On Criteria for Large Cyclotomic λ-invariants for Imaginary Quadratic Fields

by

Christopher Mathewson Stokes

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

Approved March 2023 by the
Graduate Supervisory Committee:

Nancy Childress, Chair
Florian Sprung
Jonathan Montaño
Julian Paupert
Steven Kaliszewski

ARIZONA STATE UNIVERSITY

May 2023

ABSTRACT

Iwasawa theory is a branch of number theory that studies the behavior of certain objects associated to a $\mathbb{Z}_p$-extension. The work in this thesis will focus on the cyclotomic $\mathbb{Z}_p$-extensions of imaginary quadratic fields for varying primes p, and will give some conditions for when the corresponding lambda-invariants are greater than 1.

DEDICATION

For my Grandmothers, Barbara and Elizabeth.

ACKNOWLEDGMENTS

I want to express my deepest appreciation and gratitude towards my advisor Nancy Childress for all of her support over the years. I am also in debt to John Cosgrave and Karl Dilcher for their helpful advice and interest in my work. I also wish to thank the referee for many helpful comments and suggestions, and my committee members Florian Sprung, Jonathan Montaño, Julian Paupert, and Steve Kaliszewski. Finally, thank you to all of my family and friends for sticking with me through the years.

TABLE OF CONTENTS

CHAPTER Page

Chapter 1

INTRODUCTION AND STATEMENT OF MAIN RESULTS

Let p be an odd prime, and $d > 0$ a square-free integer. Denote $K = \mathbb{Q}(\sqrt{-d})$ and let $\lambda_p(K)$ be Iwasawa's λ-invariant for the cyclotomic $\mathbb{Z}_p$-extension of K. In (10), Dummit, Ford, Kisilevsky and Sands compute $\lambda_p(K)$ for various primes and imaginary quadratic fields. They define the non-trivial primes of K to be those which satisfy $\lambda_p(K) > 1$ (non-trivial since $\lambda_p(K) > 0$ whenever p splits in K, see (19)). For example, Table 1 gives the non-trivial primes for $K = \mathbb{Q}(\sqrt{-3})$ and $K = \mathbb{Q}(i)$ for primes $p < 10^7$ (see Table 1 in (10) for all other imaginary quadratic fields with discriminants up to 1,000).

Table 1.1: Non-trivial primes $p < 10^7$ of $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(i)$.

$K = \mathbb{Q}(\sqrt{-3})$	13	181	2521	76543	489061	6811741
$K = \mathbb{Q}(i)$	29789					

Note that the values from Table 1 come from (10), which were computed in 1989 (it would be interesting to compute these values further with modern computational power). Authors such as Ellenberg, Jain, and Venkatesh (11), Horie (17), Ito (18), and Sands (33) have studied $\lambda_p(K)$ by fixing a prime p and varying the imaginary quadratic field K. Dummit, Ford, Kisilevsky, and Sands (10), and Gold (13) have studied the case when K is fixed and p varies (which is the point of view we take in this paper), but less seems to be known in this situation. Another point of view might

be to fix both p and K and vary the $\mathbb{Z}_p$-extension of K. Interestingly, Sands (32) has shown that if p does not divide the class number of K, and the cyclotomic λ-invariant $\lambda_p(K) \leq 2$, then every other $\mathbb{Z}_p$-extension K_∞/K has $\lambda_p \leq 2$ and $\mu_p = 0$. Therefore, knowing the non-trivial primes p of K is important for our overall understanding of the other $\mathbb{Z}_p$-extensions of K.

On the other hand, for $m \in \mathbb{Z}^+$ we have the seemingly unrelated 1-exceptional primes p for m studied by Cosgrave and Dilcher, that is, primes $p \equiv 1 \pmod{m}$ such that $\left(\frac{p^2-1}{m}\right)_p^{p-1}! = \left(\prod_{\substack{a=1 \\ \gcd(a,p)=1}}^{\frac{p^2-1}{m}} a\right)^{p-1} \equiv 1 \pmod{p^2}$. Surprisingly, the primes p in Table 1 are exactly the 1-exceptional primes for $m = 3$ and $m = 4$ respectively, with $p < 10^7$ (see the next section, or (7) and (8) to learn about 1-exceptional primes).

This thesis is dedicated to finding conditions for which the cyclotomic λ-invariants of imaginary quadratic fields surpass a given value n, with a focus on $n = 1$ and 2.

The first main result is Theorem 3.1.1, which is a criterion in terms of Gauss factorials that gives $\lambda_p(K) > 1$ (this is a condition that works for every imaginary quadratic field K and any prime p that splits in K and is congruent to 1 modulo the absolute discriminant of K). This will be proven in two ways: first using the Gross-Koblitz formula (16) and Gold's criterion (13) (see Theorem 3.1.2), the second using the p-adic L-function associated to the imaginary quadratic field K. From this, we obtain an explanation for the apparent connection between the 1-exceptional primes for $m = 3$ and $m = 4$, and the non-trivial primes of $K = \mathbb{Q}(\sqrt{-3})$ and $K = \mathbb{Q}(i)$, as well as some similar results for $K = \mathbb{Q}(\sqrt{-d})$ with $d = 2, 5$ and 6:

Theorem 1.0.1. *Let $K = \mathbb{Q}(\sqrt{-d})$ and $D = 2d$ if $d \equiv 3 \pmod{4}$ and $D = 4d$ otherwise. Let p be a prime such that $p \equiv 1 \pmod{D}$, and suppose that p does not*

divide the class number of K. Then for $d = 1, 2, 3, 5$ and 6 we have

$$\lambda_p(K) > 1 \iff \left(\frac{\left(\frac{p^2-1}{D}\right)_p^2 !}{\left(\frac{p^2-1}{D/2}\right)_p !} \right)^{p-1} \equiv 1 \pmod{p^2}.$$

In particular, p is 1-exceptional for $m = 3$ if and only if $\lambda_p(\mathbb{Q}(\sqrt{-3}) > 1$ and p is 1-exceptional for $m = 4$ if and only if $\lambda_p(\mathbb{Q}(i)) > 1$.

The proof of Theorem 1.0.1 relies on the fact the fields $K = \mathbb{Q}(\sqrt{-d})$, where $d = 1, 2, 3, 5$ and 6, have so called *"maximal class numbers"* (see Definition 8). We will prove Theorem 3.1.4 which tells us that these are the only imaginary quadratic fields with such class numbers, under the assumption that the generalized Riemann hypothesis is true.

As a corollary of Theorem 1.0.1 we will see that primes p of the form $p^2 = 3x^2 + 3x + 1$ with $x \in \mathbb{Z}$ always give $\lambda_p(\sqrt{-3}) > 1$. However, the converse does not hold (see Remark 2). Theorem 1.0.1 also leads to

Corollary 1. *For $K = \mathbb{Q}(\sqrt{-d})$ for $d = 1, 2, 3, 5$ and 6, we have*

$$\lambda_p(K) > 1 \iff B_p(2/D) \equiv 2^p B_p(1/D) \pmod{p^3}$$

where $B_n(x)$ is the n-th Bernoulli polynomial.

In particular, we obtain some interesting conditions for the non-trivial primes of $K = \mathbb{Q}(i)$ and $K = \mathbb{Q}(\sqrt{-3})$ in terms of Glaisher and Euler numbers respectively. Recall the Euler numbers $\{E_n\}$ and Glaisher numbers $\{G_n\}$ are defined by

$$\sum_{n=0}^{\infty} E_n \frac{x^n}{n!} = \frac{2}{e^x + e^{-x}} \quad \text{and} \quad \sum_{n=0}^{\infty} G_n \frac{x^n}{n!} = \frac{3/2}{e^x + e^{-x} + 1}.$$

We will prove:

Corollary 2. *Let $p \equiv 1 \pmod 4$ be a prime and E_n denote the n-th Euler number. Then $\lambda_p(\mathbb{Q}(i)) > 1$ if and only if $E_{p-1} \equiv 0 \pmod{p^2}$.*

Corollary 3. *Let $p \equiv 1 \pmod 3$ be a prime and G_n denote the n-th Glaisher number. Then $\lambda_p(\mathbb{Q}(\sqrt{-3})) > 1$ if and only if $G_{p-1} \equiv 0 \pmod{p^2}$.*

Remark 1. *The numbers $\{G_n\}$ were studied by Glaisher in (14) and (15) in which they are referred to as I-numbers.*

In Section 4, we will find another unexpected relation, that is, between the lambda invariant of an imaginary quadratic field and the number of points on a reduced elliptic curve with complex multiplication. We state the main Theorem of that section:

Theorem. *Let $p > 3$ be a prime and K be an imaginary quadratic field such that p does not divide the class number of K, and $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$, $\tilde{K}$ the field obtained by adding certain torsion coordinates of E to the Hilbert class field of K, and $\mathfrak{P}$ a prime of $\tilde{K}$ above $\mathfrak{p}$ (see section 4 for more details). Then $\lambda_p(K) > 1$ if and only if $\#\tilde{E}(\mathbb{F}_q) \equiv 0 \pmod{p^2}$, where $q = p^{p-1}$, and $\tilde{E}$ is the reduction of E modulo $\mathfrak{P}$.*

As a result, we can relate certain Gauss factorials to elliptic curves with complex multiplication, as well as the Euler and Glaisher numbers:

Theorem. *Let $p \equiv 1 \pmod 3$, and consider $E/\mathbb{F}_p : y^2 = x^3 - 1$. Then p is 1-exceptional for $m = 3$ if and only if $G_{p-1} \equiv 0 \pmod{p^2}$ if and only if $\#E(\mathbb{F}_{p^{p-1}}) \equiv 0 \pmod{p^2}$.*

Theorem. *Let $p \equiv 1 \pmod 4$, and consider $E/\mathbb{F}_p : y^2 = x^3 + x$. Then p is 1-exceptional for $m = 4$ if and only if $E_{p-1} \equiv 0 \pmod{p^2}$ if and only if $\#E(\mathbb{F}_{p^{p-1}}) \equiv 0 \pmod{p^2}$.*

Next, in the absence of Gold's result for $\lambda_p(K)$, we will again use the p-adic L-function associated to K to obtain a criterion for $n < \lambda_p(K) < p$. In particular, we will get a "Gold like" criterion for $\lambda_p(K) > 2$. In this case we will also get a result analogous to Theorem 3.1.1. Finally, we will obtain a partial result in the spirit of Theorem 3.1.2 for $\lambda_p(K) > 2$.

Chapter 2

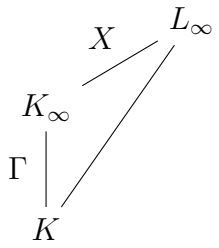
PRELIMINARIES

2.1 Brief Overview of Iwasawa Theory

Iwasawa theory can be described as the study of objects $\{A_n\}_{n\in\mathbb{N}}$ associated to an infinite tower of number fields $K \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_\infty = \bigcup_n K_n$ such that the Galois group $\mathrm{Gal}(K_\infty/K)$ is isomorphic to the p-adic integers $\mathbb{Z}_p$. We will always denote $\Gamma = \mathrm{Gal}(K_\infty/K)$, and refer to K_∞/K as a $\mathbb{Z}_p$-extension.

Here is the most basic example of such an extension: Let $\zeta_n = \zeta_{p^n}$ be a primitive p^n-th root of unity and K an Abelian number field such that $\zeta_n \notin K$. Then $K(\zeta_{n+1})/K$ is a cyclic Galois extension of degree $p^n(p-1)$, and thus contains a sub-extension K_n/K such that $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$. Taking $K_\infty = \bigcup_n K_n$ we have that $\Gamma = \mathrm{Gal}(K_\infty/K) = \varprojlim \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p$. In this case K_∞/K is referred to as the cyclotomic $\mathbb{Z}_p$-extension of K.

Returning to the general case, let K_∞/K be a $\mathbb{Z}_p$-extension and denote $C(K_n)$ to be the ideal class group of K_n, and A_n to be its Sylow p-subgroup. Let us now get a rough idea of how a $\mathbb{Z}_p$-extension allows one to study $\{A_n\}$. By class field theory, there exists an unramified Abelian extension L_n/K_n such that $\mathrm{Gal}(L_n/K_n) \cong A_n$. Then taking $L_\infty = \bigcup_n L_n$, we have that $X = \mathrm{Gal}(L_\infty/K_\infty) = \varprojlim \mathrm{Gal}(L_n/K_n)$, and L_∞/K is also Galois.



We have that Γ acts on X, and even more, X is a finitely generated $\Lambda = \mathbb{Z}_p[[\Gamma]]$ module. We shall refer to Λ as the Iwasawa algebra. One might think of X as having encoded all the information of each A_n, and viewing X as a Λ-module allows us to access this information. There exists an element $\gamma \in \Gamma$ such that γ generates a dense subgroup which gives rise to an isomorphism $\Lambda \cong \mathbb{Z}_p[[T]]$, where T is identified with $\gamma - 1$ (γ is called a topological generator). We say that two Λ-modules M and N are pseudo-isomorphic, and write $M \sim N$, if there exists an exact sequence of Λ-modules

$$0 \to A \to M \to N \to B \to 0$$

such that A and B are finite. Then with the Λ-module X as above, it can be shown that

$$X \sim \bigoplus_{i=0}^{t} \Lambda/p^{a_i}\Lambda \oplus \bigoplus_{i=0}^{m} \Lambda/f_i(T)^{b_i}\Lambda$$

where $f_i \in \Lambda$ are irreducible distinguished polynomials ($f_i(T) = c_r T^r + \cdots + c_1 T + c_0$ is distinguished if $p \mid c_i$ for $0 \leq i \leq r-1$, and $p \nmid c_r$), $a_i, b_i \in \mathbb{Z}^+$, and $A_n \cong \mathrm{Gal}(L_n/K_n) \cong X/(\gamma^{p^n} - 1)X$ (see Theorem 13.12 and Proposition 13.19 in Chapter 13 of (39)). We define the Iwasawa invariants $\mu = \mu_p(K_\infty/K) = \mu_p(K)$ and $\lambda = \lambda_p(K_\infty/K) = \lambda_p(K)$ as

$$\mu = \sum_{i=0}^{t} a_i, \quad \lambda = \sum_{i=0}^{m} \deg(f_i) b_i$$

and we call the ideal generated by $f(T) = p^{\mu} \prod_{i=0}^{m} f_i(T)^{b_i}$ the characteristic ideal of Λ.

Theorem 2.1.1 (Iwasawa's Theorem)**.** *For n sufficiently large*

$$|A_n| = |X/(\gamma^{p^n} - 1)X| = p^{n\lambda + p^n \mu + \nu}.$$

where $\mu, \lambda \in \mathbb{Z}^+$ and $\nu \in \mathbb{Z}$.

If K is Abelian and K_∞/K is the cyclotomic $\mathbb{Z}_p$-extension, then $\mu = 0$ by the Theorem of Fererro-Washington (12). In general, if K_∞/K is not the cyclotomic $\mathbb{Z}_p$-extension then there are known instances where $\mu \neq 0$ (see (22)). On the other hand, we know many simple cases where $\lambda > 0$. For example, if $K = \mathbb{Q}(\sqrt{-d})$ is an imaginary quadratic field then $\lambda_p(K) > 0$ if and only if p splits K, or p divides the class number of K (more on this later). There is still much to learn about λ even under basic assumptions (see, for example, (10), (32) and, (33)). For more on classical Iwasawa theory, see chapter 13 in Washington (39).

2.2 p-adic Measure Theory and the Iwasawa Isomorphism

Let p be a prime number.

Definition 1. *Let $k/\mathbb{Q}_p$ be a finite extension of $\mathbb{Q}_p$. A k-valued measure is a function*

$$\alpha : \{\textit{compact open subsets of } \mathbb{Z}_p\} \to k$$

such that

i. for $A \cap B = \emptyset$, $\alpha(A \cup B) = \alpha(A) + \alpha(B)$

ii. $\{|\alpha(A)|_p\}_A$ is bounded.

We define Λ_k to be the set of all $\mathcal{O}_k$-valued measures on $\mathbb{Z}_p$.

Definition 2. *We define the indicator function for $a + p^n\mathbb{Z}_p$ by*

$$g_{a,p^n}(x) = \begin{cases} 1 & \text{if } x \in a + p^n\mathbb{Z}_p \\ 0 & \text{else} \end{cases}.$$

We say that $f : \mathbb{Z}_p \to K$ is locally constant if there exists $N \in \mathbb{N}$ such that

$$f(x) = \sum_{a=0}^{p^N-1} f(a) g_{a,p^N}(x).$$

We can now start to define an integral on $\mathbb{Z}_p$ against a measure α.

Definition 3. *If α is a k-valued measure and $f : \mathbb{Z}_p \to k$ is locally constant, then we define*

$$\int_{\mathbb{Z}_p} f(x)\, d\alpha(x) = \sum_{a=0}^{p^N-1} f(a)\alpha(a + p^N\mathbb{Z}_p).$$

Now let $f : \mathbb{Z}_p \to k$ be continuous. Then there is a sequence $(f_n)_{n\in\mathbb{Z}^+}$ such that $f_n : \mathbb{Z}_p \to k$ is locally constant, and $f_n \to f$ uniformly.

Definition 4. *If α is a k-valued measure and $f : \mathbb{Z}_p \to k$ is continuous, then we define*

$$\int_{\mathbb{Z}_p} f(x)\, d\alpha(x) = \lim_{n\to\infty} \int_{\mathbb{Z}_p} f_n(x)\, d\alpha(x)$$

where $f_n \to f$.

It is easy to show that this integral is independent of the choice of sequence (f_n).

Theorem 2.2.1. *There is an isomorphism of rings $(\Lambda_k, +, *) \cong (\mathcal{O}_k[[T-1]], +, \cdot)$ given by*

$$\alpha \mapsto \sum_{n=0}^{\infty} \left(\int_{\mathbb{Z}_p} \binom{x}{n} d\alpha(x) \right) (T-1)^n$$

where $*$ is convolution of measures.

We will often view Λ_k as a ring of measures or power series interchangeably.

2.3 L-functions

Let χ be a Dirichelt character with conductor f. Then the Dirichlet L-function attached to χ is defined to be

$$L(s,\chi) = \sum_{n=0}^{\infty} \frac{\chi(n)}{n^s}$$

which converges for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$. It is well known that $L(s,\chi)$ has an Euler product

$$L(s,\chi) = \prod_{p \text{ prime}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

which again converges for $\mathrm{Re}(s) > 1$. These Dirichlet L-functions can be analytically continued to the entire complex plane (except when $\chi = 1$, in which case there is a simple pole at $s = 1$) via the functional equation

$$\Gamma(s)\cos\left(\frac{\pi(s-\delta)}{2}\right) L(s,\chi) = \frac{\tau(\chi)}{2i^\delta}\left(\frac{2\pi}{f}\right)^s L(1-s,\bar{\chi})$$

where $\bar{\chi}(a) = \overline{\chi(a)}$, $\Gamma(s) = \int_0^\infty x^{s-1}e^{-x}\,dx$ is the gamma function, $\tau(\chi) = \sum_{a=0}^{f} \chi(a)e^{2\pi ia/f}$ is the Gauss sum for χ, and

$$\delta = \begin{cases} 1 & \text{if } \chi(-1) = -1 \\ 0 & \text{if } \chi(-1) = 1 \end{cases}.$$

Now, consider the Bernoulli numbers B_n given by

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$$

the Bernoulli polynomials $B_n(X)$ given by

$$B_n(X) = \sum_{k=0}^{n} \binom{n}{k} B_k X^{n-k}$$

and the generalized Bernoulli numbers $B_{n,\chi}$ given by

$$\sum_{a=1}^{f} \chi(a) \frac{te^{at}}{e^{ft}-1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}.$$

Then the Dirichlet L-functions have the generalized Bernoulli numbers as their special values, that is, for $n \in \mathbb{Z}^+$,

$$L(1-n,\chi) = -\frac{B_{n,\chi}}{n}.$$

2.4 p-adic L-functions

Kubota and Leopoldt (24) found a p-adic analogue $L_p(s,\chi)$ of $L(s,\chi)$ such that $L_p(s,\chi) : \mathbb{Z}_p \to \mathbb{C}_p^{\times}$ is continuous, and

$$L_p(1-n,\chi) = (1-\chi(p)p^{n-1})L(1-n,\chi)$$

if n is divisible by $p-1$, and

$$L_p(1-n,\chi) = (1-\chi\omega^{-n}(p)p^{n-1})L(1-n,\chi\omega^{-n})$$

if n is not divisible by $p-1$. Here $\omega : (\mathbb{Z}/p\mathbb{Z})^{\times} \to \mathbb{C}^{\times}$ is the Teichmüller character. In 2.5 we will see that we can construct p-adic L-functions via p-adic measures. Other constructions can be found in (23), (27), and (39).

2.5 Iwasawa's Power Series and Rational Functions

We shall restrict our attention to $K = \mathbb{Q}(\sqrt{-d})$, where the situation is simplified compared to the more general CM case. Denote k to be the $\mathfrak{p}$-adic completion of K where $\mathfrak{p} \cap \mathbb{Z} = p$. Denote $U = 1 + p\mathbb{Z}_p$, $V \subseteq \mathbb{Z}_p$ the $(p-1)$-st roots of unity, and π the maximal ideal in $\mathcal{O}_k$. We also denote $\mathrm{ord}(\cdot)$ to be the valuation of $\mathbb{C}_p$ such that

$\mathrm{ord}(p) = 1$. As before, we denote Λ_k to be the set of all $\mathcal{O}_k$-valued measures on $\mathbb{Z}_p$. We will write $F_\alpha(T) \in \mathcal{O}_k[[T-1]]$ as the power series corresponding to $\alpha \in \Lambda$, as in Theorem 2.2.1. Now, for $F_\alpha(T) \in \Lambda_k$, with $F_\alpha(T) = \sum_{n=0}^{\infty} a_n (T-1)^n$, we denote

$$\mu(F_\alpha) = \mu(\alpha) = \min_n \{\mathrm{ord}(a_n)\} \quad \text{and} \quad \lambda(F_\alpha) = \lambda(\alpha) = \min\{n \,:\, \mathrm{ord}(a_n) = \mu(\alpha)\}.$$

Let c be any positive integer such that $\gcd(c, dp) = 1$, and define the periodic function

$$\epsilon(a) = \begin{cases} \chi(a) & \text{if } c \nmid a \\ \chi(a)(1-c) & \text{if } c \mid a \end{cases}.$$

If f is any multiple of cdp, it can be shown that

$$\frac{\sum_{a=1}^{f} \epsilon(a) T^a}{1 - T^f} \in \mathcal{O}_k[[T-1]].$$

We thus associate the above rational function with the power series $F_\alpha(T)$, where $\alpha \in \Lambda_k$ (see Proposition 4.1 in (37)). Given a topological generator u (that is, $u \in 1 + p\mathbb{Z}_p$ but $u \notin 1 + p^2\mathbb{Z}_p$) we have an isomorphism $\varphi : \mathbb{Z}_p \to U$ given by $x \mapsto u^x$. For $x \in \mathbb{Z}_p$ we will also write $\langle x \rangle = x/\omega(x)$. The Γ-transform of α is the function from $\mathbb{Z}_p$ to $\mathbb{C}_p$ defined by

$$\Gamma_\alpha(s) = \int_{\mathbb{Z}_p^\times} \langle x \rangle^s \, d\alpha(x) = \sum_{a=1}^{p-1} \int_U \langle \omega(a)x \rangle^s \, d\alpha(\omega(a)x) = \int_U x^s \, \beta(x) = \int_{\mathbb{Z}_p} u^{sx} \, d\tilde{\beta}(x)$$

where $\beta = \sum_{a=1}^{p-1} d\alpha(\omega(a)x)$ and $\tilde{\beta} = \beta \circ \varphi$. Now, consider $G_\chi(T) \in \Lambda_k$ given by

$$G_\chi(T) = \int_{\mathbb{Z}_p} T^x \, d\tilde{\beta}(x) = \sum_{n=0}^{\infty} \left(\int_{\mathbb{Z}_p} \binom{x}{n} d\tilde{\beta}(x) \right) (T-1)^n$$

Then $G_\chi(T)$ is essentially the p-adic L function, or more precisely, $G_\chi(u^s) = -(1 - \chi(c)c\langle c \rangle^s) L_p(-s, \chi\omega)$. We say that $G_\chi(T)$ is the Iwasawa series for α. Now choose $t \in \mathbb{Z}_p$ such that $u^t = \langle c \rangle$ and set $H_\chi(T) = 1 - \chi(c)cT^t$ from which we obtain

$L_p(s, \chi\omega) = G_\chi(u^{-s})/H_\chi(u^{-s})$. We denote $g_\chi(T) = G_\chi(T^{-1})/H_\chi(T^{-1})$, and we shall write

$$g_\chi(T) = \sum_{n=0}^{\infty} b_n (T-1)^n. \tag{2.1}$$

Then since K is an imaginary quadratic field, we have

$$\lambda_p(K) = \lambda(g_\chi) \quad \text{and} \quad \mu_p(K) = \mu(g_\chi).$$

We also have that K is Abelian over $\mathbb{Q}$, so the Ferrero-Washington Theorem (12) says that $\mu_p(K) = 0$ (see (37) for another proof using rational functions). Hence, to calculate $\lambda_p(K)$, we must find the smallest index n such that $b_n \not\equiv 0 \pmod{p}$.

One issue with the power series g_χ is that the composition with φ makes certain computations difficult. The next theorem due to Childress (3), (4), and later improved by Satoh (34), will give us a better rational function to work with later on,

Theorem 2.5.1 (Childress (3))**.** *Let ϵ, V, and f be as above. Then*

$$F(T) = \sum_{\zeta \in V} \left(\sum_{\substack{a=1 \\ a \equiv \zeta \pmod{p}}}^{f} \epsilon(a) T^{\zeta^{-1} a} \Big/ (1 - T^{\zeta^{-1} f}) \right). \tag{2.2}$$

Then $H_\chi(T), F(T) \in \mathcal{O}_k[[T-1]]$, and p divides $\lambda_p(F)$. Also $\lambda_p(g_\chi) = \frac{1}{p}\lambda_p(F) - \lambda_p(H_\chi)$.

Notice that $F(T)$ is almost the power series obtained from the Γ-transform of α (it is missing the composition with φ).

2.6 Some Results of Class Field Theory

Let k be a number field, and $\mathfrak{m}$ an ideal of $\mathcal{O}_k$. We denote $I_\mathfrak{m}$ to be the set of fractional ideals $\mathfrak{a}$ such that $\mathfrak{m} \nmid \mathfrak{a}$. For $\alpha \in k$ we say that α is totally positive if

$\tau(\alpha) > 0$ for every real embedding τ of k. We denote $P_{\mathfrak{m}}$ to be the set of principle ideals $\langle\alpha\rangle$ of $\mathcal{O}_k$ such that $\alpha \equiv 1 \pmod{\mathfrak{m}}$ and α is totally positive.

