Computing the Iwasawa lambda invariant of an abelian number field in Magma

A Thesis Presented

by

Michael J. Musty

to

The Faculty of the Graduate College

of

The University of Vermont

In Partial Fullfillment of the Requirements
for the Degree of Master of Science
Specializing in Mathematics

May, 2014

Accepted by the Faculty of the Graduate College, The University of Vermont, in partial fulfillment of the requirements for the degree of Master of Science, specializing in Mathematics.

Thesis Examination Committee:

Jonathan W. Sands, Ph.D. — Advisor

Richard M. Foote, Ph.D.

Byung S. Lee, Ph.D. — Chairperson

Cynthia J. Forehand, Ph.D. — Dean, Graduate College

Date: March 25, 2014

Abstract

In this work we describe a method for computing the Iwasawa λ-invariant of a number field with abelian Galois group. We then provide some explicit computations using the Magma Computational Algebra System (see [1]).

The classical study of Iwasawa invariants of number fields dates back to Iwasawa's original work in the 1950s. Given a number field K and a prime p, let K_n denote the n-th layer in the cyclotomic $\mathbf{Z}_p$-extension of K. In [10], Iwasawa proves an asymptotic formula for the exact power of p dividing the class number of K_n. The Iwasawa invariants are defined by this asymptotic formula.

A general description of the Iwasawa λ-invariants remains elusive, and a great deal of work has been done to compute this invariant in the case where K is an imaginary quadratic field (see [4]). For this case, an algorithm for computing the λ-invariant explicitly can be found in [13]. Yet for more complicated examples, no such implementation appears to exist. Even in the next simplest case, where K is a cyclotomic field, we find, after a thorough search through the literature, only one paper where these λ-invariants are computed explicitly (see [2]).

Following the work in [4, 2, 8, 13], we provide an explicit method to obtain λ-invariants for K a cyclotomic field. We then include examples from our implementation of this method in Magma [1] which, at present, does not possess any functionality of this kind.

Acknowledgements

Above all I would like to thank Professor Jonathan Sands for his patience and guidance throughout this project. This work would certainly not have been possible without his support. I would also like to thank Professor John Voight for his guidance from afar. His expertise in all things computational was also a vital part of this work. Lastly, I would like to thank my committee members Professor Richard Foote and Professor Byung Lee.

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Iwasawa Invariants

Fix an odd prime p and number field K. For any positive integer m let ζ_m denote a primitive m-th root of unity. Let $\mathbf{Q}_n$ be the unique extension of degree p^n over $\mathbf{Q}$ contained in $\mathbf{Q}(\zeta_{p^{n+1}})$. In other words, consider the tower in Figure 1.

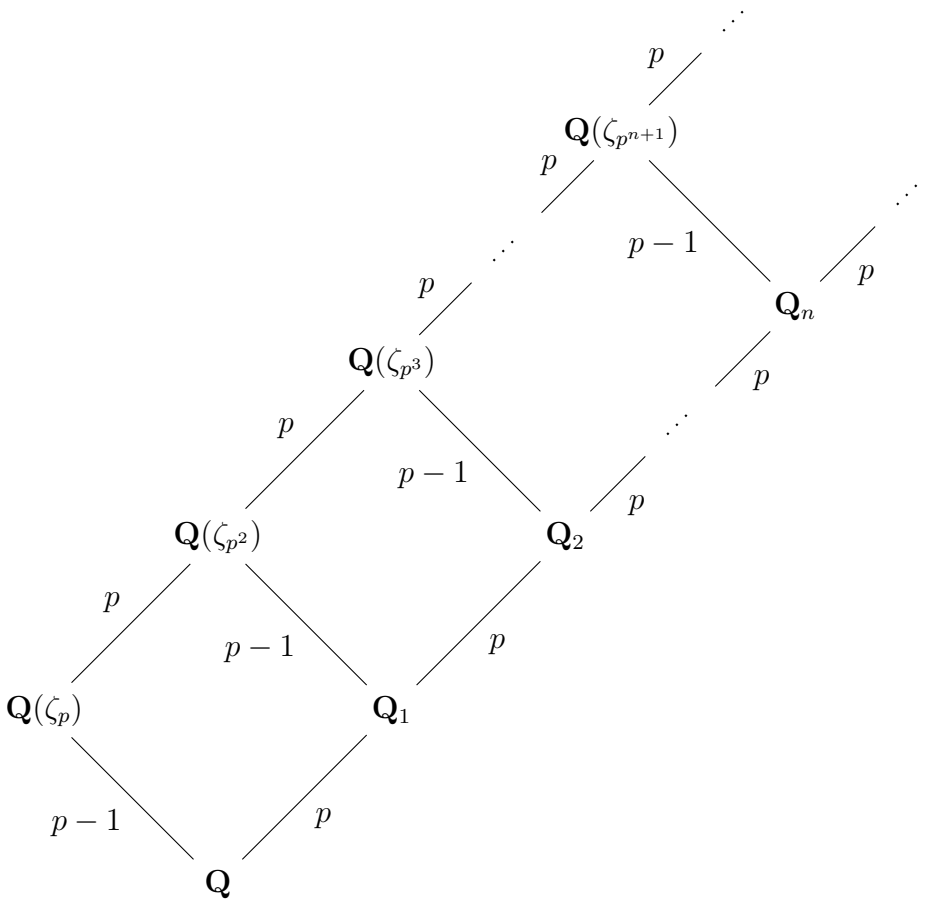

Figure 1: The tower $\mathbf{Q} = \mathbf{Q}_0 \subset \mathbf{Q}_1 \subset \mathbf{Q}_2 \subset \cdots \subset \mathbf{Q}_n \subset \cdots$.

Let $\mathbf{Q}_\infty = \cup_{n=1}^{\infty} \mathbf{Q}_n$. Let $G_n = \mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})$ and note that $G_n \cong (\mathbf{Z}/p^n\mathbf{Z})^\times$. Since the natural projection maps form a coherent system, we can identify $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$ as an inverse limit. Since this group is isomorphic to the additive group of p-adic integers, it is often referred to as a $\mathbf{Z}_p$-extension of $\mathbf{Q}$. Similarly we construct a $\mathbf{Z}_p$-extension of K by defining K_n to be the unique field of degree p^n over K in $K\mathbf{Q}_\infty$. We refer to this as the cyclotomic $\mathbf{Z}_p$ extension. Let $h(K_n)$ denote the class number of K_n. In [11] Iwasawa shows that the exact power of p dividing $h(K_n)$ is given by $\mu p^n + \lambda n + \nu$ for n sufficiently large. The integers $\mu = \mu_p(K), \lambda = \lambda_p(K)$, and $\nu = \nu_p(K)$ are called the Iwasawa invariants for p and K. For K an abelian number field, Ferrero and Washington show in [7] that $\mu = 0$ for every p. By the Kronecker-Weber Theorem (see [14, Chapter 14]) every abelian number field can be embedded in a cyclotomic extension $\mathbf{Q}(\zeta_\ell)$ for some integer ℓ. From now on we restrict to the case where $K = \mathbf{Q}(\zeta_\ell)$ with $\ell \geq 3$ a positive integer not divisible by p. By K^+ we denote $\mathbf{Q}(\zeta_\ell + \zeta_\ell^{-1})$, the totally real subfield of K and define $\lambda_p^-(K) = \lambda_p(K) - \lambda_p(K^+)$. For K an abelian number field it is conjectured in [9] that $\lambda_p(K^+) = 0$ so that $\lambda_p(K) = \lambda_p^-(K)$ in this case. This work is concerned with implementing (in Magma [1]) a method to determine $\lambda_p^-(K)$ explicitly for p an odd prime and $K = \mathbf{Q}(\zeta_\ell)$.

1.2 Related Work and Original Contributions

At present, the only explicit implementations to compute $\lambda_p^-(K)$ are for K an imaginary quadratic field (see [13]). Moreover, no functionality of this kind exists in Magma [1]. Although we closely follow some of the methodologies to compute

$\lambda_p^-(K)$ found in [4, 2, 8, 13], the explicit implementations to compute $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$ in Magma [1] are new.

In Section 2 we describe a method to compute $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$. In Section 3 and Section 4 we describe some results on p-adic L-functions and their relationship with class numbers. These results appear in [14, 11] and are merely included as background material for Section 2. Section 5 includes some explicit examples. In Section 6 we describe our implementation from a computational perspective including a brief complexity analysis. Section 6 also contains tables of $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$ for $3 \leq p \leq 331$ and $3 \leq \ell \leq 100$. Section 7 includes some directions for future work.

2 Description of the Method

Fix an odd prime p and number field $K = \mathbf{Q}(\zeta_\ell)$ with $\ell \geq 3$ not divisible by p. Let $\mathbf{Z}_p$ and $\mathbf{Q}_p$ denote the p-adic ring and field respectively. We compute $\lambda_p^-(K)$ explicitly using the methods from [8, 4, 6] described below. Let $G = \mathrm{Gal}(K/\mathbf{Q}) \cong (\mathbf{Z}/\ell\mathbf{Z})^\times$. A complex Dirichlet Character is a group homomorphism $\chi : (\mathbf{Z}/\ell\mathbf{Z})^\times \to \mathbf{C}^\times$. Complex Dirichlet characters are described in detail in [14, Chapter 3]. We say that χ is an odd character if $\chi(-1) = -1$. Let f be the minimum divisor of ℓ such that χ factors through the natural map $(\mathbf{Z}/\ell\mathbf{Z})^\times \to (\mathbf{Z}/f\mathbf{Z})^\times$. Such an f is called the conductor of χ. If χ is defined modulo its conductor, we say that χ is primitive. We call the set of primitive Dirichlet characters defined on $(\mathbf{Z}/\ell\mathbf{Z})^\times$ to be the set of characters associated to K. If χ_1 and χ_2 are primitive Dirichlet characters of conductors f_1 and f_2 respectively, then we can define a Dirichlet character

$$\chi_1\chi_2 : (\mathbf{Z}/\mathrm{lcm}(f_1, f_2)\mathbf{Z})^\times \to \mathbf{C}^\times$$

by $\chi_1\chi_2(a) = \chi_1(a)\chi_2(a)$. The resulting character need not be primitive, so we define $\chi_1\chi_2$ to be the primitive character inducing $\chi_1(a)\chi_2(a)$ of conductor dividing $\mathrm{lcm}(f_1, f_2)$. For example, if $\chi_2 = \chi_1^{-1}$ and $f_1 = f_2$, then the primitive character $\chi_1\chi_2$ has conductor 1. In this way we can define an abelian group structure on the set of primitive Dirichlet characters associated to K.

