Computations in Galois Cohomology and Hecke Algebras

Computations in Galois Cohomology and Hecke Algebras

By

Tara C. Davis, B.A.

A Thesis

Submitted to the School of Graduate Studies

in Partial Fulfilment of the Requirements

for the Degree

Master of Science

McMaster University

MASTER OF SCIENCE (2006) McMaster University
(Mathematics) Hamilton, Ontario

TITLE: Computations in
Galois Cohomology and
Hecke Algebras

AUTHOR: Tara C. Davis
B.A. (University of Hawaii at Manoa)

SUPERVISOR: Dr. Romyar Sharifi

NUMBER OF PAGES: x, 84

Acknowledgments

Thanks to my supervisor, Dr. Romyar Sharifi, for giving me the idea for this project, and seeing it through to the end. I appreciate that you took the time to meet with me every single week; your helpful conversations and advice were invaluable to me in completing this thesis. Many mahalos to Adam and Katie; without great friends like you two to talk and procrastinate with I would definitely not have remained sane throughout this process. Finally, thanks to my parents: never mind you don't understand the math; it was you who inspired me to set my goals high and taught me never to give up.

Abstract

We study two objects: an ideal of a Hecke algebra, and a pairing in Galois cohomology.

Let h be the Hecke algebra of cusp forms of weight 2, level n, and a fixed Dirichlet character modulo n generated by all Hecke operators, where n is an odd prime p or a product of two distinct odd primes N and p. We study the Eisenstein $\mathbf{I}$ ideal of h. We wrote a computer program to test whether $U_p - 1$ generates this ideal, where U_p is the p^{th} Hecke operator in h. We found many cases of n and the character so that $U_p - 1$ alone generates $\mathbf{I}$. On the other hand, we found one example with $N = 3$ and $p = 331$ where $U_p - 1$ does not generate $\mathbf{I}$.

Let $K = \mathbb{Q}(\mu_n)$ be the n^{th} cyclotomic field. Let S be the set of primes above p in K, and let $G_{K,S}$ be the Galois group of the maximal extension of K unramified outside S. We study a pairing on cyclotomic p-units that arises from the cup product on $H^1(G_{K,S}, \mu_p)$. This pairing takes values in a $\mathrm{Gal}(K/\mathbb{Q})$-eigenspace of the p-part of the class group of K. Sharifi has conjectured that this pairing is surjective. We studied this pairing in detail by imposing linear relations on the possible pairing values. We discovered many values of n and the character such that these relations single out a unique nontrivial possibility for the pairing, up to a possibly zero scalar.

Sharifi showed in [S2] that, under an assumption on Bernoulli numbers, the element $U_p - 1$ generates the Eisenstein ideal $\mathbf{I}$ if and only if pairing with the single element p is surjective. In particular, in the instances for which we found a unique nontrivial possibility for the pairing, then if $U_p - 1$ generates $\mathbf{I}$, we know that the scalar up to which it is determined cannot be zero.

Contents

Introduction

In this thesis, we study generators of an ideal of the Hecke algebra of modular forms and an equivalent statement about a pairing on the p-units of a cyclotomic field $K = \mathbb{Q}(\mu_{Np})$, where $N = 1$ or $N \geq 3$ is a prime and $p \geq 5$ is a prime as well.

We let h be the Hecke algebra over $\mathbb{Z}_p$ of cusp forms of weight 2 and level Np generated by all Hecke and diamond operators. We require that $\varphi(N) \mid \varphi(p)$, where φ denotes the Euler phi function. Let χ be a fixed even nontrivial Dirichlet character modulo Np, and let ω be the Teichmüller character. We assume that p divides the generalized Bernoulli number $B_{1,\chi\omega^{-1}}$. We also assume that $\chi\,|_{(\mathbb{Z}/p\mathbb{Z})^\times} \neq \omega\,|_{(\mathbb{Z}/p\mathbb{Z})^\times}$ and $\chi\,|_{(\mathbb{Z}/p\mathbb{Z})^\times} \neq \omega^2\,|_{(\mathbb{Z}/p\mathbb{Z})^\times}$.

We define the Eisenstein ideal $\mathbf{I}$ of h to be the ideal generated by all $T_l - 1 - l\chi(l)$ and $\langle l \rangle - \chi(l)$ for $l \nmid n$ and by $U_l - 1$ when $l \mid n$. Here T_l and U_l represent the usual Hecke operators, and $\langle l \rangle$ the diamond operator. We wrote a computer program to test whether the single element $U_p - 1$ generates the Eisenstein ideal. Sharifi found in [McS] that if $N = 1$ then for all χ and $p < 1000$, it is true that $U_p - 1$ generates $\mathbf{I}$.

Theorem. *For all but one triple (N, p, χ) as above with $Np < 1000$, and $p^2 \nmid B_{2,\chi\omega^{-1}}$, the element $U_p - 1$ generates $\mathbf{I}$ in weight 2 and level Np. For*

$N = 3, p = 331$, *and* $\chi = \psi\omega^{149}$, *where* ω *is the Teichmüller character and* ψ *is the unique nontrivial Dirichlet character of conductor* 3, *the element* $U_p - 1$ *alone does not generate* $\mathbf{I}$.

Let $K = \mathbb{Q}(\mu_{Np})$ be the Np^{th} cyclotomic field. Let S be a set of primes of K including all primes above Np, and let $G_{K,S}$ be the Galois group of the maximal extension of K unramified outside S. We consider the cup product

$$H^1(G_{K,S}, \mu_p) \otimes H^1(G_{K,S}, \mu_p) \to H^2(G_{K,S}, \mu_p \otimes \mu_p)$$

on the first cohomology group of $G_{K,S}$ with coefficients in p^{th} roots of unity μ_p. Let $\mathcal{C}$ be the group of cyclotomic p-units of K. Using Kummer theory, $\mathcal{C}/\mathcal{C}^p$ is isomorphic to a subgroup of $H^1(G_{K,S}, \mu_p)$. Let $A_K^{(\omega\chi^{-1})}$ be the $\mathrm{Gal}(K/\mathbb{Q})$-eigenspace of the p-part of the class group of K with an $\omega\chi^{-1}$-action. There is an injection from $A_K^{(\omega\chi^{-1})} \otimes \mu_p$ to the 2^{nd} cohomology group $H^2(G_{K,S}, \mu_p^{\otimes 2})$. The pairing that arises from the cup product is as follows:

$$(\ ,\ )_\chi \colon \mathcal{C} \times \mathcal{C} \to A_K^{(\omega\chi^{-1})} \otimes \mu_p.$$

Theorem (Sharifi). *[S2], Theorem 5.6. Suppose the following hold*

1. $p \mid B_{1,\chi\omega^{-1}}$,
2. $p \nmid B_{1,\chi^{-1}\omega}$,
3. $\chi\,|_{(\mathbb{Z}/p\mathbb{Z})^\times} \neq \omega^2\,|_{(\mathbb{Z}/p\mathbb{Z})^\times}$, *and*
4. $\chi^2\,|_{(\mathbb{Z}/p\mathbb{Z})^\times} \neq \omega^2\,|_{(\mathbb{Z}/p\mathbb{Z})^\times}$.

Then $U_p - 1$ *generates the ideal* $\mathbf{I}$ *of* h *if and only if the pairing* $(p,\ )_\chi$ *induced by taking cup products with* p *is surjective.*

Corollary. *For all but one triple (N, p, χ) with $Np < 1000$ and $p^2 \nmid B_{2,\chi\omega^{-2}}$, the pairing $(p,\ )_\chi$ induced by taking cup products with p is surjective. For $Np = 993$, and χ as in the first Theorem of this section, the pairing with p is not surjective.*

We studied the values of this pairing in detail by imposing relations arising from the fact that $(x, 1-x)_\chi = 0$ if x and $1-x$ are both p-units in K, as found in [McS], Section 5. We viewed the relations as linear equations over $\mathbb{F}_p$, and in this way were able to compute the nullspace of the matrix of coefficients. In particular, we compute the following.

Theorem. *For all but at most six triples (N, p, χ) as above with $N \geq 3$ and $Np < 1000$, the dimension of the nullspace of coefficients of relations is equal to one. For the remaining triples, this nullity is greater than one.*

Corollary. *For the N, p and χ for which the calculated nullspace was 1-dimensional, the pairing $(\ ,\ )_\chi$ induced by the cup product is completely determined up to a single possibly zero scalar in $\mathbb{Z}/p\mathbb{Z}$.*

Combining our two Corollaries we obtain:

Theorem. *For all but at most seven triples (N, p, χ) with $Np < 1000$ and $p^2 \nmid B_{2,\chi\omega^{-2}}$, the pairing $(\ ,\ )_\chi$ is completely determined up to a single nonzero scalar in $\mathbb{Z}/p\mathbb{Z}$.*

1 The Eisenstein Ideal

1.1 Dirichlet Characters and Bernoulli Numbers

Definition 1.1. *A Dirichlet character modulo m is a homomorphism of unit groups*

$$(\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$$

for $m \in \mathbb{Z}, m \geq 2$.