Theorem 2.6.1. *Suppose that H is such that $P_{\mathfrak{m}} < H < I_{\mathfrak{m}}$. Then there exists an abelian extension K/k such that $Gal(K/k) \cong I_{\mathfrak{m}}/H$. Further, K/k is ramified only at the primes dividing $\mathfrak{m}$.*

We say that K is the ray class field of k for H. If $H = P_{\mathfrak{m}}$ then we say that K is the ray class field for k of conductor $\mathfrak{m}$. The isomorphism in the theorem is induced by the so called Artin map.

Let k be a number field and K/k a finite Galois extension. Let $\mathfrak{p}$ be a prime of k and $\mathfrak{P}$ a prime of K above $\mathfrak{p}$. Denote

$$Z = Z(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(K/k) \,:\, \sigma(\mathfrak{P}) = \mathfrak{P}\}$$
$$T = T(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in Z(\mathfrak{P}/\mathfrak{p}) \,:\, \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}} \text{ for all } \alpha \in \mathcal{O}_K\}.$$

We call Z and T the decomposition and inertia groups respectively for $\mathfrak{P}/\mathfrak{p}$. Now, if K_T is the fixed field for T, then $\mathfrak{p}$ is unramified in K_T/k and $\mathfrak{p}_T = \mathfrak{P} \cap \mathcal{O}_{K_T}$ is totally ramified in K/K_T.

Now, $(\mathcal{O}_K/\mathfrak{P})/(\mathcal{O}_k/\mathfrak{p})$ is a finite extension of fields, with Galois group generated by the Frobenius automorphism $\sigma_{\mathfrak{P}}$ given by

$$\sigma_{\mathfrak{P}}(x + \mathfrak{P}) = x^{N_{k/\mathbb{Q}}(\mathfrak{p})} + \mathfrak{P}.$$

We have the exact sequence

$$1 \to T \to Z \to \mathrm{Gal}((\mathcal{O}_K/\mathfrak{P})/(\mathcal{O}_k/\mathfrak{p})) \to 1$$

and if $\mathfrak{p}$ is unramified in K/k, then $T = 1$ and $Z \cong \mathrm{Gal}((\mathcal{O}_K/\mathfrak{P})/(\mathcal{O}_k/\mathfrak{p}))$. Hence, we may view the Frobenius $\sigma_{\mathfrak{P}}$ as an element of Z with the property

$$\sigma_{\mathfrak{P}}(x) \equiv x^{N_{k/\mathbb{Q}}(\mathfrak{p})} \pmod{\mathfrak{P}}.$$

Now, if $\tau \in \mathrm{Gal}(K/k)$, then $\tau\mathfrak{P}$ is a prime above $\mathfrak{p}$ and unramified in K/k. It is easy to see that $\sigma_{\tau\mathfrak{P}} = \tau\sigma_{\mathfrak{P}}\tau^{-1} = \sigma_{\mathfrak{P}}$ since $\mathrm{Gal}(K/k)$ is Abelian. In other words, the Frobenius automorphism only relies upon $\mathfrak{p}$, and we can then write $\sigma_{\mathfrak{p}} = \sigma_{\mathfrak{P}}$. If $\mathfrak{D}$ is the relative discriminant of K/k then for any prime ideal $\mathfrak{p} \in I_{\mathfrak{D}}$ we have that $\mathfrak{p}$ is unramified in K/k. Therefore, we can define the Artin map $I_{\mathfrak{D}} \to \mathrm{Gal}(K/k)$ on the prime ideals $\mathfrak{p} \in I_{\mathfrak{D}}$ as

$$\mathfrak{p} \mapsto \sigma_{\mathfrak{p}}.$$

which extends naturally to arbitrary $\mathfrak{m} \in I_{\mathfrak{D}}$. See (2) for more on class field theory.

2.7 Elliptic Curves With Complex Multiplication

Let K be an imaginary quadratic field. Recall that an elliptic curve E defined over a field F with $\mathrm{char}(F) \neq 2$ or 3, is the set of points $(x, y) \in \bar{F}$ such that $y^2 = x^3 + Ax + B$, where $A, B \in F$ and $\Delta = -16(4A^3 + 27B^2) \neq 0$ (the condition $\Delta \neq 0$ means that the curve is non-singular). For a subfield $L \subseteq \bar{F}$, we write

$$E(L) = \{(x, y) \,:\, y^2 = x^3 + Ax + B \text{ such that } x, y \in L\}.$$

If E_1 and E_2 are two elliptic curves , an isogeny from (E_1, O_1) to (E_2, O_2) is a morphism $\varphi : E_1 \to E_2$ such that $\varphi(O_1) = O_2$. We write $\mathrm{Hom}(E_1, E_2)$ to be the set of isogenies from E_1 to E_2. Then $\mathrm{Hom}(E_1, E_2)$ is a group under addition. If E is an elliptic curve then we denote $\mathrm{Hom}(E, E) = \mathrm{End}(E)$, which is then a ring under addition and composition. Hence, we call $\mathrm{End}(E)$ the endomorphism ring of E (see

Chapter III in (36)). Since an elliptic curve E has a group operation $+$, we have for each $m \in \mathbb{Z}^+$ an isogeny $[m] : E \to E$ given by

$$[m]P = P + P + \cdots + P \quad (\ m\text{-times }).$$

The isogeny $[-m]$ is defined in the obvious way. We see then that there is a natural map $\mathbb{Z} \to \mathrm{End}(E)$. In fact,

Theorem 2.7.1 (Corollary 9.4 in (36))**.** *The endomorphism ring End(E) of E/F is isomorphic to either $\mathbb{Z}$, an order in an imaginary quadratic field, or an order in a quaternion algebra. If char$(F) = 0$, then only the first two are possible.*

In light of this theorem, we say that E/F has complex multiplication by $\mathcal{O}_K$ if $\mathrm{End}(E) \cong \mathcal{O}_K$, and we denote the image of $\gamma \in \mathcal{O}_K$ as $[\gamma] \in \mathrm{End}(E)$.

Suppose that $m \in \mathbb{Z}$ and $P \in E$ such that $[m]P = O$. Then we say that P is an m-torsion point of E, and we denote the group of m-torsion points of E as

$$E[m] = ker[m].$$

We know about the structure of this group:

Theorem 2.7.2 (Corollary 6.4 in (36))**.** *Let E/F be an elliptic curve and $m \in \mathbb{Z}$ with $m \neq 0$. Then*

i. If char$(F) = 0$, or $p =$ char$(F) > 0$ and $\gcd(p, m) = 1$, then

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}.$$

ii. . If char$(F) = p > 0$, then either $E[p^r] = \{O\}$ for all $r \in \mathbb{Z}^+$, or $E[p^r] = \mathbb{Z}/p^r\mathbb{Z}$ for all $r \in \mathbb{Z}^+$.

If E/F has complex multiplication by $\mathcal{O}_K$, and $\mathfrak{c}$ is an integral ideal of $\mathcal{O}_K$, then we also have the $\mathfrak{c}$-torsion points of E, defined as

$$E[\mathfrak{c}] = \{P \in E : [\gamma]P = O \text{ for all } \gamma \in \mathcal{O}_K\}.$$

For an extension L/F, and a prime $\mathfrak{P}$ of L above $p \in \mathbb{Z}$, denote $L_\mathfrak{P}$ to be the completion of L with respect to the $\mathfrak{P}$-adic absolute value. Let $\mathcal{O}_{L_\mathfrak{P}} = \{x \in L_\mathfrak{P} : |x|_\mathfrak{P} \leq 1\}$ be the ring of integers in $L_\mathfrak{P}$, and $M_\mathfrak{P}$ the maximal ideal of $\mathcal{O}_{L_\mathfrak{P}}$. Then $\mathcal{O}_{L_\mathfrak{P}}/M_\mathfrak{P} \cong \mathbb{F}_{p^f}$, where f is the residue degree of $L/\mathbb{Q}$. Now, if $E : y^2 = x^3 + A'x + B'$ is an elliptic curve with points in $L_\mathfrak{P}$, by making a variable substitution, we may obtain a curve such that the coefficients $A, B \in \mathcal{O}_{L_\mathfrak{P}}$, and the $\mathfrak{P}$-adic valuation of Δ is minimized (we say that E has a minimal Weierstrass equation, see Chapter VII.1 (36)). Consider the map $\mathcal{O}_{L_\mathfrak{P}} \to \mathcal{O}_{L_\mathfrak{P}}/M_\mathfrak{P}$, denoted by $x \mapsto \tilde{x}$. We can define $\tilde{E}/\mathbb{F}_{p^f} : y^2 = x^3 + \tilde{A}x + \tilde{B}$, which may or may not be singular ($\tilde{E}$ is non-singular if and only if $\Delta \equiv 0 \pmod{\mathfrak{P}}$). If $P \in E(L_\mathfrak{P})$, then there are homogeneous coordinates $P = [x, y, z]$ with $x, y, z \in \mathcal{O}_{L_\mathfrak{P}}$ so we have a modulo $\mathfrak{P}$ reduction map $E(L_\mathfrak{P}) \to \tilde{E}(\mathbb{F}_{p^f})$ given by $[x, y, z] \mapsto [\tilde{x}, \tilde{y}, \tilde{z}]$. One nice thing about this reduction map is that torsion is mostly well behaved:

Proposition 1 (Proposition 3.1 in (36))**.** *Keep all of the notation from above. Suppose that $m \geq 1$ is relatively prime to p. Suppose $\tilde{E}/\mathbb{F}_{p^f}$ is non-singular. Then the reduction map $E(L_\mathfrak{P})[m] \to \tilde{E}(\mathbb{F}_{p^f})$ is injective, where $E(L_\mathfrak{P})[m] = \{P \in L_\mathfrak{P} : [m]P = O\}$.*

One may ask what happens to the p-power torsion in the modulo $\mathfrak{P}$ reduction of E. There are two possibilities:

1. $\tilde{E}[p^r] = \{O\}$ for all $r \in \mathbb{Z}^+$

2. $\tilde{E}[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ for all $r \in \mathbb{Z}^+$.

If the first item holds then we say that E has super-singular reduction at $\mathfrak{P}$, and if the second item holds we say that E has ordinary reduction at $\mathfrak{P}$. If E/F has complex multiplication, we can say more about which situation actually occurs:

Theorem 2.7.3 (Deuring's reduction criterion (9))**.** *Let $F/\mathbb{Q}$ be a finite extension, E/F an elliptic curve with complex multiplication by $\mathcal{O}_K$, and $\mathfrak{P}$ a prime of F above p for which E has good reduction. Then E has ordinary reduction at $\mathfrak{P}$ if and only if p splits in K.*

2.8 Gauss Factorials and Exceptional Primes

In this section we define Gauss factorials and exceptional primes, as well as state some results that will be needed for the proof of Theorem 1.0.1 as well as Corollary 4. For $N, n \in \mathbb{Z}^+$ the Gauss factorial of N with respect to n is defined as

$$N_n! = \prod_{\substack{i=1 \\ \gcd(i,n)=1}}^{N} i$$

In (8), Cosgrave and Dilcher investigate multiplicative orders modulo powers of p of the following Gauss factorials

$$\left(\frac{p^\alpha - 1}{m}\right)_p !$$

where $m, \alpha \in \mathbb{Z}^+$, with m and α greater than 2, and $p \equiv 1 \pmod{m}$. If $\gamma^m_{\alpha+1}(p)$ is the multiplicative order of $\left(\frac{p^{\alpha+1}-1}{m}\right)_p !$ modulo $p^{\alpha+1}$, then Cosgrave and Dilcher define p to be α-exceptional for m if $\gamma^m_{\alpha+1}(p)$ and $\gamma^m_\alpha(p)$ are the same modulo a factor of $2^{\pm 1}$ (otherwise $\gamma^m_{\alpha+1}(p) = p\gamma^m_\alpha(p)$ or $\gamma^m_{\alpha+1}(p) = 2^{\pm 1}p\gamma^m_\alpha(p)$, see Theorem 1 and Definition 1 in (8)). Further, Theorem 3 in (8) shows that if p is α exceptional for m, then p is

also $(\alpha-1)$-exceptional for m. For our purposes, we will not need this much precision on the multiplicative orders, and we will instead use the equivalent definition:

Definition 5. *For $\alpha \in \mathbb{Z}^+$, we say that p is α-exceptional for m if and only if $\left(\frac{p^{\alpha+1}-1}{m}\right)_p^{p-1}! \equiv 1 \pmod{p^{\alpha+1}}$.*

We contrast Definition 5 with the following definition:

Definition 6. *Given an imaginary quadratic field K, we say that p is non-trivial for K if $\lambda_p(K) > 1$.*

Theorem 1.0.1 will show that the primes in Definitions 5 and 6 are the same when $m = 3$ and $K = \mathbb{Q}(\sqrt{-3})$, and when $m = 4$ and $K = \mathbb{Q}(i)$. For the other imaginary quadratic fields, a more complicated condition involving Gauss factorials will hold (see Theorem 3.1.1).

Example 1. *Let $p = 13$ and $m = 3$. Then $\gamma_1^3(13) = 12$, $\gamma_2^3(13) = 12$, $\gamma_3^3(13) = 12 \cdot 13$, $\gamma_4^3(13) = 12 \cdot 13^2$, $\gamma_5^3(13) = 12 \cdot 13^3$ and so on ("and so on" since Theorem 3 in (8) says that p is $(\alpha+1)$-exceptional for m implies p is also α-exceptional for m). The next few values of p such that $\gamma_1^3(p) = \gamma_2^3(p)$ are $p = 181, 2521, 76543$ and so on. On the other hand, if $m = 4$ and $p = 29789$, then $\gamma_2^4(p) = \frac{1}{2}\gamma_1^4(p)$, and is the only known such example for $p < 10^{11}$ (see also Table 1 in (7) for $\gamma_\alpha^4(p)$ with $1 \leq \alpha \leq 5$, $p \leq 37$ and $p \equiv 1 \pmod 4$).*

The following results of Cosgrave and Dilcher will be important later on:

Theorem 2.8.1 (Cosgrave-Dilcher (8))**.** *Let $p \equiv 1 \pmod 6$ be a prime. Then p is 1-exceptional for $m = 3$ if and only if p is 1-exceptional for $m = 6$.*

Theorem 2.8.2 (Cosgrave-Dilcher (8))**.** *Let $p \equiv 1 \pmod 6$ be a prime and $n \in \mathbb{Z}^+$. Then*

$$\left(\left(\frac{p^n-1}{3}\right)_p!\right)^{24} \equiv \left(\left(\frac{p^n-1}{6}\right)_p!\right)^{12} \pmod{p^n}.$$

Theorem 2.8.3 (Cosgrave-Dilcher (7))**.** *Every prime $p \equiv 1 \pmod 6$ that satisfies $p^2 = 3x^2 + 3x + 1$ for some $x \in \mathbb{Z}$ is 1-exceptional for $m = 3$. Equivalently, if $\gamma = 2 + \sqrt{3}$ and $q \in \mathbb{Z}^+$, then any prime of the form*

$$p = \frac{\gamma^q + \gamma^{-q}}{4}$$

is 1-exceptional for $m = 3$.

Definition 7. *We shall refer to the primes $p \equiv 1 \pmod 3$ such that $p^2 = 3x^2+3x+1$ for some $x \in \mathbb{Z}$ as Cosgrave-Dilcher primes.*

Remark 2. *In (7) and (8) Cosgrave and Dilcher rearranged the equation $p^2 = 3x^2 + 3x+1$ into $(2p)^2-3(2x+1)^2 = 1$, which can be viewed as the Pell equation $X^2-3Y^2 = 1$. It is from the theory of these equations that we obtain the primes $p = (\gamma^q+\gamma^{-q})/4$. Also, q is necessarily prime (see lemma 7 in (7)). It should be mentioned that the converse of Theorem 2.8.3 does not hold. For example, $p = 76543$ is 1-exceptional for 3 but is not a Cosgrave-Dilcher prime ($p = 76543$ is the only such example for $p < 10^{12}$). It is unknown whether or not there are infinitely many Cosgrave-Dilcher primes, and the question seems to be analogous to that of the infinitude of Fibonacci primes. In a moment we will list some new Cosgrave-Dilcher primes (see Example 2).*

Chapter 3

CONNECTION BETWEEN GAUSS FACTORIALS AND THE CYCLOTOMIC λ-INVARIANTS OF IMAGINARY QUADRATIC FIELDS

In this section we will prove Theorem 1.0.1 from which we immediately obtain as a Corollary:

Corollary 4. *Let $p \equiv 1 \pmod 6$ be a Cosgrave-Dilcher prime. Then $\lambda_p(\mathbb{Q}(\sqrt{-3})) > 1$.*

Example 2. *Using Corollary 4 we may add to the non-trivial primes of $\mathbb{Q}(\sqrt{-3})$ in Table 1 by searching for Cosgrave-Dilcher primes. The following table contains $p = (\gamma^q + \gamma^{-q})/4$ with $q \leq 79$:*

$q = 3$	$p = 13$
$q = 5$	$p = 181$
$q = 7$	$p = 2521$
$q = 11$	$p = 489061$
$q = 13$	$p = 6811741$
$q = 17$	$p = 1321442641$
$q = 19$	$p = 18405321661$
$q = 79$	$p = 381765135195632792959100810331957408101589361$

One may further verify using any standard CAS that the primes $79 < q \leq 10,000$ giving 1-exceptional primes $p = (\gamma^q + \gamma^{-q})/4$ for $m = 3$ (and therefore non-trivial primes of $\mathbb{Q}(\sqrt{-3})$) are $q = 151$, 199, 233, 251, 317, 863, 971, and $q = 3049$, 7451,

and 7487 *giving probable primes* p *(the non-trivial probable prime corresponding to* $q = 7487$ *is* 4282 *digits long).*

3.1 Proof of Main Theorems

Let d be a square-free integer, $K = \mathbb{Q}(\sqrt{-d})$, $D = 2d$ if $d \equiv 3 \pmod 4$ and $D = 4d$ otherwise. Let $p > 2$ be a prime such that $p \equiv 1 \pmod D$ with $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ and $\mathcal{P}$ be a prime in $\mathbb{Q}(\zeta_D)$ above $\mathfrak{p}$, where ζ_D is a primitive D-th root of unity. Let $\bar{\mathcal{P}}$ be the complex conjugate of $\mathcal{P}$. Denote $G = \mathrm{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q})$ and $\chi_K = \chi$ to be the imaginary quadratic character for K. We have for $x \in \mathbb{Q}(\zeta_D)$

$$\mathrm{N}_{\mathbb{Q}(\zeta_D)/K}(x) = \prod_{\substack{i=1 \\ \chi(i)=1 \\ \gcd(i,D)=1}}^{D} \sigma_i(x) \in K$$

where $\sigma_i \in G$ acts by $\sigma_i(\zeta_D) = \zeta_D^i$. We will also denote $\mathcal{P}_i = \sigma_i(\mathcal{P})$ so that $\mathrm{N}_{\mathbb{Q}(\zeta_D)/K}(\mathcal{P}_i) = \mathfrak{p}$. We will now work towards proving the following result from which Theorem 1.0.1 will follow.

Theorem 3.1.1. *Let* $K = \mathbb{Q}(\sqrt{-d})$ *be any imaginary quadratic field, and* D *be as above. Let* p *be a prime such that* $p \equiv 1 \pmod D$, $p \nmid h_K$, *and* $p \neq 3$ *whenever* $\chi_K(2) = -1$ *and* $K \neq \mathbb{Q}(\sqrt{-3})$. *Then,*

$$\lambda_p(K) > 1 \iff \left(\prod_{\substack{i=D/2 \\ \chi(i)=1 \\ \gcd(i,D)=1}}^{D} \frac{\left((D-i)\frac{p^2-1}{D}\right)_p^2!}{\left((D-i)\frac{p^2-1}{D/2}\right)_p!} \prod_{\substack{i=1 \\ \chi(i)=1 \\ \gcd(i,D)=1}}^{D/2} \frac{\left(i\frac{p^2-1}{D/2}\right)_p!}{\left(i\frac{p^2-1}{D}\right)_p^2!} \right)^{p-1} \equiv 1 \pmod{p^2}.$$

The first step of the proof is to write $\bar{\mathfrak{p}}$ in terms of Jacobi sums. Consider the multiplicative character $\psi : \mathcal{O}_{\mathbb{Q}(\zeta_D)}/\mathcal{P} \to \mathbb{C}^\times$ of order D modulo $\mathcal{P}$. We denote

$$J(\psi) = \sum_{a \in \mathbb{F}_p} \psi(a)\psi(1-a)$$

to be the Jacobi sum for ψ. Denote $0 \leq L(j) < D$ to be reduction of j modulo D, and for $1 \leq i < D/2$ we define

$$S_i(D) = \{j \,:\, 0 < j < D;\, \gcd(j, D) = 1;\, L(ji) < D/2\}.$$

Then from Theorem 2.1.14 in (1) we have

$$J(\psi^i)\mathcal{O}_{\mathbb{Q}(\zeta_D)} = \prod_{j \in S_i(D)} \mathcal{P}_{j^{-1}}.$$

Proposition 2. *Denote $h_K = h$ to be the class number for $K = \mathbb{Q}(\sqrt{-d})$. With the notation fixed above, we have*

$$\bar{\mathfrak{p}}^t = \left(\prod_{\substack{i=D/2 \\ \chi(i)=1 \\ \gcd(i,D)=1}}^{D} J(\psi^i) \Big/ \prod_{\substack{i=1 \\ \chi(i)=1 \\ \gcd(i,D)=1}}^{D/2} J(\psi^{-i}) \right) \mathcal{O}_{\mathbb{Q}(\zeta_D)}$$

where $t = \pm h(2 - \chi(2))$ if $d \neq 1$ or 3, else $t = \pm 1$. The sign of t depends on the number of quadratic residues modulo D between 1 and $D/2$.

Proof. Denote

$$a^+ = \#\{0 < j < D/2 \;\; \gcd(j, D) = 1,\, \chi(j) = 1\}$$

$$a^- = \#\{0 < j < D/2 \;\; \gcd(j, D) = 1,\, \chi(j) = -1\}.$$

It is well known that $\pm h = (a^+ - a^-)/(2 - \chi(2))$ when d is not 1 or 3 (it is easy to see what happens in those cases, so we will assume $d > 3$). If N is the norm from $\mathbb{Q}(\zeta_D)$ to K then

$$N(J(\psi^{-1}))\mathcal{O}_{\mathbb{Q}(\zeta_D)} = \prod_{\substack{j=1 \\ \gcd(j,D)=1}}^{D/2} N(\bar{\mathcal{P}}_{j^{-1}}) = \mathfrak{p}^{a^-}\bar{\mathfrak{p}}^{a^+}$$

and also $J(\psi^i)J(\psi^{-i}) = p$. Then the ideal

$$\left(\prod_{\substack{i=D/2 \\ \chi(i)=1 \\ \gcd(i,D)=1}}^{D} J(\psi^i) \Big/ \prod_{\substack{i=1 \\ \chi(i)=1 \\ \gcd(i,D)=1}}^{D/2} J(\psi^{-i}) \right) = \left(\prod_{\substack{i=D/2 \\ \chi(i)=1 \\ \gcd(i,D)=1}}^{D} J(\psi^i) \prod_{\substack{i=D/2 \\ \chi(i)=1 \\ \gcd(i,D)=1}}^{D} J(\psi^{-i}) \Big/ \prod_{\substack{i=1 \\ \chi(i)=1 \\ \gcd(i,D)=1}}^{D/2} J(\psi^i) \prod_{\substack{i=D/2 \\ \chi(i)=1 \\ \gcd(i,2m)=1}}^{D} J(\psi^{-i}) \right)$$

$$= \left(\prod_{\substack{i=D/2 \\ \chi(i)=1 \\ \gcd(i,D)=1}}^{D} p \Big/ N(J(\psi^{-1})) \right) = \frac{(\mathfrak{p}\bar{\mathfrak{p}})^{a^-}}{\mathfrak{p}^{a^-}\bar{\mathfrak{p}}^{a^+}} = \bar{\mathfrak{p}}^{\pm h(2-\chi(2))}.$$

□

Theorem 3.1.1 will now follow from Gold's criterion:

Theorem 3.1.2 (Gold's criterion (Theorem 4 in (13)))**.** *Let K be an imaginary quadratic field, and $p > 2$ be a prime such that p does not divide the class number h_K of K.*

i. If p splits in K then $\lambda_p(K) > 0$.

ii. Suppose $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ and write $\mathfrak{p}^{h_K} = (\alpha)$. Then $\lambda_p(K) > 1$ if and only if $\alpha^{p-1} \equiv 1 \pmod{\bar{\mathfrak{p}}^2}$.

Proof of Theorem 3.1.1. Suppose $p \equiv 1 \pmod{D}$. Working inside the localization $K_{\mathfrak{p}} \cong \mathbb{Q}_p$, we have $J(\psi^{-i}) \equiv \frac{\left(i\frac{p^2-1}{D/2}\right)_p!}{\left(i\frac{p^2-1}{D}\right)_p^2!} \pmod{p^2\mathbb{Z}_p}$ from (9.3.6) in (1) (which is essentially the Gross-Koblitz formula). The result now follows from Proposition 2 and Gold's criterion 3.1.2. □

We will see that the condition in Theorem 3.1.1 becomes more compact for a certain family of imaginary quadratic fields.

Definition 8. *Let $\chi_K = \chi$ be the imaginary quadratic character for K and D be as above. We say that K has maximal class number if $\chi_K(i) = 1$ for each i co-prime to D and $1 \leq i \leq D/2$.*

If h_K is the class number for $K \neq \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$, we have that $(2 - \chi(2))h_K = \left|\sum_{i=1}^{D/2} \chi(i)\right|$. Then $\chi(i) = 1$ for each i co-prime to D and $1 \leq i \leq D/2$ if and only if $h_K = \varphi(D)/2(2 - \chi(2))$.