In a similar way we can define p-adic characters taking values in p-adic fields. Note in our case, χ takes values in the cyclotomic extension $\mathbf{Q}(\zeta_{\varphi(\ell)})$. We would

like to complete this field with respect to a non-archimedean absolute value that extends the p-adic absolute value on $\mathbf{Q}$. To do this let $\mathfrak{p}$ be a prime ideal in the factorization of p in $\mathbf{Q}(\zeta_{\varphi(\ell)})$. We can define a non-archimedean absolute value on $\mathbf{Q}(\zeta_{\varphi(\ell)})$ explicitly. For $c \in (0,1)$ and $\alpha \in \mathbf{Q}(\zeta_{\varphi(\ell)})$ we have

$$|\,\alpha\,| = \begin{cases} c^{\mathrm{ord}_{\mathfrak{p}}(\alpha)} & \text{if } \alpha \neq 0 \\ 0 & \text{if } \alpha = 0 \end{cases}$$

is an absolute value on $\mathbf{Q}(\zeta_{\varphi(\ell)})$ extending the corresponding p-adic absolute value on $\mathbf{Q}$. Note that different values of c yield equivalent absolute values. For our purposes we define c so that

$$|\,p\,| = \frac{1}{p}.$$

We will refer to this as the $\mathfrak{p}$-adic absolute value on $\mathbf{Q}(\zeta_{\varphi(\ell)})$.

The completion of $\mathbf{Q}(\zeta_{\varphi(\ell)})$ with respect to the $\mathfrak{p}$-adic absolute value is a field containing $\mathbf{Q}_p$. We will denote this field by $\mathbf{Q}_p(\chi)$ to emphasize that it contains all the character values for χ associated to $K = \mathbf{Q}(\zeta_\ell)$. Let $\mathcal{O}_\chi$ denote the ring of integers in $\mathbf{Q}_p(\chi)$. In this way we can view χ as taking values in the p-adic ring $\mathcal{O}_\chi$.

One particular p-adic character that we will need is the Teichmüller Character. Since the group of $(p-1)$st roots of unity are contained in $\mathbf{Z}_p^\times$ we can define a p-adic character $\omega : (\mathbf{Z}/p\mathbf{Z})^\times \to \mathbf{Z}_p^\times$ by defining $\omega(a)$ to be the unique $(p-1)$st root of unity in $\mathbf{Z}_p^\times$ such that $\omega(a) \equiv a \pmod{p}$. We call ω the Teichmüller character modulo p. Note that ω is a primitive Dirichlet character of conductor p taking

values in $\mathbf{Z}_p \subseteq \mathcal{O}_\chi$. Also note that ω is always odd. Since we assume that $\ell \neq 0 \pmod{p}$, if χ is any primitive Dirichlet character on $\mathrm{Gal}(K/\mathbf{Q})$ of conductor f dividing ℓ, then $\chi\omega$ is a primitive Dirichlet character of conductor pf. Let V be the cyclic group of $(p-1)$st roots of unity in $\mathbf{Z}_p^\times$ and let $D = \{1 + pa \mid a \in \mathbf{Z}_p\}$. Then

$$\mathbf{Z}_p^\times = V \times D.$$

Since $\omega(a) \in V$ for every $a \in \mathbf{Z}_p$, we can define $\langle a \rangle = a\omega(a)^{-1}$ so that every $a \in \mathbf{Z}_p$ can be written uniquely as

$$a = \omega(a)\langle a \rangle$$

where $\omega(a)$ and $\langle a \rangle$ denote the projection maps onto V and D respectively. Let $\mathbf{C}_p$ be the completion of an algebraic closure of $\mathbf{Q}_p$. We can identify V with the subgroup of $(p-1)$st roots of unity in $\mathbf{C}^\times$ by embedding the field of algebraic numbers in $\mathbf{C}_p$. In this way we can consider ω as a complex or p-adic character.

Fix a primitive Dirichlet character χ on $\mathrm{Gal}(K/\mathbf{Q})$ with conductor f. Define the Dirichlet L-function $L(s, \chi)$ by

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{q \text{ prime}} (1 - \chi(q)q^{-s})^{-1}.$$

This function converges for $\mathrm{Re}\, s > 1$ and can be analytically continued to a meromorphic function on all of $\mathbf{C}$. The values of $L(s, \chi)$ at the negative integers are given in terms of generalized Bernoulli numbers. Since there are several conventions for writing Bernoulli numbers, we follow those in [14]. For n a positive integer,

define the Bernoulli number B_n by

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

so that

$$B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_3 = 0, B_4 = -\frac{1}{30}, B_5 = 0, B_6 = \frac{1}{42}, \ldots.$$

Now let χ be a primitive Dirichlet character of conductor f and define the generalized Bernoulli number $B_{n,\chi}$ by

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

Also define the Bernoulli polynomial $B_n(X)$ by

$$\frac{te^{Xt}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(X) \frac{t^n}{n!}.$$

Using these definitions, we are now able to describe the values of $L(s, \chi)$ at the negative integers.

Proposition 1. *Let F be any multiple of f. Then*

$$B_{n,\chi} = F^{n-1} \sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right).$$

Proof. [14, Page 32] □

Theorem 2. *For $n \geq 1$ a positive integer we have that $L(1-n,\chi) = -B_{\chi,n}/n$.*

Proof. [14, Page 32] □

By interpolating the values of $L(s,\chi)$ at the negative integers one is able to obtain a p-adically continuous function on $\mathbf{Z}_p$ except at $s=1$ when χ is the trivial character. The resulting Leopoldt-Kubota p-adic L-function was first constructed in [12]. In Section 3 we describe these functions in a different way following Iwasawa's "alternate method" in [11, Section 8]. For completeness we include the following theorem without proof.

Theorem 3. *Let $\mathbf{C}_p$ denote the completion of an algebraic closure of $\mathbf{Q}_p$. Then there exists a p-adic meromorphic function $L_p(s,\chi)$ on $\{s \in \mathbf{C}_p \mid |\, s \,| < p^{1-1/(p-1)}\}$ such that for every positive integer n we have*

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

Proof. [14, Page 57] □

Next define the Dirichlet character $\rho : (\mathbf{Z}/p^2\mathbf{Z})^\times \to \mathbf{C}^\times$ by

$$\rho(a^p(1+p)^k) = \zeta_p^k$$

for every $a \in \{1,2,\ldots,p-1\}$ and $k \in \{0,1,\ldots,p-1\}$. Then ρ is a primitive Dirichlet character of conductor p^2 taking values in $\mathbf{Q}(\zeta_p)$. Moreover, this defines

p distinct characters ρ as ζ_p varies over all p-th roots of unity. Let

$$u = \exp_p(p)$$

where $\exp_p(s)$ is defined by the usual power series and converges for $s \in \mathbf{Z}_p$ with $|\, s \,| < p^{-1/(p-1)}$. Note that we can view ρ as a character on $\mathbf{Z}_p$ and define $\zeta_\rho = \rho(u)$ so that $\zeta_\rho^p = 1$. Then under these assumptions we have the following result in [4, Page 101].

Theorem 4. *For every χ a primitive Dirichlet character on $(\mathbf{Z}/\ell\mathbf{Z})^\times$ and every ρ defined in the above way, the p-adic L-function $L_p(s, \chi\omega)$ is associated with a power series (independent of ρ)*

$$G(T, \chi\omega) = \sum_{m=0}^{\infty} a_m T^m$$

with coefficients in $\mathcal{O}_\chi$ such that for any ρ as above we have

$$L_p(s, \chi\omega\rho) = G(\zeta_\rho^{-1} u^s - 1, \chi\omega).$$

for $|\, s \,| < p^{1-1/(p-1)}$.

Proof. See Section 3, [14, Chapter 7], and [11]. □

Let $w(T) = (1+T)^p - 1$. Since every coefficient of $w(T)$ except for the leading coefficient is in $\mathfrak{p}$ we say that $w(T)$ is a distinguished polynomial. Therefore we can

write

$$G(T, \chi\omega) = q(T)w(T) + F(T)$$

with $q(T) \in \mathcal{O}_\chi[[T]]$ and $F(T) \in \mathcal{O}_\chi[T]$ with degree less than the degree of $w(T)$. For the details of the above argument see [14, Proposition 7.2]. Therefore we have

$$G(T, \chi\omega) \equiv F(T) \pmod{w(T)} \tag{5}$$

where

$$F(T) = \sum_{k=0}^{p-1} b_k (1+T)^k \tag{6}$$

and $b_k \in \mathcal{O}_\chi$ for every k. We would like to find the coefficents of $G(T, \chi\omega)$ explicitly. Therefore we have

$$\begin{aligned} G(T, \chi\omega) = \sum_{m=0}^{\infty} a_m T^m &\equiv F(T) \\ &= \sum_{k=0}^{p-1} b_k (1+T)^k \\ &= \sum_{k=0}^{p-1} b_k \left(\sum_{m=0}^{k} \binom{k}{m} T^m \right) \\ &= \sum_{m=0}^{p-1} \left(\sum_{k=m}^{p-1} b_k \binom{k}{m} \right) T^m \pmod{w(T)} \end{aligned}$$

so that for $m < p$ we have

$$a_m \equiv \sum_{k=m}^{p-1} b_k \binom{k}{m} \pmod{\mathfrak{p}}. \tag{7}$$

Now substituting $T = \zeta_\rho^{-1} - 1$ we see that $w(\zeta_\rho^{-1} - 1) = 0$ and therefore

$$\sum_{k=0}^{p-1} b_k \zeta_\rho^{-k} = F(\zeta_\rho^{-1} - 1) = G(\zeta_\rho^{-1} - 1, \chi\omega). \tag{8}$$

Now substituting $s = 0$ into the equation from Theorem 4 we get

$$L_p(0, \chi\omega\rho) = G(\zeta_\rho^{-1} - 1, \chi\omega)$$

so that Equation 8 imples that

$$\sum_{k=0}^{p-1} b_k \zeta_\rho^{-k} = L_p(0, \chi\omega\rho).$$

Now by Theorem 3 we have

$$L_p(0, \chi\omega\rho) = -(1 - \chi\rho(p))B_{1,\chi\rho} = -B_{1,\chi\rho}.$$

Now by Proposition 1 and since $B_1(X) = X - 1/2$ we have

$$\begin{aligned}
-B_{1,\chi\rho} &= \sum_{i=1}^{fp^2} \chi\rho(i) B_1\left(\frac{i}{fp^2}\right) = \sum_{i=1}^{fp^2} \chi\rho(i)\left(\frac{i}{fp^2} - \frac{1}{2}\right) = \frac{-1}{fp^2} \sum_{\substack{i=1 \\ (i,p)=1}}^{fp^2} i\chi\rho(i) \\
&= \frac{-1}{fp^2} \sum_{\substack{i=1 \\ (i,p)=1}}^{p^2} \sum_{j=0}^{f-1} (i + jp^2)\chi(i + jp^2)\rho(i) \\
&= \frac{-1}{fp^2} \sum_{\substack{i=1 \\ (i,p)=1}}^{p^2} \sum_{j=0}^{f-1} jp^2\chi(i + jp^2)\rho(i) \\
&= \frac{-1}{f} \sum_{\substack{i=1 \\ (i,p)=1}}^{p^2} \sum_{j=0}^{f-1} j\chi(i + jp^2)\rho(i).
\end{aligned}$$

