \tag{5.2}$$

Thus, if we show $L(\alpha^{1/p})/L$ ramifies for $\alpha \in \gamma_\chi(U/U^p)$ as we did in the previous section, then demonstrating $|\gamma_\chi A[p]| = p$ will allow us to conclude $\gamma_{\chi^{-1}\psi}A$ is cyclic. Kucuksakalli did this for $p = 307$ and $K = \mathbb{Q}(\sqrt{-163})$ and so we can conclude part of the class group is cyclic. Unlike Kucuksakalli we only performed enough of Schoof's algorithm to verify divisibility by p. With minor modifications one could verify this for the remaining 5 highly irregular primes and assuming the Cohen-Lenstra heuristics it is very likely they are also cyclic.

5.3 Directly Constructing Extensions of Ray Class Fields

One might try to directly construct $K_{(p)}$. If we could do this, we could look for singular primary elements here and hopefully construct the unramified abelian extension we were looking for in section 5.1. This ends up being technically possible but not practical. With $K = \mathbb{Q}(\sqrt{-11})$ we were able to construct $K_{(5)}$. Note that here $5 = (1+\omega)(2-\omega)$ and $h_K = 1$ so that if $\mathfrak{p} = (1+\omega)$ then $K_{(5)} = K_{\mathfrak{p}\bar{\mathfrak{p}}}$. In this case, $K_{(5)}$ is a degree $(5-1)^2/2 = 8$ extension of K and since (5) is fixed by complex conjugation, $K_{(5)}$ is Galois over $\mathbb{Q}$ (which was not the case for the $K_{\mathfrak{p}}$ in the previous sections). On the other hand, $K_{(5)}/\mathbb{Q}$ is not abelian.

We would like a K-basis for $K_{(p)}$. In previous sections, we had been generating a K-basis for $K_{\mathfrak{p}}$ using our elliptic units. However, there are several options for a finite index subgroup in $K_{(p)}$. We can try the units described by Ramachandra in [9]. We can go with a simplification of these by Stark in [11] which we used in previous sections. Last we can try to generalize a subgroup used by Agathocleous in [1] to compute in $\mathbb{Q}_{(p)(q)}$ when $(p,q)=1$.

What we find is that the specific unit group has a big effect on the amount of precision we need to find its generators, and that these effects do not appear to be completely consistent across different ray class fields. On the other hand, the Ramachandra units appear to always be much too large to use in practice.

Agathocleous in [1] used the subgroup of the units in $\mathbb{Q}_{(p)(q)} = \mathbb{Q}(\zeta_{pq})^+$ generated by units of the form

$$\zeta_{pq}^{-(p+q)}(1-\zeta_{pq}^{p+q})^2 \frac{\zeta_p^{-a/2}}{\zeta_p^{-1/2}} \frac{(1-\zeta_p^a)}{(1-\zeta_p)} \frac{\zeta_q^{-b/2}}{\zeta_q^{-1/2}} \frac{(1-\zeta_q^b)}{(1-\zeta_q)}.$$

These are products of the standard generators of the cyclotomic units of $\mathbb{Q}(\zeta_p)^+$ and $\mathbb{Q}(\zeta_q)^+$ multiplied by $\zeta_{pq}^{-(p+q)}(1-\zeta_{pq}^{p+q})^2$ (a value which is only a unit when $\mathbb{Q}(\zeta_{pq})^+$ is the ray class field over a conductor which is the product of two primes).

We similarly could construct a unit in $K_{(p)}$. Note that $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ are distinct primes whose product is (p). Thus our version of Agathocleous's units are the product of the generators of the elliptic units in $K_{\mathfrak{p}}$ and $K_{\bar{\mathfrak{p}}}$ along with $\phi_{(p)}(K)$ (which Stark showed is a unit when our ideal is the product of at least two distinct primes, and $p = \mathfrak{p}\bar{\mathfrak{p}}$). Writing this out we get

$$\phi_{(p)}(\mathcal{I}) \frac{\phi_{\mathfrak{p}}(\mathcal{I}^a)}{\phi_{\mathfrak{p}}(K)} \frac{\phi_{\bar{\mathfrak{p}}}(\mathcal{I}^b)}{\phi_{\bar{\mathfrak{p}}}(K)}.$$