Theorem 3.1.3. *Suppose that $p \equiv 1 \pmod{D}$ and all other notation is as above. If K has maximal class number, and $p \nmid h_K$, then*

$$\lambda_p(K) > 1 \iff \left(\frac{\left(\frac{p^2-1}{D}\right)_p^2 !}{\left(\frac{p^2-1}{D/2}\right)_p !} \right)^{p-1} \equiv 1 \pmod{p^2}.$$

Proof. Here we will view $K \subseteq K_{\mathfrak{p}} \cong \mathbb{Q}_p$. If K has maximal class number, then $S_1(D)$ accounts for all of the quadratic residues between 1 and $D/2$, and so $J(\psi^{-1}) \in N(\bar{\mathcal{P}}) = \bar{\mathfrak{p}}$. Therefore, if $\bar{\mathfrak{p}}^{h_K} = (\alpha)$ for some $\alpha \in K$, we have $J(\psi^{-1})^{h_K} \equiv \alpha u \pmod{p^2\mathbb{Z}_p}$ where $u \in \mathcal{O}_K^\times$. Now, since $p \nmid h_K$ we have $J(\psi^{-1})^{h_K(p-1)} \equiv 1 \pmod{p^2\mathbb{Z}_p}$ if and only if $J(\psi^{-1})^{(p-1)} \equiv 1 \pmod{p^2\mathbb{Z}_p}$. The result now follows from Gold's criterion and the fact that $u^{p-1} = 1$. □

Remark 3. *When $D = 6$, the combination of Theorems 2.8.1 and 2.8.2 imply that $\lambda_p(\mathbb{Q}(\sqrt{-3})) > 1$ if and only if p is 1-exceptional for $m = 3$. When $D = 4$, we have that $\left(\frac{p^2-1}{2}\right)_p^{p-1} ! \equiv 1 \pmod{p^2}$ (a corollary of Wilson's theorem), so $\lambda_p(\mathbb{Q}(i)) > 1$ if and only if p is 1-exceptional for $m = 4$.*

Theorem 1.0.1 now follows as a special case of Theorem 3.1.3. Computations show that $K = \mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-5})$ and $\mathbb{Q}(\sqrt{-6})$ are the only imaginary

quadratic fields $K = \mathbb{Q}(\sqrt{-d})$ with $d < 10,000$ having maximal class number. In fact,

Theorem 3.1.4. *Assuming the generalized Riemann hypothesis (GRH) holds for every non-principle primitive imaginary quadratic character, the only imaginary quadratic fields with maximal class number are* $K = \mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-5})$ *and* $\mathbb{Q}(\sqrt{-6})$.

Proof. Let $d > 0$ be a square free integer and let D and $\chi_D = \chi$ be as above. Denote $K = \mathbb{Q}(\sqrt{-d})$ and h_K to be the class number of K, and assume that $h_K = \varphi(D)/2(2 - \chi(2))$ (i.e. h_K is maximal). From Theorem 15 in (31), we have

$$\varphi(D) > \frac{D}{e^{\gamma} \log\log(D) + \frac{3}{\log\log(D)}}$$

where $e = \exp(1)$ and $\gamma = 0.577215665...$ is Euler's constant. On the other hand, under the assumption of the generalized Riemann hypothesis, Littlewood (30) gave the inequality $h_K < ce^{\gamma} \log\log(D)\sqrt{D}$, where c is an absolute constant. Recently, this bound has been improved (see (25) and (26)) to

$$h_K \leq \frac{2e^{\gamma}}{\pi}\sqrt{D}\left(\log\log(D) - \log(2) + \frac{1}{2} + \frac{1}{\log\log(D)}\right)$$

for $D \geq 5$, and assuming GRH holds. Thus, when h_K is maximal and $D \geq 5$, the two inequalities above imply

$$\sqrt{D} < \frac{12e^{\gamma}}{\pi}\left(e^{\gamma}(\log\log(D))^2 + \frac{3}{(\log\log(D))^2} + e^{\gamma} + 3\right) < 14(\log\log(D))^2 + 140.$$

This inequality does not hold for long. Indeed, set $f(x) = \sqrt{x} - 14(\log\log(x))^2 + 140$ and notice that $f'(x) = \frac{1}{2\sqrt{x}} - \frac{28\log\log(x)}{x\log(x)} > 0$ precisely when $x\log(x) > 56\sqrt{x}\log\log(x)$, which will eventually hold for all x sufficiently large (e.g. for all $x > 300$). Therefore,

we have that $f(x)$ is strictly increasing on $[300, \infty)$. We also have that $f(300) > 0$, so the inequality $\sqrt{D} > 14(\log\log(D))^2 + 140$ holds for all $D > 300$. Therefore, there are no imaginary quadratic fields with $D > 300$ having maximal class number. It is easy to check that the only imaginary quadratic fields with $D \leq 300$ and maximal class number are the ones listed above. □

3.2 Proof of Corollaries

We now turn to the proofs of Corollaries 1, 2 and 3 for which we will need some preliminary results. For a co-prime to p the Fermat quotient is defined as $q_p(a) = (a^{p-1} - 1)/p$, which is an integer by Fermat's little Theorem. The Fermat quotient has logarithmic properties, that is, for a and b co-prime to p,

$$q_p(a) + q_p(b) \equiv q_p(ab) \pmod{p} \quad \text{and} \quad q_p(a) - q_p(b) \equiv q_p(a/b) \pmod{p}$$

as well as

$$q_p(a+p) \equiv q_p(a) - \frac{1}{a} \pmod{p}.$$

Denote $H_n = \sum_{a=1}^{n} 1/a$ to be the n-th harmonic number and $w_p = ((p-1)! + 1)/p$ to be the Wilson quotient (also an integer by Wilson's Theorem). It is well known that $w_p \equiv \sum_{a=1}^{p-1} q_p(a) \pmod{p}$.

Lemma 1. *Let $p > 2$ be a prime. For any $b \in (\mathbb{Z}/p^2\mathbb{Z})^\times$ such that $b = b_0 + b_1 p$ with $1 \leq b_0 \leq p-1$ and $0 \leq b_1 \leq p-1$, we can write $b \equiv b_0^p \left(1 + \left(\frac{b_1}{b_0} - q_p(b_0)\right) p\right) \pmod{p^2}$.*

Proof. Let $b \in (\mathbb{Z}/p^2\mathbb{Z})^\times$ such that $b = b_0 + b_1 p$ with $1 \leq b_0 \leq p-1$ and $0 \leq b_1 \leq p-1$. Then setting $x = b_1/b_0$, we see that $1 + px \equiv (pq_p(b_0) + 1)(1 + px - pq_p(b_0)) \pmod{p^2}$. Since $b_0^{p-1} = 1 + pq_p(b_0)$, we obtain the result by multiplying through by b_0. □

Proposition 3. *Suppose $m \in \mathbb{Z}$ with $m \geq 2$ and $p \equiv 1 \pmod{m}$ is a prime. Then*

$$\left(\frac{p^2-1}{m}\right)_p^{p-1}! \equiv 1 \pmod{p^2} \iff \frac{1}{m}(w_p - H_{\frac{p-1}{m}}) - \sum_{a=1}^{\frac{p-1}{m}} q_p(a) \equiv 0 \pmod{p}.$$

Proof. Using Lemma 1, we have

$$\begin{aligned}\left(\frac{p^2-1}{m}\right)_p^{p-1}! &= \prod_{\substack{a=1 \\ \gcd(a,p)=1}}^{\frac{p^2-1}{m}} a^{p-1} = \left(\prod_{a=1}^{p-1}\prod_{b=0}^{\frac{p-1}{m}-1}(a+bp)^{p-1}\right)\left(\prod_{a=1}^{\frac{p-1}{m}}\left(a+\frac{p-1}{m}p\right)^{p-1}\right) \\ &\equiv \left(\prod_{a=1}^{p-1}\prod_{b=0}^{\frac{p-1}{m}-1}\left(1+\left(\frac{b}{a}-q_p(a)\right)p\right)\right)\left(\prod_{a=1}^{\frac{p-1}{m}}\left(1+\left(\frac{\frac{p-1}{m}}{a}-q_p(a)\right)p\right)\right) \\ &\equiv \left(\prod_{a=1}^{p-1}\prod_{b=0}^{\frac{p-1}{m}-1}(1+p)^{\frac{b}{a}-q_p(a)}\right)\left(\prod_{a=1}^{\frac{p-1}{m}}(1+p)^{\frac{\frac{p-1}{m}}{a}-q_p(a)}\right) \pmod{p^2}.\end{aligned}$$

Combining all the factors of $(1+p)$ we get the desired sum in the exponent which is taken modulo p (since $1+p$ is a p-th root of unity modulo p^2). It is known that $H_{p-1} \equiv 0 \pmod{p}$. Hence, $\sum_{a=1}^{p-1}\sum_{b=0}^{\frac{p-1}{m}-1}\frac{b}{a} \equiv 0 \pmod{p}$. The result now follows. $\square$

Recall that the Bernoulli numbers $\{B_n\}$ and the Bernoulli polynomials $\{B_n(t)\}$ are defined by

$$\sum_{n=0}^{\infty} B_n \frac{x^n}{n!} = \frac{x}{e^x-1} \quad \text{and} \quad \sum_{n=0}^{\infty} B_n(t)\frac{x^n}{n!} = \frac{xe^{xt}}{e^x-1}.$$

Lemma 2. *Let p be a prime such that $p \equiv 1 \pmod{2m}$. Then*

$$\left(\frac{\left(\frac{p^2-1}{m}\right)_p!}{\left(\frac{p^2-1}{2m}\right)_p^2!}\right)^{p-1} \equiv 1 \pmod{p^2} \iff \frac{B_p(1/m) - 2^p B_p(1/2m)}{p^2} \equiv 0 \pmod{p}.$$

Proof. For any $n \in \mathbb{Z}^+$ with $p \equiv 1 \pmod{n}$, we use the relation $B_p(x+1) - B_p(x) = px^{p-1}$ along with the properties of the Fermat quotient to obtain

$$\sum_{a=1}^{\frac{p-1}{n}} q_p(a) \equiv \left(\frac{n^{p-1}}{p}\left(\frac{p^2}{n}B_{p-1} - B_p(1/n)\right) - \frac{p-1}{n}\right) + \frac{1}{n}q_p(n) - \frac{1}{n}H_{\frac{p-1}{n}} \pmod{p}.$$

Then for $p \equiv 1 \pmod{2m}$, a straightforward computation gives

$$\sum_{a=1}^{\frac{p-1}{m}} q_p(a) - 2\sum_{a=1}^{\frac{p-1}{2m}} q_p(a) \equiv -\frac{B_p(1/m) - 2^p B_p(1/2m)}{p^2} - \frac{1}{m} H_{\frac{p-1}{m}} + \frac{1}{m} H_{\frac{p-1}{2m}} \pmod{p}.$$

From Proposition 3 we know that $\left(\frac{\left(\frac{p^2-1}{m}\right)_p^!}{\left(\frac{p^2-1}{2m}\right)_p^{2!}} \right)^{p-1} \equiv (1+p)^{\xi} \pmod{p^2}$, where

$$\begin{aligned} \xi &= \frac{1}{m}(w_p - H_{\frac{p-1}{m}}) - \sum_{a=1}^{\frac{p-1}{m}} q_p(a) - 2\left(\frac{1}{2m}(w_p - H_{\frac{p-1}{2m}}) - \sum_{a=1}^{\frac{p-1}{2m}} q_p(a) \right) \\ &\equiv -\frac{B_p(1/m) - 2^p B_p(1/2m)}{p^2} \pmod{p}. \end{aligned}$$

The result now follows. □

Corollary 1] is an immediate consequence of Lemma 2. We also have,

Proof of Corollary 2. Let $p \equiv 1 \pmod 4$. We have seen from Lemma 2 that p is 1-exceptional for 4 if and only if $B_p(1/2) - 2^p B_p(1/4) \equiv 0 \pmod{p^3}$. But from (28) we know that $B_p(1/2) = 0$ and $B_p(1/4) = -pE_{p-1}/4^p$. Corollary 2 now follows from Theorem 1.0.1. □

Remark 4. *The proof also shows that* $E_{p-1} \equiv 0 \pmod p$ *when* $p \equiv 1 \pmod 4$*, although this was already observed by Zhang in (41).*

The proof of Corollary 3 will be similar to that of Corollary 2, but will instead involve the Glaisher numbers $\{G_n\}$. Since these numbers are less well known we will take a moment to view some of their properties. In particular, we will see that for odd $n \geq 1$, $B_n(1/3) = -(n+1)G_{n-1}/3^{n-1}$. Recall the Glaisher numbers $\{G_n\}$ are defined by

$$\frac{3/2}{e^x + e^{-x} + 1} = \sum_{n=0}^{\infty} G_n \frac{x^n}{n!}.$$

Notice that $2\sum_{n=0}^{\infty} G_{2n+1}\frac{x^{2n+1}}{(2n+1)!} = \sum_{n=0}^{\infty} G_n\frac{x^n}{n!} - \sum_{n=0}^{\infty} G_n\frac{(-x)^n}{n!} = 0$ so that $G_n = 0$ whenever n is odd, and $\sum_{n=0}^{\infty} G_n\frac{x^n}{n!} = \sum_{n=0}^{\infty} G_{2n}\frac{x^{2n}}{(2n)!}$. We also know from (15) that G_n can only have powers of 3 in the denominator.

Example 3. *In the following table we list all primes* $p \equiv 1 \pmod 3$ *and* $7 \leq p \leq 193$ *in the first column, along with the reduced values of* $G_{p-1} \pmod p$ *in the second column and* $G_{p-1} \pmod{p^2}$ *in the third column:*

7	0	42	97	0	1940
13	0	0	103	0	1133
19	0	342	109	0	7521
31	0	434	127	0	16002
37	0	1332	139	0	5282
43	0	559	151	0	15855
61	0	3660	157	0	785
67	0	3685	163	0	24939
73	0	803	181	0	0
79	0	2844	193	0	26441

Notice that 13 *and* 181 *are the first two* 1*-exceptional primes for* $m = 3$. *It also appears that* $G_{p-1} \equiv 0 \pmod p$ *for all* $p \equiv 1 \pmod 3$, *which we will soon see is true.*

We will now show that $B_n(1/3) = -(n+1)G_{n-1}/3^{n-1}$ for odd $n \geq 1$. It should be noted that this result is already known (see page 352 in (28)), but not commonly

stated or proven in the literature. Observe that

$$\frac{-x}{e^{\frac{1}{3}x}+e^{-\frac{1}{3}x}+1} = -\frac{2}{3}x\frac{3/2}{e^{\frac{1}{3}x}+e^{-\frac{1}{3}x}+1} = -\frac{2}{3}x\sum_{n=0}^{\infty}G_{2n}\frac{\left(\frac{1}{3}x\right)^{2n}}{(2n)!}$$
$$= 2\sum_{n=0}^{\infty}-\frac{(2n+1)G_{2n}}{3^{2n+1}}\frac{x^{2n+1}}{(2n+1)!}$$

and at the same time

$$2\sum_{n=0}^{\infty}B_{2n+1}(1/3)\frac{x^{2n+1}}{(2n+1)!} = \frac{x(e^{\frac{1}{3}x}-e^{\frac{2}{3}x})}{e^x-1} = \frac{xe^{\frac{1}{3}x}(1-e^{\frac{1}{3}x})}{(e^{\frac{1}{3}x}-1)(e^{\frac{2}{3}x}+e^{\frac{1}{3}x}+1)} = \frac{-x}{e^{\frac{1}{3}x}+e^{-\frac{1}{3}x}+1}$$

Therefore,

$$\sum_{n=0}^{\infty}-\frac{(2n+1)G_{2n}}{3^{2n+1}}\frac{x^{2n+1}}{(2n+1)!} = \sum_{n=0}^{\infty}B_{2n+1}(1/3)\frac{x^{2n+1}}{(2n+1)!}$$

which implies,

$$B_{2n+1}(1/3) = -\frac{(2n+1)G_{2n}}{3^{2n+1}}.$$

For $k, n \in \mathbb{Z}^+$, we also have Raabe's multiplication formula $B_n(kx) = k^{n-1}\sum_{j=0}^{n-1}B_n(x+j/k)$. So, with $x = 1/6$ and $k = 2$ we have

$$B_{2n+1}(1/6) = \frac{2^{2n}+1}{2^{2n}}B_{2n+1}(1/3)$$

Proof of Corollary 3. Let $p \equiv 1 \pmod 3$. Then from Lemma 2 p is 1-exceptional for $m = 3$ if and only if

$$\frac{B_p(1/3)-2^pB_p(1/6)}{p^2} = -\frac{(1+2^p)B_p(1/3)}{p^2} = \left(\frac{1+2^p}{3^p}\right)\frac{G_{p-1}}{p} \equiv 0 \pmod p.$$

The result now follows from Theorem 1.0.1. □

Remark 5. *From the proof of Corollary 3 we also have that* $G_{p-1} \equiv 0 \pmod p$ *for all primes* $p \equiv 1 \pmod 3$.

Chapter 4

CM ELLIPTIC CURVES AND THE CYCLOTOMIC λ-INVARIANTS OF IMAGINARY QUADRATIC FIELDS

Let K be an imaginary quadratic field, and fix a prime $p > 3$ that does not divide the class number of K. In this section we prove that $\lambda_p(K) > 1$ if and only if the number of points on a certain reduced elliptic curve is divisible by p^2.

4.1 Introduction

Let $p > 3$ be a prime and K be an imaginary quadratic field such that p does not divide the class number of K, which we denote by h_K, and also write $Cl(K)$ to be the class group of K. We will always assume that $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. Denote $\lambda_p(K)$ to be Iwasawa's λ-invariant for the cyclotomic $\mathbb{Z}_p$-extension of K. It is well known that $\lambda_p(K) > 0$ when p splits in K. We will consider an elliptic curve E that has complex multiplication by $\mathcal{O}_K$, i.e. $\mathrm{End}(E) \cong \mathcal{O}_K$. For any elliptic curve E and $m \in \mathbb{Z}$, we let $E[m] = \{P \in E(\bar{K}) : [m]P = O\}$ denote the m-torsion points of E (as usual, $\bar{K}$ is the algebraic closure of K). From the theory of complex multiplication, we can obtain Abelian extensions of K by essentially adjoining the torsion points of E. More precisely, if F/K is an abelian extension, then there exists some $m \in \mathbb{Z}^+$ such that

$$F \subseteq K(j(E), E[m]) = K(j(E), \{x, y \in \bar{K} : (x, y) \in E[m]\})$$

where $j(E)$ is the j-invariant of E. Something interesting happens when we adjoin the x-coordinates of the torsion points of E. Consider the Webber function $\Phi : E[m] \to \bar{K}$

given by

$$\Phi(x,y) = \begin{cases} x^2 & \text{if } K = \mathbb{Q}(i) \\ x^3 & \text{if } K = \mathbb{Q}(\sqrt{-3}) \\ x & \text{else} \end{cases}$$

Since E has complex multiplication by $\mathcal{O}_K$, we may also define for a fractional ideal $\mathfrak{c}$ of K, the $\mathfrak{c}$-torsion points of E,

$$E[\mathfrak{c}] = \{P \in E(\bar{K}) \,:\, [\alpha]P = O \text{ for all } \alpha \in \mathfrak{c}\},$$

and the abelian extension $K(j(E), \Phi(E[\mathfrak{c}]))/K$, where

$$K(j(E), \Phi(E[\mathfrak{c}])) = K(j(E), \{\Phi(P) \,:\, P \in E[\mathfrak{c}]\}).$$

Then we have that $K(j(E), \Phi(E[\mathfrak{c}]))$ is the ray class field of K modulo $\mathfrak{c}$.

Let $\mathfrak{P}$ be a prime of $K(j(E), E[\bar{\mathfrak{p}}^2])$ above $\mathfrak{p}$ for which E has good reduction, and denote $\tilde{E}$ to be the reduction of E modulo $\mathfrak{P}$. Here is the main result of this section, which we will prove in 4.4:

Theorem 4.1.1. *With the notation fixed above, we have $\lambda_p(K) > 1$ if and only if $\#\tilde{E}(\mathbb{F}_q) \equiv 0 \pmod{p^2}$, where $q = p^{p-1}$.*

While $\#\tilde{E}(\mathbb{F}_q)$ may be difficult to compute modulo p^2, there is a relatively efficient way to check if $\lambda_p(K) > 1$ (see Theorem 3.1.2, and (13)). So, Theorem 4.1.1 may be seen as an efficient way to check the p^2 divisibility of the number of points of certain elliptic curves over finite fields. That is,

Corollary 5. *Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field, $p > 3$ such that $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, and $r \in \mathbb{Z}^+$ such that $\mathfrak{p}^r$ is principle. Then we can write $p^r = a^2 + b^2 d$ for*

some $a, b \in \mathbb{Z}$. Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$, denote $\mathfrak{P}$ to be a prime of $K(j(E), E[\bar{\mathfrak{p}}^2])$ above $\mathfrak{p}$ for which E has good reduction, and $\tilde{E}$ to be the reduction of E modulo $\mathfrak{P}$. Then $\#\tilde{E}(\mathbb{F}_{p^{p-1}}) \equiv 0 \pmod{p^2}$ if and only if $(2a)^{p-1} \equiv 1 \pmod{p^2}$.

4.2 A Few Examples

Before we get to the proof of Theorem 4.1.1, let us first check some computations. Given a prime $p > 3$, we will denote $q = p^{p-1}$. In the following example, each field K has class number 1, so the corresponding elliptic curves with complex multiplication by $\mathcal{O}_K$ are defined over $\mathbb{Q}$. Therefore, we may reduce each curve by the rational prime p. One should compare the data in the following tables with Table 1 in (10).

$K = \mathbb{Q}(\sqrt{-3})$

$E : y^2 = x^3 - 1$

$3 < p < 70$ such that p splits in K	$\#\tilde{E}(\mathbb{F}_q) \pmod{p^2}$
7	42
13	0
19	342
31	527
37	1332
43	559
61	3660
67	3685

$K = \mathbb{Q}(\sqrt{-11})$

$E : y^2 = x^3 - 264x - 1694$

$3 < p < 70$ such that p splits in K	$\#\tilde{E}(\mathbb{F}_q) \pmod{p^2}$
5	0
23	230
31	527
47	1222
53	1007
59	59
67	1340

$K = \mathbb{Q}(\sqrt{-19})$

$E : y^2 = x^3 - 608x - 5776$

$3 < p < 70$ such that p splits in K	$\#\tilde{E}(\mathbb{F}_q) \pmod{p^2}$
5	20
7	28
11	0
17	102
23	506
43	1806
47	893
61	3355

4.3 Some Preliminary Results

The main idea for the proof of Theorem 4.1.1 is that $\lambda_p(K) > 1$ if and only if $\mathfrak{p}$ splits in an extension of K obtained by adding some of the $\bar{\mathfrak{p}}^2$ torsion points of E, that is, the p-ray class field of K modulo $\bar{\mathfrak{p}}^2$. This fact was proven in (13), which we reformulate as,

Proposition 4 (Gold)**.** *Let H be the p-ray class field modulo $\bar{\mathfrak{p}}^2$, and $\sigma_{\mathfrak{p}} \in Gal(H/K)$ the image of $\mathfrak{p}$ under the Artin map. Then $\lambda_p(K) > 1$ if and only if $\sigma_{\mathfrak{p}} = 1$.*

Proof. From Theorem 3, and the proof of Theorem 4 in (13), we have that $\lambda_p(K) > 1$ if and only if $\mathfrak{p}$ splits in H/K. Since $[H : K] = p$, the prime $\mathfrak{p}$ splits in H/K if and only if it splits completely in H/K. The Proposition now follows. □

For the remainder of this section we will assume that $E/K(j(E))$ is an elliptic curve with complex multiplication by $\mathcal{O}_K$, and that $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. Denote H to be the p-ray class field of K, and $\widetilde{K} = K(j(E), E[\bar{\mathfrak{p}}^2])$. Let $g_{\mathfrak{p}}$ denote the order of the class of $\mathfrak{p}$ in $Cl(K)$, and let $\mathfrak{P}$ be a prime of $\widetilde{K}$ above $\mathfrak{p}$. Consider $\mathcal{E}(K)$, the isomorphism classes of elliptic curves with complex multiplication by $\mathcal{O}_K$. If $L = K(j(E))$ (which is the Hilbert class field of K), then there is an action of the class group $Cl(K) \cong \mathrm{Gal}(L/K)$ on $\mathcal{E}(K)$. Indeed, if E represents a class in $\mathcal{E}(K)$, with $E \cong \mathbb{C}/\mathcal{L}$ for some lattice in $\mathbb{C}$, then the action of $Cl(K)$ is determined by $\mathfrak{a} * E \cong \mathbb{C}/\mathfrak{a}^{-1}\mathcal{L}$, which again represents a class in $\mathcal{E}(K)$ (see Proposition 1.2 in Chapter II of (35)). On the other hand, if E/L is given by the Weierstrass equation $E : y^2 = x^3 + Ax + B$, then $\tau \in \mathrm{Gal}(\bar{K}/K)$ acts on E by $E^\tau : y^2 = x^3 + \tau(A)x + \tau(B)$. In fact, there is a well defined map $F : \mathrm{Gal}(\bar{K}/K) \to Cl(K)$, such that $E^\tau = F(\tau) * E$, which factors as

$$F : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Gal}(L/K) \to Cl(K)$$

where the first map is restriction to L, and the second is the inverse of the Artin map.

We now seek to understand how certain p-power torsion points of E reduce modulo $\mathfrak{P}$. To that end, we have the following:

Theorem 4.3.1 (Deuring's reduction criterion (9))**.** *Let $F/\mathbb{Q}$ be a finite extension, E/F an elliptic curve with complex multiplication by $\mathcal{O}_K$, and $\mathfrak{P}$ a prime of F above p for which E has good reduction. Then E has ordinary reduction at $\mathfrak{P}$ if and only if p splits in K.*

Lemma 3. *Let $E/K(j(E))$ be an elliptic curve with complex multiplication by $\mathcal{O}_K$, and let $r \in \mathbb{Z}^+$. If $\mathfrak{P}$ is a prime of $\widetilde{K}$ above $\mathfrak{p}$ such that E has good reduction at $\mathfrak{P}$, then,*

a. $E[p^r] \cong E[\mathfrak{p}^r] \oplus E[\bar{\mathfrak{p}}^r]$.

b. The reduction modulo $\mathfrak{P}$ map $E[\bar{\mathfrak{p}}^r] \to \tilde{E}[p^r]$ is an isomorphism.