To continue, we define the function $L(i)$ as follows. The p-adic logarithm defined by the power series

$$\log_p(1 + x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$$

converges for $|\, x \,| < 1$ and defines a group isomorphism $D \to W$ with inverse $\exp_p(x)$ where

$$D = \{1 + pa \mid a \in \mathbf{Z}_p\} = 1 + p\mathbf{Z}_p$$

$$W = \{x \in \mathbf{Z}_p \mid |\, x \,| < p^{-1/(p-1)}\} = p\mathbf{Z}_p.$$

Then for $(i, p) = 1$ we have $\log_p(i) = \log_p(\langle i \rangle)$. Define $L(i)$ to be the unique integer

$$L(i) \equiv \frac{\log_p(i)}{p} \pmod{p}$$

with

$$-p < L(i) \leq 0.$$

Proposition 9. *With $L(i)$ defined as above for $(i,p)=1$ we have that $\rho(i) = \zeta_\rho^{L(i)}$.*

Proof. [4, Page 103]

$$\begin{aligned} L(i) = -k &\implies \log_p(i) \equiv -kp && \pmod{p^2} \\ &\implies \langle i \rangle \equiv \exp_p(-kp) = \exp_p(p)^{-k} = u^{-k} && \pmod{p^2} \\ &\implies \rho(i) = \rho(\langle i \rangle) = \rho(u^{-k}) = \rho(u)^{-k} = \zeta_\rho^{-k}. \end{aligned}$$

□

Continuing we have

$$\sum_{k=0}^{p-1} b_k \zeta_\rho^{-k} = \frac{-1}{f} \sum_{k=0}^{p-1} \left(\sum_{\substack{1 \leq i \leq p^2 \\ (i,p)=1 \\ L(i)=-k}} \sum_{j=0}^{f-1} j\chi(i+jp^2) \right) \zeta_\rho^{-k}. \tag{10}$$

Since Equation 10 defines a nondegenerate system of equations for the b_k we get

$$b_k = \frac{-1}{f} \sum_{\substack{1 \leq i \leq p^2 \\ (i,p)=1 \\ L(i)=-k}} \sum_{j=0}^{f-1} j\chi(i+jp^2). \tag{11}$$

Substituting this expression for b_k into Equation 7 we obtain the following theorem.

Theorem 12. *Using the same notation as above, for $m < p$ we have that*

$$-fa_m \equiv \sum_{\substack{i=1 \\ (i,p)=1}}^{p^2} \binom{-L(i)}{m} \sum_{j=0}^{f-1} j\chi(i+jp^2) \pmod{\mathfrak{p}}$$

where we use the convention that $\binom{k}{m} = 0$ if $m > k$.

Our main computational task in computing $\lambda_p^-(K)$ lies in the explicit use of Theorem 12. Next we describe how this theorem allows us to compute $\lambda_p^-(K)$.

Definition 13. *Let χ be a primitive Dirichlet character and $G(T,\chi) = \sum_{m=0}^{\infty} a_m T^m$ the power series in Theorem 4. Define $\lambda_p(\chi)$ to be the least m such that a_m is not in the unique maximal ideal $\mathfrak{p}$ of $\mathcal{O}_\chi$.*

Theorem 14. *Let p be an odd prime and $K = \mathbf{Q}(\zeta_\ell)$ with p not dividing ℓ. Then*

$$\lambda_p^-(K) = \sum_{\chi \text{ odd}} \lambda_p(\chi)$$

where the sum runs over the odd characters associated with K.

Proof. This is a consequence of the analytic class number formula and is described in Section 4. Also [11, Section 7], [14, Section 7.3]. □

From Theorem 14 it is now clear how to compute $\lambda_p^-(K)$. For every odd χ associated to K, compute the coefficients of the power series $G(T,\chi\omega)$ as in Theorem 12. Using these coefficients, compute $\lambda_p(\chi)$ by reducing the coefficients modulo $\mathfrak{p}$. Adding up the values of $\lambda_p(\chi)$, we obtain the desired value $\lambda_p^-(K)$.

Remark 15. It is important to note that in the above method, $\lambda_p(\chi)$ is only computed correctly if $\lambda_p(\chi) < p$. This process can be modified slightly (see [4]) to detect $\lambda_p(\chi) \geq p$. In practice $\lambda_p(\chi)$ is rarely larger than $p-1$. Indeed for the computations in Section 6 there are no instances of $\lambda_p(\chi) \geq p$. In fact, the first example with $\lambda_p(\chi) \geq p$ occurs when $p = 3$ and $\ell = 148$.

Remark 16. Since every abelian number field K embeds into $\mathbf{Q}(\zeta_\ell)$ for some ℓ, we can compute $\lambda_p^-(K)$ by summing $\lambda_p(\chi)$ over the characters corresponding to K in Theorem 14.

3 p-adic L-functions and Power Series

In this section we summarize some results from Iwasawa's "alternate method" (see [11, Section 6] and [14, Chapter 7]) to construct p-adic L-functions. One consequence of this construction is Theorem 4.

Definition 17. *Let ψ be a primitive Dirichlet character of conductor f_ψ. We say that ψ is of the first kind for p if $(f_\psi, p) = 1$ or $f_\psi = m_0 p$ with $(m_0, p) = 1$. If f_ψ is a power of p with $\psi(a)$ depending only on $\langle a \rangle$, then we call ψ a character of the second kind for p. The character $\psi = 1$ is considered a character of the second kind.*

To start let p be an odd prime and let m_0 be a positive integer with $(m_0, p) = 1$. For each nonnegative integer n define

$$q_n = m_0 p^{n+1}.$$

Now suppose χ is a primitive Dirichlet character of conductor $f_\chi = q_n$. Then by the isomorphisms

$$\begin{aligned}(\mathbf{Z}/m_0 p^{n+1}\mathbf{Z})^\times &\cong (\mathbf{Z}/m_0\mathbf{Z})^\times \times (\mathbf{Z}/p^{n+1}\mathbf{Z})^\times \\ (\mathbf{Z}/p^{n+1}\mathbf{Z})^\times &\cong (\mathbf{Z}/p\mathbf{Z})^\times \times \Big((1 + p\mathbf{Z}_p)/(1 + p^{n+1}\mathbf{Z}_p)\Big)\end{aligned}$$

we see that every such χ can be written uniquely as a character of the first kind for p multiplied by a character of the second kind for p.

By the construction of q_n we observe that $(a, q_n) = 1$ if and only if $(a, q_0) = 1$. For such integers a let $\sigma_n(a)$ be the residue class of a modulo q_n. The set of $\sigma_n(a)$ such that $(a, q_0) = 1$ form the multiplicative group

$$G_n = (\mathbf{Z}/q_n\mathbf{Z})^\times.$$

For $m \geq n \geq 0$ we have a natural projection map $G_m \to G_n$ defined by

$$\sigma_m(a) \mapsto \sigma_n(a)$$

for $(a, q_0) = 1$. Let Γ_n denote the kernel of the map $G_n \to G_0$. That is,

$$\Gamma_n = \{\sigma_n(a) \mid a \equiv 1 \pmod{q_0}\}.$$

Then Γ_n is a cyclic subgroup of G_n of order p^n. Also define

$$\Delta_n = \{\sigma_n(a) \mid a^{p-1} \equiv 1 \pmod{p^{n+1}}\}.$$

Then Δ_n is also a subgroup of G_n, and we have

$$G_n = \Gamma_n \times \Delta_n.$$

Now for $m \geq n \geq 0$, the maps $G_m \to G_n$ induce a surjective group homomorphism

$$\Gamma_m \to \Gamma_n$$

and a group isomorphism

$$\Delta_m \cong \Delta_n.$$

We can now construct

$$G = \varprojlim G_n, \quad \Gamma = \varprojlim \Gamma_n, \quad \Delta = \varprojlim \Delta_n$$

with respect to these group homomorphisms. Now observe that

$$G = \Gamma \times \Delta$$

and

$$\Delta \cong \Delta_0 = G_0.$$

Now for $a \in \mathbf{Z}$ with $(a, q_0) = 1$, let

$$\sigma_n(a) = \gamma_n(a)\delta_n(a)$$

under the direct decomposition $G_n = \Gamma_n \times \Delta_n$ for all $n \geq 0$. Then we have

$$\sigma(a) = \gamma(a)\delta(a)$$

under $G = \Gamma \times \Delta$ in the natural way.