A Dirichlet character is called even if $\chi(-1) = 1$ and odd otherwise: if $\chi(-1) = -1$. The minimal n dividing m such that χ factors through $(\mathbb{Z}/n\mathbb{Z})^\times$ is called the conductor of χ. The set of all Dirichlet characters with a fixed modulus m forms a group, called the Dirichlet group modulo m.

We may extend a Dirichlet character χ modulo m to a map $\chi\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ by setting $\chi(a) = 0$ if $(a, m) > 1$.

Definition 1.2. *Given a Dirichlet character $\chi\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ of conductor f, the generalized Bernoulli numbers $B_{n,\chi}$ are defined by*

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

Definition 1.3. *The ordinary Bernoulli numbers B_n are defined by*

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

Definition 1.4. *The Bernoulli polynomials $B_n(x)$ are defined by*

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

Lemma 1.5. *The generalized Bernoulli numbers can be computed using*

$$B_{n,\chi} = m^{n-1} \sum_{c=0}^{m-1} \chi(c) B_n\left(\frac{c}{m}\right) = F^{n-1} \sum_{c=1}^{F-1} \chi(c) B_n(\frac{c}{F}),$$

where F is any multiple of f.

Proof. See [W], Proposition 4.1. □

Definition 1.6. *For a prime number p, the p-adic integers are the inverse limit*

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}.$$

Definition 1.7. *Let p be a prime. The Teichmüller character ω is the map $\mathbb{F}_p^\times \to \mathbb{Z}_p^\times$ taking any $a \in \mathbb{F}_p^\times$ to the unique $(p-1)^{st}$ root of unity in $\mathbb{Z}_p^\times$ with $a \equiv \omega(a) \bmod p$.*

Note: The Teichmüller character is well-defined because of a Corollary of Hensel's lemma, which states that the number of $(p-1)^{st}$ roots of unity in $\mathbb{Z}_p$ is $p-1$ and that they are all distinct modulo p.

Until this point, we only considered complex valued Dirichlet characters. We will also want to consider Dirichlet characters $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{Z}_p^\times$. To this point, we fix, once and for all, an isomorphism between the $p-1^{st}$ roots of unity in $\mathbb{C}$ and the $p-1^{st}$ roots of unity in $\mathbb{Z}_p$. In this way we identify p-adic Dirichlet characters with complex-valued Dirichlet characters when needed.

1.2 Modular Forms

Remark 1.8. *For proofs of the results found in the remainder of this section, we refer the reader to [DS], Chapter 1.*

Definition 1.9. *Let N be an integer. The principal congruence subgroup of level N is*

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon a, d \equiv 1 \bmod N; b, c \equiv 0 \bmod N \right\}.$$

A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is called a congruence subgroup of level N if

$$\Gamma(N) \subseteq \Gamma,$$

and N is the smallest integer for which containment holds.

Two examples are the following:

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon a, d \equiv 1 \bmod N; c \equiv 0 \bmod N \right\}$$

and

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon c \equiv 0 \bmod N \right\}.$$

Definition 1.10. *The complex upper half plane is*

$$\mathcal{H} = \{\tau \in \mathbb{C} \colon \mathrm{Im}\tau > 0\}.$$

Proposition 1.11. *The set $\mathrm{SL}_2(\mathbb{Z})$ of invertible 2×2 matrices of determinant 1 acts on $\mathcal{H}$ by way of the usual fractional linear transformation:*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (\tau) = \frac{a\tau + b}{c\tau + d}.$$

Definition 1.12. *For any congruence subgroup Γ, the modular curve*

$$Y_\Gamma := \{\Gamma\tau : \tau \in \mathcal{H}\}$$

is the set of coset orbits of Γ in $\mathcal{H}$.

We let $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ be the extended half plane. We have that $SL_2(\mathbb{Z})$ acts on $\mathbb{Q} \cup \{\infty\}$ as it does on $\mathcal{H}$. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. A Γ-equivalence class of points in $\mathbb{Q} \cup \{\infty\}$ is called a cusp.

Definition 1.13. *The upper half plane $\mathcal{H}$ can be viewed as a subspace of $\mathbb{R}^2$ and thus inherits the Euclidean topology, meaning that a basis of open sets is given by open balls. The natural surjection $\pi : \mathcal{H} \to Y_\Gamma$ affords the curve Y_Γ the quotient topology, meaning that a set S in Y_Γ is an open set if and only if the inverse image $\pi^{-1}(S)$ is open in $\mathcal{H}$.*

Proposition 1.14. *We can complete Y_Γ to a compact Riemann surface by taking the quotient*

$$X_\Gamma := \Gamma\backslash\mathcal{H}^* = Y_\Gamma \cup \Gamma\backslash(\mathbb{Q} \cup \{\infty\}).$$

Proof. See [DS], Chapter 1. □

Definition 1.15. *For any $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ and $k \in \mathbb{Z}$, define the operator $[\alpha]_k$ on functions $f : \mathcal{H} \to \mathbb{C}$ by*

$$f[\alpha]_k(\tau) = (c\tau + d)^{-k} f(\alpha(\tau))$$

for $\tau \in \mathcal{H}$ and

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Definition 1.16. *Let Γ be a congruence subgroup of level N. Then a function $f\colon \mathcal{H} \to \mathbb{C}$ is called a modular form of weight k with respect to Γ if*

1. *f is holomorphic on $\mathcal{H}$*
2. *For all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, $f[\alpha]_k$ is holomorphic at ∞. It is sufficient to show that $f[\alpha]_k(\tau)$ is bounded as the imaginary part of τ approaches ∞.*
3. *$f(\gamma\tau) = (c\tau + d)^k f(\tau)$ for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, \tau \in \mathcal{H}$.*

Proposition 1.17. *Any modular form f has a Fourier expansion*

$$f(\tau) = \sum_{n=0}^{\infty} a_n q^n,$$

where $q = e^{2\pi i n \tau}$.

Definition 1.18. *A modular form is called a cusp form if, in the Fourier expansion, the term a_0 equals zero.*

The space of all modular forms of weight k for Γ is denoted $\mathcal{M}_k(\Gamma)$. The space of all cusp forms of weight k for Γ is denoted $\mathcal{S}_k(\Gamma)$.

Definition 1.19. *If χ is a Dirichlet character modulo N then the space $\mathcal{M}_k(\Gamma_1(N), \chi)$ of modular forms of weight $2k$, level N and character χ is the complex vector space of $f \in \mathcal{M}_k(\Gamma_1(N))$ with*

$$\left\{ f(\alpha(\tau)) = \chi(d)(c\tau + d)^k f(\tau)\ \forall \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N), \tau \in \mathcal{H} \right\}.$$

This subspace is sometimes referred to as the χ-eigenspace of $\mathcal{M}_k(\Gamma_1(N))$.

1.3 Hecke Operators

Next we will introduce two operators on modular forms, known as the diamond and Hecke operators. Fix integers N and k. Recall that because $\Gamma_1(N) \subseteq \Gamma_0(N)$ we have that $\mathcal{M}_k(\Gamma_0(N)) \subseteq \mathcal{M}_k(\Gamma_1(N))$. First we set up the definition of the diamond operators.

Note that the map

$$\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^\times : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \bmod N$$

is a surjective homomorphism with kernel $\Gamma_1(N)$. This implies that the quotient $\Gamma_0(N)/\Gamma_1(N)$ is isomorphic to the image, $(\mathbb{Z}/N\mathbb{Z})^\times$. The group $\Gamma_0(N)$ acts on $\mathcal{M}_k(\Gamma_1(N))$ by $(\alpha, f) \mapsto f[\alpha]_k$ where $\alpha \in \Gamma_0(N), f \in \mathcal{M}_k(\Gamma_1(N))$.

Since $f \in \mathcal{M}_k(\Gamma)$, we have by definition that $f[\alpha]_k = f$ for all $\alpha \in \Gamma_1(N)$, so the action factors through the quotient, which is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^\times$. The action of any α is determined by $d \bmod N$.

Definition 1.20. *The diamond operator attached to $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ is*

$$\langle d \rangle : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N)) \ , \ f \mapsto f[\alpha]_k$$

for any

$$\alpha = \begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \Gamma_0(N)$$

with $\delta \equiv d \bmod N$.

We now extend the definition of the diamond operators $\langle n \rangle$ to include all positive integers n. Say $n \in \mathbb{Z}^+$ and $(n, N) = 1$. Then the diamond operator $\langle n \rangle$ is determined by looking at $n \bmod N$. If $n \in \mathbb{Z}^+$, and $(n, N) > 1$, then let $\langle n \rangle = 0$, the zero operator on $\mathcal{M}_k(\Gamma_1(N))$.

Proposition 1.21. *The diamond operators are multiplicative: for any positive integers n and m, we have that*

$$\langle nm \rangle = \langle n \rangle \langle m \rangle.$$

The second type of Hecke operator is given by double cosets.