Proof. Proof of (a): Let $P \in E[\mathfrak{p}^r]$. Since $p^r \in \mathfrak{p}^r\bar{\mathfrak{p}}^r$, we have $p^r = \sum \alpha_i\bar{\alpha}_i$, where $\alpha_i \in \mathfrak{p}^r$ and $\bar{\alpha}_i \in \bar{\mathfrak{p}}^r$. Then

$$[p^r]P = \left[\sum \alpha_i\bar{\alpha}_i\right] P = \sum [\bar{\alpha}_i]([\alpha_i]P) = \sum [\bar{\alpha}_i]O = O$$

so that $P \in E[p^r]$. Similarly, $E[\bar{\mathfrak{p}}^r] \subseteq E[p^r]$. From Proposition 1.4 in Chapter II of (35), we have that both $E[\mathfrak{p}^r]$ and $E[\bar{\mathfrak{p}}^r]$ are free $\mathcal{O}_K/\mathfrak{p}^r$-modules of rank 1. Hence $E[\mathfrak{p}^r] \cong E[\bar{\mathfrak{p}}^r] \cong \mathbb{Z}/p^r\mathbb{Z}$. Now let t be a multiple of h_K. Then we have that $\mathfrak{p}^t = (a + bi)$ and $\bar{\mathfrak{p}}^t = (a - bi)$, for some $a, b \in \mathbb{Z}$. Suppose that there is $P \in E[p^t]$ such that $[a + bi]P = [a - bi]P$. Then $[bi]P = [-bi]P$, which is only possible if $[bi]P = O$, which in turn is only possible if $P = O$, since b is co-prime to p. Hence, $E[\mathfrak{p}^t] \cap E[\bar{\mathfrak{p}}^t] = \{O\}$, and since $E[\mathfrak{p}^r] \subseteq E[p^t]$, we have $E[\mathfrak{p}^r] \cap E[\bar{\mathfrak{p}}^r] = \{O\}$ for all

positive integers $r < t$. This now holds for all $r \in \mathbb{Z}^+$ since t can be made arbitrarily large. Part (a) now follows.

Proof of (b): Before the proof, recall that if L/F is Galois with $\mathfrak{Q}$ a prime of L above a prime $\mathfrak{q}$ of F, then we have the decomposition subgroup with respect to $\mathfrak{Q}/\mathfrak{q}$

$$Z(\mathfrak{Q}/\mathfrak{q}) = \{\sigma \in \mathrm{Gal}(L/F) \,:\, \sigma\mathfrak{Q} = \mathfrak{Q}\}$$

and the inertia group with respect to $\mathfrak{Q}/\mathfrak{q}$

$$T(\mathfrak{Q}/\mathfrak{q}) = \{\sigma \in Z(\mathfrak{Q}/\mathfrak{q}) \,:\, \sigma(x) \equiv x \pmod{\mathfrak{Q}} \text{ for all } x \in L\}.$$

If $G(\mathfrak{Q}/\mathfrak{q}) = \mathrm{Gal}(\mathcal{O}_L/\mathfrak{Q}/\mathcal{O}_F/\mathfrak{q})$, then we have a map $Z(\mathfrak{Q}/\mathfrak{q}) \to G(\mathfrak{Q}/\mathfrak{q})$, given by

$$\sigma \mapsto \bar{\sigma} : x + \mathfrak{Q} \mapsto \sigma(x) + \mathfrak{Q}.$$

Now, back to the proof. Consider $\widetilde{L} = K(j(E), E[p^{g_\mathfrak{p}}])$, and $L = K(j(E))$. The field $\widetilde{K} \subseteq \widetilde{L}$ will be as it was defined above. Let $\mathcal{P}$ be a prime of L above $\mathfrak{p}$, and $\mathscr{P}$ be a prime of $\widetilde{L}$ above $\mathcal{P}$. Let $\tau_\mathfrak{p} \in \mathrm{Gal}(L/K)$ be the image of $\mathfrak{p}$ under the Artin map, and $\tau \in \mathrm{Gal}(\widetilde{L}/K)$ such that τ maps to the Frobenius automorphism in $G(\mathscr{P}/\mathfrak{p})$. Thus, $\tau|_L = \tau_\mathfrak{p}$, and $E^{\tau^{g_\mathfrak{p}}} = F(\tau^{g_\mathfrak{p}}) * E = \mathfrak{p}^{g_\mathfrak{p}} * E$. Then $\tau^{g_\mathfrak{p}}$ induces an isogeny $\eta : E \to E$ that gives rise to the commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{[\alpha]} & E \\ \downarrow & & \downarrow \\ \tilde{E} & \xrightarrow{\varphi} & \tilde{E} \end{array}$$

where $\tilde{E}$ is the reduction of $E(\widetilde{L})$ modulo $\mathscr{P}$, the map φ is the $p^{g_\mathfrak{p}}$-th power Frobenius, and $\mathfrak{p}^{g_\mathfrak{p}} = (\alpha)$ (see Theorem 5.3 and Corollary 5.4 in (35)). Since $E[\mathfrak{p}^{g_\mathfrak{p}}] = \ker[\alpha]$, we have that $\tilde{E}[\mathfrak{p}^{g_\mathfrak{p}}] \subseteq \ker\varphi$, so that $\tilde{E}[\mathfrak{p}^{g_\mathfrak{p}}]$ is trivial. But by Deuring's reduction criterion 4.3.1, we have that $\tilde{E}[p^{g_\mathfrak{p}}] \cong \mathbb{Z}/p^{g_\mathfrak{p}}\mathbb{Z}$. So it must be that $\tilde{E}[p^{g_\mathfrak{p}}] = \tilde{E}[\bar{\mathfrak{p}}^{g_\mathfrak{p}}]$. Now, for

a positive integer $r < g_{\mathfrak{p}}$, define $\widetilde{K}_r = K(j(E), E[\bar{\mathfrak{p}}^r]) \subseteq \widetilde{L}$, and let $\mathfrak{P}_r = \mathscr{P} \cap \widetilde{K}_r$. Notice we can view any $P \in E(\widetilde{K}_r)$ an element of $E(\widetilde{L})$. Therefore, the reduction of P modulo $\mathscr{P}$ is the same as reduction modulo $\mathfrak{P}_r$. We now have the commutative diagram

$$\begin{array}{ccc} E(\widetilde{K}_r) & \longrightarrow & E(\widetilde{L}) \\ {\scriptstyle (\mathrm{mod}\ \mathfrak{P}_r)}\downarrow & & \downarrow{\scriptstyle (\mathrm{mod}\ \mathscr{P})} \\ \tilde{E}(\mathcal{O}_{\widetilde{K}_r}/\mathfrak{P}_r) & \longrightarrow & \tilde{E}(\mathcal{O}_{\widetilde{L}}/\mathscr{P}) \end{array}$$

where the horizontal maps are inclusion, and the vertical maps are reduction modulo $\mathfrak{P}_r$ and $\mathscr{P}$ respectively. From this diagram, we see that $E[\bar{\mathfrak{p}}^r] \subseteq E[\bar{\mathfrak{p}}^{g_{\mathfrak{p}}}]$ is non-trivial modulo $\mathscr{P}$, so $E[\bar{\mathfrak{p}}^r]$ is non-trivial modulo $\mathfrak{P}_r$. □

4.4 Proof of Theorem 4.1.1

Proof of Theorem 4.1.1. As before, let H be the p-ray class group of K modulo $\mathfrak{p}^2$, denote $\widetilde{K} = K(j(E), E[\bar{\mathfrak{p}}^2])$, $\mathscr{P}$ a prime of H above $\mathfrak{p}$, and $\mathfrak{P}$ a prime of $\widetilde{K}$ above $\mathscr{P}$. We have the following commutative diagram,

$$\begin{array}{ccccccccc} 1 & \longrightarrow & T(\mathfrak{P}/\mathfrak{p}) & \longrightarrow & Z(\mathfrak{P}/\mathfrak{p}) & \longrightarrow & G(\mathfrak{P}/\mathfrak{p}) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & T(\mathscr{P}/\mathfrak{p}) & \longrightarrow & Z(\mathscr{P}/\mathfrak{p}) & \longrightarrow & G(\mathscr{P}/\mathfrak{p}) & \longrightarrow & 1 \end{array}$$

where the vertical maps are restriction from $\widetilde{K}$ to H. Let $\tau \in Z(\mathfrak{P}/\mathfrak{p})$ be a lift of $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p}) \in G(\mathfrak{P}/\mathfrak{p})$, and $\bar{\tau} \in \mathrm{Gal}(K(E[\bar{\mathfrak{p}}^2])/K)$ the restriction of τ to $\widetilde{H} = K(E[\bar{\mathfrak{p}}^2])$. Then $\bar{\tau}|_H = \sigma_{\mathfrak{p}}$. From Lemma 3 we have another commutative diagram

$$\begin{array}{ccc} E[\bar{\mathfrak{p}}^2] & \xrightarrow{\bar{\tau}} & E[\bar{\mathfrak{p}}^2] \\ \cong\downarrow & & \downarrow\cong \\ \tilde{E}[p^2] & \xrightarrow{\varphi} & \tilde{E}[p^2] \end{array}$$

where φ is the p-power Frobenius automorphism. Let $\widetilde{\mathfrak{P}} = \mathfrak{P} \cap \mathcal{O}_{\widetilde{H}}$. Then the reduction of $E[\bar{\mathfrak{p}}^2]$ modulo $\mathfrak{P}$ is the same as reduction modulo $\widetilde{\mathfrak{P}}$. If $f = [\mathcal{O}_{\widetilde{H}}/\widetilde{\mathfrak{P}} : \mathcal{O}_K/\mathfrak{p}] > 1$, then for any positive integer $a < f$, we have that $\bar{\tau}^a$ will act non-trivially on $E[\bar{\mathfrak{p}}^2]$.

Assume that $\lambda_p(K) > 1$. Then $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(H/K)$ is trivial by Proposition 4, and from the proof of Theorem 2.3 in Chapter II of (35), we have that $[\widetilde{H} : K]$ divides $p(p-1)$. Thus, f divides $p-1$ so that $\bar{\tau}^{p-1}$ acts trivially on $E[\bar{\mathfrak{p}}^2]$. From the commutative diagram, we then have that the p^{p-1}-power Frobenius fixes $\tilde{E}[p^2]$, which gives the forward implication.

Now assume that $\sigma_{\mathfrak{p}}$ is non-trivial in $\mathrm{Gal}(H/K)$ (i.e. $\lambda_p(K) \leq 1$). Then, $\mathfrak{p}$ is unramified and does not split in H/K. Hence, the residue degree of $\mathfrak{p}$ in H/K is p, and $f \geq p > p-1$. So, $\bar{\tau}^{p-1}$ does not act trivially on $E[\bar{\mathfrak{p}}^2]$, hence the p^{p-1}-power Frobenius does not act trivially on $\tilde{E}[p^2]$. This gives the reverse implication. □

4.5 Some Special Cases

From the results in the previous section, we now have:

Theorem 4.5.1. *Let $p \equiv 1 \pmod 3$, and consider $E/\mathbb{F}_p : y^2 = x^3 - 1$. Then p is 1-exceptional for $m = 3$ if and only if $G_{p-1} \equiv 0 \pmod{p^2}$ if and only if $\#E(\mathbb{F}_q) \equiv 0 \pmod{p^2}$, where $q = p^{p-1}$, and $\{G_n\}$ are the Glaisher numbers given by*

$$\frac{3/2}{e^x + e^{-x} + 1} = \sum_{n=0}^{\infty} G_n \frac{x^n}{n!}.$$

Corollary 6. *Let $p \equiv 1 \pmod 3$, and consider $E/\mathbb{F}_p : y^2 = x^3 - 1$. If $p^2 = 3n^2 + 3n + 1$ for some $n \in \mathbb{Z}$, then $\#E(\mathbb{F}_q) \equiv 0 \pmod{p^2}$.*

Proof. This follows from Theorem 4.5.1 and Corollary 6 in (7). □

Theorem 4.5.2. *Let $p \equiv 1 \pmod 4$, and consider $E/\mathbb{F}_p : y^2 = x^3 + x$. Then p is 1-exceptional for $m = 4$ if and only if $E_{p-1} \equiv 0 \pmod{p^2}$ if and only if $\#E(\mathbb{F}_q) \equiv 0 \pmod{p^2}$, where $q = p^{p-1}$, and $\{E_n\}$ are the Euler numbers given by*

$$\frac{2}{e^x + e^{-x}} = \sum_{n=0}^{\infty} E_n \frac{x^n}{n!}.$$

Chapter 5

CONDITIONS FOR LARGE CYCLOTOMIC λ-INVARIANTS

Childress (4) was able to re-write (2.2) as

$$F(T) = \sum_{\zeta \in V} \left(\sum_{\substack{a=1 \\ a \equiv \zeta \pmod{p}}}^{f} \epsilon(a) T^{\zeta^{-1} a} \Big/ (1 + T^{\zeta^{-1} f}) \right) \tag{5.1}$$

under the assumption that $d \equiv 3 \pmod 4$ and $c = 2$ so that $\epsilon(a) = \chi(a)(-1)^{a+1}$ (note that we require c to be co-prime to the discriminant of K). The upshot is that we may now evaluate

$$b_0 = F(1) = \frac{1}{2} \sum_{\substack{a=1 \\ p \nmid a}}^{dp} \epsilon(a) = (1 - \chi(p)) \frac{1}{2} \sum_{a=1}^{d} \chi(a)(-1)^{a+1}.$$

This can be seen as a rediscovery of the fact that $\lambda_p(K) > 0$ if and only if p splits in K or p divides the class number of K. In general, Childress (4), (5) obtains congruences modulo p for the coefficients of the Iwasawa series associated to a Dirichlet character of odd conductor. This makes it possible to compute the relative cyclotomic Iwasawa invariants of a CM field.

In this section we only focus on imaginary quadratic fields, and first extend (5.1) to the case $d \not\equiv 3 \pmod 4$. Then we will find (without restrictions on the discriminant of K) congruences modulo p for the coefficients b_n of the Iwasawa series $\sum b_n (T-1)^n$ by computing $(d/dT)^{np} \,|_{T=1} F(T)/(np)! \pmod p$, but assuming that $1 \leq n < p$. The congruences we obtain are essentially the same as ones found in (5), however the method used to obtain them is new. One should also compare these congruences

to Propositions 3.1 and 3.2 in (10). We then use the congruences to find imaginary quadratic fields K for which $\lambda_p(K)$ is greater than a given value ($p = 5, 7, 11$ and 13). Finally, we will use the congruences to find another proof of Theorem 3.1.1, then prove an analogous condition for $\lambda_p(K) > 2$ using this new technique.

5.1 Even Discriminants

Suppose $d \not\equiv 3 \pmod 4$, and χ the primitive imaginary quadratic character belonging to $\mathbb{Q}(\sqrt{-d})$. Then χ has conductor $4d$. Let p be co-prime to $4d$, and let $f = 4dp$, $c \in \mathbb{Z}$ and ϵ be as they were defined above. Because imaginary quadratic fields have $\mathbb{Q}$ as their maximal real subfield, and χ is the only non-trivial element of $\mathrm{Gal}(\mathbb{Q}(\sqrt{-d})$, we have

$$\lambda_p^-(g_\chi) = \lambda_p(g_\chi) = \lambda_p(\mathbb{Q}(\sqrt{-d})).$$

We may choose c such that $c \not\equiv \pm 1 \pmod p$. Hence

$$H_\chi(T) = (1 - c\chi(c)) - c\chi(c) \sum_{n=1}^{\infty} \binom{t}{n} (T-1)^n$$

implies $\lambda_p(H_\chi) = 0$. Therefore, $p\lambda_p(F) = \lambda_p(\mathbb{Q}(\sqrt{-d}))$. For convenience we will write

$$\sum_{i \equiv c}^{r} x_i \;=\; \sum_{\substack{i=1 \\ i \equiv c \pmod n}}^{r} x_i$$

whenever the modulus n is clear from context. Given $\zeta \in V$, we write

$$\tilde{F}_\zeta(T) = \frac{\displaystyle\sum_{a \equiv \zeta \pmod p}^{cf} \epsilon(a) T^{\zeta^{-1}a}}{1 - T^{\zeta^{-1}cf}}$$

and

$$F_\zeta(T) \;=\; \frac{\displaystyle\sum_{a \equiv \zeta \pmod p}^{cf} \chi(a) T^{\zeta^{-1}a}}{1 - T^{\zeta^{-1}cf}}.$$

Hence, $F(T) = \sum_\zeta \tilde{F}_\zeta(T)$. In (4), a key step is in obtaining the expression for $F(T)$ in equation 5.1 is to set $c = 2$ which gives $\epsilon(a) = (-1)^a\chi(a)$. Part of the challenge now is that 2 is no longer co-prime to the conductor of χ. We will try to get around this:

Proposition 5.

$$F(T) = \sum_{\zeta\in V} F_\zeta(T) - c\chi(c)\sum_{\zeta\in V} F_{\zeta,c}(T)$$

where

$$F_{\zeta,c}(T) = \frac{\displaystyle\sum_{a\equiv c^{-1}\zeta \pmod{p}}^{f} \chi(a)T^{(c^{-1}\zeta)^{-1}a}}{1 - T^{(c^{-1}\zeta)^{-1}f}}$$

Proof. For $\zeta \in V$,

$$\sum_{a\equiv\zeta}^{cf} \epsilon(a)T^{\zeta^{-1}a} = \sum_{\substack{a\equiv\zeta\\ c\nmid a}}^{cf} \chi(a)T^{\zeta^{-1}a} + \sum_{ca\equiv\zeta}^{f} \chi(ca)(1-c)T^{\zeta^{-1}ca}.$$

Now,

$$\begin{aligned}\sum_{\substack{a\equiv\zeta\\ c\nmid a}}^{cf} \chi(a)T^{\zeta^{-1}a} &= \sum_{a\equiv\zeta}^{cf} \chi(a)T^{\zeta^{-1}a} - \sum_{ca\equiv\zeta}^{f} \chi(ca)T^{\zeta^{-1}ca}\\ &= \sum_{a\equiv\zeta}^{cf} \chi(a)T^{\zeta^{-1}a} - \chi(c)\sum_{a\equiv c^{-1}\zeta}^{f} \chi(a)T^{(c^{-1}\zeta)^{-1}a}\end{aligned}$$

and

$$\sum_{ca\equiv\zeta}^{f} \chi(ca)(1-c)T^{\zeta^{-1}ca} = (1-c)\chi(c)\sum_{a\equiv c^{-1}\zeta}^{f} \chi(a)T^{(c^{-1}\zeta)^{-1}a}.$$

The proposition now follows. □

Lemma 4. *For odd $k \in \mathbb{Z}$, we have $\chi(a + 2kd) = -\chi(a)$. In other words, for any $a, n \in \mathbb{N}$, with $\gcd(a, 4d) = 1$,*

$$\chi(a + 2nd) = (-1)^n\chi(a).$$

Proof. For each $a \in \mathbb{Z}$ co-prime to $4d$, either $\chi(a+2kd) = \chi(a)$ or $\chi(a+2kd) = -\chi(a)$. Now, suppose that $a, b \in \mathbb{Z}$ with a and b co-prime to $4d$. Then a and b are odd, and $a + b = 2e$ for some $e \in \mathbb{Z}$. So,

$$(a + 2d)(b + 2d) \equiv (ab + 2d(a + b)) \equiv ab \pmod{4d}.$$

Hence,

$$\chi(a + 2d)\chi(b + 2d) = \chi(a)\chi(b).$$

Now, suppose that a and b are co-prime to $4d$ with $\chi(a+2d) = -\chi(a)$ and $\chi(b+2d) = \chi(b)$. Then

$$\chi(a + 2d)\chi(b + 2d) = -\chi(a)\chi(b)$$

which is a contradiction. Thus, it must be that either $\chi(a+2d) = -\chi(a)$ for all $a \in \mathbb{Z}$, or $\chi(a + 2d) = \chi(a)$ for all $a \in \mathbb{Z}$. But the latter cannot be true, since then χ would have conductor $2d$ instead of $4d$. Hence $\chi(a + 2d) = -\chi(a)$ for all a. If $k = 2e + 1$ for some $e \in \mathbb{Z}$, then

$$\chi(a + 2kd) = \chi(a + (2e + 1)2d) = \chi(a + 2d) = -\chi(a).$$

□

Proposition 6. *Let $n \in \mathbb{Z}^+$ and $f = 4dp$. Then*

$$\frac{\sum_{a \equiv \zeta}^{nf} \chi(a) T^{\zeta^{-1}a}}{1 - T^{\zeta^{-1} nf}} = \frac{\sum_{a \equiv \zeta}^{f} \chi(a) T^{\zeta^{-1}a}}{1 - T^{\zeta^{-1} f}}$$

Proof. Let $X = T^{\zeta^{-1}}$ and $1 - X^{nf} = (1 - X^f)Q(X)$. It is easy to see that $Q(X) =$

$\sum_{k=0}^{n-1} X^{kf}$. Therefore,

$$\begin{aligned}\frac{\sum_{a\equiv\zeta}^{nf}\chi(a)X^a}{1-X^{nf}} &= \frac{\sum_{k=0}^{n-1}\sum_{a+kf\equiv\zeta}^{f}\chi(a+kf)X^{a+kf}}{Q(X)(1-X^f)}\\ &= \frac{\left(\sum_{k=0}^{n-1}X^{kf}\right)\left(\sum_{a\equiv\zeta}^{f}\chi(a)X^a\right)}{Q(X)(1-X^f)}\\ &= \frac{\sum_{a\equiv\zeta}^{f}\chi(a)X^a}{1-X^f}.\end{aligned}$$

□

Proposition 7.

$$F_\zeta(T) = \frac{\sum_{a\equiv\zeta}^{f/2}\chi(a)T^{\zeta^{-1}a}}{1+T^{\zeta^{-1}f/2}}$$

and

$$F_{\zeta,c}(T) = \frac{\sum_{a\equiv c^{-1}\zeta}^{f/2}\chi(a)T^{\zeta^{-1}ca}}{1+T^{\zeta^{-1}cf/2}}$$

Proof. Using Lemmas 4 and 6, we have

$$\begin{aligned}\frac{\sum_{a\equiv\zeta}^{cf}\chi(a)T^{\zeta^{-1}a}}{1-T^{\zeta^{-1}cf}} &= \frac{\sum_{a\equiv\zeta}^{f}\chi(a)T^{\zeta^{-1}a}}{1-T^{\zeta^{-1}f}}\\ &= \frac{\sum_{a\equiv\zeta}^{f/2}\chi(a)T^{\zeta^{-1}a}}{1-T^{\zeta^{-1}f}} + \frac{\sum_{a\equiv\zeta}^{f/2}\chi(a+2dp)T^{\zeta^{-1}(a+f/2)}}{1-T^{\zeta^{-1}f}}\\ &= \frac{\sum_{a\equiv\zeta}^{f/2}\chi(a)T^{\zeta^{-1}a}}{1-T^{\zeta^{-1}f}} - \frac{\sum_{a\equiv\zeta}^{f/2}\chi(a)T^{\zeta^{-1}(a+f/2)}}{1-T^{\zeta^{-1}f}}\\ &= \sum_{a\equiv\zeta}^{cf/2}\chi(a)T^{\zeta^{-1}a}\frac{1-T^{\zeta^{-1}f/2}}{1-T^{\zeta^{-1}f}}\\ &= \frac{\sum_{a\equiv\zeta}^{f/2}\chi(a)T^{\zeta^{-1}a}}{1+T^{\zeta^{-1}f/2}}.\end{aligned}$$

The second equality follows in a similar fashion. □

We now have that $F_{\zeta,c}(T) = F_\zeta(T^c)$, and so we have

Theorem 5.1.1. *Let $n \in \mathbb{Z}^+$. Then*

$$(d/dT)^n|_{T=1}(F_\zeta(T) - c\chi(c)F_{\zeta,c}(T)) = (1 - c^2\chi(c))F_\zeta^{(n)}(1)$$

where $F_\zeta^{(n)}(T) = (d/dT)^n F_\zeta(T)$.

Proof. Using $F_{\zeta,c}(T) = F_\zeta(T^c)$, and the chain rule, we have

$$(d/dT)^n|_{T=1}(F_\zeta(T) - c\chi(c)F_{\zeta,c}(T)) = F_\zeta^{(n)}(1) - c^2\chi(c)F_\zeta^{(n)}(1) = (1 - c^2\chi(c))F_\zeta^{(n)}(1).$$

□

5.2 Coefficients of the Iwasawa Series Associated to an Imaginary Quadratic Field

Let $f = 2Dp$, and define ψ by

$$\psi(a) = \begin{cases} \chi(a)(-1)^a & \text{if } d \equiv 3 \pmod 4 \\ \chi(a) & \text{else} \end{cases}$$

If $m \in \mathbb{Z}^+$ and $H(T) \in \mathcal{O}_k[[T-1]]$, we will often write $(d/dT)^m|_{T=1}H(T) = H^{(m)}(1) = H^{(m)}$.

For $d \not\equiv 3 \pmod 4$, and c co-prime to f such that $c\chi(c) \not\equiv 1 \pmod p$, we have from Theorem 5.1.1 that $(d/dT)^{pn}|_{T=1}(F_\zeta(T) - c\chi(c)F_{\zeta,c}(T)) = (1 - c^2\chi(c))F_\zeta^{(pn)}(1)$. So we will carry out essentially the same computation, that is, $(d/dT)^{pn}|_{T=1}F_\zeta(T)$, whatever the reduction of d modulo 4 happens to be. For $1 \leq n < p$ and $\zeta \in V$, we denote

$$S_\zeta(T) = \sum_{\substack{a=1 \\ a \equiv \zeta \pmod p}}^{f/2} \psi(a)T^{\zeta^{-1}a}, \quad R_\zeta(T) = 1 + T^{\zeta^{-1}f/2}, \quad F_\zeta(T) = S_\zeta(T)/R_\zeta(T)$$

so that $F(T) = \sum_{\zeta \in V} F_\zeta(T)$.