Now let $a, b \in \mathbf{Z}$ both relatively prime to q_0. Then $\gamma_n(a) = \gamma_n(b)$ if and only if $\langle a \rangle \equiv \langle b \rangle \pmod{p^{n+1}\mathbf{Z}_p}$. Therefore $\gamma(a) = \gamma(b)$ if and only if $\langle a \rangle = \langle b \rangle$. From this

we have isomorphisms

$$\Gamma_n \cong (1 + p\mathbf{Z}_p)/(1 + p^{n+1}\mathbf{Z}_p)$$
$$\gamma_n(a) \mapsto \langle a \rangle (1 + p^{n+1}\mathbf{Z}_p)$$

and

$$\Gamma \cong 1 + p\mathbf{Z}_p$$
$$\gamma(a) \mapsto \langle a \rangle.$$

Let K be a finite extension of $\mathbf{Q}_p$ with ring of integers $\mathfrak{o}$ and maximal ideal $\mathfrak{p}$. Let $\Lambda = \mathfrak{o}[[X]]$ the ring of formal power series in X over $\mathfrak{o}$. For each $n \geq 0$, let R_n be the group ring of Γ_n over $\mathfrak{o}$. That is,

$$R_n = \mathfrak{o}[\Gamma_n] \subset K[\Gamma_n].$$

Now for $m \geq n \geq 0$, the group homomorphisms $\Gamma_m \to \Gamma_n$ induce compatible group ring homomorphisms

$$R_m \to R_n$$

and

$$K[\Gamma_m] \to K[\Gamma_n]$$

so we can define

$$R = \varprojlim R_n.$$

Theorem 18. *There exists a unique isomorphism* $\Lambda = \mathfrak{o}[[T]] \cong R = \mathfrak{o}[[\Gamma]]$ *given by*

$$1 + X \mapsto \gamma(1 + q_0).$$

Proof. For each $n \geq 0$ we have an isomorphism

$$\Lambda/(1 - (1 + X)^{p^n}) \cong R_n = \mathfrak{o}[\Gamma_n]$$

given by

$$1 + X \pmod{1 - (1 - X)^{p^n}} \mapsto \gamma_n(1 + q_0).$$

The limit of these isomorphisms gives the isomorphism $1 + X \mapsto \gamma(1 + q_0)$. □

Let π be a character of the second kind for p with conductor f_π and let K be a field containing the character values with ring of integers $\mathfrak{o}$ as above. Let $n_0 \geq 0$ be the least positive integer such that f_π divides q_n for every $n \geq n_0$. Now for a fixed integer t consider the residue class

$$\pi(a)^{-1}\langle a \rangle^{-t} \pmod{q_n\mathfrak{o}}$$

for $a \in \mathbf{Z}$ relatively prime to q_0. For all $n \geq n_0$, this residue class depends only on the residue class of $\gamma_n(a)$. Therefore for every $n \geq n_0$ we have maps

$$\phi^\pi_{t,n} : R_n = \mathfrak{o}[\Gamma_n] \to \mathfrak{o}/q_n\mathfrak{o}$$

given by

$$\gamma_n(a) \mapsto \pi(a)^{-1}\langle a\rangle^{-t} \pmod{q_n\mathfrak{o}}.$$

for $a \in \mathbf{Z}$ relatively prime to q_0. Now the set of all such maps for $m \geq n \geq n_0$ define a coherent system of maps and therefore we can define

$$\phi_t^\pi = \lim \phi_{t,n}^\pi : R = \mathfrak{o}[[\Gamma]] \to \mathfrak{o}$$

by

$$\phi_t^\pi(\gamma(a)) = \pi(a)^{-1}\langle a\rangle^{-t}$$

for $a \in \mathbf{Z}$ relatively prime to q_0. In particular,

$$\phi_t^\pi(\gamma(1+q_0)) = \zeta(1+q_0)^{-t}$$

where $\zeta = \pi(1+q_0)^{-1}$ is a root of unity in K. Under these conditions, we have the following result.

Theorem 19. *Let $f(X) \mapsto \xi$ under the isomorphism $\Lambda \cong R$ in Theorem 18. Then*

$$\phi_t^\pi(\xi) = f(\zeta(1+q_0)^{-t} - 1)$$

with

$$\zeta = \pi(1+q_0)^{-1}.$$

Proof. Let $f(X) = 1 + X$. Then $\xi = \gamma(1 + q_0)$ so that

$$\phi_t(\gamma(1 + q_0)) = \zeta(1 + q_0)^{-t} = f(\zeta(1 + q_0)^{-t} - 1).$$

This implies the same formula works for arbitrary $f(X) \in \mathfrak{o}[X]$ and thus, by density and continuity, for any $f(X) \in \mathfrak{o}[[X]]$. □

Let θ be an even Dirichlet character of the first kind for p with conductor $f_\theta = m_0$ or $f_\theta = m_0 p$ with $(m_0, p) = 1$. Let K be a finite extension of Q_p containing the values of θ. Also, let $\theta_1 = \theta\omega^{-1}$ so that

$$\langle a \rangle \theta(a) = a\theta_1(a)$$

for every a relatively prime to q_0. Now for $n \geq 0$ define

$$\begin{aligned} \xi_n^\theta &= -\frac{1}{2q_n} \sum_{\substack{0 \leq a < q_n \\ (a, q_0) = 1}} \langle a \rangle \theta(a) \gamma_n(a)^{-1} \\ &= -\frac{1}{2q_n} \sum_{\substack{0 \leq a < q_n \\ (a, q_0) = 1}} a\theta_1(a) \gamma_n(a)^{-1}. \end{aligned}$$

Now let

$$\eta_n^\theta = (1 - (1 + q_0)\gamma_n(1 + q_0)^{-1} \xi_n^\theta.$$

Both elements ξ_n^θ and η_n^θ are elements of $K[\Gamma_n]$ and in general one can show that for $m \geq n \geq 0$,

$$\xi_m^\theta \mapsto \xi_n^\theta, \quad \eta_m^\theta \mapsto \eta_n^\theta$$

under the map $K[\Gamma_m] \to K[\Gamma_n]$. Next one can show that η_n^θ is actually an element of $R_n = \mathfrak{o}[\Gamma_n]$ and for $m \geq n \geq 0$ we have

$$\eta_m^\theta \mapsto \eta_n^\theta$$

under the map $R_m \to R_n$. We can therefore define an element $\eta_\infty^\theta \in R$ by

$$\eta_\infty^\theta = \varprojlim \eta_n^\theta.$$

Now let

$$g(X, \theta) \mapsto \eta_\infty^\theta$$

under the isomorphism $\Lambda = \mathfrak{o}[[X]] \cong R$ in Theorem 18. The power series $g(X, \theta)$ has integral coefficients in the field containing the values of θ viewed as an extension of $\mathbf{Q}_p$. Thus we can identify every even Dirichlet character θ with a power series $g(X, \theta)$ depending only on θ. If we also suppose that θ is not the trivial character, then one can prove that ξ_n^θ is in R_n and for every $m \geq n \geq 0$ we have

$$\xi_m^\theta \mapsto \xi_n^\theta$$

under the map $R_m \to R_n$. Thus, as with η_∞^θ and $g(X, \theta)$, we can define $\xi_\infty^\theta \in R$ by

$$\xi_\infty^\theta = \varprojlim \xi_n^\theta$$

and

$$f(X,\theta) \mapsto \xi_\infty^\theta$$

under the isomorphism $\Lambda \cong R$ from Theorem 18. Now define

$$h(X,\theta) = 1 - \frac{1+q_0}{1+X} = 1 - (1+q_0)\sum_{n=0}^{\infty}(-1)^n X^n$$

and notice that

$$h(X,\theta) \mapsto 1 - (1+q_0)\gamma(1+q_0)^{-1}$$

under the isomorphism in Theorem 18. Now we can observe that

$$\eta_\infty^\theta = (1 - (1+q_0)\gamma_n(1+q_0)^{-1})\xi_\infty^\theta$$

and therefore

$$g(X,\theta) = h(X,\theta)f(X,\theta).$$

We can now describe the construction of the p-adic L-function $L_p(s,\chi)$. Let χ be an even Dirichlet character of conductor f_χ. Let

$$\chi = \theta\pi$$

with θ of the first kind and π of the second kind of conductors f_θ and f_π respectively. Then $f_\theta = m_0$ or $f_\theta = m_0 p$ with m_0 relatively prime to p. Let

$$q_0 = m_0 p$$

and

$$\zeta = \chi(1+q_0)^{-1} = \pi(1+q_0)^{-1}.$$

Since $\langle -1 \rangle = (-1)/\omega(-1)^{-1} = 1$ we have $\pi(-1) = 1$ and therefore θ is an even character. Therefore we can construct $f(X,\theta) \in \mathfrak{o}[[T]]$ as above where $\mathfrak{o}$ is the ring of integers in a finite extension of $\mathbf{Q}_p$ containing the values of θ. Note that since we allow for π to be the trivial character, $f_\chi = m_0$ or $f_\chi = m_0 p^{e+1}$ for some $e \geq 0$. Under these hypothesis we have the following theorem.

Theorem 20. *For every positive integer $n \geq 1$ we have*

$$2f(\zeta(1+q_0)^{1-n} - 1, \theta) = -(1 - \chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n}.$$

Proof. See [11, Section 6, Lemma 3]. □

In summary, we obtain elements of $\mathfrak{o}[\Gamma_n]$ for each n in a compatible way so as to obtain an element of $\mathfrak{o}[[\Gamma]]$. By the isomorphism in Theorem 18 we obtain a power series in $\mathfrak{o}[[T]]$ which gives us the p-adic L-functions.

4 The Analytic Class Number Formula

In this section we show how the power series in Section 3 allow us to compute Iwasawa λ-invariants by Theorem 14. We would like to compute $\lambda_p^-(K)$ for p an odd prime and $K = \mathbf{Q}(\zeta_\ell)$ with $(\ell, p) = 1$. Following the notation in Section 3 let

$$q_n = \ell p^{n+1}.$$

Then the cyclotomic $\mathbf{Z}_p$-extension of $K = \mathbf{Q}(\zeta_\ell)$ is

$$K_0 \subset K_1 \subset K_2 \cdots$$

where $K_n = \mathbf{Q}(\zeta_{\ell p^{n+1}}) = \mathbf{Q}(\zeta_{q_n})$ for every positive integer n. Let $h_n^- = h^-(K_n)$. By the analytic class number formula [14, Theorem 4.17] we have

$$h^-(K) = Qw \prod_{\chi \text{ odd}} \left(-\frac{1}{2} B_{1,\chi}\right) \tag{21}$$

where w is the number of roots of unity in K, Q is either 1 or 2, and χ is an odd character associated to K. By [14, Corollary 4.13], $Q = 2$ for every K_n. Let $w_n = \operatorname{lcm}(q_n, 2)$ be the number of roots of unity in K_n. Then following Equation 21 we obtain

$$h_n^- = 2w_n \prod_{\chi} \left(-\frac{1}{2} B_{1,\chi}\right) \tag{22}$$

where the product is taken over the odd χ with conductor dividing q_n. Since $w_n = w_0 p^n$, we get

$$h_n^- = h_0^- p^n \prod_{\substack{\chi \text{ odd} \\ f_\chi | q_n \\ f_\chi \nmid q_0}} \left(-\frac{1}{2} B_{1,\chi} \right). \tag{23}$$

Now write $\chi\omega = \theta\psi$ where θ is of the first kind for p and ψ is of the second kind for p, and let

$$\zeta_\psi = \psi(1 + f_\psi p)^{-1}.$$

Then by Theorem 20 we get that

$$2f(\zeta_\psi - 1, \theta) = -B_{1,\chi}.$$

Moreover, as χ varies (as in Equation 23), θ varies over the even characters with conductor dividing q_0 and ζ_ψ varies over all p^n-th roots of unity not equal to 1. Therefore, we have

$$h_n^- = h_0^- p^n \prod_{\substack{\theta \text{ even} \\ f_\theta | q_0}} \prod_{\substack{\zeta^{p^n} = 1 \\ \zeta \neq 1}} f(\zeta - 1, \theta). \tag{24}$$

Now let $\mathcal{O}$ be the ring containing the character values and define

$$A(T) = \prod_{\substack{\theta \text{ even} \\ f_\theta | q_0 \\ \theta \neq 1}} f(T, \theta) \quad \in \mathcal{O}[[T]]$$

so that Equation 24 becomes

$$h_n^- = h_0^- \prod_{\substack{\zeta^{p^n}=1 \\ \zeta \neq 1}} A(\zeta - 1). \tag{25}$$

Let $\mathfrak{p}$ be a prime above p in $\mathcal{O}$ with ramification index e and let r be the exact power of p dividing h_n^-. Then taking the $\mathfrak{p}$-adic valuation of Equation 25, for n sufficiently large we get

$$\mathfrak{p}^{er} = \prod_{\substack{\chi \text{ odd} \\ f_\chi | q_0}} \mathfrak{p}^{e(n\lambda_p(\chi)+\nu)} = \mathfrak{p}^{e\left(n\sum_\chi \lambda_p(\chi)+\nu\right)} \tag{26}$$

for some constant ν not depending on n. Theorem 14 now follows from Equation 26.