Definition 1.22. *Let p be a prime number. The p^{th} Hecke operator is*

$$\mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N)),\ f \mapsto \sum_i f[\beta_i]_k$$

where

$$\Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N) = \bigcup_i \Gamma_1(N)\beta_i$$

is a disjoint union of left cosets. If p does not divide N, we call this operator T_p and this can be written more simply in terms of the action of matrices as

$$T_p f = f\Big(\Big[\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\Big]_k + \sum_{i=0}^{p-1} \Big[\begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix}\Big]_k\Big).$$

If p divides N, the p^{th} operator is denoted U_p and

$$U_p f = f\Big(\sum_{i=0}^{p-1} \Big[\begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix}\Big]_k\Big).$$

We extend inductively the definition of T_n in the case that n is not prime as follows.

Definition 1.23. *Let p be a prime. We define*

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1}\langle p \rangle T_{p^{r-2}} \tag{1}$$

for any $r \geq 2$. *Given any* $n \in \mathbb{Z}$, *factor* $n = \prod_i p_i^{e_i}$ *as a product of prime numbers, and define*

$$T_n = \prod_i T_{p_i^{e_i}}.$$

Note that $T_1 = 1$ is the identity operator.

We have the following obvious proposition.

Proposition 1.24. *We have* $T_{nm} = T_n T_m$ *if* $(n, m) = 1$.

Proposition 1.25. *The Hecke and diamond operators are commutative endomorphisms of the vector space of modular forms* $\mathcal{M}_k(\Gamma)$.

Proof. See [DS], Chapter 5. □

The following object is central to our study in this chapter.

Definition 1.26. *The cuspidal Hecke algebra* $h_k(N) = h(\mathcal{S}_k(\Gamma_1(N)))$ *of weight* k *for* $\Gamma_1(N)$ *is the subalgebra of* $\mathbb{Z}$*-linear endomorphisms of the space of cusp forms* $S_k(\Gamma_1(N))$ *generated by all diamond and Hecke operators.*

The Hecke and diamond operators act on the space $\mathcal{S}_k(\Gamma_1(N), \chi)$ for a character χ.

Definition 1.27. *The cuspidal Hecke algebra* $h_k(N, \chi) = h(\mathcal{S}_k(\Gamma_1(N), \chi))$ *of weight* k *and character* χ *for* $\Gamma_1(N)$ *is the subalgebra of* $\mathbb{Z}$*-linear endomorphisms for the space of cusp forms* $\mathcal{S}_k(\Gamma_1(N), \chi)$ *generated by all diamond and Hecke operators.*

1.4 Modular Symbols

We define these objects following [St].

Let M be the free abelian group with basis the set of symbols $\{\alpha, \beta\}$ with $\alpha, \beta \in \mathbb{Q} \cup \{\infty\}$ modulo the relation $\{\alpha, \beta\} + \{\beta, \gamma\} + \{\gamma, \alpha\}$ and any torsion.

We have a left action

$$\mathrm{GL}_2(\mathbb{Q}) \times M \to M \colon (g, \{\alpha, \beta\}) \mapsto \{g(\alpha), g(\beta)\},$$

where g acts on α and β by way of the usual fractional linear transformation. Let H be the submodule of M generated by all elements of the form $x - g(x)$ such that $x \in M, g \in \Gamma_1(N)$.

Definition 1.28. *The space $\mathcal{M}(\Gamma_1(N))$ of modular symbols for $\Gamma_1(N)$ is the maximal torsion free quotient of M/H.*

Definition 1.29. *The diamond operator attached to $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ acts on modular symbols by*

$$\langle d \rangle \{\alpha, \beta\} = \begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \{\alpha, \beta\},$$

where $\begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \Gamma_0(N)$ *and* $\delta \equiv d \bmod N$.

We extend the definition of the diamond operators $\langle n \rangle$ to include all positive integers n in the same fashion as diamond operators acting on modular forms.

Definition 1.30. *Let p be a prime not dividing N. We define the action of*

Hecke operators on modular symbols by

$$T_p(\{\alpha,\beta\}) = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \{\alpha,\beta\} + \sum_{r=1}^{p-1} \begin{pmatrix} 1 & r \\ 0 & p \end{pmatrix} \{\alpha,\beta\},$$

and

$$U_p(\{\alpha,\beta\}) = \sum_{r=1}^{p-1} \begin{pmatrix} 1 & r \\ 0 & p \end{pmatrix} \{\alpha,\beta\}.$$

We extend the defintion to include the cases where p is not a prime in a similar fashion to that of Defintion 1.23.

Let $B(\Gamma_1(N))$ be the free abelian group with basis equal to the finite set of cusps for $\Gamma_1(N)$: $\Gamma_1(N)\backslash\mathbb{Q}\cup\{\infty\}$.

Definition 1.31. *The boundary map is*

$$\delta\colon M(\Gamma_1(N)) \to B(\Gamma_1(N))\colon \{\alpha,\beta\} \mapsto \{\beta\} - \{\alpha\},$$

where $\{\beta\}$ denotes the element of $B(\Gamma_1(N))$ corresponding to $\beta \in \mathbb{Q}\cup\{\infty\}$.

Definition 1.32. *The kernel of δ is the space of cuspidal modular symbols, denoted $\mathcal{S}(\Gamma_1(N))$.*

Remark 1.33. *The space $\mathcal{S}(\Gamma_1(N))$ is isomorphic to the integral homology $H_1(X_1(N),\mathbb{Z})$ under the map taking $\{\alpha,\beta\}$ to the class of the path from α to β in the upper half plane that is a circle of possibly infinite radius intersecting the x-axis perpendicularly, where α and β are equivalent cusps, not both ∞.*

Let $h(\mathcal{S}(\Gamma_1(N)))$ be the subalgebra of $\mathbb{Z}$-linear endomorphisms of the space of cuspidal modular symbols $\mathcal{S}(\Gamma_1(N))$ generated by all Hecke and diamond operators.

Definition 1.34. *Let $\mathcal{S}(\Gamma_1(N))^+$ be the subspace of cuspidal modular symbols fixed under the involution*

$$\{\alpha, \beta\} \mapsto \{-\alpha, -\beta\}.$$

Let $h(\mathcal{S}(\Gamma_1(N))^+)$ be the Hecke algebra of endomorphisms of $\mathcal{S}(\Gamma_1(N))^+$ generated by the action of all Hecke and diamond operators.

Theorem 1.35. *The identity map on Hecke operators extends to an isomorphism*

$$h(S_2(\Gamma_1(N))) \to h(\mathcal{S}(\Gamma_1(N))^+).$$

Proof. We give a sketch of the proof. We have an integration pairing

$$\langle , \rangle \colon S_2(\Gamma_1(N)) \times \mathcal{S}(\Gamma_1(N)) \to \mathbb{C} \colon \langle f, \{\alpha, \beta\} \rangle = 2\pi i \int_\alpha^\beta f(z) dz,$$

where the integral is over the path described in Remark 1.33. As shown in [M], this induces a nondegenerate pairing

$$S_2(\Gamma_1(N)) \times (\mathcal{S}(\Gamma_1(N))^+ \otimes_{\mathbb{Z}} \mathbb{C}) \to \mathbb{C}.$$

Further, the integration pairing is compatible with Hecke operators:

$$\langle Tf, \{\alpha, \beta\} \rangle = \langle f, T\{\alpha, \beta\} \rangle$$

for any Hecke or diamond operator T. See, for instance, [C], Section 2.4. The isomorphism follows, since this implies that the identity map on Hecke operators is well-defined in both directions. □

Definition 1.36. *The space of cuspidal modular symbols with respect to a Dirichlet character χ modulo N, denoted $\mathcal{S}(\Gamma_1(N), \chi)$ is*

$$\{x \in \mathcal{S}(\Gamma_1(N)) \otimes_{\mathbb{Z}} \mathbb{Z}[\chi] \mid \langle d \rangle x = \chi(d) x \ \forall d \in (\mathbb{Z}/N\mathbb{Z})^\times\},$$

where $\mathbb{Z}[\chi]$ is the ring generated over $\mathbb{Z}$ by the values of χ.

We may take the plus and minus spaces under the involution

$$\{\alpha, \beta\} \mapsto \{-\alpha, -\beta\}$$

as in Definition 1.34, but on the space of cusp forms with respect to a Dirichlet character.

Also as before, we define $h(\mathcal{S}(\Gamma_1(N), \chi)^+)$ to be the algebra of endomorphisms of $\mathcal{S}(\Gamma_1(N), \chi)^+$ generated by all Hecke operators.

Corollary 1.37. *Let χ be a Dirichlet character modulo N. Then the identity map on Hecke operators extends to an isomorphism*

$$h(S_2(\Gamma_1(N), \chi)) \to h(\mathcal{S}(\Gamma_1(N), \chi)^+).$$

1.5 The Eisenstein ideal

Let $p \geq 5$ be a prime and $N = 1$ or $N \geq 3$ be a prime with $(N, p) = 1$. Let T_l for $l \nmid Np$ and U_l for $l \mid Np$ be the usual Hecke operators.