Now, if $v_p(\cdot)$ is the p-adic valuation, then $v_p((np)!) = n$. Hence, $b_n \equiv 0 \pmod{p}$ if and only if $F^{(np)}(1) \equiv 0 \pmod{p^{n+1}}$. We also have

$$F_\zeta^{(np)}(T) = \frac{S_\zeta^{(np)}(T) - \sum_{i=0}^{np-1} \binom{np}{i} F_\zeta^{(i)}(T) R_\zeta^{(np-i)}(T)}{R_\zeta(T)}.$$

Lemma 5. *For $1 \leq n < p$, we have*

$$v_p\left(\binom{np}{i}\right) = \begin{cases} 1 & \text{if } p \nmid i \\ 0 & \text{else .} \end{cases}$$

Further, for $1 \leq b \leq n$, we have

$$\binom{np}{bp} \equiv \binom{n}{b} \pmod{p}.$$

Proof. For $s, t \in \mathbb{Z}^+$ we have from Lagrange's formula

$$v_p\left(\binom{s}{t}\right) = \frac{s_p(t) - s_p(s) + s_p(s-t)}{p-1}$$

where $s_p(s)$ denotes the sum of the p-adic digits of s. Suppose that $1 \leq i \leq np$ and let $i = a + bp$ be the base p expansion of i and notice that if $a \neq 0$ then $(n-b-1)p + (p-a)$ is the base p expansion of $np - i$, and if $a = 0$ then $(n-b)p$ is the base p-expansion. Then

$$v_p\left(\binom{np}{i}\right) = \frac{s_p(i) - s_p(np) + s_p(np-i)}{p-1} = \begin{cases} 1 & \text{if } a \neq 0 \\ 0 & \text{if } a = 0 \end{cases}.$$

Next, if $1 \leq n < p$, we have

$$\begin{aligned} \frac{(np)!}{p^n} &= \frac{1}{p^n} \prod_{j=0}^{p-1} \prod_{i=0}^{n-1} (np - ip - j) = n! \prod_{j=1}^{p-1} \prod_{i=0}^{n-1} (np - ip - j) \\ &\equiv n! \prod_{i=0}^{n-1} \prod_{j=1}^{p-1} (-j) \equiv n!(p-1)!^n \equiv n!(-1)^n \pmod{p} \end{aligned}$$

(the last congruence follows from Wilson's Theorem). Hence

$$\binom{np}{bp} = \frac{(np)!}{(bp)!((n-b)p)!} \equiv \frac{(-1)^n n!}{(-1)^n b!(n-b)!} \equiv \binom{n}{b} \pmod{p}.$$

□

Lemma 6. *Let $\zeta \in V$ and suppose that $0 \leq b < n$. Then*

i. $S_\zeta^{(i)} \equiv 0 \pmod{p^{b+1}}$, *for* $bp < i \leq (b+1)p$

ii. $R_\zeta^{(i)} \equiv 0 \pmod{p^{b+1}}$, *for* $bp \leq i < (b+1)p$, *and* $i \neq 0$.

Proof. Suppose, $bp < i \leq (b+1)p$, and recall that $f \equiv 0 \pmod{p}$.

Proof of (i.): Notice that

$$S_\zeta^{(i)} = \sum_{\substack{a=1 \\ a \equiv \zeta \pmod{p}}}^{f/2} \psi(a) \prod_{j=0}^{i-1} (\zeta^{-1}a - j)$$

and $(\zeta^{-1}a - j) \equiv 0 \pmod{p}$ whenever $j \equiv 1 \pmod{p}$, and there are $b+1$ such j between 0 and $i-1$.

Proof of (ii.): We have $R_\zeta^{(i)} = \prod_{j=0}^{i-1}(\zeta^{-1}f - j)$, and $(\zeta^{-1}f - j) \equiv 0 \pmod{p}$ if and only if $j \equiv 0 \pmod{p}$, and there are $b+1$ many j divisible by p such that $0 \leq j \leq i-1$. □

Lemma 7. *Suppose that $1 \leq b < n$, and $bp < m \leq (b+1)p$. If $m > 1$, then* $F_\zeta^{(m)} \equiv 0 \pmod{p^b}$.

Proof. We will prove that for all $j \in \{0, 1, \ldots, m-1\}$, we have $F_\zeta^{(j)} R_\zeta^{(m-j)} \equiv 0 \pmod{p^b}$, which will prove the lemma since

$$F_\zeta^{(m)} = \frac{1}{2}\left(S_\zeta^{(m)} - \sum_{j=0}^{m-1} \binom{m}{j} F_\zeta^{(j)} R_\zeta^{(m-j)}\right) \equiv 0 \pmod{p}$$

and from Lemma 6 (i), $S_\zeta^{(m)} \equiv 0 \pmod{p^b}$. For $j = 0$, we have $F_\zeta R_\zeta^{(m)} \equiv 0 \pmod{p^b}$ by Lemma 6 (ii). Now, let $j \in \{0, 1, \ldots, m-1\}$, $r \leq b$ with $rp \leq j \leq (r+1)p$, and suppose that $F_\zeta^{(i)} R_\zeta^{(m-i)} \equiv 0 \pmod{p^b}$ for all $i < j$. Then, by this assumption, and Lemma 6 (i), which says $S_\zeta^{(j)} \equiv 0 \pmod{p^r}$, we have

$$F_\zeta^{(j)} = \frac{1}{2}\left(S_\zeta^{(j)} - \sum_{i=0}^{j-1} \binom{j}{i} F_\zeta^{(i)} R_\zeta^{(i-j)}\right) \equiv 0 \pmod{p^r}.$$

At the same time, $R_\zeta^{m-j} \equiv 0 \pmod{p^{b-r}}$, again by Lemma 6 (ii). Therefore, $F_\zeta^{(j)} R_\zeta^{(m-j)} \equiv 0 \pmod{p^b}$. □

Definition 9. *For fixed $\zeta \in V$ and $i, j \in \mathbb{Z}^+$, we denote*

$$\theta_\zeta(i,j) = \sum_{\substack{a=1 \\ a \equiv \zeta \pmod{p}}}^{f/2} \zeta^{-j} a^i \psi(a) \quad \text{and} \quad \theta(i,j) = \sum_{a=1}^{f/2} a^i \omega^{-j}(a)\psi(a).$$

Note that when $j \neq 0$, we have $\sum_{\zeta \in V} \theta_\zeta(i,j) = \theta(i,j)$. If $j = 0$, then $\sum_{\zeta \in V} \theta_\zeta(i,0) = \sum_{\substack{a=1 \\ p \nmid a}}^{f/2} a^i \psi(a)$.

Lemma 8. *Let $0 < b \leq n$. Then*

$$S_\zeta^{(bp)} \equiv (-1)^b \sum_{j=1}^{b} \sum_{i=0}^{j} \binom{j}{i} \begin{bmatrix} b \\ j \end{bmatrix} p^{b-j} (-1)^{j-i} \theta(i,i) = \sum_{i=0}^{b} c_i(b) \theta_\zeta(i,i) \pmod{p^{b+1}} \quad (5.2)$$

where $c_i(b) = \sum_{j=i}^{b} \binom{j}{i} \begin{bmatrix} b \\ j \end{bmatrix} p^{b-j}(-1)^{j-i}$, and

$$R_\zeta^{(bp)} \equiv (-p)^b \sum_{i=1}^{b} \begin{bmatrix} b \\ i \end{bmatrix} (\zeta^{-1} 2D)^i \pmod{p^{b+1}} \quad (5.3)$$

Where $\begin{bmatrix} m \\ i \end{bmatrix}$ are the Stirling numbers of the first kind, defined by $\prod_{i=0}^{m-1}(x-i) = \sum_{i=1}^{m} \begin{bmatrix} m \\ i \end{bmatrix} x^i$.

Proof. First, we have

$$S_\zeta^{(bp)} = \sum_{\substack{a=1 \\ a\equiv\zeta \pmod p}}^{f/2} \psi(a) \prod_{j=0}^{bp-1} (\zeta^{-1}a - j)$$

and

$$\begin{aligned}
\prod_{j=0}^{bp-1} (\zeta^{-1}a - j) &= \prod_{i=0}^{p-1}\prod_{j=0}^{b-1} (\zeta^{-1}a - (i+pj)) \\
&\equiv \left(\prod_{\substack{i=0 \\ i\neq 1}}^{p-1}\prod_{j=0}^{b-1} (1-i)\right)\left(\prod_{j=0}^{b} (\zeta^{-1}a - (1+pj))\right) \pmod{p^{b+1}} \\
&\equiv (-(p-2)!)^b \sum_{j=1}^{b} \begin{bmatrix} b \\ j \end{bmatrix} p^{b-j} (\zeta^{-1}a - 1)^j \pmod{p^{b+1}} \\
&\equiv (-1)^b \sum_{j=1}^{b}\sum_{i=0}^{j} \binom{j}{i} \begin{bmatrix} b \\ j \end{bmatrix} p^{b-j} (-1)^{j-i} (\zeta^{-1}a)^i \pmod{p^{b+1}}.
\end{aligned}$$

Hence

$$\begin{aligned}
S^{(bp)} &\equiv (-1)^b \sum_{j=1}^{b}\sum_{i=0}^{j} \binom{j}{i} \begin{bmatrix} b \\ j \end{bmatrix} p^{b-j} (-1)^{j-i} \theta(i,i) \pmod{p^{b+1}} \\
&\equiv (-1)^b \sum_{i=0}^{b}\sum_{j=i}^{b} \binom{j}{i} \begin{bmatrix} b \\ j \end{bmatrix} p^{b-j} (-1)^{j-i} \theta(i,i) \pmod{p^{b+1}}.
\end{aligned}$$

$R_\zeta^{(bp)}$ is calculated in a similar way. □

Lemma 9. *Let $0 < b \leq n$, and $(a_i), (c_i)$ be sequences. Then*

$$\sum_{i=1}^{b}\sum_{j=1}^{n-b} a_i c_j x^{i+j} = \sum_{m=2}^{n} t_m x^m$$

where

$$t_m = \sum_{r=\max\{1,m+b-n\}}^{\min\{m-1,b\}} a_r c_{m-r}$$

Proof. We have that

$$\sum_{i=1}^{b}\sum_{j=1}^{n-b} a_i c_j x^{i+j} = \sum_{m=2}^{n} t_m x^m$$

where $t_m = \sum_{r=1}^{m} a_r c_{m-r}$, with $a_r = 0$ for $b < r$ and $c_r = 0$ for $n - b < r$. □

For fixed $\zeta \in V$ and $1 \leq n \leq p-1$, we can now show that $F_\zeta^{(np)}$ can be defined recursively in terms of $F_\zeta^{(bp)}$, with $0 \leq b < n$.

Proposition 8. *Let $0 \leq n \leq p-1$. Then*

$$F_\zeta^{(np)} \equiv \frac{1}{2}\left(S_\zeta^{(np)} - \sum_{b=0}^{n-1}\binom{n}{b} F_\zeta^{(bp)} R_\zeta^{((n-b)p)}\right) \pmod{p^{n+1}} \tag{5.4}$$

Proof. Let $j \in \{0, 1, \ldots, np\}$, and $1 \leq b < n$ such that $bp < j < (b+1)p$. Then by Lemma 6 (ii.), we have $R_\zeta^{(np-j)} \equiv 0 \pmod{p^{n-b+1}}$, and by Lemma 7 we have $F_\zeta^{(j)} \equiv 0 \pmod{p^b}$. Hence, $F_\zeta^{(j)} R_\zeta^{(np-j)} \equiv 0 \pmod{p^{n+1}}$ whenever j is not divisible by p. Now, if $j = bp$, we have $F_\zeta^{(bp)} \equiv 0 \pmod{p^{b-1}}$, and $R_\zeta^{(np-bp)} \equiv 0 \pmod{p^{n-b+1}}$, so $F_\zeta^{(bp)} R_\zeta^{(np-bp)} \equiv 0 \pmod{p^n}$. Further, by Lemma 5, we have $\binom{np}{bp} \equiv \binom{n}{b} \pmod{p}$, and these do not contribute any factors of p to the bp-th term of $\sum_{j=0}^{np-1}\binom{np}{j} F_\zeta^{(j)} R_\zeta^{(np-j)}$. Whence the stated congruence. □

Let us now use Proposition 8 to write out some congruences which will determine if $\lambda_p(K) > n$, for $n = 0, 1, 2, 3$, and $p \geq 5$. First, we prove a lemma which will ease some of the computations to come.

Lemma 10. *For any $j \in \mathbb{Z}$ with $j \neq 0$, we have that $\theta(0, j) = 0$.*

Proof. Notice that $\chi\omega^{-j}(-a) = \chi\omega^{-j}(a)$. First suppose $d \equiv 3 \pmod 4$. Then,

$$\begin{aligned}\sum_{a=1}^{dp} \chi\omega^{-j}(a)(-1)^a &= \sum_{a=1}^{(dp-1)/2} \chi\omega^{-j}(a)(-1)^a + \sum_{a=1}^{(dp-1)/2} \chi\omega^{-j}(dp-a)(-1)^{dp-a} \\ &= \sum_{a=1}^{(dp-1)/2} \chi\omega^{-j}(a)(-1)^a - \sum_{a=1}^{(dp-1)/2} \chi\omega^{-j}(a)(-1)^a = 0.\end{aligned}$$

If $d \not\equiv 3 \pmod 4$, then $\chi(a+2di) = \chi(a)(-1)^i$. Therefore,

$$\sum_{a=1}^{2dp} \chi\omega^{-j}(a) = \sum_{a=1}^{dp} \chi\omega^{-j}(a) + \sum_{a=1}^{dp} \chi\omega^{-j}(2dp-a) = \sum_{a=1}^{dp} \chi\omega^{-j}(a) - \sum_{a=1}^{dp} \chi\omega^{-j}(a) = 0.$$

□

From Lemma 10, any instances of $\theta_\zeta(0,j)$, with $j \neq 0$, appearing in the expression for $F_\zeta^{(np)}$ will vanish once we sum over $\zeta \in V$. In other words, write $F_\zeta^{(bp)} = \sum_{i,j} c_{i,j}^b \theta_\zeta(i,j)$ and $S_\zeta^{(bp)} = \sum_{i,j} e_{i,j}^b \theta_\zeta(i,j)$, with $c_{i,j}^b, e_{i,j}^b \in \mathbb{Z}_p$ (if there is no confusion, we will suppress the superscripts for $c_{i,j}$ and $e_{i,j}$), and define

$$\bar{F}_\zeta^{(bp)} = F_\zeta^{(bp)} - \sum_j c_{0,j}\theta_\zeta(0,j) \quad \text{and} \quad \bar{S}_\zeta^{(bp)} = S_\zeta^{(bp)} - \sum_j e_{0,j}\theta_\zeta(0,j).$$

Then $\sum_\zeta \bar{F}_\zeta^{(np)} = \sum_\zeta F_\zeta^{(np)} - c_{0,0}^n \theta(0,0)$, and as we will see, if $\lambda_p(K) > 0$, then $\theta(0,0) \equiv 0 \pmod p$. Furthermore, since $\zeta^{-i}\theta_\zeta(0,j) = \theta_\zeta(0,j+i)$, it follows from (5.3) that $\sum_\zeta F_\zeta^{(j)} R_\zeta^{(i)} - c_{0,0}^j \theta_\zeta(0,0) R_\zeta^{(i)} = \sum_\zeta \bar{F}_\zeta^{(j)} R_\zeta^{(i)}$. Thus, when $\lambda_p(K) > 0$, it suffices to compute

$$\bar{F}_\zeta^{(np)} \equiv \frac{1}{2}\left(\bar{S}_\zeta^{(np)} - \sum_{b=1}^{n-1} \binom{n}{b} \bar{F}_\zeta^{(bp)} R_\zeta^{((n-b)p)}\right) \pmod{p^{n+1}} \tag{5.5}$$

(note that $\bar{F}_\zeta R_\zeta^{(np)} = \sum r_j \theta_\zeta(0,j)$ for some $r_j \in \mathbb{Z}_p$).

Proposition 9. *Suppose* $\bar{F}_\zeta^{(np)} = \sum_{i=1}^n \sum_{j=1}^n c_{i,j}(n)\theta_\zeta(i,j)$, *for some* $c_{i,j}(b) \in \mathbb{Z}_p$. *Then*

i. $c_{i,j}(n) = 0$, *whenever* $i > j$

ii. $c_{i,i}(n) = (1/2)\sum_{r=i}^n \binom{r}{i} \begin{bmatrix} n \\ r \end{bmatrix} p^{n-r}(-1)^{n+i-r}$

iii. $c_{i,j}(n) = \sum_{b=i}^{n-1} \binom{n}{b}(-p)^b t_{i,j}(b)$, *if* $i < j$, *where*

$$t_{i,j}(b) = \sum_{m=\max\{1,j+b-n\}}^{\min\{j-1,b\}} \begin{bmatrix} n-b \\ j-m \end{bmatrix} D^{j-m} c_{i,m}(b)$$

Proof. (i) is clear and (ii) follows from Lemma 8. For (iii), denote $\alpha_{r,b} = \begin{bmatrix} n-b \\ r \end{bmatrix} d^r$, $\beta_b = \binom{n}{b}(-p)^b$, and $t_{i,j}(b)$ as above. Then

$$\begin{aligned}
\sum_{b=1}^{n-1} \binom{n}{b} R_\zeta^{(n-b)} \bar{F}_\zeta^{(b)} &= \sum_{b=1}^{n-1} \binom{n}{b} \sum_{i=1}^{b} \sum_{j=1}^{b} c_{i,j}(b)\theta_\zeta(i,j)(-p)^b \sum_{r=1}^{n-b} \begin{bmatrix} n-b \\ r \end{bmatrix} (\zeta^{-1}d)^r \\
&= \sum_{b=1}^{n-1} \sum_{i=1}^{b} \beta_b \left(\sum_{j=1}^{b} \sum_{r=1}^{n-b} \alpha_{r,b} c_{i,j}(b)\theta_\zeta(i, j+r) \right) \\
&= \sum_{b=1}^{n-1} \sum_{i=1}^{b} \beta_b \sum_{j=2}^{n} t_{i,j}(b)\theta_\zeta(i,j) \\
&= \sum_{j=2}^{n} \sum_{b=1}^{n-1} \sum_{i=1}^{b} \beta_b t_{i,j}(b)\theta_\zeta(i,j) \\
&= \sum_{j=2}^{n} \sum_{i=1}^{n-1} \sum_{b=i}^{n-1} \beta_b t_{i,j}(b)\theta_\zeta(i,j) \\
&= \sum_{j=2}^{n} \sum_{i=1}^{j} c_{i,j}(n)\theta_\zeta(i,j)
\end{aligned}$$

where we have used Lemma 9 moving from lines two to three. □

5.3 Conditions for $\lambda > n$

Using the recursive formulas in Proposition 9, we will write down some conditions for when $\lambda_p(K) > n$ for $n = 1, 2, 3, 4$ (the congruences become more complicated for $n > 4$). These congruences were already known to Childress (see the final page of (5)) although in a slightly different form, and only in the case when the discriminant is odd. It should be noted that Childress' congruences work for CM fields. Similar

congruences can be found in Proposition 3.1 and 3.2 of (10). As always, we denote $K = \mathbb{Q}(\sqrt{-d})$, and $D = d$ if $d \equiv 3 \pmod 4$ and $D = 2d$ otherwise. Again, write $\psi(a) = \chi(a)(-1)^a$ if $d \equiv 3 \pmod 4$ and $\psi(a) = \chi(a)$ otherwise. Throughout we will also assume that p does not divide the class number of K.

Proposition 10 ($\lambda_p(K) > 1$)**.** *Suppose that $\chi(p) = 1$. Here we have already seen that $\lambda_p(K) > 1$ if and only if*

$$\sum_{a=1}^{Dp} a\psi(a)\omega^{-1}(a) \equiv 0 \pmod{p^2}.$$

Proposition 11 ($\lambda_p(K) > 2$)**.** *If $\lambda_p(K) > 1$, then $\lambda_p(K) > 2$ if and only if*

$$\sum_{a=1}^{Dp} a^2\psi(a)\omega^{-2}(a) - 2\sum_{a=1}^{Dp} a\psi(a)\omega^{-1}(a) - Dp\sum_{a=1}^{Dp} a\psi(a)\omega^{-2}(a) \equiv 0 \pmod{p^3}.$$

Proposition 12 ($\lambda_p(K) > 3$)**.** *Suppose that $\lambda_p(K) > 2$, and recall our notation $\theta(i,j) = \sum_{a=1}^{Dp} a^i\psi(a)\omega^{-j}(a)$. Then $\lambda_p(K) > 3$ if and only if*

$$\sum_{j=1}^{3}\sum_{i=1}^{j} c_{i,j}(3)\theta(i,j) \equiv 0 \pmod{p^4}$$

where

$$c_{1,1}(3) = -p^2 - 3p - (3/2)$$

$$c_{1,2}(3) = -(3/4)D(p+2)p - (3/4)Dp^2$$

$$c_{2,2}(3) = (3/2)p + (3/2)$$

$$c_{1,3}(3) = 0$$

$$c_{2,3}(3) = (3/4)Dp$$

$$c_{3,3}(3) = -1/2$$

Proposition 13 ($\lambda_p(K) > 4$)**.** *Suppose that* $\lambda_p(K) > 3$*. Then* $\lambda_p(K) > 4$ *if and only if*

$$\sum_{j=1}^{4} \sum_{i=1}^{j} c_{i,j}(4)\theta(i,j) \equiv 0 \pmod{p^5}$$

where

$$c_{1,1}(4) = -3p^3 - 11p^2 - 9p - 2$$

$$c_{1,2}(4) = -(3/2)D(p+2)p^2 - 2Dp^3 - (2p^2 + 6p + 3)Dp$$

$$c_{2,2}(4) = (11/2)p^2 + 9p + 3$$

$$c_{1,3}(4) = 3D^2p^3 - (3/2)(D(p+2)p + Dp^2)Dp + (3/2)(D^2(p+2) - D^2p)p^2$$

$$c_{2,3}(4) = 3D(p+1)p + (3/2)Dp^2$$

$$c_{3,3}(4) = -3p - 2$$

$$c_{1,4}(4) = (1/2)D^3p^3$$

$$c_{2,4}(4) = 0$$

$$c_{3,4}(4) = -Dp$$

$$c_{4,4}(4) = 1/2$$

As an application, we fix a small prime p, and use the recursive formulas to search for imaginary quadratic fields K for which $\lambda_p(K)$ is large. As p becomes larger, the computations become slower, hence the range for the discriminant of K will be smaller. In each example we are still assuming that p does not divide the class number of K, hence these lists are not entirely complete.

Example 4 ($p = 5$)**.** *When* $p = 5$ *we have the imaginary quadratic fields* K *with absolute value of the discriminant* $\mathcal{D}_K$ *less than 10,000, giving* $\lambda_5(K) = 3$ *are* $\mathcal{D}_K =$ *519, 599, 664, 799, 964, 1051, 1311, 1839, 1951, 2251, 2391, 2679, 2699, 3064, 3496,*

3704 3893, 3851, 4231, 4264, 4291, 4331, 4371, 4859, 5556, 5671, 5811, 5891, 6119, 6199, 6371 6376, 6616, 6739, 6771, 6819, 7259, 7291, 7796, 7816, 8011, 8079, 8151, 8331, 8491, 8531, 8571, 9011, 9051, 9379, 9419, 9444, 9899, and 9956.

On the other hand, the imaginary quadratic fields K with $\mathcal{D}_K < 10,000$, giving $\lambda_5(K) \geq 4$ are $\mathcal{D}_K = 311, 3044, 3864, 3471, 5039,$ and 9859.

Example 5 ($p = 7$)**.** *When $p = 7$ we have the imaginary quadratic fields K with $\mathcal{D}_K < 5,000$, giving $\lambda_7(K) = 3$ are $\mathcal{D}_K = 143, 580, 776, 1956, 2036, 2071, 2120, 2211, 2267, 2488, 2708, 3923, 3995, 4303, 4408, 4511,$ and 4679.*

There are no fields K with discriminant under 5,000 having $\lambda_7(K) \geq 4$.

Example 6 ($p = 11$)**.** *When $p = 11$ we have the imaginary quadratic fields K with $\mathcal{D}_K < 2,000$, giving $\lambda_{11}(K) = 3$ are $\mathcal{D}_K = 723, 1491, 1623$.*

There are no fields K with discriminant under 2,000 having $\lambda_{11}(K) \geq 4$.

Example 7 ($p = 13$)**.** *When $p = 13$ we have the imaginary quadratic fields K with $\mathcal{D}_K < 5,000$, giving $\lambda_{13}(K) = 3$ are $\mathcal{D}_K = 443, 1608$*

There are no fields K with discriminant under 2,000 having $\lambda_{13}(K) \geq 4$.

One can confirm that the examples match the table in (10), for $\mathcal{D}_K < 1000$.

Chapter 6

ANOTHER "GOLD LIKE" CRITERION (THE $\delta_{\chi,P}$ PRODUCT).

Let $K = \mathbb{Q}(\sqrt{-d})$ and χ the imaginary quadratic character for K. First assume that $d \equiv 3 \pmod 4$.

Proposition 14. *For $k \in \mathbb{N}$, we have*

$$\sum_{a=0}^{dp} a\chi\omega^{-1}(a)(-1)^a = \sum_{a=1}^{dp^k} a\chi\omega^{-1}(a)(-1)^a$$

Proof. Let $k \in \mathbb{N}$. Then,

$$\begin{aligned}
\sum_{a=0}^{dp^k} a\chi\omega^{-1}(a)(-1)^a &= \sum_{i=0}^{p^{k-1}-1} \sum_{a=1}^{dp} (a+dpi)\chi\omega^{-1}(a+dpi)(-1)^{a+dpi} \\
&= \sum_{r=0}^{p^{k-1}-1} (-1)^i \left(\sum_{a=1}^{dp} a\chi\omega^{-1}(a)(-1)^a + dpi \sum_{a=0}^{dp} \chi\omega(a)(-1)^a \right) \\
&= \left(\sum_{a=1}^{dp} a\chi\omega^{-1}(a)(-1)^a \right) \left(\sum_{i=0}^{p^{k-1}-1} (-1)^i \right) \\
&= \sum_{a=1}^{dp} a\chi\omega^{-1}(a)(-1)^a.
\end{aligned}$$

□

Now, using the fact that $\omega(a) \equiv \omega^p(a) \pmod{p^2}$, we see that

$$\begin{aligned}
\sum_{a=0}^{dp^{2r}} a\chi\omega^{-1}(a)(-1)^a &\equiv \sum_{\substack{a=0 \\ p\nmid a}}^{dp^{2r}} a^{(p-1)^2}\chi(a)(-1)^a \pmod{p^2} \\
&= \sum_{\substack{a=0 \\ p\nmid a}}^{dp^{2r}} \chi(a)(-1)^a + p\sum_{\substack{a=0 \\ p\nmid a}}^{dp^{2r}} q_p(a^{p-1})\chi(a)(-1)^a \\
&= p(p-1)\sum_{\substack{a=0 \\ p\nmid a}}^{dp^{2r}} q_p(a)\chi(a)(-1)^a \\
&\equiv -p\sum_{\substack{a=0 \\ p\nmid a}}^{dp^{2r}} q_p(a)\chi(a)(-1)^a \pmod{p^2}
\end{aligned}$$

and by the logarithmic properties of the Fermat quotient

$$\sum_{\substack{a=0 \\ p\nmid a}}^{dp^{2r}} q_p(a)\chi(a)(-1)^a \equiv q_p(\delta_{\chi,p}) \pmod{p}$$

where

$$\delta_{\chi,p} = \delta = \prod_{\substack{a=0 \\ p\nmid a}}^{dp^{2r}} a^{\chi(a)(-1)^a}.$$

Observe that $q_p(\delta) \equiv 0 \pmod{p}$ if and only if $\delta^{p-1} \equiv 1 \pmod{p^2}$. Similarly, if $d \not\equiv 3 \pmod 4$,

$$\begin{aligned}
\sum_{a=1}^{2dp^{2r}} a\chi\omega^{-1}(a) &\equiv \sum_{a=1}^{2dp^{2r}} a^{(p-1)^2}\chi(a) \pmod{p^2} \\
&\equiv -p\sum_{a=1}^{2dp^{2r}} q_p(a)\chi(a) \pmod{p^2} \\
&\equiv -pq_p(\delta) \pmod{p^2}
\end{aligned}$$

where

$$\delta_{\chi,p} = \delta = \prod_{\substack{a=0 \\ p\nmid a}}^{2dp^{2r}} a^{\chi(a)}.$$

Once again, $q_p(\delta) \equiv 0 \pmod{p}$ if and only if $\delta^{p-1} \equiv 1 \pmod{p^2}$. We thus define

$$\delta_{\chi,p} = \begin{cases} \prod_{\substack{a=0 \\ p\nmid a}}^{dp^{2r}} a^{\chi(a)(-1)^a} & \text{if } d \equiv 3 \pmod 4 \\ \prod_{\substack{a=0 \\ p\nmid a}}^{2dp^{2r}} a^{\chi(a)} & \text{if } d \not\equiv 3 \pmod 4 \end{cases}$$

We have thus shown the following:

Proposition 15. *Denote $K = \mathbb{Q}(\sqrt{-d})$, and χ to be the imaginary quadratic character for K. Then*

$$\lambda_p(K) > 1 \iff \delta_{\chi,p}^{p-1} \equiv 1 \pmod{p^2}.$$

Remark 6. *Compare proposition 15 to Gold's criterion (theorem 3.1.2).*

6.1 Expressing $\delta_{\chi,p}$ as Gauss Factorials ($d \equiv 3 \pmod 4$)

In this section we will see once again that $\delta_{\chi,p}$ is essentially congruent to a product of Gauss factorials modulo p^2. The difference is that we have arrived at the result via the Iwasawa series, and not using Gold's criterion 3.1.2. Hence, this method might be seen as an alternative proof of Theorem 3.1.2.