5 Examples

In this section we illustrate the computation of $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$ for specific p and ℓ.

Example 27. Let $p = 13$ and $\ell = 3$. Then there is a unique odd character χ on $\mathrm{Gal}(\mathbf{Q}(\zeta_\ell)/\mathbf{Q})$ which takes values in $\mathbf{Q}$. Computing $F(T)$ as in Equation 6 we get

$$\begin{aligned} F(T) = &-6T^{12} - 84T^{11} - 528T^{10} - 1974T^9 - 4896T^8 - 8496T^7 \\ &- 10590T^6 - 9570T^5 - 6246T^4 - 2892T^3 - 906T^2 - 156T. \end{aligned}$$

Now reducing the coefficients modulo p we get $\lambda_{13}(\chi) = 2$ and therefore by Theorem 14 we get that $\lambda_{13}^-(\mathbf{Q}(\zeta_3)) = 2$.

Example 28. Let $p = 11$ and $\ell = 5$. Then there are two odd characters χ_1 and $\chi_2 = \chi_1^3$ on $\mathrm{Gal}(\mathbf{Q}(\zeta_\ell)/\mathbf{Q})$ taking values in $\mathbf{Q}(i)$. Let $F_1(T)$ and $F_2(T)$ denote the polynomials as in Equation 6 for χ_1 and χ_2 respectively. Then we have

$$\begin{aligned} F_1(T) = &\ 10T^{10} + (10i + 100)T^9 + (80i + 460)T^8 + (270i + 1270)T^7 \\ &+ (480i + 2300)T^6 + (430i + 2810)T^5 + (70i + 2310)T^4 \\ &+ (-240i + 1240)T^3 + (-230i + 410)T^2 + (-70i + 70)T \\ F_2(T) = &\ 10T^{10} + (10i + 100)T^9 + (80i + 460)T^8 + (270i + 1270)T^7 \\ &+ (480i + 2300)T^6 + (430i + 2810)T^5 + (70i + 2310)T^4 \\ &+ (-240i + 1240)T^3 + (-230i + 410)T^2 + (-70i + 70)T. \end{aligned}$$

Now let $\mathfrak{p}$ be a prime above 11 in $\mathbf{Q}(i)$ and reduce the coefficients modulo $\mathfrak{p}$. Since

11 is inert in the ring of integers of $\mathbf{Q}(i)$ we have $\mathfrak{p} = (11)$ and therefore we can just reduce modulo 11 to get that $\lambda_{11}(\chi_1) = \lambda_{11}(\chi_2) = 1$. Thus $\lambda_{11}^{-}(\mathbf{Q}(\zeta_5)) = 2$.

Example 29. Let $p = 37$ and $\ell = 7$. Then there are three odd characters $\chi_1, \chi_2 = \chi_1^3$, and $\chi_3 = \chi_1^5$ on $\mathrm{Gal}(\mathbf{Q}(\zeta_\ell)/\mathbf{Q})$ taking values in $\mathbf{Q}(\zeta)$ where ζ is a primitive 6-th root of unity. Let $F_1(T), F_2(T)$, and $F_3(T)$ denote the polynomials as in Equation 6 for χ_1, χ_2, and χ_3 respectively. Then we have

$$F_1(T) = (-50\zeta + 24)T^{36} + \cdots + (37436\zeta - 39046)T^2 + (1910\zeta - 1880)T - 2\zeta - 8$$
$$F_2(T) = -28T^3 6 + \cdots - 158382T^2 - 8554T$$
$$F_3(T) = (50\zeta - 26)T^{36} + \cdots + (-37436\zeta - 1610)T^2 + (-1910\zeta + 30)T + 2\zeta - 10.$$

In the ring of integers of $\mathbf{Q}(\zeta)$ we have $(p) = \mathfrak{p}_1\mathfrak{p}_2$. Using either prime above p we compute $\lambda_{37}(\chi_1) = 0$, $\lambda_{37}(\chi_2) = 1$, and $\lambda_{37}(\chi_3) = 0$. Thus $\lambda_{37}^{-}(\mathbf{Q}(\zeta_7)) = 1$.

6 Computations

In this section we describe our implementation of the algorithm described in Section 2, analyze its complexity, and tabulate $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$ for $3 \leq p \leq 331$ and $3 \leq \ell \leq 100$.

6.1 Algorithm and Complexity

Below we analyze the algorithm described in Section 2 to compute $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$.

Algorithm 30. Let p be an odd prime, and $\ell \geq 3$ a positive integer.

1. Create $F = \mathbf{Q}(\zeta_{\varphi(\ell)})$ and $\mathbf{Z}_F = \mathbf{Z}[\zeta_{\varphi(\ell)}]$.
2. Create G the group of Dirichlet characters on $(\mathbf{Z}/\ell\mathbf{Z})^\times$.
3. Compute $\mathfrak{p}$ a prime above p in $\mathbf{Z}_F$.
4. Initialize $\lambda_p^-(\mathbf{Q}(\zeta_\ell)) \leftarrow 0$.
5. For each odd $\chi \in G$ compute $\lambda_p(\chi)$ as in Definition 13.
   (a) Initialize $m \leftarrow 0$.
   (b) Compute the coefficient $a_m \in \mathbf{Z}_F$ as in Theorem 12.
   (c) Compute $\mathrm{ord}_{\mathfrak{p}}(a_m)$.
      i. If $\mathrm{ord}_{\mathfrak{p}}(a_m) > 0$ then assign $m \leftarrow m + 1$ and go to Step 5(b).
      ii. Else assign $\lambda_p^-(\mathbf{Q}(\zeta_\ell)) \leftarrow \lambda_p^-(\mathbf{Q}(\zeta_\ell)) + m$.
6. Return $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$.

By Theorem 14 we obtain the correct value of $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$ after a finite number of iterations of Step 5. The methods for carrying out Step 1, Step 2, Step 3, and Step 5(c) can be found in[3]. For Step 5(b) we follow Theorem 12. Since Step 5(b) is the dominant factor in the running time of this algorithm, we only analyze this step. To do this, first note that addition in $\mathbf{Z}_F$ can be done in $O(\varphi(\ell)\log p)$ bit operations, and multiplication in $\mathbf{Z}_F$ can be done in $O(\varphi(\ell)^2\log^2 p)$ bit operations. Computing the inner sum on the right hand side of the congruence in Theorem 12 requires $f \leq \ell$ multiplications in $\mathbf{Z}_F$. The f additions in this inner sum can be absorbed into the running time of the multiplications, and we can therefore obtain the inner sum in $O(\ell^3\log^2 p)$ bit operations. The binomial coefficient in Theorem 12 is negligible. The outer sum requires less than p^2 computations of the inner sum which absorbs the p^2 multiplications and additions at this stage. Thus we can compute Step 5(b) in $O(p^2\ell^3\log^2 p)$ bit operations. Since the number of iterations of Step 5(b) is less than ℓ, we can compute $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$ in $O(p^2\ell^4\log^2 p)$ bit operations.

6.2 Tables of $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$

In the following tables we compute $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$ for $3 \leq p \leq 331$ and $3 \leq \ell \leq 100$. All computations were done in Magma [1]. We verified these values with those in [2], and the boxed entries denote what we believe to be corrections to those values.

Table 1: The values $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$ for $3 \leq p \leq 97$ and $3 \leq \ell \leq 26$.

ℓ \ p	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97
3	$*$	0	1	0	2	0	1	0	0	1	1	0	1	0	0	0	1	1	0	1	1	0	0	1
4	0	1	0	0	1	1	0	0	1	0	1	1	0	0	1	0	1	0	0	1	0	0	1	1
5	0	$*$	0	2	0	0	0	0	0	2	0	2	0	0	0	0	2	0	2	0	0	0	0	0
6	$*$	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	1	0	0	0	1
7	0	0	$*$	1	0	0	0	1	3	0	1	0	3	0	1	0	0	1	3	0	1	0	0	0
8	1	1	0	1	1	2	1	0	1	0	1	2	1	0	1	1	1	1	0	2	0	1	2	2
9	$*$	0	1	0	2	0	4	0	0	1	3	0	1	0	0	0	1	1	0	3	1	0	0	1
10	0	$*$	0	0	0	0	0	0	0	0	0	2	0	0	0	0	2	0	0	0	0	0	0	0
11	1	10	0	$*$	0	0	0	5	0	1	1	0	0	1	1	1	0	5	1	0	0	0	5	1
12	$*$	1	0	0	2	0	0	0	1	0	2	0	0	0	1	0	2	0	0	2	0	0	0	2
13	6	0	0	0	$*$	$\boxed{0}$	0	0	2	0	0	0	0	0	6	0	2	0	0	0	6	0	0	0
14	6	2	$*$	0	1	0	0	0	3	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
15	$*$	$*$	0	0	0	1	1	1	0	4	0	0	0	1	1	0	4	0	0	0	1	1	0	0
16	1	1	2	1	1	4	1	2	1	0	1	2	1	0	1	1	1	1	2	2	0	1	2	5
17	0	0	0	0	0	$*$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	$*$	0	0	0	1	0	1	0	0	0	3	0	0	0	0	0	1	0	0	3	1	0	0	1
19	0	1	7	4	0	1	$*$	1	0	0	0	0	1	1	0	0	1	0	0	1	0	3	0	0
20	1	$*$	2	1	0	0	0	1	1	0	1	4	1	2	0	0	3	1	0	0	0	1	2	0
21	$*$	1	$*$	0	2	1	0	1	0	0	0	0	6	1	0	1	0	0	0	0	0	0	1	2
22	0	0	0	$*$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5	0
23	1	0	0	0	1	0	0	$*$	1	1	0	1	0	11	0	1	0	$\boxed{0}$	1	1	0	0	0	0
24	$*$	3	1	1	2	0	0	0	2	1	2	0	0	0	2	1	2	0	0	3	1	1	0	4
25	0	$*$	0	2	0	0	0	0	0	2	0	2	0	0	0	0	2	0	2	0	0	0	0	0
26	6	0	0	0	$*$	1	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0

Table 2: The values $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$ for $3 \leq p \leq 97$ and $27 \leq \ell \leq 50$.