Let ω be the Teichmüller character. Fix a nontrivial even Dirichlet character $\chi\colon (\mathbb{Z}/Np\mathbb{Z})^\times \to \overline{\mathbb{Q}_p}^\times$ of conductor N or Np. We assume that $\chi\,|_{(\mathbb{Z}/p\mathbb{Z})^\times} \neq \omega\,|_{(\mathbb{Z}/p\mathbb{Z})^\times}$ and $\chi\,|_{(\mathbb{Z}/p\mathbb{Z})^\times} \neq \omega^2\,|_{(\mathbb{Z}/p\mathbb{Z})^\times}$. Let $\mathcal{O}$ be the ring generated over $\mathbb{Z}_p$ by the values of χ. Suppose that $\varphi(N) \mid \varphi(p)$, where φ denotes the Euler phi function.

Proposition 1.38. *If $\varphi(N) \mid \varphi(p)$ then $\mathcal{O} = \mathbb{Z}_p$.*

Proof. Since $\varphi(N) \mid \varphi(p)$ we actually have χ as a map from

$$(\mathbb{Z}/Np\mathbb{Z})^\times \cong (\mathbb{Z}/N\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/\varphi(p)\mathbb{Z} \times \mathbb{Z}/\varphi(N)\mathbb{Z}.$$

Thus, the order of $\mathrm{Im}(\chi)$ divides $\varphi(p) = p-1$. Hence χ must actually map $(\mathbb{Z}/Np\mathbb{Z})^\times$ into $(p-1)^{st}$ roots of unity in $\mathbb{Z}_p$. This is because $\mu_{N-1} \subset \mu_{p-1}$. That is, the image of χ must be contained in $\mathbb{Z}_p$. □

We now consider the Hecke algebra $h = h_2(Np, \chi\omega^{-2}) \otimes_{\mathbb{Z}[\mu_{p-1}]} \mathbb{Z}_p$. Note that

$$h \cong \{T \in h_2(Np) \otimes_{\mathbb{Z}} \mathbb{Z}_p \mid \langle d \rangle T = \chi(d)T \ \forall d \in (\mathbb{Z}/Np\mathbb{Z})^\times\}$$

noting Proposition 1.38.

We are now ready to define the central object of our study.

Definition 1.39. *The Eisenstein ideal* $\mathbf{I}$ *is the ideal of of* h *generated by* $T_l - 1 - l\chi(l)$ *for* $l \nmid Np$ *and by* $U_l - 1$ *when* $l \mid Np$.

Lemma 1.40. *We have that* $h/\mathbf{I} \cong \mathbb{Z}_p/B_{2,\chi\omega^{-2}}$ *via the map taking* T_l *to* $1 + l\chi(l)$ *for* $l \nmid Np$ *and* U_p *to* 1 *for* $l \mid Np$.

Proof. We sketch the proof, and refer the reader to the similar argument of [K], Lemma 3.1 for more details. The Eisenstein series $G_{2,\chi\omega^{-2}}$, which equals

$$\frac{-B_{2,\chi\omega^{-2}}}{2} + \sum_{n=1}^{\infty} \sum_{\substack{t \geq 1 \\ t \mid n}} \chi\omega^{-2}(t) t q^n$$

is congruent to a cusp form modulo $p^{v_p(B_{2,\chi\omega^{-2}})}$, where v_p is the usual additive p-adic valuation. The map on h takes a Hecke operator to the corresponding eigenvalue of the Eisenstein series modulo $p^{v_p(B_{2,\chi\omega^{-2}})}$. The kernel of this map is precisely $\mathbf{I}$. The result then follows (as in [K], Lemma 3.1), using the duality between h and cusp forms of weight 2, level p and character χ with $\mathbb{Z}_p$-coefficients. The map is a ring homomorphism because of the duality and the fact that $G_{2,\chi\omega^{-2}}$ is an eigenform. □

We assume that $p \mid B_{2,\chi\omega^{-2}}$ and $p^2 \nmid B_{2,\chi\omega^{-2}}$ so that $h/\mathbf{I} \cong \mathbb{Z}/p\mathbb{Z}$.

In [S2], Section 5, Sharifi showed that $\mathbf{I}$ is principal in many cases, generated by the Hecke operator $U_p - 1$.

Theorem 1.41 (Sharifi). *Let $N = 1$. Suppose $p < 1000$. Let k be a positive even integer less than p with $p \mid B_k$. Then the element $U_p - 1$ generates the Eisenstein ideal $\mathbf{I}$ for the character ω^{k-2}.*

This leads of course to the natural extension of the above question: we want to know whether $U_p - 1$ generates $\mathbf{I}$ in general.

Theorem 1.42. *With the exception of one value of χ for $N = 3$ and $p = 331$ we have that for all p and χ as above with N prime and $Np < 1000$, as well as for all χ with $N = 11$, $p = 101$ and $N = 3$ and $p \leq 397$ we have that $U_p - 1$ generates $\mathbf{I}$ in weight 2 and level Np.*

However, it is very interesting to note that it is not always the case the the element $U_p - 1$ generates $\mathbf{I}$. By running the program written by Sharifi to prove Theorem 1.41, we were able to find the following counterexample.

Theorem 1.43. *Let $\chi = \psi\omega^{149}$, where ψ is the unique character of $(\mathbb{Z}/Np\mathbb{Z})^\times$ with $\psi\,|_{(\mathbb{Z}/p\mathbb{Z})^\times} = 1$ and $\psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$. Then for $N = 3$, $p = 331$ and character $\chi\omega^{-1}$, we have that $U_p - 1$ alone does not generate the Eisenstein ideal.*

This was computed using a modification of a program written by Sharifi in the language Magma. We describe the steps of that program, as a sketch of the proof of the theorem.

Proposition 1.44. *The ring $h_2(N, \chi\omega^{-2})$ of Hecke operators acting on the space $S_2(\Gamma_1(N), \chi\omega^{-2})$ of cusp forms of weight 2, level Np and character*

$\chi\omega^{-2}$ is generated as an abelian group by the Hecke operators T_n with

$$n \leq \frac{(N+1)(p+1)}{6}.$$

Proof. This follows from [AS], Theorem 5.1. □

For each pair (N, p) and character χ, let l be the integer of Proposition 1.44 so that $T_1, \ldots, T_l$ generate $h_2(N, \chi\omega^{-2})$. Recall that in 1.37 we showed that $h(S_2(\Gamma_1(N), \chi))$ and $h(\mathcal{S}(\Gamma_1(N), \chi)^+)$ are isomorphic. Hence, to compute Hecke operators, it suffices to do so on a basis of $h(\mathcal{S}(\Gamma_1(N), \chi)^+)$. We did this, computing in Magma the matrices representing the Hecke operators U_p and T_n for $n \leq l$ as elements of the matrix ring $M_{d\times d}(\mathbb{Z}[\mu_{p-1}])$ where d is the rank of $\mathcal{S}(\Gamma_1(N), \chi)^+$.

Our earlier identification of $(p-1)^{st}$ roots of unity in $\mathbb{C}$ and $\mathbb{Z}_p$ provides a map $\mathbb{Z}[\mu_{p-1}] \to \mathbb{Z}_p$, and there is a canonical quotient map $\mathbb{Z}_p \to \mathbb{Z}/p^2\mathbb{Z}$. By composition we may map the matrices representing the Hecke operators into the matrix ring $M_{d\times d}(\mathbb{Z}/p^2\mathbb{Z})$. We denote the images of the matrices U_p and T_n in $M_{d\times d}(\mathbb{Z}/p^2\mathbb{Z})$ by $\overline{U_p}$ and $\overline{T_n}$, respectively.

Let $M = \text{span}(\overline{T_1}, \ldots, \overline{T_l})$, the subgroup of $M_{d\times d}(\mathbb{Z}/p^2\mathbb{Z})$ spanned by the $\overline{T_n}$. Then, by a simple iteration, we found the smallest integer m such that $\overline{T_1}, \ldots, \overline{T_m}$ generate M as a $\mathbb{Z}/p^2\mathbb{Z}$-module. Recalling that $p^2 \nmid B_{2,\chi\omega^{-2}}$, we have the following.

Proposition 1.45. *The ideal* $\mathbf{I}$ *is generated over* $\mathbb{Z}_p$ *by*

$$pT_1 \text{ and } T_n - \sum_{0<e|n} \chi\omega^{-1}(e) \text{ with } 1 \leq n \leq m.$$

Proof. See [S2], Section 5. □

Proposition 1.46. *$U_p - 1$ generates $\mathbf{I}$ as a $\mathbb{Z}_p$-module if and only if $U_p - 1$ generates the abelian group $\mathbf{I}/\mathbf{I}^2$.*

Proof. This follows as a consequence of [S2], Lemma 5.5. □

We create the Eisenstein ideal in Magma using Propositon 1.45: we use the elements

$$\{\overline{T_m} - \sum_{k|m} \chi\omega^{-1}(k), \ldots, \overline{T_2} - \sum_{k|2} \chi\omega^{-1}(k), p\overline{T_1}\}$$

and their products to compute the images I and J, of $\mathbf{I}$ and $\mathbf{I}^2$, respectively, in M. Then we test that $\mathrm{I} = \mathrm{J} + \langle \overline{U}_p - 1 \rangle$. This suffices to prove that $\mathbf{I} = \mathbf{I}^2 + \langle U_p - 1 \rangle$.