As before, let p be a prime such that $p \equiv 1 \pmod{d}$. Denote

$$\sigma_k^+ = \prod_{\substack{a=1 \\ a\equiv k \pmod d \\ a \text{ is even}}}^{p^{2r}}{}^{*} a, \quad \sigma_k^- = \prod_{\substack{a=1 \\ a\equiv k \pmod d \\ a \text{ is odd}}}^{p^{2r}}{}^{*} a$$

and

$$\epsilon_k^+ = \prod_{\substack{a=1 \\ a\equiv k \pmod d \\ a \text{ is even}}}^{dp^{2r}}{}^{*} a, \quad \epsilon_k^- = \prod_{\substack{a=1 \\ a\equiv k \pmod d \\ a \text{ is odd}}}^{dp^{2r}}{}^{*} a.$$

Here, we always view the subscript k modulo d accordingly. We also define

$$\pm(i) = \begin{cases} + & \text{if } i \text{ is even} \\ - & \text{if } i \text{ is odd} \end{cases}.$$

Observe that

$$\epsilon_k^+ \equiv \prod_{i=0}^{m-1} \sigma_{k-i}^{\pm(i)}, \quad \text{and} \quad \epsilon_k^- \equiv \prod_{i=0}^{m-1} \sigma_{k-i}^{\pm(i+1)}.$$

Consider the set

$$A_{r,m}(k) = \left\{ a \in \mathbb{N} \,:\, k\frac{p^{2r}-1}{m} \leq a \leq (k+1)\frac{p^{2r}-1}{m} \text{ and } \gcd(a,p) = 1 \right\}$$

We know the exact size of $A_{r,m}$ when $p \equiv 1 \pmod{m}$. That is,

Lemma 11. *Let $m \in \mathbb{Z}^+$ such that $p \equiv 1 \pmod{m}$. Then*

$$\#A_{1,m}(k) = p \cdot \frac{p-1}{m}$$

Proof. We have that

$$\frac{p^2-1}{m} = (p+1) \cdot \frac{p-1}{m}.$$

If $a \in \mathbb{Z}^+$ such that $a \leq (p-1)/m$, then

$$ap \leq p\frac{p-1}{m} < (p+1)\frac{p-1}{m}.$$

On the other hand, if $a = (p-1)/m + 1$, then

$$ap = \left(\frac{p-1}{m} + 1\right) p = p\frac{p-1}{m} + p > p\frac{p-1}{m} + \frac{p-1}{m} = (p+1)\frac{p-1}{m}.$$

Hence, the elements of $\left\{ a \,:\, 1 \leq a \leq \frac{p^2-1}{m} \text{ and } \gcd(a,p) > 1 \right\}$ consist of ap with $1 \leq a \leq (p-1)/m$. Therefore,

$$\begin{aligned}
&\#\left\{ a \,:\, 1 \leq a \leq \frac{p^2-1}{m} \text{ and } \gcd(a,p) = 1 \right\} \\
&\quad = \frac{p^2-1}{m} - \#\left\{ a \,:\, 1 \leq a \leq \frac{p^2-1}{m} \text{ and } \gcd(a,p) > 1 \right\} \\
&\quad = p \cdot \frac{p-1}{m}
\end{aligned}$$

□

Lemma 12. *Let $k, n, r \in \mathbb{Z}^+$ such that $p^r \equiv 1 \pmod{n}$. Then*

$$\frac{\left((k+1)\frac{p^{2r}-1}{n}\right)_p!}{\left(k\frac{p^{2r}-1}{n}\right)_p!} \equiv n^{A_{r,n}(k)} \prod_{a=0}^{\frac{p^{2r}-1}{n}-1}{}^{*} (na+(n-k)) \pmod{p^2}$$

Proof. Observe that

$$\begin{aligned}\frac{\left((k+1)\frac{p^{2r}-1}{n}\right)_p!}{\left(k\frac{p^{2r}-1}{n}\right)_p!} &\equiv \prod_{a=k\frac{p^{2r}-1}{n}+1}^{(k+1)\frac{p^{2r}-1}{n}}{}^{*} a \equiv \prod_{a=1}^{\frac{p^{2r}-1}{n}}{}^{*}\left(a+k\frac{p^{2r}-1}{n}\right) \\ &\equiv n^{A_{r,n}(k)} \prod_{a=0}^{\frac{p^{2r}-1}{n}-1}{}^{*} (na+(n-k)) \pmod{p^2}.\end{aligned}$$

□

Lemma 13. *For $1 \le k \le d$*

$$\sigma^+_{d-k} \equiv \begin{cases} C\dfrac{\left((k+1)\frac{p^2-1}{2d}\right)_p!}{\left(k\frac{p^2-1}{2d}\right)_p!} & \text{if } k \text{ even} \\ C\dfrac{\left((d+k+1)\frac{p^2-1}{2d}\right)_p!}{\left((d+k)\frac{p^2-1}{2d}\right)_p!} & \text{if } k \text{ odd} \end{cases} \quad \text{and} \quad \sigma^-_{d-k} \equiv \begin{cases} C\dfrac{\left((d+k+1)\frac{p^2-1}{2d}\right)_p!}{\left((d+k)\frac{p^2-1}{2d}\right)_p!} & \text{if } k \text{ even} \\ C\dfrac{\left((k+1)\frac{p^2-1}{2d}\right)_p!}{\left(k\frac{p^2-1}{2d}\right)_p!} & \text{if } k \text{ odd} \end{cases}$$

modulo p^2, where $C^{p-1} \equiv 1 \pmod{p^2}$.

Proof. First, if k is even, then $da-k$ is even when a is even. Hence, by Lemma 12

$$\sigma^+_{d-k} = \prod_{a=1}^{\frac{p^2-1}{2d}}{}^{*}(2da-k) \equiv C\frac{\left((k+1)\frac{p^2-1}{2d}\right)_p!}{\left(k\frac{p^2-1}{2d}\right)_p!}.$$

On the other hand, if k is odd $da-k$ is even when a is odd, and

$$\sigma^+_{d-k} = \prod_{a=1}^{\frac{p^2-1}{2d}}{}^{*}(2da-(d+k)) \equiv C\frac{\left((d+k+1)\frac{p^2-1}{2d}\right)_p!}{\left((d+k)\frac{p^2-1}{2d}\right)_p!}.$$

The congruences for σ^-_{d-k} follow in a similar way. □

Lemma 14. *Let $1 \leq k \leq d$. Then*

$$\epsilon_k^+ \equiv \begin{cases} C\dfrac{\left(k\frac{p^2-1}{d}\right)_p!}{\left(k\frac{p^2-1}{2d}\right)_p^2!} & \text{if } k \text{ even} \\ C\dfrac{\left(k\frac{p^2-1}{2d}\right)_p^2!}{\left(k\frac{p^2-1}{d}\right)_p!} & \text{if } k \text{ odd} \end{cases} \quad \text{and} \quad \epsilon_k^- \equiv \begin{cases} C\dfrac{\left(k\frac{p^2-1}{2d}\right)_p^2!}{\left(k\frac{p^2-1}{d}\right)_p!} & \text{if } k \text{ even} \\ C\dfrac{\left(k\frac{p^2-1}{d}\right)_p!}{\left(k\frac{p^2-1}{2d}\right)_p^2!} & \text{if } k \text{ odd} \end{cases}$$

modulo p^2, where $C^{p-1} \equiv 1 \pmod{p^2}$.

Proof. Suppose k is odd. We again have the telescopic product

$$\begin{aligned} \epsilon_k^+ &= \prod_{i=0}^{k} \sigma_{d-(d-k+i)}^{\pm(i+1)} \prod_{i=1}^{d-k-1} \sigma_{d-i}^{\pm(i+1)} \\ &\equiv C \prod_{i=0}^{k} \frac{\left((2d-k+i+1)\frac{p^2-1}{2d}\right)_p!}{\left((2d-k+i)\frac{p^2-1}{2d}\right)_p!} \prod_{i=1}^{d-k-1} \frac{\left((i+1)\frac{p^2-1}{2d}\right)_p!}{\left(i\frac{p^2-1}{2d}\right)_p!} \\ &\equiv C\frac{\left((d-k)\frac{p^2-1}{2d}\right)_p!}{\left((2d-k)\frac{p^2-1}{2d}\right)_p!} \equiv C'\frac{\left(k\frac{p^2-1}{2d}\right)_p!}{\left((d+k)\frac{p^2-1}{2d}\right)_p!} \equiv C''\frac{\left(k\frac{p^2-1}{2d}\right)_p^2!}{\left(k\frac{p^2-1}{d}\right)_p!} \pmod{p^2} \end{aligned}$$

The other congruences follow in a similar way. Further, $(C'')^{p-1} \equiv 1 \pmod{p^2}$ by Lemma 11. □

Putting all the pieces together, we have:

Theorem 6.1.1. *Suppose $d \equiv 3 \pmod 4$. Then*

$$\delta_{\chi,p}^{p-1} \equiv 1 \pmod{p^2} \iff \left(\prod_{\substack{k=1 \\ k \text{ even}}}^{d} \frac{\left(k\frac{p^2-1}{d}\right)_p^2!}{\left(k\frac{p^2-1}{2d}\right)_p^4!} \prod_{\substack{k=1 \\ k \text{ odd}}}^{d} \frac{\left(k\frac{p^2-1}{2d}\right)_p^4!}{\left(k\frac{p^2-1}{d}\right)_p^2!} \right)^{p-1} \equiv 1 \pmod{p^2}$$

Proof. Note that

$$\begin{aligned}
\delta_{\chi,p} &= C \prod_{\substack{k=1\\ \chi(k)=1\\ k \text{ even}}}^{d} \frac{\epsilon_k^+ \epsilon_{d-k}^-}{\epsilon_k^- \epsilon_{d-k}^+} \prod_{\substack{k=1\\ \chi(k)=1\\ k \text{ odd}}}^{d} \frac{\epsilon_k^+ \epsilon_{d-k}^-}{\epsilon_k^- \epsilon_{d-k}^+} \\
&\equiv C \prod_{\substack{k=1\\ \chi(k)=1\\ k \text{ even}}}^{d} \frac{\left(k\frac{p^2-1}{d}\right)_p^2! \left((d-k)\frac{p^2-1}{2d}\right)_p^4!}{\left(k\frac{p^2-1}{2d}\right)_p^4! \left((d-k)\frac{p^2-1}{d}\right)_p^2!} \prod_{\substack{k=1\\ \chi(k)=1\\ k \text{ odd}}}^{d} \frac{\left(k\frac{p^2-1}{2d}\right)_p^4! \left((d-k)\frac{p^2-1}{d}\right)_p^2!}{\left(k\frac{p^2-1}{d}\right)_p^2! \left((d-k)\frac{p^2-1}{2d}\right)_p^4!} \pmod{p^2} \\
&\equiv C \prod_{\substack{k=1\\ k \text{ even}}}^{d} \frac{\left(k\frac{p^2-1}{d}\right)_p^2!}{\left(k\frac{p^2-1}{2d}\right)_p^4!} \prod_{\substack{k=1\\ k \text{ odd}}}^{d} \frac{\left(k\frac{p^2-1}{2d}\right)_p^4!}{\left(k\frac{p^2-1}{d}\right)_p^2!} \pmod{p^2}
\end{aligned}$$

where $C^{p-1} \equiv 1 \pmod{p^2}$. □

6.2 Expressing $\delta_{\chi,p}$ as Gauss Factorials ($d \not\equiv 3 \pmod 4$)

Suppose $d \not\equiv 3 \pmod 4$, $p \equiv 1 \pmod{4d}$ and let χ be the imaginary quadratic character for $K = \mathbb{Q}(\sqrt{-d})$. Denote

$$\sigma_k \;=\; \prod_{\substack{a=1\\ a\equiv k \pmod{4d}}}^{p^2}{}^{*} a, \qquad \epsilon_k \;=\; \prod_{\substack{a=1\\ a\equiv k \pmod{4d}}}^{2dp^2}{}^{*} a.$$

Lemma 15. *Let $1 \le k \le 2d$. Then*

$$\epsilon_k \equiv C \frac{\left(k\frac{p^2-1}{4d}\right)_p^2!}{\left(k\frac{p^2-1}{2d}\right)_p!} \pmod{p^2} \quad \textit{and} \quad \epsilon_{2d+k} \equiv C \frac{\left(k\frac{p^2-1}{2d}\right)_p!}{\left(k\frac{p^2-1}{4d}\right)_p^2!} \pmod{p^2}$$

where $C^{p-1} \equiv 1 \pmod{p^2}$.

Proof. Notice that for $1 \le j \le 4d$, we have the telescopic product

$$\epsilon_j \equiv C \prod_{i=0}^{2d-1} \frac{\left((j-i)\frac{p^2-1}{4d}\right)_p!}{\left((j-1-i)\frac{p^2-1}{4d}\right)_p!} \equiv \begin{cases} C \dfrac{\left(j\frac{p^2-1}{4d}\right)_p!}{\left((j-2d)\frac{p^2-1}{4d}\right)_p!} & \text{if } j \ge 2d \\ C \dfrac{\left((2d-j)\frac{p^2-1}{4d}\right)_p!}{\left((4d-j)\frac{p^2-1}{4d}\right)_p!} & \text{if } j \le 2d \end{cases} \pmod{p^2}$$

□

Putting these pieces together, we have:

Theorem 6.2.1. *Suppose* $d \not\equiv 3 \pmod 4$. *Then*

$$\delta_{\chi,p}^{p-1} \equiv 1 \pmod{p^2} \iff \left(\prod_{\substack{k=1 \\ \chi(k)=1}}^{2d} \frac{\left(k\frac{p^2-1}{4d}\right)_p^4!}{\left(k\frac{p^2-1}{2d}\right)_p^2!} \prod_{\substack{k=1 \\ \chi(k)=-1}}^{2d} \frac{\left(k\frac{p^2-1}{2d}\right)_p^2!}{\left(k\frac{p^2-1}{4d}\right)_p^4!} \right)^{p-1} \equiv 1 \pmod{p^2}$$

Chapter 7

A "GOLD LIKE" CRITERION FOR $\lambda > 2$ (THE $\Delta_{\chi,P}$ PRODUCT).

Let p be a prime, $K = \mathbb{Q}(\sqrt{-d})$, χ be the imaginary quadratic character for K, $D = d$ if $d \equiv 3 \pmod 4$ and $D = 2d$ otherwise, and $\psi(a) = (-1)^a \chi(a)$ if $d \equiv 3 \pmod 4$ and $\psi(a) = \chi(a)$ otherwise. As in the previous section, we will transform the sum

$$\sum_{a=1}^{Dp} a^2 \psi(a)\omega^{-2}(a) - 2\sum_{a=1}^{Dp} a\psi(a)\omega^{-1}(a) - Dp\sum_{a=1}^{Dp} a\psi(a)\omega^{-2}(a)$$

into a product. Recall that $\lambda_p(K) > 2$ if and only if this sum is divisible by p^3. For a co-prime to p, we denote $q_{p^n}(a) = (a^{p^{n-1}(p-1)} - 1)/p^n$ to be the generalized Fermat quotient, which is an integer. We will need a few preliminary results.

Lemma 16. *Let a and b be co-prime to p and $r \in \mathbb{Z}$. Then*

i. $q_p(a) + q_p(b) = q_p(ab) - pq_p(a)q_p(b)$

ii. $(q_p(a))^2 + (q_p(b))^2 \equiv (q_p(ab))^2 - 2q_p(a)q_p(b) \pmod p$

iii. $q_{p^2}(ab) \equiv q_{p^2}(a) + q_{p^2}(b) \pmod{p^2}$

iv. $q_{p^2}(a^r) \equiv rq_{p^2}(a) \pmod{p^2}$

Proof. For (i)

$$\begin{aligned} q_p(a) + q_p(b) &= \frac{a^{p-1} - 1 + b^{p-1} - 1 + (ab)^{p-1} - (ab)^{p-1}}{p} \\ &= \frac{(ab)^{p-1} - 1}{p} + \frac{a^{p-1} - (ab)^{p-1}}{p} + \frac{b^{p-1} - 1}{p} \\ &= q_p(ab) - (a^{p-1} - 1)q_p(b) \\ &= q_p(ab) - pq_p(a)q_p(b). \end{aligned}$$

Next, (ii) is an easy consequence of the logarithmic properties of q_p. The proof for (iii) and (iv) are similar to the arguments for the logarithmic properties of q_p. $\square$

Lemma 17. *With all of the notation as above,*

$$\sum_{a=1}^{Dp^2} a^2\psi(a)\omega^{-2}(a) = \sum_{a=1}^{Dp} a^2\psi(a)\omega^{-2}(a) + D(p+1)p\sum_{a=1}^{Dp} a\psi(a)\omega^{-2}(a)$$

and

$$\sum_{a=1}^{Dp^2} a\psi(a)\omega^{-2}(a) = \sum_{a=1}^{Dp} a\psi(a)\omega^{-2}(a).$$

Proof. Suppose that $k > 1$. First, assume $\psi(a) = \chi(a)(-1)^a$, so that $\psi(a + dpi) = \chi(a)(-1)^{a+i}$. Then $\sum_{i=0}^{p-1}(-1)^i = 1$, $\sum_{i=0}^{p-1}(-1)^i i = (p+1)/2$, and $\sum_{a=1}^{Dp}\psi(a)\omega^{-2}(a) = 0$

$$\begin{aligned}
\sum_{a=1}^{Dp^2} a^2\psi(a)\omega^{-2}(a) &= \sum_{i=0}^{p-1}\sum_{a=1}^{Dp}(a+Dpi)^2\psi(a+Dpi)\omega^{-2}(a+dpi) \\
&= \sum_{a=1}^{Dp} a^2\psi(a)\omega^{-2}(a)\sum_{i=0}^{p-1}(-1)^i + 2Dp\sum_{a=1}^{Dp} a\psi(a)\omega^{-2}(a)(-1)^a\sum_{i=0}^{p-1} i(-1)^i \\
&\quad + (Dp)^2\sum_{i=0}^{p-1} i^2(-1)^i\sum_{a=1}^{Dp}\psi(a)\omega^{-2}(a) \\
&= \sum_{a=1}^{Dp} a^2\psi(a)\omega^{-2}(a) + D(p+1)p\sum_{a=1}^{Dp} a\psi(a)\omega^{-2}(a).
\end{aligned}$$

If $\psi(a) = \chi(a)$, then $\chi(a + Dpi) = \chi(a)(-1)^i$ from Lemma 4, and so the same calculation carries through. The second equality follows in a similar way. $\square$

From the Lemma, we have

$$\begin{aligned}
&\sum_{a=1}^{Dp} a^2\psi(a)\omega^{-2}(a) - 2\sum_{a=1}^{Dp} a\psi(a)\omega^{-1}(a) - Dp\sum_{a=1}^{Dp} a\psi(a)\omega^{-2}(a) \\
&\qquad = \sum_{a=1}^{Dp^2} a^2\psi(a)\omega^{-2}(a) - 2\sum_{a=1}^{Dp^2} a\psi(a)\omega^{-1}(a) - Dp(p+2)\sum_{a=1}^{Dp^2} a\psi(a)\omega^{-2}(a)
\end{aligned}$$

We now make the observation that

$$a^{-2(p^2-1)} = (p^2 q_{p^2}(a^{-2}) + 1)(pq_p(a^{-2}) + 1) \equiv p^2 q_{p^2}(a^{-2}) + pq_p(a^{-2}) + 1 \pmod{p^3}$$

and similarly

$$a^{-(p^2-1)} = (p^2 q_{p^2}(a^{-1}) + 1)(pq_p(a^{-1}) + 1) \equiv p^2 q_{p^2}(a^{-1}) + pq_p(a^{-1}) + 1 \pmod{p^3}.$$

We have from the previous proposition that

$$p^2(q_{p^2}(a^{-2}) - 2q_{p^2}(a^{-1})) \equiv 0 \pmod{p^3}$$

and

$$p(q_p(a^{-2}) - 2q_p(a^{-1})) = p(2q_p(a^{-1}) + p(q_p(a^{-1}))^2 - 2q_p(a^{-1})) = p^2(q_p(a^{-1}))^2.$$

Therefore,

$$\sum_{a=1}^{Dp^2} a^2\psi(a)\omega^{-2}(a) - 2\sum_{a=1}^{Dp^2} a\psi(a)\omega^{-1}(a) \equiv p^2 \sum_{\substack{a=1 \\ p\nmid a}}^{Dp^2} q_p(a^{\psi(a)q_p(a)}) \equiv p^2 q_p(\Phi_{\chi,p}) \pmod{p^3}$$

where

$$\Phi_{\chi,p} = \prod_{\substack{a=1 \\ p\nmid a}}^{Dp^2} a^{\psi(a)q_p(a)}.$$

Next we will look at the sum $\sum_{a=1}^{Dp^2} a\psi(a)\omega^{-2}(a)$ modulo p^2.

Lemma 18. *With all of the notation as above,*

$$\sum_{\substack{a=1 \\ p\nmid a}}^{Dp^2} \frac{\psi(a)}{a} \equiv 0 \pmod{p^2}$$

Proof. For $a \in \mathbb{Z}$, consider the map $\mathbb{Z}/D\mathbb{Z} \to \mathbb{Z}/D\mathbb{Z}$ given by $i \mapsto a + ip^2 \pmod{D}$. Since $\gcd(p, D) = 1$, we have that $a + ip^2 \equiv a + jp^2$ implies $i \equiv j \pmod{D}$. Hence

this map is a bijection, and $\sum_{i=0}^{D-1} \psi(a+ip^2) = \sum_{b=0}^{D-1} \psi(b)$. Therefore,

$$\sum_{\substack{a=1 \\ p\nmid a}}^{Dp^2} \frac{\psi(a)}{a} = \sum_{i=0}^{D-1} \sum_{\substack{a=1 \\ p\nmid a}}^{p^2-1} \frac{\psi(a+ip^2)}{a+ip^2} \equiv \sum_{b=0}^{D-1} \psi(b) \sum_{\substack{a=1 \\ p\nmid a}}^{p^2-1} \frac{1}{a} \equiv 0 \pmod{p^2}$$

since $\sum_{\substack{a=1 \\ p\nmid a}}^{p^2-1} \frac{1}{a} \equiv 0 \pmod{p^2}$. To see this, notice

$$\sum_{\substack{a=1 \\ p\nmid a}}^{p^2-1} \frac{1}{a} = \sum_{i=0}^{p-1} \sum_{a=1}^{p-1} \frac{1}{a+ip}$$

and

$$\frac{1}{a+ip} \equiv (a+ip)^{p(p-1)-1} = \sum_{j=0}^{p(p-1)-1} \binom{p(p-1)-1}{j} (ip)^j a^{p(p-1)-1-j} \equiv \frac{1}{a} - \frac{ip}{a^2} \pmod{p^2}.$$

Hence,

$$\sum_{\substack{a=1 \\ p\nmid a}}^{p^2-1} \frac{1}{a} \equiv \sum_{i=0}^{p-1} \sum_{a=1}^{p-1} \left(\frac{1}{a} - \frac{ip}{a^2} \right) \equiv \sum_{i=0}^{p-1} \sum_{a=1}^{p-1} \frac{1}{a} - p \sum_{a=1}^{p-1} \frac{1}{a^2} \sum_{i=0}^{p-1} i \equiv 0 \pmod{p^2}$$

since it is well known that $\sum_{a=1}^{p-1} 1/a \equiv 0 \pmod{p^2}$. □

Now, using the Lemma and the identity $a^2\omega^{-2}(a) \equiv (1 + pq_p(a^{-2})) \pmod{p^2}$, we have

$$\sum_{a=1}^{Dp^2} a\psi(a)\omega^{-2}(a) \equiv \sum_{\substack{a=1 \\ p\nmid a}}^{Dp^2} (1 + pq_p(a^{-2})) \frac{\psi(a)}{a} \equiv p \sum_{\substack{a=1 \\ p\nmid a}}^{Dp^2} q_p(a^{-2}) \frac{\psi(a)}{a} \pmod{p^2}.$$

Therefore,

$$Dp(p+2) \sum_{a=1}^{Dp^2} a\psi(a)\omega^{-2}(a) \equiv p^2 \sum_{\substack{a=1 \\ p\nmid a}}^{Dp^2} q_p(a^{-4D\psi(a)a^{p-2}}) \equiv p^2 q_p(\Psi_{\chi,p}) \pmod{p^3}$$

where

$$\Psi_{\chi,p} = \prod_{\substack{a=1 \\ p\nmid a}}^{Dp^2} a^{-4D\psi(a)a^{p-2}}.$$

So, we have that

$$\sum_{a=1}^{Dp^2} a^2\psi(a)\omega^{-2}(a) - 2\sum_{a=1}^{Dp^2} a\psi(a)\omega^{-1}(a) - Dp(p+2)\sum_{a=1}^{Dp^2} a\psi(a)\omega^{-2}(a) \equiv p^2 q_p(\Delta_{\chi,p}) \pmod{p^3}$$

where $\Delta_{\chi,p} = \Phi_{\chi,p}/\Psi_{\chi,p}$. From this we have

Theorem 7.0.1. *Suppose $\lambda_p(K) > 1$, and p does not divide the class number of K. Then $\lambda_p(K) > 2$ if and only if*

$$\Delta_{\chi,p}^{p-1} \equiv \prod_{\substack{a=1 \\ p\nmid a}}^{Dp^2} a^{\Sigma(a)(p-1)} \equiv 1 \pmod{p^2}$$

where $\Sigma(a) = \psi(a)q_p(a + 4Dp)$.