ℓ \ p	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97
27	$*$	0	1	0	2	0	4	0	0	1	3	0	1	0	0	0	1	1	0	3	1	0	0	1
28	6	2	$*$	0	4	0	0	0	5	0	1	2	0	0	0	0	0	0	0	0	0	0	0	2
29	0	0	14	0	0	0	0	2	$*$	0	0	0	0	0	2	14	0	0	0	0	0	2	0	0
30	$*$	$*$	1	0	0	1	0	0	0	0	0	0	0	0	0	0	4	1	0	0	0	0	0	0
31	3	5	1	0	0	0	1	0	0	$*$	0	1	0	3	0	1	0	5	1	0	0	0	0	3
32	1	1	2	1	1	4	1	2	1	0	1	2	1	4	1	1	1	1	2	2	4	1	2	9
33	$*$	0	0	$*$	1	0	0	0	0	0	0	1	4	0	0	0	0	10	0	0	1	0	0	0
34	0	0	0	0	0	$*$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
35	12	$*$	$*$	1	4	1	0	0	3	0	0	4	0	1	0	0	0	0	12	1	1	3	0	3
36	$*$	1	0	0	2	2	1	0	1	0	6	0	0	0	3	0	2	0	0	6	1	0	2	2
37	0	0	2	0	0	0	0	0	0	0	$*$	0	0	6	2	0	0	0	2	0	0	2	0	0
38	0	0	3	0	0	0	$*$	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
39	$*$	5	0	1	$*$	0	0	0	0	3	0	1	2	4	0	1	1	0	1	2	12	3	1	0
40	1	$*$	3	2	1	0	3	2	3	2	2	7	1	3	1	3	3	1	2	0	0	1	3	0
41	0	0	0	$\boxed{2}$	0	0	0	0	0	0	4	$*$	0	0	0	4	0	0	0	0	0	20	0	0
42	$*$	0	$*$	1	1	1	0	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	1
43	0	0	0	3	1	1	0	1	0	1	0	3	$*$	3	1	3	0	1	0	0	7	1	0	3
44	0	4	0	$*$	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	10	0
45	$*$	$*$	0	0	0	3	3	1	0	4	0	0	0	1	3	0	4	0	4	0	1	1	0	0
46	0	0	0	0	0	0	0	$*$	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0
47	2	1	1	0	0	2	0	0	0	0	1	0	0	$*$	1	1	1	0	1	0	1	1	1	1
48	$*$	5	1	1	2	2	0	2	2	3	2	2	0	0	2	1	2	0	2	3	3	1	2	8
49	0	0	$*$	1	0	0	0	1	3	0	1	0	4	0	1	0	0	7	3	0	7	0	0	0
50	0	$*$	0	0	0	0	0	0	0	0	0	2	0	0	0	0	2	0	0	0	0	0	0	0

Table 3: The values $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$ for $3 \le p \le 97$ and $51 \le \ell \le 75$.

ℓ \ p	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97
51	$*$	3	0	1	3	$*$	1	1	1	0	0	2	1	4	2	3	0	7	2	0	0	3	4	0
52	9	3	1	1	$*$	2	1	0	1	4	0	0	0	3	11	1	1	2	1	2	0	3	0	0
53	0	0	0	0	26	0	0	0	0	0	0	0	0	2	$*$	0	0	0	0	0	0	0	2	2
54	$*$	0	0	0	1	0	2	0	0	0	3	0	0	0	0	0	1	0	0	3	1	0	0	1
55	0	$*$	1	$*$	1	1	0	0	0	1	0	0	7	0	0	1	0	0	1	1	0	1	5	0
56	14	3	$*$	0	7	0	1	1	5	0	1	5	2	0	0	1	1	0	3	0	1	5	0	4
57	$*$	0	3	0	0	0	$*$	0	1	2	8	0	0	0	1	0	0	1	0	0	0	0	0	0
58	0	0	0	0	0	0	0	0	$*$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
59	1	1	1	0	0	1	1	0	29	0	0	1	0	0	1	$*$	0	0	1	0	1	0	0	0
60	$*$	$*$	1	2	0	1	2	0	2	0	0	0	0	0	0	0	6	1	2	0	2	0	3	1
61	0	0	0	0	10	0	0	0	0	0	0	1	0	10	0	0	$*$	0	0	2	0	2	0	0
62	0	0	0	2	0	0	0	0	0	$*$	0	0	2	0	0	0	0	0	0	0	0	0	0	0
63	$*$	1	$*$	2	2	1	0	3	0	2	2	0	6	1	2	1	2	4	6	0	4	0	1	2
64	1	1	2	1	1	5	1	2	1	8	1	2	1	4	1	1	1	1	2	2	4	1	2	9
65	0	$*$	0	0	$*$	2	2	2	2	4	0	2	2	0	0	2	4	0	0	0	6	0	2	0
66	$*$	0	0	$*$	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
67	0	0	0	0	0	1	1	1	$\boxed{11}$	0	11	0	0	1	0	$\boxed{3}$	0	$*$	1	1	0	1	3	0
68	1	0	1	2	3	$*$	2	1	0	1	0	0	2	4	1	2	0	0	1	0	1	2	3	1
69	$*$	0	0	0	0	2	0	$*$	0	0	0	1	0	0	0	0	1	1	0	0	0	0	1	0
70	9	$*$	$*$	0	1	0	1	0	2	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
71	1	35	7	0	0	0	1	0	2	0	5	0	1	0	0	0	0	0	$*$	1	1	1	1	0
72	$*$	3	1	1	2	4	3	0	2	1	6	0	0	0	6	1	2	0	0	11	2	1	4	4
73	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	$*$	0	0	4	0
74	0	1	0	0	0	0	2	0	0	0	$*$	0	0	0	0	0	0	0	0	0	0	0	0	0
75	$*$	$*$	4	1	0	1	1	1	0	4	0	1	4	1	1	0	4	0	0	0	1	1	0	0

Table 4: The values $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$ for $3 \leq p \leq 97$ and $76 \leq \ell \leq 100$.

ℓ \ p	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97
76	1	0	4	0	0	0	∗	0	0	1	9	1	0	0	0	0	0	0	0	0	0	1	0	0
77	3	4	∗	∗	0	1	2	4	0	0	0	0	12	0	0	1	0	4	2	0	0	0	1	2
78	∗	0	0	1	∗	0	0	0	0	1	0	0	1	0	1	1	1	0	0	0	0	0	1	1
79	0	1	0	1	13	0	1	13	0	1	0	0	0	0	1	0	0	3	0	1	∗	1	3	3
80	3	∗	3	2	3	0	3	2	3	6	4	7	3	5	3	3	3	3	4	2	0	3	7	0
81	∗	0	1	0	2	0	4	0	0	1	3	0	1	0	0	0	1	1	0	3	1	0	0	1
82	0	0	0	0	0	0	0	0	0	0	0	∗	0	0	0	0	0	0	0	0	0	0	0	0
83	1	0	1	1	0	2	0	1	1	1	1	82	0	0	0	1	1	0	0	0	0	∗	0	0
84	∗	1	∗	3	3	2	1	2	3	2	1	3	1	0	0	0	0	0	3	0	0	0	1	1
85	6	∗	2	0	0	∗	4	2	2	0	2	0	4	0	4	4	0	8	0	3	2	4	8	2
86	0	1	0	0	0	0	0	0	0	0	0	0	∗	0	0	0	0	0	0	0	0	0	0	0
87	∗	1	13	2	1	7	0	1	∗	0	1	7	0	1	0	0	1	1	0	0	1	1	1	0
88	0	8	0	∗	2	0	1	7	2	1	0	0	9	1	0	0	1	4	1	1	0	1	19	1
89	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	∗	4
90	∗	∗	3	0	0	1	0	0	0	1	0	0	0	0	0	0	4	1	0	1	0	0	0	0
91	15	6	∗	2	∗	0	4	5	7	5	3	3	3	3	5	3	4	2	0	3	5	9	3	3
92	0	1	0	0	1	0	0	∗	1	0	1	1	0	0	1	0	1	1	0	0	0	0	0	0
93	∗	6	0	0	0	0	1	0	0	∗	4	0	0	0	0	0	14	4	0	1	0	0	0	2
94	0	0	0	0	1	0	0	0	0	0	1	0	0	∗	0	0	0	0	0	0	0	0	1	0
95	9	∗	0	7	3	0	∗	0	0	4	10	0	0	0	1	0	1	1	0	0	0	0	0	2
96	∗	5	1	1	2	7	0	2	2	7	2	2	0	4	2	1	2	0	2	3	3	1	2	12
97	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16	0	0	0	0	0	0	∗
98	6	2	∗	0	1	0	0	0	3	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0
99	∗	0	0	∗	1	0	0	0	0	2	2	1	4	0	2	0	0	10	2	0	1	0	10	0
100	1	∗	6	3	0	0	0	1	1	0	1	4	5	2	0	0	3	1	0	0	0	1	2	0

Table 5: The values $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$ for $101 \leq p \leq 199$ and $3 \leq \ell \leq 26$.