For example, the polynomial we get from the Agathocleous-style units over

$K_{(5)}/\mathbb{Q}$ is

$$x^{16} + 23922414x^{14} + 60598212297x^{12} + 88210179093022x^{10} +$$

$$285548021874380x^8 - 35444893310522x^6 + 1205555306897x^4 + 418177286x^2 + 1.$$

By comparison, the minimal polynomial for the units obtained from Ramachandra's method in this case is

$$x^8 + 37925313474x^7 + 15420470282938225x^6 - 7475050214671930974x^5 +$$

$$899666793076055571124x^4 + 168000852503600362302 6x^3 +$$

$$688783180273825x^2 + 129529074x + 1.$$

Note that although this polynomial is over $\mathbb{Z}$ (instead of $\mathcal{O}_K$) it is only half the degree of the field extension over $\mathbb{Q}$. As a result, we can conclude that $K_{(5)}/\mathbb{Q}$ is not an abelian extension. The other thing to note is that the largest coefficient of the first polynomial (which defines the whole field) is 14 digits, while the largest for the second (which defines a non-Galois subfield) is 21. This is indicative of other examples we computed: the minimal polynomial for Ramachandra's units typically have very large coefficients.

The degrees of these polynomials are small enough that we can use the PARI command bnfinit() to compute the class number directly (which is 1). By comparison, when we look at $K_{(5)}$ for $K = \mathbb{Q}(\sqrt{-19})$ the Agathocleous-style units have a 40 digit term (and also lie in a non-Galois subfield) which is too large for bnfinit() to succeed after several hours of computation.

The degree of $K_{(5)}/\mathbb{Q}$ is also low enough that we can use algdep() to compute the minimal polynomial of elements of the field. For instance, we know that some root of the unit $\phi_{(5)}(\mathcal{I})$ is in the field for every $\mathcal{I}$ (and the root we take divides $12 * 5$). As a result, for every m dividing 60, we can multiply $\phi_{(5)}(\mathcal{I})^{1/m}$ by 60th roots of unity until algdep() returns a monic polynomial of degree 16. Doing this we get polynomials with terms that range from 18 to 25 digits long, so this set of units seems to not be useful, being larger than Agathocleous's units.

To get a comparison of how large these polynomials for $K_{(p)}$ are compared to those for the elliptic units in the earlier sections of this paper, the minimal polynomial associated to the elliptic units for $\mathfrak{p}$ over 11 in the field $K = \mathbb{Q}(\sqrt{-10})$ is

$$x^{10} + 2\omega x^9 - (17+\omega)x^8 + (16-8\omega)x^7 + (26+12\omega)x^6 -$$
$$(54-9\omega)x^5 - (29+17\omega) * x^4 + (35-6\omega)x^3 + (9+5\omega)x^2 - 5x + 1.$$

The norm of the largest element here is only 3 digits (and similar degree to the above polynomials). In other words, all the units we tried computing in $K_{(p)}$ have much larger minimal polynomials in practice (and therefore much higher precision requirements) than those corresponding to the elliptic units of $K_{\mathfrak{p}}$.

Of the 6 known highly irregular primes, $\mathfrak{p}$ over 41 in $K = \mathbb{Q}(\sqrt{-267})$ has the lowest degree class field, but even $K_{(41)}/K$ is a degree $40 * 40 = 1600$ extension, which is well beyond the size of anything we (or Kucuksakalli) computed before. As such, at the moment it appears direct calculation of a polynomial which splits over $K_{(p)}$ is well outside the bounds of practicality for all highly irregular primes.

As it appears that we run into practical computational bounds for field extensions whose degree is in the hundreds, a future direction would be to look at imaginary quadratic fields K of small class number h so that $h(p-1)^2/2$ (the degree of $K_{(p)}/\mathbb{Q}$) is a few hundred and $(h,p)=1$. If one could find a highly irregular prime in such a field, one might be able to actually construct $K_{(p)}$ using a unit subgroup and look for singular primary elements directly. On the other hand, given how the units scale in our small example above, it is quite likely that constructing the finite index unit group could still require lots of precision.