In the expression for $\Sigma(a)$, we have used the congruence $q_p(a + bp) \equiv q_p(a) - b/a \pmod{p}$. Again, compare this Theorem 3.1.2.

7.1 Generalized Hyper Gauss Factorials

We naturally define the hyper Gauss factorial of n with respect to p as

$$H_p(n) = \prod_{\substack{a=1 \\ \gcd(a,p)=1}}^{n} a^a$$

and if $\tau : \mathbb{Z} \setminus p\mathbb{Z} \to \mathbb{Z}$ is any function, then we define the generalized hyper Gauss factorial of n with respect to τ and p as

$$(n)_{p,\tau}! = \prod_{\substack{a=1 \\ \gcd(a,p)=1}}^{n} a^{\tau(a)}.$$

Definition 10. *If $r \in \mathbb{Z}^+$ such that $p^r \equiv 1 \pmod{m}$, then we say that p is 1-exceptional for m and $\tau : \mathbb{Z} \setminus p\mathbb{Z} \to \mathbb{Z}$ if*

$$\left(\frac{p^{2r}-1}{m}\right)_{p,\tau}^{p-1}! \equiv 1 \pmod{p^2}.$$

The next proposition can be viewed as Wilson's theorem for a certain generalized hyper Gauss factorials.

Proposition 16. *Suppose that,* $\tau(a) = (p-1)q_p(a)$ *for a co-prime to* p*. Then*

$$(p^m - 1)_{p,\tau}! \equiv 1 \pmod{p^m}$$

and

$$\left(\frac{p^m - 1}{2}\right)_{p,\tau}! \equiv \pm 1 \pmod{p^m}$$

Proof. Let g be a primitive root modulo $\mathbb{Z}/p^m\mathbb{Z}$. Then

$$(p^m)_{p,\tau}! \equiv \prod_{k=1}^{p^{m-1}(p-1)} (g^k)^{\tau(g^k)} \pmod{p^m}$$

(in the product above modulo p^m, the argument of $\tau(\cdot) = q_p(\cdot)(p-1)$ can be taken mod p^m by Euler's Theorem). So

$$\prod_{k=1}^{p^{m-1}(p-1)} (g^k)^{\tau(g^k)} = g^{\sum_{k=1}^{p^{m-1}(p-1)} k\tau(g^k)}.$$

We will look at the sum in the exponent of g, but first, recall one of the properties of the Fermat quotient is that for a, b co-prime to p,

$$q_p(ab) = q_p(a) + q_p(b) + pq_p(a)q_p(b).$$

From this we get for $k > 1$

$$\begin{aligned} q_p(a^k) &= kq_p(a) + pq_p(a)\left(\sum_{i=1}^{k-1} q_p(a^i)\right) = kq_p(a) + q_p(a)\left(\sum_{i=1}^{k-1}(a^{i(p-1)} - 1))\right) \\ &= kq_p(a) + q_p(a)\left(\sum_{i=1}^{k-1}(a^{i(p-1)} - 1))\right) = kq_p(a) + q_p(a)\left(\frac{a^{p-1} - a^{k(p-1)}}{1 - a^{p-1}} - k + 1\right). \end{aligned}$$

Then, assuming $a^{p-1} \not\equiv 1 \pmod{p^m}$ (which is the case for the primitive root g)

$$\sum_{k=1}^{p^{m-1}(p-1)} kq_p(a^k) = q_p(a) \sum_{k=1}^{p^{m-1}(p-1)} \left(\frac{a^{p-1} - a^{k(p-1)}}{1 - a^{p-1}} + k \right) \equiv 0 \pmod{p^{m-1}}$$

since,

$$\sum_{k=1}^{p^{m-1}(p-1)} a^{k(p-1)} = a^{p-1} \frac{1 - a^{p^{m-1}(p-1)}}{1 - a^{p-1}} \equiv 0 \pmod{p^m}$$

and

$$\sum_{k=1}^{p^{m-1}(p-1)} k \equiv 0 \pmod{p^{m-1}}$$

Therefore, $(p-1) \sum_{k=1}^{p^{m-1}(p-1)} kq_p(g^k) \equiv 0 \pmod{(p-1)p^{m-1}}$, and $(p^m)_{p,\tau}! \equiv 1 \pmod{p^m}$.

Notice that

$$\begin{aligned} 1 &\equiv \prod_{a=1}^{p^m}{}^{*} a^{(p-1)q_p(a)} \\ &\equiv \left(\prod_{a=1}^{\frac{p^m-1}{2}}{}^{*} a^{(p-1)q_p(a)} \right) \left(\prod_{a=1}^{\frac{p^m-1}{2}}{}^{*} (a+p^m)^{(p-1)q_p(a+p^m)} \right) \pmod{p^m} \\ &\equiv \left(\frac{p^m-1}{2} \right)_{p,\tau}^2 ! \pmod{p^m}. \end{aligned}$$

which implies that $\left(\frac{p^2-1}{2}\right)_{p,\tau}! \equiv \pm 1 \pmod{p^2}$. □

Proposition 17. *Let $m > 1$ in $\mathbb{Z}^+$ and suppose that, for a co-prime to p, $\tau(a) = (p-1)a^r$ for some $r \in \mathbb{Z}$ (if $r < 0$ then $\eta : \mathbb{Z} \setminus p\mathbb{Z} \to \mathbb{Z}$ which sends a to $(p-1)b$ such that $1 \leq b \leq p-1$ and $a^r b \equiv 1 \pmod{p}$). Then*

$$(p^m - 1)_{p,\tau}! \equiv 1 \pmod{p^m}$$

and

$$\left(\frac{p^m - 1}{2} \right)_{p,\tau} ! \equiv \pm 1 \pmod{p^m}$$

Proof. The proof will be similar to that of 16. Let g be a primitive root modulo p^m. Then g is also a primitive root modulo p^{m-1}. If $a \in \mathbb{Z}$ is co-prime to p, then $a \equiv g^k \pmod{p^m}$, and $a \equiv g^k \pmod{p^{m-1}}$ for some $k \in \mathbb{Z}$. So

$$(p^m - 1)_{p,\tau}! \equiv g^{(p-1)\sum_{k=1}^{p^{m-1}(p-1)} kg^{rk}} \pmod{p^m}.$$

Because $\gcd(r, p(p-1)) = 1$, $g_0 = g^r$ is a primitive root modulo p^{m-1}, and

$$\sum_{k=1}^{p^{m-1}(p-1)} kg_0^k \equiv 0 \pmod{p^{m-1}}.$$

Indeed,

$$\sum_{k=1}^{n} kx^{k-1} = \frac{d}{dx}\sum_{k=1}^{n} x^k = \frac{(1-x)(1-(n+1)x^n) + (x - x^{n+1})}{(1-x)^2}$$

and substituting $x = g_0$, and $n = p^{m-1}(p-1)$ gives the desired result. The second congruence follows by the same argument in Proposition 16. □

7.2 $\Delta_{\chi,p}$ as Generalized Hyper Gauss Factorials

In this section we prove two Theorems which are analogues of Theorems 6.1.1 and 6.2.1. The proofs are very similar, so we will suppress some of the details. Let $K = \mathbb{Q}(\sqrt{-d})$ and let χ be the corresponding imaginary quadratic character of K. We first assume $d \not\equiv 3 \pmod 4$. Denote $\tau(a) = (p-1)q_p(a)$, and $\eta(a) = (p-1)/a$ (again, we consider $\eta : \mathbb{Z} \setminus p\mathbb{Z} \to \mathbb{Z}$ which sends a to $(p-1)b$ such that $1 \leq b \leq p-1$ and $ab \equiv 1 \pmod p$). Let $\varphi : \mathbb{Z} \setminus p\mathbb{Z} \to \mathbb{Z}$ with $\varphi(a) \equiv \varphi(b) \pmod{p(p-1)}$, whenever $a \equiv b \pmod{p^2}$, and denote

$$\theta_{k,\varphi} = \prod_{\substack{a=1 \\ a \equiv k \pmod{4d}}}^{2dp^2 *} a^{\varphi(a)}, \qquad \text{and} \qquad \nu_{k,\varphi} = \prod_{\substack{a=1 \\ a \equiv k \pmod{4d}}}^{p^2 *} a^{\varphi(a)}.$$

If $\varphi(a) = \varphi(b)$ for $a \equiv b \pmod{p^2}$, then

$$\theta_{k,\varphi} \equiv \prod_{i=0}^{2d-1} \nu_{k-i,\varphi} \pmod{p^2}.$$

We will now prove analogues to some of the lemmas found in the previous section:

Lemma 19. *Suppose that $p \equiv 1 \pmod{4d}$. Then*

$$\frac{\left((k+1)^{\frac{p^2-1}{4d}}\right)_{p,\tau}!}{\left(k^{\frac{p^2-1}{4d}}\right)_{p,\tau}!} \equiv \nu_{-k,\tau}(4d)^{u_k(4d)}\sigma_{-k}^{-\tau(4d)} \pmod{p^2}$$

and

$$\frac{\left((k+1)^{\frac{p^2-1}{4d}}\right)_{p,\eta}!}{\left(k^{\frac{p^2-1}{4d}}\right)_{p,\eta}!} \equiv \nu_{-k,\eta}^{4d}(4d)^{4dt_k(4d)} \pmod{p^2}$$

where

$$\sigma_k = \prod_{\substack{a=1 \\ a\equiv k \pmod{4d}}}^{p^2}{}^{*} a, \quad u_k(n) = -(p-1)\sum_{\substack{a=1 \\ p\nmid na-k}}^{k^{\frac{p^2-1}{n}}} q_p(na-k), \quad t_k(n) = -(p-1)\sum_{\substack{a=1 \\ p\nmid na-k}}^{k^{\frac{p^2-1}{n}}} \frac{1}{na-k}.$$

Proof. Note that

$$\begin{aligned}\frac{\left((k+1)^{\frac{p^2-1}{4d}}\right)_{p,\tau}!}{\left(k^{\frac{p^2-1}{4d}}\right)_{p,\tau}!} &= \prod_{a=1}^{\frac{p^2-1}{4d}}{}^{*}\left(a+k\frac{p^2-1}{4d}\right)^{\tau\left(a+k\frac{p^2-1}{4d}\right)} \\ &\equiv (4d)^{u_k(4d)}\prod_{a=1}^{\frac{p^2-1}{4d}}{}^{*}(2da-k)^{\tau(4da-k)}\prod_{a=1}^{\frac{p^2-1}{4d}}{}^{*}(4da-k)^{-\tau(4d)} \pmod{p^2}.\end{aligned}$$

For the congruence involving η, we have

$$\begin{aligned}\frac{\left((k+1)\frac{p^2-1}{4d}\right)_{p,\eta}!}{\left(k\frac{p^2-1}{4d}\right)_{p,\eta}!} &= \prod_{a=1}^{\frac{p^2-1}{4d}}{}^{*}\left(a+k\frac{p^2-1}{4d}\right)^{\eta\left(a+k\frac{p^2-1}{4d}\right)} \\ &\equiv \left(\prod_{a=1}^{\frac{p^2-1}{4d}}{}^{*}\left(a+k\frac{p^2-1}{4d}\right)^{\eta(4da-k)}\right)^{4d} \pmod{p^2} \\ &\equiv \left((4d)^{t_k(4d)}\prod_{a=1}^{\frac{p^2-1}{4d}}{}^{*}(4da-k)^{\eta(4da-k)}\right)^{4d} \pmod{p^2}.\end{aligned}$$

□

Lemma 20. *Let $p \equiv 1 \pmod{4d}$ and $k \in \mathbb{Z}^+$. Then*

$$\left((2d+k)\frac{p^2-1}{4d}\right)_{p,\tau}! \equiv 2^{x_k(4d)-z_k(4d)}\frac{\left(k\frac{p^2-1}{2d}\right)_{p,\tau}!}{\left(k\frac{p^2-1}{4d}\right)_{p,\tau}!}\left(\left(k\frac{p^2-1}{2d}\right)_{p}!\right)^{-\tau(2)} \pmod{p^2}$$

and

$$\left((2d+k)\frac{p^2-1}{4d}\right)_{p,\eta}! \equiv \pm 2^{2y_k(4d)-v_k(4d)}\frac{\left(k\frac{p^2-1}{2d}\right)_{p,\eta}^2!}{\left(k\frac{p^2-1}{4d}\right)_{p,\eta}!} \pmod{p^2}$$

where

$$x_k(4d) = -(p-1)\sum_{\substack{a=1\\ p\nmid 2a-1}}^{k\frac{p^2-1}{4d}} q_p(2a-1), \quad z_k(4d) = (p-1)\sum_{\substack{a=1\\ p\nmid a}}^{k\frac{p^2-1}{4d}} q_p(a)$$

and

$$y_k(4d) = -(p-1)\sum_{\substack{a=1\\ p\nmid 2a-1}}^{k\frac{p^2-1}{4d}} \frac{1}{2a-1}, \quad v_k(4d) = (p-1)\sum_{\substack{a=1\\ p\nmid a}}^{k\frac{p^2-1}{4d}} \frac{1}{a}$$

Proof. Note,

$$\left((2d+k)\frac{p^2-1}{4d}\right)_{p,\tau}! = \left(\frac{p^2-1}{2}\right)_{p,\tau}! \prod_{a=1}^{k\frac{p^2-1}{4d}}{}^{*} \left(a+\frac{p^2-1}{2}\right)^{\tau\left(a+\frac{p^2-1}{2}\right)}$$

$$\equiv 2^{x_k(4d)} \prod_{a=1}^{k\frac{p^2-1}{4d}}{}^{*} (2a-1)^{\tau(2a-1)} \prod_{a=1}^{k\frac{p^2-1}{4d}}{}^{*} (2a-1)^{-\tau(2)}$$

$$\equiv 2^{x_k(4d)-z_k(4d)} \left(\frac{\left(k\frac{p^2-1}{2d}\right)_{p,\tau}!}{\left(k\frac{p^2-1}{4d}\right)_{p,\tau}!}\right)\left(\frac{\left(k\frac{p^2-1}{4d}\right)_{p}!}{\left(k\frac{p^2-1}{4d}\right)_{p}!\left(k\frac{p^2-1}{2d}\right)_{p}!}\right)^{\tau(2)} \pmod{p^2}$$

where we have again used the identity

$$\prod_{a=1}^{2n} \varphi(2a-1) = \frac{\prod_{a=1}^{n}\varphi(a)}{\prod_{a=1}^{2n}\varphi(2a)}$$

where φ is some function on $\mathbb{Z}^+$. Also,

$$\left((2d+k)\frac{p^2-1}{4d}\right)_{p,\eta}! = \left(\frac{p^2-1}{2}\right)_{p,\eta}! \prod_{a=1}^{k\frac{p^2-1}{4d}}{}^{*} \left(a+\frac{p^2-1}{2}\right)^{\eta\left(a+\frac{p^2-1}{2}\right)}$$

$$\equiv \pm 2^{2y_k(4d)} \prod_{a=1}^{k\frac{p^2-1}{4d}}{}^{*} (2a-1)^{2\eta(2a-1)} \equiv \pm 2^{2y_k(4d)-v_k(4d)} \frac{\left(k\frac{p^2-1}{2d}\right)_{p,\eta}^2!}{\left(k\frac{p^2-1}{4d}\right)_{p,\eta}!} \pmod{p^2}$$

□

Now, similar to the previous section (see Lemma 15), $\theta_{-k,\tau} \equiv \prod_{i=0}^{2d-1} \nu_{-(k+i),\tau}$ is a partially telescopic product, and applying Lemmas 19 and 20 (for $1 \le k \le 2d$),

$$\theta_{-k,\tau} \equiv \prod_{i=0}^{2d-1} \nu_{-(k+i)} \equiv \prod_{i=0}^{2d-1} \frac{\left((k+i+1)\frac{p^2-1}{4d}\right)_{p,\tau}!}{\left((k+i)\frac{p^2-1}{4d}\right)_{p,\tau}!} (4d)^{u_{k+i}(4d)} \sigma_{-(k+i)}^{\tau(4d)} \pmod{p^2}$$

$$\equiv (4d)^{U_k} \epsilon_{-k}^{\tau(4d)} \frac{\left((2d+k)\frac{p^2-1}{4d}\right)_{p,\tau}!}{\left(k\frac{p^2-1}{4d}\right)_{p,\tau}!} \equiv (4d)^{U_k} \epsilon_{-k}^{\tau(4d)} \frac{\left(k\frac{p^2-1}{2d}\right)_{p,\tau}! 2^{x_k(4d)-z_k(4d)}}{\left(k\frac{p^2-1}{4d}\right)_{p,\tau}^2! \left(k\frac{p^2-1}{2d}\right)_{p}^{\tau(2)}!} \pmod{p^2}$$

where $U_k = -\sum_{i=0}^{2d-1} u_{k+i}(4d)$ and ϵ_k are as in Lemma 15. Similarly, for $1 \le k \le 2d$,

$$\theta_{-(2d+k),\tau} \equiv (4d)^{U_{2d+k}} \epsilon_{-(2d+k)}^{\tau(4d)} \frac{\left(k\frac{p^2-1}{4d}\right)_{p,\tau}^2 ! \left(k\frac{p^2-1}{2d}\right)_p^{\tau(2)} !}{\left(k\frac{p^2-1}{2d}\right)_{p,\tau} ! 2^{x_k(4d)-z_k(4d)}} \pmod{p^2}.$$

On the other hand, for $1 \le k \le 2d$, we have modulo p^2,

$$\theta_{-k,\eta}^{4d} \equiv \pm \frac{\left(k\frac{p^2-1}{2d}\right)_{p,\eta}^2 !}{\left(k\frac{p^2-1}{4d}\right)_{p,\eta}^2 !} (4d)^{T_k} 2^{2y_k(4d)-v_k(4d)}, \qquad \theta_{-(k+2d),\eta}^{4d} \equiv \pm \frac{\left(k\frac{p^2-1}{4d}\right)_{p,\eta}^2 !}{\left(k\frac{p^2-1}{2d}\right)_{p,\eta}^2 !} (4d)^{T_{2d+k}} 2^{v_k(4d)-2y_k(4d)}$$

where $T_k = -4d\sum_{i=0}^{2d-1} t_{k+i}(4d)$. Now recall

$$\Delta_{\chi,p}^{p-1} \equiv \prod_{\substack{a=1 \\ p\nmid a}}^{2dp^2} a^{\Sigma(a)(p-1)} \equiv 1 \pmod{p^2}$$

where $\Sigma(a) = \chi(a) q_p(a+8dp) \equiv \chi(a)(q_p(a) - 8d/a) \pmod{p}$. Then we have

$$\Delta_{\chi,p}^{p-1} \equiv \left(\prod_{k=1}^{2d-1} (\theta_{k,\tau}/\theta_{2d+k,\tau})^{\chi(k)} \Big/ \prod_{k=1}^{2d-1} (\theta_{k,\eta}/\theta_{2d+k,\eta})^{8d\chi(k)} \right) \pmod{p^2}$$

and

Theorem 7.2.1. *Suppose $m \not\equiv 3 \pmod 4$, $\tau(a) = q_p(a)(p-1)$ and $\eta(a) = (p-1)/a$. Then*

$$\Delta_{\chi,p}^{p-1} \equiv 1 \pmod{p^2} \iff \delta_{\chi,p}^{-\tau(2d)} \mathcal{AB}\Phi_\tau/\Phi_\eta \equiv 1 \pmod{p^2}$$

where

$$\Phi_\tau = \prod_{k=1}^{2d-1} \left(\frac{\left(k\frac{p^2-1}{4d}\right)_{p,\tau}^4 !}{\left(k\frac{p^2-1}{2d}\right)_{p,\tau}^2 !} \right)^{\chi(k)}$$

$$\Phi_\eta = \prod_{k=1}^{2d-1} \left(\frac{\left(k\frac{p^2-1}{4d}\right)_{p,\eta} !}{\left(k\frac{p^2-1}{2d}\right)_{p,\eta} !} \right)^{4\chi(k)}$$

$$\mathcal{A} = \prod_{k=1}^{2d-1} \left(\left(k\frac{p^2-1}{2d} \right)_p ! \right)^{2\chi(k)\tau(2)}$$

and the error factor

$$\mathcal{B} = (4d)^{U-T} 2^{X-V}$$

where

$$U = \sum_{k=1}^{2d-1} \chi(k)(U_{4d-k} - U_{2d-k}), \quad T = \sum_{k=1}^{2d-1} \chi(k)(T_{2d-k} - T_{4d-k})$$

$$X = 2\sum_{k=1}^{2d-1} \chi(k)(x_{4d-k}(4d) - z_{4d-k}(4d)), \quad V = 4\sum_{k=1}^{2d-1} \chi(k)(2y_{4d-k}(4d) - v_{4d-k}(4d)).$$

Next, assume $d \equiv 3 \pmod 4$. If $\varphi : \mathbb{Z} \setminus p\mathbb{Z} \to \mathbb{Z}$ such that $\varphi(a) \equiv \varphi(b) \pmod{p(p-1)}$ whenever $a \equiv b \pmod{p^2}$, we denote

$$\theta^+_{k,\varphi} = \prod_{\substack{a=1 \\ a\equiv k \pmod d \\ a \text{ even}}}^{dp^2}{}^{*} a^{\varphi(a)}, \quad \theta^-_{k,\varphi} = \prod_{\substack{a=1 \\ a\equiv k \pmod d \\ a \text{ odd}}}^{dp^2}{}^{*} a^{\varphi(a)}$$

and

$$\nu^+_{k,\varphi} = \prod_{\substack{a=1 \\ a\equiv k \pmod d \\ a \text{ even}}}^{p^2}{}^{*} a^{\varphi(a)}, \quad \nu^-_{k,\varphi} = \prod_{\substack{a=1 \\ a\equiv k \pmod d \\ a \text{ odd}}}^{p^2}{}^{*} a^{\varphi(a)}.$$

Lemma 21. *For* $1 \le k \le d$

$$\nu^+_{-k,\tau} \equiv \begin{cases} \dfrac{\left((k+1)\frac{p^2-1}{2d}\right)_{p,\tau}!}{\left(k\frac{p^2-1}{2d}\right)_{p,\tau}!}(\sigma^+_{-k})^{\tau(2d)}(2d)^{-u_k(2d)} & \text{if } k \text{ even} \\ \dfrac{\left((d+k+1)\frac{p^2-1}{2d}\right)_{p,\tau}!}{\left((d+k)\frac{p^2-1}{2d}\right)_{p,\tau}!}(\sigma^+_{-k})^{\tau(2d)}(2d)^{-u_k(2d)} & \text{if } k \text{ odd} \end{cases} \pmod{p^2}$$

and

$$\nu^-_{-k,\tau} \equiv \begin{cases} \dfrac{\left((d+k+1)\frac{p^2-1}{2d}\right)_{p,\tau}!}{\left((d+k)\frac{p^2-1}{2d}\right)_{p,\tau}!}(\sigma^-_{-k})^{\tau(2d)}(2d)^{-u_k(2d)} & \text{if } k \text{ even} \\ \dfrac{\left((k+1)\frac{p^2-1}{2d}\right)_{p,\tau}!}{\left(k\frac{p^2-1}{2d}\right)_{p,\tau}!}(\sigma^-_{-k})^{\tau(2d)}(2d)^{-u_k(2d)} & \text{if } k \text{ odd} \end{cases} \pmod{p^2}.$$

Also,

$$(\nu^{+}_{-k,\eta})^{2d} \equiv \begin{cases} \frac{\left((k+1)\frac{p^2-1}{2d}\right)_{p,\eta}!}{\left(k\frac{p^2-1}{2d}\right)_{p,\eta}!}(2d)^{-2dt_k(2d)} & \text{if } k \text{ even} \\ \frac{\left((d+k+1)\frac{p^2-1}{2d}\right)_{p,\eta}!}{\left((d+k)\frac{p^2-1}{2d}\right)_{p,\eta}!}(2d)^{-2dt_k(2d)} & \text{if } k \text{ odd} \end{cases} \pmod{p^2}$$

and

$$(\nu^{-}_{-k,\eta})^{2d} \equiv \begin{cases} \frac{\left((d+k+1)\frac{p^2-1}{2d}\right)_{p,\eta}!}{\left((d+k)\frac{p^2-1}{2d}\right)_{p,\eta}!}(2d)^{-2dt_k(2d)} & \text{if } k \text{ even} \\ \frac{\left((k+1)\frac{p^2-1}{2d}\right)_{p,\eta}!}{\left(k\frac{p^2-1}{2d}\right)_{p,\eta}!}(2d)^{-2dt_k(2d)} & \text{if } k \text{ odd} \end{cases} \pmod{p^2}.$$

Proof. If k is even, then $da-k$ is even when a is even. Hence from Lemma 19

$$\nu^{+}_{-k,\tau} = \prod_{a=1}^{\frac{p^2-1}{2d}}{}^{*}(2da-k)^{\tau(2da-k)} \equiv \frac{\left((k+1)\frac{p^2-1}{2d}\right)_{p,\tau}}{\left(k\frac{p^2-1}{2d}\right)_{p,\tau}!}(\sigma^{+}_{-k})^{\tau(2d)} \pmod{p^2}.$$

The other congruences follow similarly. □

Similar to $\delta_{\chi,p}$ we get a partial telescopic product $\theta^{\pm}_{k,\tau} = \prod_{i=0}^{m-1}\nu^{\pm}_{k,\tau}$ (the difference, just like in the case for $d \not\equiv 3 \pmod 4$ is that we pick up some additional factors that amounted to $\mathcal{A}$, $\mathcal{B}$ and $\delta_{\chi,p}$ in Theorem 7.2.1). Therefore, we have

Theorem 7.2.2. *Suppose* $d \equiv 3 \pmod 4$ *and* $\tau(a) = q_p(a)(p-1)$ *and* $\eta(a) = (p-1)/a$. *Then*

$$\Delta^{p-1}_{\chi,p} \equiv 1 \pmod{p^2} \iff \delta^{-\tau(2d)}_{\chi,p}\mathcal{A}\Phi_\tau/\Phi_\eta \equiv 1 \pmod{p^2}$$

where

$$\Phi_\tau = \prod_{k=1}^{d}\left(\frac{\left(k\frac{p^2-1}{d}\right)^2_{p,\tau}!}{\left(k\frac{p^2-1}{2d}\right)^4_{p,\tau}!}\right)^{(-1)^k}$$

$$\Phi_\eta = \prod_{k=1}^{d} \left(\frac{\left(k\frac{p^2-1}{d}\right)_{p,\eta}!}{\left(k\frac{p^2-1}{2d}\right)_{p,\eta}!} \right)^{2(-1)^k}$$

$$\mathcal{A} = \prod_{k=1}^{d} \left(\left(k\frac{p^2-1}{2d}\right)_p ! \right)^{2(-1)^k\tau(2)}.$$

and the error factor

$$\mathcal{B} = (2d)^{U-T}2^{X-V}$$

where

$$U = \sum_{k=1}^{d-1} \chi(k)(U_{2d-k} - U_{2d-k}), \quad T = \sum_{k=1}^{d-1} \chi(k)(T_{2d-k} - T_{2d-k})$$

$$X = 2\sum_{k=1}^{d-1} \chi(k)(x_{d-k}(4d) - z_{d-k}(4d)), \quad V = 4\sum_{k=1}^{d-1} \chi(k)(2y_{2d-k}(2d) - v_{2d-k}(2d)).$$

7.3 Some Examples

In this section we will take a closer look at $\Delta_{\chi,p}$ for $K = \mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$. We will again let $\tau(a) = q_p(a)(p-1)$ and $\eta(a) = (p-1)/a$. Recall that for a and b co-prime to p

$$q_p(a) - b/a \equiv q_p(a+bp) \pmod{p} \quad \text{and} \quad rq_p(a) \equiv q_p(a^r) \pmod{p}$$

which we will use below.