ℓ \ p	101	103	107	109	113	127	131	137	139	149	151	157	163	167	173	179	181	191	193	197	199
3	0	1	0	1	0	1	0	0	1	0	1	1	1	0	0	0	2	0	1	0	1
4	1	0	0	1	1	0	0	1	0	1	0	1	0	0	1	0	1	0	1	1	0
5	2	0	0	0	0	0	2	0	0	0	2	0	0	0	0	0	2	2	0	0	0
6	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	0	0
7	0	0	1	1	3	3	0	1	0	1	1	0	1	0	0	1	0	1	1	3	0
8	1	0	1	1	2	0	1	2	1	1	0	1	1	0	1	1	1	0	2	1	0
9	0	1	0	3	0	3	0	0	1	0	1	1	3	0	0	0	4	0	1	0	3
10	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0
11	0	1	0	0	1	0	0	1	0	0	0	1	1	0	0	1	1	1	0	0	5
12	1	0	0	2	0	0	0	0	0	1	0	2	0	0	1	0	2	0	2	1	0
13	0	0	2	0	2	0	6	0	2	0	0	6	0	0	0	0	0	2	0	0	0
14	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0
15	0	0	1	1	1	0	0	1	1	0	4	0	0	1	1	0	4	0	0	1	1
16	1	2	1	1	4	0	1	2	1	1	2	1	1	2	1	1	1	0	4	1	2
17	0	8	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	3	0	0	0	0	0	0	0	1	0	0	0	0	3	0	1	0	0
19	1	0	0	0	0	0	1	1	1	1	0	1	3	0	0	0	0	9	0	3	1
20	3	1	1	1	0	2	1	0	0	1	0	1	1	2	0	0	3	0	0	1	0
21	1	0	1	0	0	6	1	0	2	1	0	0	0	0	1	0	2	1	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	1	0	0	0	0	1	1	0	11	0	1	0	1	1	1	1	0	0	1	1	0
24	2	1	1	2	0	1	2	0	0	2	1	2	0	0	2	1	2	0	4	2	1
25	11	0	0	0	0	0	2	0	0	0	10	0	0	0	0	0	2	2	0	0	0
26	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0

Table 6: The values $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$ for $101 \leq p \leq 199$ and $27 \leq \ell \leq 50$.

ℓ \ p	101	103	107	109	113	127	131	137	139	149	151	157	163	167	173	179	181	191	193	197	199
27	0	1	0	9	0	3	0	0	1	0	1	1	9	0	0	0	4	0	1	0	3
28	0	0	0	0	6	0	0	1	0	0	0	0	0	0	0	0	3	0	1	5	0
29	0	2	2	0	0	0	0	0	2	0	0	0	0	0	0	0	3	0	0	2	2
30	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0
31	3	1	1	3	1	0	1	0	0	5	0	3	3	0	1	0	0	5	1	0	0
32	1	2	1	1	4	0	1	2	1	1	2	1	1	2	1	1	1	0	8	1	2
33	0	0	1	4	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	10
34	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0
35	0	1	0	1	0	0	0	0	0	1	1	1	0	3	1	1	4	1	0	0	0
36	1	0	0	6	0	0	0	0	0	1	0	2	0	0	1	0	6	0	2	3	0
37	0	0	2	0	0	2	0	6	0	18	0	2	0	0	0	0	2	0	0	2	0
38	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
39	0	5	0	2	0	1	0	1	1	1	2	12	0	1	0	0	5	0	0	1	2
40	3	2	1	3	0	3	2	0	3	3	2	2	1	3	1	3	3	2	0	2	0
41	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0
42	1	0	1	0	1	0	0	0	0	1	0	0	0	0	0	1	1	1	0	1	0
43	1	1	3	1	0	3	0	0	1	0	0	0	0	1	21	0	1	0	3	1	0
44	1	0	0	5	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	5	0
45	0	0	3	3	1	0	0	1	1	0	4	0	0	1	1	0	12	0	0	3	3
46	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
47	1	1	0	0	0	0	1	0	1	1	0	2	0	0	1	0	0	1	0	1	0
48	2	1	1	2	2	3	2	2	0	2	1	2	0	2	2	1	2	0	8	2	1
49	0	0	1	1	3	3	0	1	0	1	1	0	1	0	0	1	0	1	1	21	0
50	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0

Table 7: The values $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$ for $101 \leq p \leq 199$ and $51 \leq \ell \leq 75$.

ℓ \ p	101	103	107	109	113	127	131	137	139	149	151	157	163	167	173	179	181	191	193	197	199
51	0	16	1	0	1	1	1	0	0	4	1	3	0	1	2	2	0	4	1	1	0
52	1	0	0	3	2	0	1	0	0	0	3	11	1	1	1	0	5	1	0	0	0
53	0	0	26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
54	0	0	0	9	0	0	0	0	0	0	0	1	0	0	0	0	3	0	1	0	0
55	0	0	1	0	0	1	8	0	0	0	0	0	0	1	1	1	1	1	1	5	5
56	1	0	0	0	12	3	1	2	5	0	1	1	0	0	1	0	6	1	2	5	0
57	0	3	0	1	0	1	0	0	0	0	8	1	3	1	0	0	1	0	0	0	0
58	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
59	0	0	1	0	0	1	0	1	1	0	0	0	1	1	0	0	1	0	1	1	1
60	0	0	0	0	0	1	2	0	2	2	0	0	0	0	0	0	6	2	0	0	2
61	0	2	0	0	0	0	6	2	0	0	0	0	0	0	0	2	0	0	0	0	2
62	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
63	1	2	3	2	0	18	1	2	2	3	4	2	2	0	1	2	6	3	5	6	0
64	1	2	1	1	4	0	1	2	1	1	2	1	1	2	1	1	1	0	16	1	2
65	3	6	0	6	0	2	24	0	2	2	4	0	0	0	2	0	10	4	0	0	0
66	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
67	0	1	3	0	0	1	3	0	0	3	1	1	11	1	1	0	1	0	3	0	1
68	7	0	1	0	1	2	1	16	1	3	2	3	1	1	0	2	0	4	0	0	1
69	0	0	0	1	0	0	0	0	22	0	0	0	0	0	0	1	0	0	0	0	1
70	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
71	6	5	1	1	0	0	1	0	0	0	1	1	0	7	0	5	0	1	0	0	7
72	2	1	5	6	0	3	2	0	0	2	1	2	2	0	2	5	6	0	4	6	3
73	0	0	0	0	0	0	0	12	0	0	0	0	0	0	0	0	0	0	0	0	0
74	0	0	0	0	0	0	0	0	0	18	0	0	0	0	0	0	0	0	0	0	0
75	0	0	5	1	1	0	0	1	1	0	20	4	0	1	1	0	4	0	4	1	9

Table 8: The values $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$ for $101 \leq p \leq 199$ and $76 \leq \ell \leq 100$.

ℓ \ p	101	103	107	109	113	127	131	137	139	149	151	157	163	167	173	179	181	191	193	197	199
76	0	0	0	1	8	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	0
77	0	0	0	5	2	0	1	0	0	0	2	0	0	0	0	0	2	0	0	12	0
78	0	0	0	0	0	0	0	1	0	1	1	12	0	1	0	0	2	0	0	0	0
79	3	0	0	0	0	0	3	0	0	0	1	0	1	1	0	3	13	0	0	0	0
80	3	2	3	3	0	5	2	2	3	3	4	4	3	3	3	3	3	6	0	4	6
81	0	1	0	9	0	3	0	0	1	0	1	1	27	0	0	0	4	0	1	0	3
82	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
83	0	0	0	1	1	1	1	0	0	0	1	0	0	41	1	0	0	1	1	1	1
84	2	1	4	1	2	0	0	0	3	1	0	0	1	0	2	3	2	2	1	3	1
85	14	0	2	2	2	4	0	0	2	8	2	0	2	2	2	4	0	6	2	2	2
86	0	0	0	0	0	0	0	0	0	0	0	0	0	0	21	0	0	0	0	0	0
87	1	1	0	1	1	1	1	2	2	0	1	6	0	1	0	0	1	7	0	1	1
88	2	1	1	10	1	0	9	2	1	1	0	0	0	0	1	0	0	1	0	10	6
89	0	0	0	0	1	0	0	0	0	0	0	0	0	4	0	44	0	0	0	0	0
90	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	12	0	0	0	0
91	0	0	9	2	7	3	0	2	4	2	2	0	2	3	0	5	0	9	2	0	0
92	0	0	0	0	0	0	0	10	0	0	0	0	0	0	1	0	1	0	0	1	0
93	0	0	0	2	0	1	0	1	2	0	3	2	2	0	0	1	5	2	0	0	0
94	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
95	1	3	3	1	9	1	1	0	1	1	16	0	0	1	1	0	0	36	1	0	1
96	2	1	1	2	6	7	2	2	0	2	1	2	0	2	2	1	2	0	16	2	1
97	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
98	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	21	0
99	0	0	1	12	0	0	0	0	0	0	0	0	2	0	1	2	2	0	0	0	30
100	19	1	5	1	0	2	1	0	0	9	0	5	1	2	0	0	4	0	4	1	0

Table 9: The values $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$ for $211 \leq p \leq 331$ and $3 \leq \ell \leq 26$.

ℓ \ p	211	223	227	229	233	239	241	251	257	263	269	271	277	281	283	293	307	311	313	317	331
3	1	1	0	1	0	0	1	0	0	0	0	1	1	0	1	0	1	0	1	0	1
4	0	0	0	1	1	0	1	0	1	0	1	0	1	1	0	1	0	0	1	1	0
5	2	0	0	0	0	0	2	2	0	0	0	2	0	2	0	0	0	2	0	0	2
6	0	0	0	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0
7	3	0	0	0	1	3	0	0	0	1	0	0	1	3	0	0	0	0	0	1	1
8	1	0	1	1	2	0	2	1	2	0	1	0	1	2	1	1	1	0	2	1	1
9	1	1	0	1	0	0	1	0	0	0	0	3	1	0	1	0	3	0	1	0	1
10	0	0	0	0	0	0	2	0	0	0	0	0	0	2	0	0	0	0	0	0	0
11	0	1	0	1	0	0	0	1	1	0	1	0	0	0	0	0	0	1	1	1	5
12	0	0	0	2	0	0	2	0	0	0	1	0	2	0	0	1	0	0	2	1	0
13	2	0	0	0	0	0	0	0	0	2	2	0	0	0	0	0	0	0	6	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0
15	4	0	1	1	1	0	4	0	1	1	0	4	0	0	0	1	0	0	0	1	4
16	1	0	1	1	2	0	4	1	4	2	1	0	1	2	1	1	1	2	2	1	1
17	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0
18	0	0	0	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0
19	0	0	0	9	1	3	0	1	0	1	0	1	3	0	1	0	0	3	1	0	0
20	1	1	1	1	0	0	4	1	0	1	1	0	1	4	1	0	1	0	0	1	1
21	6	2	1	0	1	0	0	0	1	0	1	0	0	0	0	0	2	1	0	1	0
22	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1
23	1	1	0	0	1	1	0	0	1	0	1	1	11	0	0	0	1	1	0	1	1
24	0	1	1	2	0	0	4	1	0	0	2	1	2	0	0	2	0	0	3	2	0
25	2	0	0	0	0	0	2	10	0	0	0	2	0	2	0	0	0	2	0	0	2
26	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	6	0	0

Table 10: The values $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$ for $211 \leq p \leq 331$ and $27 \leq \ell \leq 50$.