2 A Pairing Arising from the Cup Product

2.1 Cohomology Groups and the Cup Product Map

Definition 2.1. *If G is a group and R is a ring then the group ring $R[G]$ is the set of formal linear combinations*

$$\{\sum_{g\in G} \alpha_g g \colon \alpha_g \in R \text{ and } \alpha_g = 0 \text{ for almost all } g \in G\}.$$

The group ring given the structure of a ring by linearly extending the opeartions of addition and multiplication of group elements, with addition and multiplication of coefficients given by the operations in R.

We fix some notation for this section: let G be a group, and let A be a module over the group ring $\mathbb{Z}[G]$.

Definition 2.2. *Let $C^0(G,A) = A$ and, for all $i \geq 1$, let $C^i(G,A)$ be the additive group* $\mathrm{Maps}(G^i, A)$.

Definition 2.3. *For $i \geq 0$, the i^{th} coboundary map is*

$$d^i \colon C^i(G,A) \to C^{i+1}(G,A)$$

such that for any $\phi \in C^i(G,A)$ and $(g_1, \ldots, g_{i+1}) \in C^{i+1}(G,A)$:

$$d^i(\phi)(g_1, \ldots, g_{i+1}) = g_1\phi(g_2, \ldots, g_{i+1}) +$$

$$\sum_{j=1}^{i}(-1)^j\phi(g_1,\ldots,g_{i-1},g_ig_{i+1},g_{i+2},\ldots,g_{i+1})+(-1)^{i+1}\phi(g_1,\ldots,g_i).$$

Definition 2.4. *The set of i-cocycles is $Z^i(G,A)=\ker(d^i)$.*

Definition 2.5. *The set of i-coboundaries is $B^i(G,A)=\mathrm{im}(d^{i-1})$.*

Definition 2.6. *The cohomology groups are*

$$H^i(G,A)=\frac{Z^i(G,A)}{B^i(G,A)} \text{ for } i\geq 1.$$

Theorem 2.7. *For $i\geq 0$, the cohomology groups $H^i(G,A)$ are abelian groups satisfying*

1. *$H^0(G,A)=A^G=\{a\in A \mid ga=a\ \forall g\in G\}$, the G-invariants of A.*
2. *If $f\colon A\to B$ is a $\mathbb{Z}[G]$-module homomorphism, then there exist group homomorphisms $f^*\colon H^i(G,A)\to H^i(G,B)$ induced by f for every $i\geq 0$.*
3. *If*

$$0\longrightarrow A\xrightarrow{k}B\xrightarrow{j}C\longrightarrow 0$$

is a short exact sequence of $\mathbb{Z}[G]$-modules, then there exists a long exact sequence of abelian groups

$$0\longrightarrow H^0(G,A)\xrightarrow{k^*}H^0(G,B)\xrightarrow{j^*}H^0(G,C)\xrightarrow{\delta}$$

$$H^1(G,A)\xrightarrow{k^*}H^1(G,B)\xrightarrow{j^*}H^1(G,C)\xrightarrow{\delta}H^2(G,A)\longrightarrow\cdots$$

Theorem 2.8. *The cup product maps are the unique family of homomorphisms satisfying*

$$H^i(G,A) \otimes_{\mathbb{Z}} H^j(G,B) \xrightarrow{\cup} H^{i+j}(G, A \otimes B)$$

for all $i, j \geq 0$ and $\mathbb{Z}[G]$-modules A and B such that

1. *If $f\colon A \to A'$ is a $\mathbb{Z}[G]$-module homomorphism then there exists a commutative diagram*

$$\begin{array}{ccc} H^i(G,A) \otimes H^j(G,B) & \xrightarrow{\cup} & H^{i+j}(G, A \otimes B) \\ \downarrow{\scriptstyle f^* \otimes id_B^*} & & \downarrow{\scriptstyle (f \otimes id_B)^*} \\ H^i(G,A') \otimes H^j(G,B) & \xrightarrow{\cup} & H^{i+j}(G, A' \otimes B) \end{array}$$

   and similarly for maps $g\colon B \to B'$.

2. *If $i = j = 0$ then*

$$\begin{array}{ccc} A^G \otimes B^G & \xrightarrow{\cup} & (A \otimes B)^G \\ \downarrow & & \downarrow \\ A \otimes B & \xrightarrow{=} & A \otimes B \end{array}$$

   commutes.

3. *If we have a short exact sequence of $\mathbb{Z}[G]$-modules*

$$0 \to A \to A' \to A'' \to 0$$

   such that

$$0 \to A \otimes B \to A' \otimes B \to A'' \otimes B \to 0$$

   is still exact then, for $f'' \in H^i(G, A'')$ and $F \in H^j(G, B)$,

$$(\delta f'') \cup F = \delta(f'' \cup F)$$

where δ is the coboundary map in the long exact sequence in cohomology.

4. *If $f \in H^i(G, A)$ and $F \in H^j(G, B)$, then there exists a natural isomorphism $H^{i+j}(G, A \otimes B) \cong H^{i+j}(G, B \otimes A)$ since $A \otimes B \cong B \otimes A$. Under this identification,*

$$f \cup F = (-1)^{ij} F \cup f.$$

2.2 The Pairing

Let K be a field containing the n^{th} roots of unity for some $n \in \mathbb{Z}$. Let S be a set of primes of K including those above n, and let K_S be the maximal extension of K unramified outside S. Let $G_{K,S}$ denote the Galois group $\mathrm{Gal}(K_S/K)$.

Definition 2.9. *If S is a set of primes of a number field K, the S-integers of K are*

$$\mathcal{O}_{K,S} = \{a \in K : \mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0 \ \forall \mathfrak{p} \notin S\}.$$

The group of S-units is

$$\mathcal{O}_{K,S}^{\times} = \{a \in K : \mathrm{ord}_{\mathfrak{p}}(\alpha) = 0 \ \forall \mathfrak{p} \notin S\}.$$

Definition 2.10. *Let K be a field containing the group μ_n of n^{th} roots of unity, for some $n \in \mathbb{Z}$. A Kummer extension of K is a field extension L/K where L is of the form $L = K(\sqrt[n]{\Delta})$ and Δ is a subgroup of $K^{\times}$ containing $K^{\times n}$, the group of n^{th} powers. That is, L is generated by all roots $\sqrt[n]{a}$ such that $a \in \Delta$.*

Theorem 2.11 (Kummer Theory). *The Kummer extensions are in bijective correspondence with the subgroups Δ of $K^\times$ containing $K^{\times n}$. Further, if $L = K(\sqrt[n]{\Delta})$ then $\Delta = L^{\times n} \cap K^\times$ and*

$$\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n) \cong \Delta / K^{\times n}$$

in a canonical fashion.

Fix notation: let $D_K = K_S^{\times n} \cap K^\times$. Note that D_K contains $\mathcal{O}_{K,S}^\times$ as, by definition,

$$\mathcal{O}_{K,S}^\times = \{x \in K^\times : \mathrm{ord}_\mathfrak{q}(x) = 0 \ , \ \forall \mathfrak{q} \notin S\} \subset$$

$$\{x \in K^\times : n \mid \mathrm{ord}_\mathfrak{q}(x) \ , \ \forall \mathfrak{q} \notin S\} = D_K.$$

As explained in [McS], Section 2, since any homomorphism from $G_{K,S}$ to μ_n factors through the maximal abelian quotient of $G_{K,S}$ of exponent n, we have by Kummer theory that

$$H^1(G_{K,S}, \mu_n) \cong \frac{D_K}{K^{\times n}}.$$

We only consider the case where K is a cyclotomic field and in particular $K = \mathbb{Q}(\mu_n)$ for n either a prime p or a product of two primes p and N. We also assume that S consists of only the primes above p in K.

Definition 2.12. *We define the pairing*

$$(\ ,\ )_S = (\ ,\ )_{n,K,S} : D_K \times D_K \to H^2(G_{K,S}, \mu_p^{\otimes 2})$$

to be that induced by the cup product

$$H^1(G_{K,S}, \mu_p) \otimes H^1(G_{K,S}, \mu_p) \to H^2(G_{K,S}, \mu_p \otimes \mu_p).$$

2.3 Case 1: $K = \mathbb{Q}(\mu_p)$, p is prime

Let $K = \mathbb{Q}(\mu_p)$, where p is an odd prime and μ_p is the group of p^{th} roots of unity. Let ζ_p be a fixed primitive p^{th} root of unity.

Proposition 2.13. *The unique prime above p in K is $(1 - \zeta_p)$.*

Proof. See [W], Section 1. □

Let S be the set containing the unique prime above p in K. As before, let $G_{K,S}$ be the Galois group of the maximal extension of K unramified outside S. Let A_K be the Sylow-p subgroup of the class group Cl_K.