If one found a highly irregular prime with $h(p-1)^2/2 < 50$ one should be able to use algdep() to more quickly construct these polynomials. But since $p \geq 5$ this really only means $p=5$ for $h \leq 6$, or $p=7$ for $h=1$ or 2, or (possibly) $p=11$, $h=1$. However we have verified none of these cases are highly irregular except possibly $p=5$ with $h \geq 3$. As there are 7 class number 3 imaginary quadratic fields where 5 splits (discriminants -31, -59, -139, -211, -331, -379, -499) and these are all guaranteed to have cyclic ray class groups (because $3 \nmid \frac{5-1}{2}$), following the probabilistic arguments of section 4 we have a $1-(4/5)^7 \approx 79\%$ chance that at least one of the primes above 5 are highly irregular.

We have not done the relevant calculations as they require some substantial modifications of the code used in Section 3 for $h_K = 2$.

Chapter A: The Uses of algdep()

We often have an element of an algebraic extension of $\mathbb{Q}$ to a certain precision in $\mathbb{C}$. We may want to either increase the precision, or verify that we are in an extension. One method of doing this involves the PARI command algdep(z, d). It takes a complex or r-adic value z and finds a polynomial of degree at most d with relatively small coefficients which evaluates to a small value at z. It does this by employing the Lenstra-Lenstra-Lovasz (LLL) algorithm for lattice basis reduction as described in, for instance, Algorithm 2.6.3 of [3]. The method (described on page 101 of [3]) uses the first d powers of z to construct a lattice, then tries to find a sum of these powers which equals 0. If one has some idea of the bounds of the coefficients of a polynomial, then one can verify that what it returned is (divisible by) the minimal polynomial of x over $\mathbb{Z}$.

Understanding why the algdep() algorithm works is fundamental to understanding when it will fail and how to work around these situations. The following well-known facts establish the behaviour:

Theorem A.0.1. *Let Λ be an n-dimensional lattice. Let $\mu(\Lambda)$ be the area of a fundamental parallelopiped of the lattice.*

1. *(Minkowski) Given S a compact, convex, symmetric set of measure greater*

than $2^n\mu(\Lambda)$, we have $|S \cap \Lambda| > 1$.

2. *In particular, using S a ball we know Λ contains a non-zero point of length $\leq 2\sqrt[n]{\Gamma(\frac{n}{2}+1)\mu(\Lambda)}/\sqrt{\pi}$. We will call this the Minkowski bound of Λ.*

3. *If $\vec{b}_1, \vec{b}_2, ..., \vec{b}_n$ is a basis of Λ that is the output of the LLL algorithm and ℓ is the length of the shortest non-zero vector in Λ then $|\vec{b}_1| \leq 2^{(n-1)/2}\ell$.*

Proof. For a proof of statement 1 see Theorem 4.19 of [6]. Statement 3 see Theorem 2.6.2 of [3] □

The function algdep() returns a polynomial whose coefficients are small when viewed as a vector in Euclidean space. So in practice if we have enough precision that (the vector formed by the coefficients of) the minimal polynomial of α is well over $2^{n/2}$ shorter than the Minkowski bound, then we expect to find said minimal polynomial.

Consider the case where we have a complex number α, a number field L, and we know that $\mu\alpha \in L$ for one of some small number of μ (say, μ is a 12th root of unity). We can easily determine which μ has $\mu\alpha \in L$. We compute algdep($\mu\alpha, [L : \mathbb{Q}]$) for each μ and for the correct μ the answer is many orders of magnitude smaller than any other choice.

Because the size of a vector is within $\sqrt{n}$ of the largest-magnitude component, we need the largest component to be smaller than the Minkowski bound.[1] We are

[1] The smallest vector the LLL algorithm finds tends to have all its terms be the same order of magnitude. This is reasonable, because if it is locating an element within 2^n of the Minkowski bound, most of the points inside the n-ball of that radius are located near the surface, and most of the surface lies far from any one axis.

often applying algdep() to a unit α. The result is that $f_\alpha(x) = x^n f_{\alpha^{-1}}(1/x)$ so we expect the jth coefficient to be about as large as the $(n-j)$th coefficient and we expect the central terms to be the largest. As a result, $(x \pm 1)f_\alpha(x)$ often has a smaller largest coefficient since either the sum or difference of the two largest components is smaller than the largest. This generalizes: given that there are a large number of low degree polynomials with very small coefficients, it is very likely that one of them multiplied by $f_\alpha(x)$ will be small, even if it is a higher degree.