ℓ \ p	211	223	227	229	233	239	241	251	257	263	269	271	277	281	283	293	307	311	313	317	331
27	1	1	0	1	0	0	1	0	0	0	0	9	1	0	1	0	3	0	1	0	1
28	0	0	0	0	1	0	0	0	0	0	0	0	0	6	0	3	0	0	0	0	0
29	0	2	2	0	14	2	0	0	2	0	0	0	2	2	0	0	0	0	2	0	0
30	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	1	0	0	0	0
31	5	0	2	0	3	0	0	0	1	0	0	0	0	3	3	1	1	15	0	1	0
32	1	0	1	1	2	4	4	1	8	2	1	4	1	2	1	1	1	2	2	1	1
33	1	0	0	0	0	1	4	0	0	0	0	0	1	0	0	0	4	0	0	0	10
34	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
35	12	3	1	0	0	3	0	4	1	0	0	0	0	12	1	3	3	0	1	0	1
36	0	0	0	2	2	0	2	0	0	0	3	0	2	0	0	1	0	0	2	1	0
37	6	18	0	2	0	0	0	0	0	0	6	2	0	0	0	2	0	0	0	0	0
38	0	0	0	9	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
39	1	0	1	2	0	3	0	0	0	0	0	0	2	4	1	1	2	0	12	3	0
40	2	2	1	3	0	0	8	2	0	2	3	2	2	7	1	1	1	2	0	2	2
41	0	4	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0
42	0	0	0	0	1	0	0	0	0	1	1	0	0	1	0	0	0	0	0	1	0
43	1	0	0	1	0	1	0	7	0	0	3	1	0	1	1	3	7	1	0	3	0
44	0	0	0	0	1	0	4	0	0	0	0	1	1	0	0	0	0	0	1	0	1
45	4	0	1	1	3	0	4	4	1	1	0	12	0	0	0	1	0	0	0	1	4
46	0	0	0	0	0	0	0	0	0	0	0	0	11	0	0	0	0	0	0	0	0
47	0	0	0	0	0	1	1	1	0	1	1	1	1	0	23	0	1	0	0	0	1
48	0	3	1	2	2	0	6	1	0	2	2	3	2	2	0	2	0	2	3	2	0
49	3	0	0	0	1	3	0	0	0	7	0	0	1	3	0	0	0	0	0	1	1
50	0	0	0	0	0	0	3	0	0	0	0	0	0	2	0	0	0	0	0	0	0

Table 11: The values $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$ for $211 \leq p \leq 331$ and $51 \leq \ell \leq 75$.

ℓ \ p	211	223	227	229	233	239	241	251	257	263	269	271	277	281	283	293	307	311	313	317	331
51	0	1	1	1	1	0	0	4	2	3	1	7	0	2	0	4	16	1	0	1	1
52	0	2	1	2	6	3	0	0	1	0	1	1	1	3	0	0	3	0	12	3	1
53	0	0	2	0	0	0	0	0	0	0	0	0	0	2	0	2	2	2	0	0	2
54	0	0	0	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0
55	0	0	1	1	1	0	9	1	0	7	1	0	1	0	1	1	5	1	0	0	20
56	2	0	1	1	2	3	0	5	0	1	1	0	0	11	1	6	5	0	0	0	0
57	0	1	0	18	0	0	0	0	0	0	0	0	3	1	0	0	0	0	0	0	3
58	0	0	0	0	14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
59	0	1	0	0	1	1	1	1	1	1	0	1	1	1	0	1	1	1	0	1	1
60	0	0	0	0	0	0	8	2	0	0	2	0	0	0	0	0	1	2	0	0	0
61	0	0	0	0	0	2	6	0	10	0	2	0	0	0	0	0	0	0	0	2	0
62	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
63	6	2	1	2	3	0	3	0	1	2	1	0	4	0	2	0	6	1	2	3	4
64	1	8	1	1	2	4	4	1	16	2	1	4	1	2	1	1	1	2	2	1	1
65	4	0	0	6	6	6	0	2	2	0	2	0	2	4	2	0	0	10	0	0	0
66	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
67	1	3	1	0	0	0	3	0	1	3	33	0	3	0	3	3	1	0	0	1	0
68	2	2	1	1	0	0	1	5	1	2	1	0	0	1	2	3	1	1	0	0	2
69	0	1	0	10	0	0	0	0	0	0	0	1	22	0	0	1	0	0	0	1	0
70	0	0	0	0	0	2	0	0	0	0	0	0	0	12	0	0	0	0	0	0	0
71	0	1	0	1	5	0	0	1	0	1	0	1	1	0	0	1	0	1	1	0	0
72	0	1	1	2	4	0	4	5	0	0	6	3	2	0	0	2	2	0	3	2	0
73	0	4	12	0	0	0	0	4	0	0	0	0	0	0	12	36	0	0	0	0	0
74	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
75	4	0	1	1	1	0	4	0	5	1	0	4	0	0	0	5	4	0	0	1	4

Table 12: The values $\lambda_p^-(\mathbf{Q}(\zeta_\ell))$ for $211 \leq p \leq 331$ and $76 \leq \ell \leq 100$.

ℓ \ p	211	223	227	229	233	239	241	251	257	263	269	271	277	281	283	293	307	311	313	317	331
76	0	0	0	17	0	0	0	0	0	0	1	0	2	0	0	2	1	1	0	0	0
77	0	2	0	0	0	0	1	2	0	5	0	1	0	0	0	0	0	0	0	0	4
78	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	12	0	0
79	0	3	0	0	0	1	1	0	1	1	1	0	1	1	3	0	0	0	1	39	0
80	2	4	3	3	2	0	14	2	0	2	3	6	4	7	3	3	3	4	2	4	2
81	1	1	0	1	0	0	1	0	0	0	0	9	1	0	1	0	3	0	1	0	1
82	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
83	0	0	1	1	0	0	1	0	0	0	0	0	1	0	0	1	0	0	1	1	0
84	0	3	0	0	1	3	0	0	1	2	2	1	1	2	1	3	3	0	0	1	1
85	0	4	2	4	2	8	0	6	4	4	2	14	2	2	2	0	0	0	2	2	2
86	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
87	0	1	0	0	0	0	1	1	1	1	1	0	1	0	1	1	6	2	2	1	6
88	1	1	1	0	1	0	9	0	1	0	0	1	2	0	1	1	9	1	2	0	5
89	0	4	0	0	0	0	0	0	0	0	4	4	0	0	4	0	0	0	0	0	4
90	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	1	0	0	0	0
91	7	3	3	3	5	7	3	0	0	9	4	3	5	6	0	3	9	0	0	2	2
92	0	0	0	11	0	0	0	0	0	0	0	0	21	0	0	0	1	0	0	0	0
93	4	4	0	0	0	0	0	1	0	1	0	2	3	0	2	0	0	0	1	0	1
94	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
95	0	1	9	9	0	3	0	1	1	0	0	1	0	0	0	3	1	7	0	1	4
96	0	7	1	2	2	4	6	1	0	2	2	3	2	2	0	2	0	2	3	2	0
97	0	0	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
98	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0
99	1	0	0	0	0	1	4	2	0	0	2	0	1	0	0	0	12	0	0	0	10
100	1	1	1	1	0	0	5	1	4	1	1	0	1	4	1	4	5	0	0	1	1

7 Future Work

In this section we describe future work related to this project. In the immediate future, we plan to produce a software package in Magma [1] to be included in future distributions of the software and to explore possible improvements to the efficiency of the algorithm. We also plan to explicitly implement this algorithm to include general abelian number fields as described in Remark 16. Another direction for this work includes implementing an algorithm to compute λ-invariants for cubic fields.

The ultimate goal is to analyze the λ-invariants to gain insight into possible results regarding these mysterious values. Some recent work to describe λ-invariants appears in [5]. One observation from the tables in Section 6 is that for ℓ an odd prime and $p \equiv 1 \pmod{\ell}$ we get $\lambda_p^-(\mathbf{Q}(\zeta_\ell)) = (\ell - 1)/2$ except for $\ell = 3$ and $p = 13, 181$. Helping to observe and prove such results is the aim of this and future work.

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust, *The magma algebra system i: The user language*, Journal of Symbolic Computation **24** (1997), no. 3, 235–265.

[2] Nancy Childress, *Examples of lambda-invariants*, manuscripta mathematica **68** (1990), no. 1, 447–453.

[3] Henri Cohen, *A course in computational algebraic number theory*, vol. 138, Springer, 1993.

[4] DS Dummit, D Ford, H Kisilevsky, and JW Sands, *Computation of iwasawa lambda invariants for imaginary quadratic fields*, Journal of Number Theory **37** (1991), no. 1, 100–121.

[5] Jordan S Ellenberg, Sonal Jain, and Akshay Venkatesh, *Modeling λ-invariants by p-adic random matrices*, Communications on Pure and Applied Mathematics **64** (2011), no. 9, 1243–1262.

[6] Bruce Ferrero and Ralph Greenberg, *On the behavior of p-adic l-functions at s=0*, Inventiones Mathematicae **50** (1978), no. 1, 91–102.

[7] Bruce Ferrero and Lawrence C Washington, *The iwasawa invariant μ vanishes for abelian number fields*, The Annals of Mathematics **109** (1979), no. 2, 377–395.

[8] Eduardo Friedman, Jonathan W Sands, and Lawrence C Washington, *On the l-adic iwasawa λ-invariant in a p-extension*, Mathematics of computation (1995), 1659–1674.

[9] Ralph Greenberg, *On the iwasawa invariants of totally real number fields*, American Journal of Mathematics **98** (1976), no. 1, 263–284.

[10] Kenkichi Iwasawa, *On gamma-extensions of algebraic number fields*, Bulletin of the American Mathematical Society **65** (1959), no. 4, 183–226.

[11] ———, *Lectures on p-adic l-functions*, no. 74, Princeton University Press, 1972.

[12] Tomio Kubota and Heinrich W Leopoldt, *Eine p-adische theorie der zetawerte. teil i: Einführung der p-adischen dirichletschen l-funktionen.*, Journal für die reine und angewandte Mathematik **214** (1964), 328–339.

[13] Yasushi Mizusawa, *Notes on computing iwasawa polynomials by pari/gp*.

[14] Lawrence C Washington, *Introduction to cyclotomic fields*, vol. 83, Springer, 1997.