Proposition 2.14. *There is an isomorphism $A_K \otimes \mu_p \to H^2(G_{K,S}, \mu_p^{\otimes 2})$ of $\mathbb{Z}_p[\Delta]$-modules.*

Proof. Recall from [McS], Section 2, that we have the short exact sequence

$$0 \longrightarrow A_K \otimes \mu_p \longrightarrow H^2(G_{K,S}, \mu_p^{\otimes 2}) \longrightarrow (\bigoplus_{v \in S} \mu_p \xrightarrow{\pi} \mu_p) \longrightarrow 0\,. \quad (2)$$

As was also explained in [McS], Section 2, we may identify

$$\bigoplus_{v \in S} \mu_p \xrightarrow{\pi} \mu_p$$

with the p-torsion in the S-part of the Brauer group, tensored with μ_p, namely $\mathrm{Br}_S(K)[p] \otimes \mu_p$. Recall that by definition

$$\mathrm{Br}_S(K)[p] \otimes \mu_p = \ker(\bigoplus_{v \in S} H^2(G_{K_v}, \mu_p) \to \mathbb{Z}/p\mathbb{Z}) \otimes \mu_p.$$

Because the cardinality of S is one,

$$\ker(\bigoplus_{v \in S} H^2(G_{K_v}, \mu_p) \to \mathbb{Z}/p\mathbb{Z}) \otimes \mu_p = \ker(H^2(G_{K_{(1-\zeta_p)}}, \mu_p) \to \mathbb{Z}/p\mathbb{Z}) \otimes \mu_p.$$

The cohomology of the local Galois group is simple:

$$H^2(G_{K_{(1-\zeta_p)}}, \mu_p) \cong \mathbb{Z}/p\mathbb{Z}.$$

Thus, we have

$$\ker(\bigoplus_{v \in S} H^2(G_{K_v}, \mu_p) \to \mathbb{Z}/p\mathbb{Z}) \otimes \mu_p \cong \ker(\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}) \otimes \mu_p = 0.$$

In this way we are able to simplify the original short exact sequence to the following:

$$0 \longrightarrow A_K \otimes \mu_p \longrightarrow H^2(G_{K,S}, \mu_p^{\otimes 2}) \longrightarrow 0\,.$$

This implies that $A_K \otimes \mu_p \cong H^2(G_{K,S}, \mu_p^{\otimes 2})$ as desired. □

We fix some notation. Let ω be the Teichmüller character, as in Definition 1.7. Let $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$.

Definition 2.15. *Let $i \in \mathbb{Z}$, and define the ω^i-eigenspace of A_K to be*

$$A_K^{(\omega^i)} = \{a \in A_K \mid \delta(a) = \omega^i(\delta)(a)\ ,\ \forall \delta \in \Delta\}.$$

Proposition 2.16. *Let p be a prime number. Let r be even with $2 \leq r \leq p-1$. Then the following are equivalent:*

1. *The prime p divides the numerator of the r^{th} Bernoulli number B_r*
2. *The eigenspace $A_K^{(\omega^{p-r})}$ is nontrivial*
3. *The prime p divides the Bernoulli number $B_{1,\omega^{r-1}}$.*

Proof. See [W], Corollary 5.15 and Theorem 6.17. □

With this proposition in mind, we make the following definition.

Definition 2.17. *A pair of integers (p, r) with p prime and r even with $2 \leq r \leq p-2$ is called irregular if p divides the numerator of the Bernoulli number B_r.*

Fix an irregular pair (p, r).

Definition 2.18. *The t^{th} Tate twist of $\mathbb{Z}/p\mathbb{Z}$ for an integer t is written $\mathbb{Z}/p\mathbb{Z}(t)$. This object is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ as a group, and it has a $\mathbb{Z}_p[\Delta]$-module structure as well. The action of $\delta \in \Delta$ on $x \in \mathbb{Z}/p\mathbb{Z}(t)$ is given by*

$$\delta(x) = \omega(\delta)^t x.$$

Conjecture 2.19 (Vandiver's Conjecture). *Let p be a prime number and L be the maximal real subfield of the p^{th} cyclotomic field; i.e. $L = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, where ζ_p is a primitive p^{th} root of unity. Then p does not divide the class number of L.*

We assume Vandiver holds for p.

Proposition 2.20. *There is a group isomorphism $A_K^{(\omega^{1-r})} \cong \mathbb{Z}_p/B_{1,\omega^{r-1}}\mathbb{Z}_p$.*

Proof. See [W], Chapter 10. □

This allows us to choose an isomorphism

$$A_K^{(\omega^{1-r})} \otimes \mu_p \cong \mathbb{Z}/p\mathbb{Z}(2-r)$$

of $\mathbb{Z}_p[\Delta]$-modules.

Proof. See [W], Chapter 8. □

This identification is possible because both modules have an ω^{2-r}-action.

Definition 2.21. *The pairing*

$$\langle\ ,\ \rangle_r \colon D_K \times D_K \to \mathbb{Z}/p\mathbb{Z}(2-r)$$

is given by composing the following isomorphisms and natural surjection:

$$H^2(G_{K,S}, \mu_p^{\otimes 2}) \cong A_K \otimes \mu_p \twoheadrightarrow A_K^{(\omega^{1-r})} \otimes \mu_p \cong \mathbb{Z}/p\mathbb{Z}(2-r).$$

Proposition 2.22. *The pairing $\langle\ ,\ \rangle_r$ is Galois equivariant, meaning that for any $\delta \in \Delta$ and a and b in D_K we have that*

$$\delta\langle a, b\rangle_r = \langle \delta a, \delta b\rangle_r.$$

Now we restrict the mapping to the cyclotomic units $\mathcal{C}$.

Definition 2.23. *The cyclotomic p-units of K are defined to be the group*

$$C_K = \left\langle \zeta_p^r - 1 \mid (r,p) = 1 \right\rangle.$$

We will technically now pass to the $\mathbb{Z}_p[\Delta]$-module $\mathcal{C} = C_K \otimes \mathbb{Z}_p$ for all further computations about the pairing.

There is a decomposition of the cyclotomic units into subspaces:

$$\mathcal{C} = \mathcal{C}^+ \oplus \mathcal{C}^-$$

where the plus and minus part are determined by the action of complex conjugation. That is, $c \in \mathcal{C}$ is an element of $\mathcal{C}^+$ if and only if c is fixed by complex conjugation; i.e. if and only if c is contained in the p-completion of the multiplicative group of the maximal real subfield $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ of $\mathbb{Q}(\mu_p)$. Note that $\mathcal{C}^-$ is just p^{th} roots of unity.

Lemma 2.24. *A prime p satisfies Vandiver's conjecture if and only if $p \nmid [\mathcal{O}_{K,S}^{\times} : C_K]$, where all notation is as above.*

Proof. See [W], Chapter 8. □

Definition 2.25. *There is a Galois equivariant pairing arising from the cup product*

$$(\ , \ )_r : \mathcal{C} \times \mathcal{C} \to A_K \otimes \mu_p$$

depending on p and r. This pairing is the $\mathbb{Z}_p$-linear extension of the restriction of $\langle \ , \ \rangle_r$.

We claim that $(\ , \ )_r$ determines $\langle \ , \ \rangle_r$ on any p-units. This in fact follows immediately from Vandiver's conjecture. We have the natural inclusion $C_K \to \mathcal{O}_{K,S}^{\times}$ and we know that $p \nmid [\mathcal{O}_{K,S}^{\times} : C_K]$ so actually $\mathcal{C} = C_K \otimes \mathbb{Z}_p \cong \mathcal{O}_{K,S}^{\times} \otimes \mathbb{Z}_p$.

Proposition 2.26. *For $x, 1-x \in \mathcal{O}_{K,S}^{\times}$, we have $(x, 1-x)_r = 0$.*

Proof. See [McS], Corollary 2.6. □

Proposition 2.27. *We have that*

$$(\zeta_p, \mathcal{C})_r = 0,$$

so we only need to compute the pairing on $\mathcal{C}^+$ to fully understand it.

Proof. Consider the p^{th} roots of unity ζ_p and ζ_p^i for some $2 \leq i \leq p-1$. By Proposition 2.26 we have that $0 = (\zeta_p^i, 1-\zeta_p^i)_r = (\zeta_p, 1-\zeta_p^i)_r^i$. Thus, $(\zeta_p, 1-\zeta_p^i)_r = 0$, so $(\zeta_p, \mathcal{C})_r = 0$ since $\mathcal{C}$ is generated by the $1-\zeta_p^i$. □

Definition 2.28. *For any $i \in \mathbb{Z}$ let*

$$\varepsilon_i = \frac{1}{p-1} \sum_{\delta \in \Delta} \omega(\delta)^{-i} \delta \in \mathbb{Z}_p[\Delta].$$

Proposition 2.29. *There is an eigenspace decomposition*

$$A_K \cong \bigoplus_{i=0}^{p-2} A_K^{(\omega^i)} = \bigoplus_{i=0}^{p-2} \varepsilon_i(A_K).$$

Proposition 2.30. *For $1 \leq i \leq p-1$ the element ε_i is an idempotent in the group ring $\mathbb{Z}_p[\Delta]$. Moreover, we may view ε_i as a surjective map projecting from the p-part of the class group to the ω^i-eigenspace of any $\mathbb{Z}_p[\Delta]$-module A:*

$$\varepsilon_i \colon A \twoheadrightarrow A^{(\omega^i)},$$

the map being multiplication by the idempotent.