Theorem 7.3.1. *Suppose p is a prime such that $p \equiv 1 \pmod 4$, $K = \mathbb{Q}(i)$ with imaginary quadratic character χ, and $\lambda_p(K) > 1$. Then*

$$\lambda_p(K) > 2 \iff \mathcal{B}\left(\frac{p^2-1}{4}\right)_{p,\Sigma}^{4(p-1)} ! \equiv 1 \pmod{p^2}$$

where $\Sigma(a) = q_p(a+p)$.

Proof. We have $\mathcal{A} = 1$, $\Phi_\tau = \left(\frac{p^2-1}{4}\right)_{p,\tau}^4 !$, and $\Phi_\eta = \left(\frac{p^2-1}{4}\right)_{p,\eta}^4 !$. Now use Theorem 7.2.1. □

Theorem 7.3.2. *Suppose p is a prime such that $p \equiv 1 \pmod 6$, $K = \mathbb{Q}(\sqrt{-3})$ with imaginary quadratic character χ, and $\lambda_p(K) > 1$. Then*

$$\lambda_p(K) > 2 \iff \mathcal{B}\left(\frac{\left(\frac{p^2-1}{6}\right)_{p,\Sigma_1}!}{\left(\frac{p^2-1}{3}\right)_{p,\Sigma_2}!}\right)^{2(p-1)} \equiv 1 \pmod{p^2}$$

where $\Sigma_1(a) = q_p(a^2 + p)$ and $\Sigma_2(a) = q_p(a^4 + 3p)$.

Proof. We have $\mathcal{A} = 1$, $\Phi_\tau = \frac{\left(\frac{p^2-1}{6}\right)_{p,\tau}^4 !}{\left(\frac{p^2-1}{3}\right)_{p,\tau}^8 !}$, and $\Phi_\eta = \frac{\left(\frac{p^2-1}{6}\right)_{p,\eta}^2 !}{\left(\frac{p^2-1}{3}\right)_{p,\eta}^6 !}$. Again, use Theorem 7.2.1. □

Chapter 8

ANOTHER (PARTIAL) CRITERION FOR $\lambda_P(K) > 2$

In this section, we attempt to get a criterion for $\lambda_p(K) > 2$ similar to that of Theorem 3.1.2 by extending the methods of Gold (13). While we have already given a criterion for $\lambda_p(K) > 2$, it would be useful for computational as well as theoretical reasons to have a criterion resembling Theorem 3.1.2 (see (10) and (33) for a computational and theoretical application of (13)). However, this is only a partial result, and the author hopes to revisit this topic in future research. We also note that the proof of Gold's criterion relies on relative genus theory (see (6)), and class field theory, (see Section 2.6 and (2)).

8.1 Preliminary Results

The next Theorem is due to Iwasawa (19), (but also see Theorem 4 in (40)),

Theorem 8.1.1 (Iwasawa)**.** *Let $k \subset L$ be number fields, such that L an unramified Abelian p-extension of k and denote H to be the p-Hilbert class field for k. Then $|A_L| = 1$ implies that $L = H$.*

Proof. Suppose that $L \neq H$. Then $|\mathrm{Gal}(H/L)| > 1$, and if H' is the p-Hilbert class field for L, then $L \subseteq H \subseteq H'$, and so $|A_L| = |\mathrm{Gal}(H'/L)| \geq |\mathrm{Gal}(H/L)| > 1$. □

Let k be an imaginary quadratic field in which $p = \mathfrak{p}\bar{\mathfrak{p}}$, and let $k_\infty = \bigcup_n k_n$ be the cyclotomic $\mathbb{Z}_p$ extension of k with $\mathrm{Gal}(k_n/k) \cong \mathbb{Z}/p^n\mathbb{Z}$. Denote $A(k_n)$ to be the class group of k_n. We will need the following result from Sands (32),

Theorem 8.1.2 (Sands)**.** *Suppose k is an imaginary quadratic field. Let $l < p-1$. Then the following are equivalent:*

(a) $|A(k_1)| = |A(k)|p^l$

(b) $\lambda_p(k) = l$

(c) $|A(k_n)| = |A(k)|p^{ln}$ *for each* $n \geq 0$.

Let H_{k_1} the p-Hilbert class field for k_1. Let L be any Abelian unramified extension of k_1 so that $k_1 \subseteq L \subseteq H_{k_1}$. If H_L is the p-Hilbert class field of L, then we have that $\mathrm{Gal}(H_{k_1}/L) \cong \mathrm{Gal}(H_L/L)/\mathrm{Gal}(H_L/H_{k_1}) \cong A_L/M$ where $M \cong \mathrm{Gal}(H_L/H_{k_1})$. We denote $A_L/M = B_L$. Now, if $\mathfrak{a} \in A_L$ and $\alpha \in G$, the Artin map $A_L \to \mathrm{Gal}(H_L/L)$ satisfies

$$\sigma_{\alpha\mathfrak{a}} = \tilde{\alpha}\sigma_{\mathfrak{a}}\tilde{\alpha}^{-1}$$

where $\tilde{\alpha}$ is any extension of $\alpha \in \mathrm{Gal}(L/E)$ to $\mathrm{Gal}(H_L/E)$. Therefore, if $[\mathfrak{a}] = \mathfrak{a}M$, we have the induced Artin map on $B_L \to \mathrm{Gal}(H_{k_1}/L)$ denoted by $\sigma_{[\mathfrak{a}]} = \left[\sigma_{\mathfrak{a}}|_{H_{k_1}}\right]$, and satisfies

$$\sigma_{[\alpha\mathfrak{a}]} = \bar{\alpha}\sigma_{[\mathfrak{a}]}\bar{\alpha}^{-1}$$

where $\bar{\alpha}$ is any extension of α to $\mathrm{Gal}(H_{k_1}/L)$. For $\mathfrak{a} \in A_L$, and $\alpha \in G$, we may also write $\sigma_{\mathfrak{a}}^{\alpha} = \alpha\sigma_{\mathfrak{a}}\alpha^{-1}$ (or $[\sigma_{[\mathfrak{a}]}^{\alpha}] = \alpha\sigma_{[\mathfrak{a}]}\alpha^{-1}$ for $[\mathfrak{a}] \in B_L$). We have the commutative diagram

$$\begin{array}{ccc} B_L & \longrightarrow & A_{k_1} \\ \cong\downarrow & & \downarrow\cong \\ \frac{\mathrm{Gal}(H_L/L)}{\mathrm{Gal}(H_L/H_{k_1})} & \longrightarrow & \mathrm{Gal}(H_{k_1}/k_1) \end{array}$$

with horizontal maps being injections. Suppose that $\mathfrak{P}$, and $\wp$ are primes above p in L, and H_{k_1} respectively. Then $\sigma_{[\mathfrak{P}]} \equiv \sigma_{\mathfrak{P}}|_{H_{k_1}} \pmod{\mathrm{Gal}(H_L/H_{k_1})}$ and if $x \in H_{k_1}$, we

have

$$\sigma_{\mathfrak{P}}(x) \equiv x^p \pmod{\wp}.$$

On the other hand, if $\mathfrak{p}_1$ is a prime above p in k_1, then for $x \in H_{k_1}$

$$\sigma_{\mathfrak{p}_1}(x) \equiv x^p \pmod{\wp}$$

and therefore $\sigma_{[\mathfrak{P}]} \mapsto \sigma_{\mathfrak{p}_1}$. Hence, if $\mathfrak{p}_1$ is non-trivial in A_{k_1}, then $[\mathfrak{P}]$ is also non-trivial in B_L, and they also have the same order.

Let k, $p = \mathfrak{p}\bar{\mathfrak{p}}$, k_1 be as above L the relative fixed field of the commutator subgroup of $\mathrm{Gal}(H_{k_1}/k)$ (the p-genus field for k_1/k, see (6)). Suppose that E is the inertia subfield for $\mathfrak{p}$ in L/k and suppose that $\mathfrak{p}$ splits in E. We have that $[E : k] = [L : E] = p$. Denote L' to be the fixed field of the commutator subgroup of $\mathrm{Gal}(H_{k_1}/E)$, where H_{k_1} is the p-Hilbert class field of k_1, and $G = \mathrm{Gal}(L/E) = \langle \tau \rangle$. If H_L is the p-Hilbert class field of L, then we have that $\mathrm{Gal}(H_{k_1}/L) \cong \mathrm{Gal}(H_L/L)/\mathrm{Gal}(H_L/H_{k_1}) \cong A_L/M$ where $M \cong \mathrm{Gal}(H_L/H_{k_1})$.

Proposition 18. *Let L, L', $G = \langle \tau \rangle$, and B_L be as above. Then Gal$(L'/L) \cong B/B^{1-\tau}$.*

Proof. Recall that $\mathrm{Gal}(L'/L)$ is the commutator subgroup of $\mathrm{Gal}(H_{k_1}/E)$. Let $a, b \in B_L$ and write $a = x\alpha$, $b = y\beta$ for $\alpha, \beta \in G$. Then a well known computation reveals

$$\begin{aligned} aba^{-1}b^{-1} &= \alpha x \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} = x^{\alpha}(yx^{-1})^{\alpha\beta}(\alpha\beta)\alpha^{-1}y^{-1}\beta^{-1} \\ &= x^{\alpha}(yx^{-1})^{\alpha\beta} y^{-\beta} = (x^{\alpha})^{1-\beta}(y^{\beta})^{\alpha-1}. \end{aligned}$$

On the other hand, if $\beta = 1$ and $\alpha = \tau$, we have that $y^{\tau-1} \in \mathrm{Gal}(L'/L)$. □

If A is a G-module, denote A^G to be the elements of A fixed by G. Then we have the exact sequence

$$0 \to B_L^G \to B_L \xrightarrow{1-\tau} B_L \to B_L/B_L^{1-\tau}.$$

But then $|B_L|/|B_L^G| = |B_L^{1-\tau}|$, which implies $|B_L^G| = |B_L/B_L^{1-\tau}|$.

Proposition 19. $[L' : L] = |B_L^G|$

Now, if $\langle\gamma\rangle = \mathrm{Gal}(L/k_1)$, let $\tilde{\gamma}$ be any extension of γ to $\mathrm{Gal}(H_{k_1}/k_1)$. Then the image of $\sigma_{[\gamma\mathfrak{P}]}$ in $\mathrm{Gal}(H_{k_1}/k_1)$ is $\tilde{\gamma}\sigma_{\mathfrak{p}_1}\tilde{\gamma}^{-1} = \sigma_{\mathfrak{p}_1}$. Therefore, $\sigma_{[\mathfrak{P}]} = \sigma_{[\gamma\mathfrak{P}]}$. Now, suppose that $\mathfrak{P}$ is a prime in L above $\mathscr{P}$ in E. Then since $\mathscr{P}$ is totally ramified in L/E, we have that G only fixes $\mathfrak{P}$, and hence, B_L^G is of order p generated by $\mathfrak{P}$. Therefore, we have

Proposition 20. *Suppose that* $\mathfrak{p}$ *splits in* E*. Then* $[L' : L] = p$*.*

Now, assume $\mathfrak{p}$ splits in E/k as $\mathfrak{p} = \mathscr{P}_1 \cdot \cdots \cdot \mathscr{P}_p$, and fix one of these primes $\mathscr{P}$ in E which lies above $\mathfrak{p}$. Denote E' to be the inertia sub-field of L'/E for $\mathscr{P}$. Notice that E'/E is Galois since $\mathrm{Gal}(L'/E')$ has index p in $\mathrm{Gal}(L'/E)$. Since $|A_E| = 1$ there must be at least one prime above $\mathfrak{p}$ that ramifies in E'/E, since if not E'/E is an unramified Abelian extension of E of degree p, so we denote

$$\mathscr{R} = \{i \,:\, \mathscr{P}_i \text{ ramifies in } E'/E\}$$

It follows that E' is the p-ray class field of conductor

$$\mathfrak{m} = \prod_{i\in\mathscr{R}} \mathscr{P}_i^{t_i}$$

for some $t_i \in \mathbb{Z}^+$. Now, if U_E are the units of E, C_E the class group of E, and $C_\mathfrak{m}$ the ray class group of E modulo $\mathfrak{m}$, we have the exact sequence

$$U_E \to (\mathcal{O}_E/\mathfrak{m})^\times \to C_\mathfrak{m} \to C_E \to 1$$

where $(\mathcal{O}_E/\mathfrak{m})^\times \to C_\mathfrak{m}$ is defined by $x + \mathfrak{m} \mapsto [x\mathcal{O}_E]$. Denoting $A_\mathfrak{m} = (C_\mathfrak{m})_p$, and taking p-parts of the exact sequence gives us

$$1 \to (\mathcal{O}_E/\mathfrak{m})_p^\times \to A_\mathfrak{m} \to 1$$

since U_E does not contain any primitive p-th roots of unity, and $|A_E| = 1$. Therefore, $(\mathcal{O}_E/\mathfrak{m})_p^\times \cong A_\mathfrak{m}$. If $A_\mathfrak{m}$ is the ray class group corresponding to E'/E, then we have $|A_\mathfrak{m}| = p$, and hence $(\mathcal{O}_E/\mathfrak{m})_p^\times \cong \prod_{i\in\mathscr{R}}(\mathcal{O}_E/\mathscr{P}_i^{t_i})_p^\times \cong \mathbb{Z}/p\mathbb{Z}$, which implies that there exists $r \in \mathscr{R}$ such that $t_r = 2$, and $t_i = 1$ for all other $i \in \mathscr{R}$. Hence,

Proposition 21. *If $\mathfrak{m}$ is the conductor for the p-ray class field extension E'/E, then $\mathfrak{m} = \mathcal{P}_r^2 \prod_{\substack{i\in\mathscr{R}\\ i\neq r}} \mathscr{P}_i$, for some $r \in \mathscr{R}$.*

Lemma 22. *Suppose that $\mathfrak{p}$ splits in E/k. Fix a prime $\mathscr{P}$ of E which lies above $\mathfrak{p}$, and denote h_E to be the class number for E such that $\mathscr{P}^{h_E} = (\alpha)$. Let E' and $\mathfrak{m}$ be as above, and let $\mathscr{P}' \mid \mathfrak{m}$ be such that $v_{\mathscr{P}'}(\mathfrak{m}) = 2$. Then the following are equivalent:*

(i.) $\mathscr{P}$ splits in E'/E

(ii.) $\mathscr{P}$ is trivial in $A_\mathfrak{m}$

(iii.) $\alpha^{p-1} \equiv 1 \pmod{(\mathscr{P}')^2}$

Proof. $(i.) \iff (ii.)$: Notice that $[E' : E] = p$, so if $\mathscr{P}$ splits in E'/E, then it splits completely. Therefore, the Frobenius automorphism $\sigma_\mathscr{P}$ is trivial, and hence $\mathscr{P}$ is trivial in $A_\mathfrak{m}$. On the other hand, if $\sigma_\mathscr{P}$ is trivial then the residue degree for E'/E is 1. Since $\mathscr{P}$ is unramified in E'/E it must be that $\mathscr{P}$ splits.

$(ii.) \iff (iii.)$: Since $A_E = 1$, we have that $\mathscr{P}$ is trivial in $A_\mathfrak{m}$ if and only if $\mathscr{P}^{h_E} = (\alpha)$ is also trivial. But then α is trivial in $(\mathcal{O}_E/\mathfrak{m})_p^\times \cong A_\mathfrak{m}$ if and only if $\alpha^{p-1} \equiv 1 \pmod{(\mathscr{P}')^2}$. □

8.2 Proof of the Partial Result

Theorem 8.2.1. *Let $k, E, \mathfrak{p}$ and $\mathscr{P}$ be as above. Suppose h_E is the class number for E and $\mathscr{P}^{h_E} = (\alpha)$. Then there exists a prime $\mathscr{P}'$ of E above p such that, if*

$\alpha^{p-1} \equiv 1 \pmod{(\mathscr{P}')^2}$, *then* $\lambda_p(K) > 2$.

Proof. Let $\mathscr{P}'$ be as in Lemma 22. Suppose that L' is the p-Hilbert class field for k_1 or equivalently, $\lambda_p(K) = 2$. If $\mathfrak{p}$ splits in E/k, then it must be that the prime $\mathfrak{p}_1$ in k_1 above $\mathfrak{p}$ also splits in L'/k. We also have that $\mathfrak{p}_1$ has order p in A_{k_1}, so $\mathfrak{p}_1$ has residue degree p in L'/k_1. Therefore, $\mathscr{P}$ has residue degree p in the degree p extension E'/E, since $\mathfrak{p}$ splits in E/k. □

Chapter 9

SOME FURTHER QUESTIONS

Dummit, Ford, Kisilevsky and Sands conjecture in (10) that given a fixed imaginary quadratic field K, there are infinitely many primes such that $\lambda_p(K) > 1$. We can now restate this conjecture in the case of $K = \mathbb{Q}(i)$ and $K = \mathbb{Q}(\sqrt{-3})$ in a way that may be of interest to those who study Euler and Glaisher numbers, as well as Gauss factorials:

Conjecture 1. *There are infinitely many primes* $p \equiv 1 \pmod 3$ *such that* $G_{p-1} \equiv 0 \pmod{p^2}$. *Equivalently, there are infinitely many primes* $p \equiv 1 \pmod 3$ *such that* p *is 1-exceptional for* $m = 3$.

Conjecture 2. *There are infinitely many primes* $p \equiv 1 \pmod 4$ *such that* $E_{p-1} \equiv 0 \pmod{p^2}$. *Equivalently, there are infinitely many primes* $p \equiv 1 \pmod 4$ *such that* p *is 1-exceptional for* $m = 4$.

REFERENCES

[1] Berndt, B.C., Evans, R.J., and Williams, K.S., Gauss and Jacobi Sums. Wiley, New York, 1998.

[2] Childress, N., Class Field Theory, Springer Science & Business Media, Oct 28, 2008, https://doi.org/10.1007/978-0-387-72490-4

[3] Childress, N., λ-invariants and Γ-transforms. Manuscripta Math., 64 (1989), 359-375.

[4] Childress, N., Examples of λ-invariants. Manuscripta Math., 68 (1990), 447-453.

[5] Childress, N., The coefficients of a p-adic measure and its Γ-transform. Manuscripta Math. 116, 249–263 (2005).

[6] Cornell, G., Relative genus theory and the class group of l-extensions. Transactions of the American Mathematical Society 277 (1983): 421-429.

[7] Cosgrave, J.B., and Dilcher, K., The multiplicative order of certain Gauss factorials. International Journal of Number Theory Vol. 07, No. 01, pp. 145-171 (2011)

[8] Cosgrave, J.B., and Dilcher, K., The multiplicative order of certain Gauss factorials, II., Funct. Approx. Comment. Math. 54 (1) 73 - 93, March 2016.

[9] Deuring, M., Die Typen der Multiplikatorenringe elliptischer Funktionenkörper Abh. Math. Sem. Hansischen Univ. 14, (1941). 197272.

[10] Dummit, D., Ford, D., Kisilevsky, H., and Sands, J., Computation of Iwasawa lambda invariants for imaginary quadratic fields. J. Number Theory, 37 (1991), 100-121.

[11] Ellenberg, J., Jain, S., and Venkatesh, A., Modelling λ-invariants by p-adic random matrices. September 2011 Communications on Pure and Applied Math- ematics 64(9):1243 - 1262

[12] Ferrero, B., and Washington, L., The Iwasawa invariant μ_p vanishes for abelian number fields. Ann. of Math., 109:377-395, 1979.

[13] Gold, R., The nontriviality of certain $\mathbb{Z}_l$-extensions, J. Number Theory 6 (1974), 369-373.

[14] Glaisher, J.W.L., On a Congruence Theorem relating to an Extensive Class of Coefficients, Proceedings of the London Mathematical Society, Volume s1-31, Issue 1, April 1899, 193–215.

[15] Glaisher, J.W.L., On a Set of Coefficients analogous to the Eulerian Numbers, Proc. London Math. Soc., 31 (1899), 216-235.

[16] Gross, B. H., Koblitz, N., Gauss Sums and the p-adic Γ-function. Annals of Mathematics, 109(3), (1979), 569–581. https://doi.org/10.2307/1971226

[17] Horie, K., A note on basic Iwasawa λ-invariants of imaginary quadratic fields, Inventiones Mathematicae, 1987, Volume 88, Number 1, Page 31

[18] Ito, A., On certain infinite families of imaginary quadratic fields whose Iwasawa λ-invariant is equal to 1, Acta Arith. 168 (2015), 301–339.

[19] Iwasawa, K., A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg, 20(1957), 257-258.

[20] Iwasawa, K., On Γ-extensions of algebraic number fields. Bull. Amer. Math. Soc., 65 (1959), 183-226.

[21] Iwasawa, K., On p-adic L-functions. Annals of Mathematics , Jan., 1969, Second Series, Vol. 89, No. 1 (Jan., 1969)

[22] Iwasawa, K, On the μ-invariants of $\mathbb{Z}_\ell$-extensions. Number Theory, Algebraic Geometry and Commutative Algebra, in Honor of Yasuo Akizuki, Kinokuniya, Tokyo (1973), pp. 1-11.

[23] Koblitz, N., p-adic Numbers, p-adic Analysis, and Zeta-Functions (Second Edition). Springer, New York, 1984.

[24] Kubota, T. and Leopoldt, H. W., Eine p-adische Theorie der Zetawerte. I. Einführung der p-adischen Dirichletschen L-funktionen. J. reine angew. Math., 214/215 (1964), 328-339.

[25] Lamzouri, Y., Li, X., Soundararajan, K., Conditional bounds for the least quadratic nonresidue and related problems, Math. Comp. 84 (2015), 2391–2412. Corrigendum ibid., Math. Comp. 86 (2017), 2551–2554

[26] Languasco, A., Trudgian, T. S., Uniform effective estimates for $|L(1,\chi)|$, Journal of Number Theory, Volume 236, 2022, Pages 245-260, ISSN 0022-314X, https://doi.org/10.1016/j.jnt.2021.07.019.

[27] Lang, S., Cyclotomic Fields I and II (Combined Second Edition), Springer, New York, 1990.

[28] Lehmer, E., On Congruences Involving Bernoulli Numbers and the Quotients of Fermat and Wilson. Annals of Mathematics, Second Series, Vol. 39, No. 2 (Apr., 1938), pp. 350-360

[29] Rosenberg, S., On the Iwasawa invariants of the Γ-transform of a rational function. Journal of Number Theory 109 (2004) 89-95

[30] Littlewood, J. E., On the class number of the corpus $P(\sqrt{-k})$, in: Collected Papers of J. E. Littlewood, Vol. II, Oxford Univ. Press, 1982, 920–934

[31] Rosser, J., Schoenfeld, L., Approximate formulas for some functions of prime numbers, Illinois Journal of Mathematics, Illinois J. Math. 6(1), 64-94, (March 1962)

[32] Sands, J., On small Iwasawa invariants and imaginary quadratic fields, Proceedings of the American Mathematical Society, Volume 112, Number 3, July 1991.

[33] Sands, J., On the non-triviality of the basic Iwasawa λ-invariant for an infinitude of imaginary quadratic fields. Acta Arithmetica 65.3 (1993): 243-248.

[34] Satoh, J., Iwasawa λ-invariants of Γ-transforms. Jounal of Number Theory 41, 98-101 (1992).

[35] Silverman, J., Advanced Topics in the Arithmetic of Elliptic Curves. Springer Science+Business Media New York 1994. https://doi.org/10.1007/978-1-4612-0851-8.

[36] Silverman, J., The Arithmetic of Elliptic Curves. Springer-Verlag New York 2009. https://doi.org/10.1007/978-0-387-09494-6.

[37] Sinnott, W. On the μ-invariant of the Γ-transform of a rational function. Invent. Math. 75, 273-282 (1984).

[38] Sloane, N. J. A., Sequence A239902 in The On-Line Encyclopedia of Integer Sequences (2014), published electronically at https://oeis.org

[39] Washington, L., Introduction to Cyclotomic Fields. Berlin-Heidelberg-New York: Springer 1982

[40] Yokoyama, A., On class numbers of finite algebraic number fields. Tohoku Mathematical Journal 17 (1965): 349-357.

[41] Zhang, W., Some identities involving the Euler and the central factorial numbers, Fibonacci Quart. 36 (2) (1998) 154–157.