For example, if we take ϵ a generating elliptic unit of $K = \mathbb{Q}(\sqrt{-5})$, $\mathfrak{p} = \langle 7, 3-\omega \rangle$ and run algdep$(\epsilon, 12)$ at 100 digits of precision we get

$$x^{12} - 10x^{11} + 40x^{10} - 88x^9 + 135x^8 - 164x^7 + 174x^6 - 160x^5$$
$$+116x^4 - 62x^3 + 24x^2 - 6x + 1$$

which has a Euclidean norm of 128,355 (and is the correct answer). By comparison running algdep$(\epsilon, 15)$ at 100 digits of precision we get

$$\begin{aligned}&x^{15} - 7x^{14} + 13x^{13} + 3x^{12} - 19x^{11} + 17x^{10} - x^9 + 5x^8 - 6x^7 - 20x^6 + 26x^5\\ &- 4x^4 - 7x^3 + 9x^2 - 3x + 1\\ =&(x+1)^3(x^{12} - 10x^{11} + 40x^{10} - 88x^9 + 135x^8 - 164x^7 +\\ &174x^6 - 160x^5 + 116x^4 - 62x^3 + 24x^2 - 6x + 1)\end{aligned}$$

which has a Euclidean norm of only 2,172.

If we are unable to compute α to any higher precision, it is always worth it to run algdep() with a higher target degree than the minimal polynomial in the hopes that you find a small multiple of f_α.

A better approach would be to actually program a new version of algdep() that takes into account the fact that we are looking for a unit (and doesn't increase the dimension of the problem). Among other things, because we know the coefficients of x^n and x^0 are both 1, we should be solving a lattice problem in two lower dimensions. Moreover, the above discussion of the central terms of the polynomial being larger could be taken into account by slightly altering the weighting of our rows. Cohen suggests ([3], page 101) that we weight the jth row proportionate to A^{n-j} for some reasonable A to try and ensure that all the powers of α show up a similar amount in the final polynomial. We suggest instead weighting them proportionally to the inverse of Binomial(n, j), so that the central terms are used more often.

(Un)fortunately the PARI/GP code is highly optimized as written and so we were not able to perform a reasonable comparison of the two methods.

Bibliography

[1] E. Agathocleous, *Class Numbers of Real Cyclotomic Fields of Conductor pq*, PhD Thesis, University of Maryland, 2009.

[2] J. Buhler, D. Harvey, *Irregular primes to 163 million*, Math. Comp, 80 (2011), 2435-2444.

[3] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin Heidelberg New York 1993.

[4] M. Deuring, *Die Klassenkorper der Kömplexen Multiplikation*, Enzykl. der Math. Wiss. Band I, 2, 23, Teubner, 1958.

[5] O. Kucuksakalli, *Class Numbers of Ray Class Fields of Imaginary Quadratic Fields*, Math. Comp. Vol. 80 (2011) pp. 1099-1122.

[6] J. Milne, *Algebraic Number Theory, version 3.05*, http://www.jmilne.org/math/CourseNotes/ANT.pdf, accessed 3/21/2013.

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

[8] PARI/GP, version 2.5.5, http://pari.math.u-bordeaux.fr/, Bordeaux, 2013.

[9] K. Ramachandra, *Applications of Kronecker's Limit Formulas*, Annals of Mathematics, Vol. 80, No. 1 (July 1964) pp.104-148

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

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

[12] H. Stark, *On Complex Quadratic Fields with Class-Number Two*, Mathematics of Computation, Vol. 29, No. 129 (Jan., 1975), pp. 289-302

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

[14] Wikipedia, *Splitting circle method*,
http://en.wikipedia.org/wiki/Splitting_circle_method accessed 10/12/2014.