Fix a primitive p^{th} root of unity ζ_p.

Definition 2.31. *Applying the idempotents we obtain the elements*

$$\eta_i := (1-\zeta_p)^{\varepsilon_{1-i}} = \prod_{\delta \in \Delta} (1-\zeta_p^{\delta})^{\omega(\delta)^{i-1}} \in C.$$

Proposition 2.32. *The elements η_i with i odd, $1 \leq i \leq p-2$ generate C^+ as a $\mathbb{Z}_p$-module. In fact, $C^{(\omega^{1-i})} = \langle \eta_i \rangle$.*

Proof. See [W], Chapter 8. □

Proposition 2.33. *We have that*

$$(\eta_i, \eta_j)_r = 0 \text{ if } i + j \not\equiv r \bmod p-1.$$

Proof. Fix an element $\delta \in \Delta$. By definition of the pairing, we have that for any i and j that $(\eta_i, \eta_j)_r$ is acted on by ω^{2-r}. Thus $\delta(\eta_i, \eta_j)_r = \omega(\delta)^{2-r}(\eta_i, \eta_j)_r$. On the other hand, by Galois equivariance of the pairing we have that $\delta(\eta_i, \eta_j)_r = (\delta\eta_i, \delta\eta_j)_r$ which by definition of η is equal to $(\eta_i^{\omega(\delta)^{1-i}}, \eta_j^{\omega(\delta)^{1-j}})_r$. This is the same as $\omega(\delta)^{2-i-j}(\eta_i, \eta_j)_r$. That is,

$$\omega(\delta)^{2-r}(\eta_i, \eta_j)_r = \omega(\delta)^{2-i-j}(\eta_i, \eta_j)_r.$$

If $i + j \not\equiv r \bmod p - 1$, then the above equation cannot hold for all δ unless $(\eta_i, \eta_j)_r = 0$. □

This leads us to define the following $\frac{p-1}{2}$ elements, the values of which completely determine the pairing on $\mathcal{C}$:

Definition 2.34. *For i odd, $1 \leq i \leq p-2$, let*

$$e_{i,r} = (\eta_i, \eta_{r-i})_r.$$

Proposition 2.35. *If $c \in \mathcal{C}$ and $1 - c = \zeta_p^k c'$ for some $k \in \mathbb{Z}$ and $c' \in \mathcal{C}$ then*

$$(c, c')_r = 0.$$

Proof. We have $0 = (c, 1-c)_r$ by Proposition 2.26. Then by hypothesis, we may write

$$(c, 1-c)_r = (c, \zeta_p^k c')_r = (c, c')_r (c, \zeta_p)_r^k.$$

By Proposition 2.27 we have that $(c, \zeta_p)_r$ is trivial. Hence $(c, c')_r = 0$. □

We will create several relations using Proposition 2.35 in this case as well as in the case where $K = \mathbb{Q}(\mu_{Np})$ where N and p are prime. In order to create the relations, we will first need to study some particular polynomials.

2.4 The Polynomials

Definition 2.36. *For $a \geq 1$, let*

$$f_a = \sum_{j=0}^{a-1} (-x)^j \in \mathbb{Z}[x].$$

Proposition 2.37. *For all $a \geq 2$, we have $1 - f_a = x f_{a-1}$.*

Proof. We have that

$$x f_{a-1} = x \sum_{j=0}^{a-2} (-x)^j = x - x^2 + x^3 + \ldots + x(-x)^{a-2}$$

$$= 1 - (1 - x + x^2 - \ldots + (-x)^{a-1}) = 1 - f_a.$$

□

Proposition 2.38. *If a is an even integer, then we have*

$$f_a = \frac{1 - x^a}{1 + x} = \frac{(1 - x^a)(1 - x)}{1 - x^2}$$

and

$$f_{a-1} = \frac{1 + x^{a-1}}{1 + x} = \frac{(1 - x^{2a-2})(1 - x)}{(1 - x^{a-1})(1 - x^2)}.$$

Proof. First recall the well-known polynomial identity

$$1 - x^a = (1 + x)(1 - x + x^2 - \ldots - x^{a-1}),$$

which holds for all x and all a even. This shows that

$$f_a = \frac{1 - x^a}{1 + x}.$$

To show that

$$\frac{1 - x^a}{1 + x} = \frac{(1 - x^a)(1 - x)}{1 - x^2},$$

notice that

$$(1-x^a)(1-x^2) = (1-x^a)(1-x)(1+x).$$

Similarly,

$$f_{a-1} = \frac{1+x^{a-1}}{1+x}$$

because of the identity

$$(1-x+x^2+\ldots+x^{a-2})(1+x) = 1+x^{a-1}.$$

Finally,

$$\frac{1+x^{a-1}}{1+x} = \frac{(1-x^{2a-2})(1-x)}{(1-x^{a-1})(1-x^2)}$$

because

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

□

From now on we let $x = \zeta$ where ζ is a root of unity. That is, we consider $\rho_a := f_a(\zeta) \in \mathbb{Q}(\mu_p)$. For now, we let $\zeta = \zeta_p$. Note that for any $a \geq 1$ we have that f_a is a p-unit or zero.

2.5 The Relations in Case 1

Proposition 2.39. *If $\delta \in \Delta$ satisfies $\delta\zeta_p = \zeta_p^a$ for some $a \in \mathbb{Z}$ then $\omega(\delta) \equiv a \bmod p$. Furthermore,*

$$(1-\zeta_p^a)^{\varepsilon_{1-i}} \equiv \eta_i^{a^{1-i}} \bmod \mathcal{C}^p.$$

Proof. The first statement is true by definition of the Teichmüller character. It is necessary, however, to notice that we may apply ω to δ by using the

isomorphism $\mathbb{Z}/p\mathbb{Z} \cong \mathrm{Gal}(K/\mathbb{Q})$ to identify δ with an integer mod p. The second statement is a simple computation:

$$(1-\zeta_p^a)^{\varepsilon_{1-i}} = (1-\delta\zeta_p)^{\varepsilon_{1-i}} = (1-\zeta_p)^{\omega(\delta)^{1-i}\varepsilon_{1-i}} \equiv \eta_i^{a^{1-i}} \bmod \mathcal{C}^p.$$

□

By the eigenspace decomposition, Proposition 2.29, we have that for any $x, y \in \mathcal{C}$,

$$(x,y)_r = \left(\prod_{i=1}^{p-1} x^{\varepsilon_{1-i}}, \prod_{j=1}^{p-1} y^{\varepsilon_{1-j}}\right)_r$$

which because the odd eigenspaces are trivial or μ_p, along with Proposition 2.33, is equal to

$$\prod_{\substack{i=1 \\ \text{i odd}}}^{p-2} \left(x^{\varepsilon_{1-i}}, y^{\varepsilon_{1-(r-i)}}\right)_r.$$

Suppose that a is even. Choosing $x = \rho_a$ and $y = \rho_{a-1}$, we see that

$$(\rho_a, \rho_{a-1})_r = \prod_{\substack{i=1 \\ \text{i odd}}}^{p-2} \left(\rho_a^{\varepsilon_{1-i}}, \rho_{a-1}^{\varepsilon_{1-(r-i)}}\right)_r.$$

We compute using Proposition 2.38 that

$$\rho_a^{\varepsilon_{1-i}} = \frac{(1-\zeta_p^a)^{\varepsilon_{1-i}}(1-\zeta_p)^{\varepsilon_{1-i}}}{(1-\zeta_p^2)^{\varepsilon_{1-i}}}$$

but by Proposition 2.39, we must have that

$$\rho_a^{\varepsilon_{1-i}} \equiv \frac{\eta_i^{a^{1-i}}\eta_i}{\eta_i^{2^{1-i}}} = \eta_i^{1-2^{1-i}+a^{1-i}} \bmod \mathcal{C}^p.$$

Similarly,

$$\rho_{a-1}^{\varepsilon_{1-(r-i)}} = \frac{(1-\zeta_p^{2a-2})^{\varepsilon_{1-(r-i)}}(1-\zeta_p)^{\varepsilon_{1-(r-i)}}}{(1-\zeta_p^{a-1})^{\varepsilon_{1-(r-i)}}(1-\zeta_p^2)^{\varepsilon_{1-(r-i)}}}.$$

But since

$$(1-\zeta_p^a)^{\varepsilon_{1-(r-i)}} = \eta_{r-i}^{a^{1-(r-i)}},$$

for some $\delta \in \Delta$ with $\delta(\zeta_p) = \zeta_p^a$ we must have

$$\rho_{a-1}^{\varepsilon_{1-(r-i)}} \equiv \frac{\eta_{r-i}^{(2(a-1))^{1-r+i}}\eta_{r-i}}{\eta_{r-i}^{(a-1)^{1-r+1}}\eta_{r-i}^{2^{1-r+i}}}$$

$$= \eta_{r-i}^{(2(a-1))^{1-r+i}+1-(a-1)^{1-r+i}-2^{1-r+i}} = \eta_{r-i}^{(1-2^{1-r+i})(1-(a-1)^{1-r+i})} \bmod \mathcal{C}^p.$$

As ρ_a is a p-unit, and by the relationship described in Proposition 2.37, we must have by Proposition 2.35 that

$$(\rho_a, \rho_{a-1})_r = 0.$$

Finally, we compute that

$$0 = \sum_{\substack{i \text{ odd} \\ 1\le i\le p-2}} (\eta_i^{1-2^{1-i}+a^{1-i}}, \eta_{r-i}^{(1-2^{1-r+i})(1-(a-1)^{1-r+i})})_r$$

which implies that the $e_{i,r}$ are solutions over $\mathbb{Z}/p\mathbb{Z}$ to

$$\sum_{\substack{\text{i odd,} \\ 1\le i\le p-2}} (1-2^{1-i}+a^{1-i})(1-2^{1-r+i})(1-(a-1)^{1-r+i})e_{i,r} = 0 \qquad (3)$$

for every a even with $2 \le a \le p-1$.

Proposition 2.40. *The pairing* $(\ ,\ )_r$ *is skew-symmetric.*

Proof. Because the pairing arises from the cup product, for any $x, y \in \mathcal{C}$ we have by part 4 of Theorem 2.8 that

$$(x,y)_r = -(y,x)_r.$$

□

Corollary 2.41. *The $e_{i,r}$ also satisfy the relation*

$$e_{i,r} + e_{r-i,r} = 0. \tag{4}$$

Theorem 2.42 (McCallum-Sharifi). *For all irregular pairs (p, r) with p less than* 25,000, *the $e_{i,r}$ with $1 \leq i \leq p-2$ odd are uniquely determined by the relations (3) and (4) up to a single scalar in $\mathbb{Z}/p\mathbb{Z}$. That is, $(\ ,\ )_r$ is determined by (3) and (4) up to a possibly zero scalar multiple.*

Proof. See [McS], Theorem 5.1. □

This theorem was proved using a computer program in the language Magma. It creates the matrix of the relations (3) and (4), and computes the nullspace of this matrix to have dimension 1.

Example 2.43. *For example, first compute the nullspace of the matrix*

$$M = (\alpha_{j,i})_{1 \leq i \leq p-2, i \text{ odd };\ 2 \leq j \leq p-1, j \text{ even}}$$

where for any i, j, we have that

$$\alpha_{j,i} = (1 - 2^{1-i} + j^{1-i})(1 - 2^{1-r+i})(1 - (j-1)^{1-r+i}).$$

2.6 Case 2: $K = \mathbb{Q}(\mu_{Np})$, N and p prime

Let N be an odd prime number relatively prime to p with $N - 1 \mid p - 1$. Recall that $K = \mathbb{Q}(\mu_{Np})$. Let S be the set of primes of K consisting of all those dividing p. Let A_K be the p-part of the class group of K. Let ω be the Teichmüller character. Let $\Delta = \mathrm{Gal}(K/\mathbb{Q})$. We fix a primitive Np^{th} root of unity ζ_{Np} such that $\zeta_{Np}^N = \zeta_p$ and define $\zeta_N = \zeta_{Np}^p$.

Let Δ^* be the Dirichlet group modulo Np. That is,

$$\Delta^* \cong \mathrm{Hom}(\Delta, \mathbb{Z}_p^\times).$$

Proposition 2.44. $\Delta^* \cong (\mathbb{Z}/N\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times$.

Proof. We have that

$$\Delta^* \cong \mathrm{Hom}((\mathbb{Z}/Np\mathbb{Z})^\times, \mathbb{Z}_p^\times) \cong \mathrm{Hom}((\mathbb{Z}/N\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times, \mathbb{Z}_p^\times)$$

by elementary group theory, and that

$$\mathrm{Hom}((\mathbb{Z}/N\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times, \mathbb{Z}_p^\times) \cong \mathrm{Hom}((\mathbb{Z}/N\mathbb{Z})^\times, \mathbb{Z}_p^\times) \times \mathrm{Hom}((\mathbb{Z}/p\mathbb{Z})^\times, \mathbb{Z}_p^\times)$$

by additivity of the Hom functor. It is obvious that $\mathrm{Hom}((\mathbb{Z}/p\mathbb{Z})^\times, \mathbb{Z}_p^\times) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, and because of the assumption that $\varphi(N) \mid \varphi(p)$ it follows that $\mathrm{Hom}((\mathbb{Z}/N\mathbb{Z})^\times, \mathbb{Z}_p^\times) \cong (\mathbb{Z}/N\mathbb{Z})^\times$. Thus we have that $\Delta^* \cong (\mathbb{Z}/N\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times$. □

Definition 2.45. *The p-completion $\mathcal{C}$ of cyclotomic p-units of K is*

$$(\langle 1 - \zeta_{Np}^i \mid i \not\equiv 0 \bmod Np \rangle \cap \mathcal{O}_{K,S}^\times) \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

We just described how $\mathcal{C}$ is generated as a pro-p group; however, we would like to know how it is generated as a $\mathbb{Z}_p[\Delta]$-module.

Fix an even character $\chi \in G$ of conductor N or Np. We will generalize the pairing of the previous section. We can think of χ as being an extension of ω^r above. Let $\psi \in \Delta^*$ be any Dirichlet character.

Definition 2.46. *Let $\psi \in \Delta^*$. We define the ψ-eigenspace of any $\mathbb{Z}_p[\Delta]$-module A to be*

$$A^{(\psi)} = \{a \in A \mid \delta(a) = \psi(\delta)a \ , \ \forall \delta \in \Delta\}.$$

Proposition 2.47. *With notation as in the definition, there is always an eigenspace decomposition*

$$A = \bigoplus_{\psi \in \Delta^*} A^{(\psi)}.$$

Proof. See [S2], Appendix A. □

Definition 2.48. *Let*

$$\varepsilon_{\omega\psi^{-1}} = \frac{1}{(N-1)(p-1)} \sum_{\delta \in \Delta} \omega^{-1}\psi(\delta)\delta.$$

Note that we view this idempotent as an element of the group ring $\mathbb{Z}_p[\Delta]$. We can also view it as a map projecting from the p-part of a $\mathbb{Z}_p[\Delta]$-module A to the $(\omega\psi^{-1})$-eigenspace:

$$\varepsilon_{\omega\psi^{-1}} \colon A \twoheadrightarrow A^{(\omega\psi^{-1})},$$

the action being multiplication by the idempotent.

Remark 2.49. *We may also write the eigenspace decomposition of 2.47 in terms of the idempotents:*

$$A = \bigoplus_{\psi \in \Delta^*} \varepsilon_{\omega\psi^{-1}}(A).$$

We fix notation: let $\chi \in \Delta^*$ be an even Dirichlet character such that $p \mid B_{1,\chi\omega^{-1}}$.

Proposition 2.50. *There is a Galois-equivariant, skew-symmetric pairing arising from the cup product*

$$\langle\ ,\ \rangle_\chi \colon \mathcal{C} \times \mathcal{C} \to H^2(G_{K,S}, \mu_p^{\otimes 2}) \twoheadrightarrow A_K^{(\omega\chi^{-1})} \otimes \mu_p \cong (A_K \otimes \mu_p)^{(\omega^2\chi^{-1})}$$

depending on N, p, and χ.

Proof. See [McS] and [S2], Section 5. □

2.7 Understanding the pairing

We now apply the idempotents.

Proposition 2.51. *There is an eigenspace decomposition of $\mathbb{Z}_p[\Delta]$modules:*

$$C = \bigoplus_{\psi \in \Delta^*} C^{(\psi)},$$

where

$$C^{(\psi)} = \begin{cases} \mathbb{Z}_p & \psi \text{ is even}, \\ \mu_p & \psi = \omega, \\ 0 & \psi \text{ is odd and } \psi \neq \omega. \end{cases}$$

Proof. See [R], Chapter 3. □

Definition 2.52. *Let*

$$\eta_\psi = (1 - \zeta_{Np})^{\varepsilon_{\omega\psi^{-1}}}$$

and

$$\eta'_\psi = (1 - \zeta_p)^{\varepsilon_{\omega\psi^{-1}}}.$$

Much as before with the η_i, the η_ψ and η'_ψ will in this case help us find a basis for the cyclotomic p-units, thus allowing us to compute the pairing by restricting our computations to just those basis elements.

Proposition 2.53. *Let ψ be an odd character in Δ^*. Then*

$$\alpha_\psi = \begin{cases} \eta_\psi & \text{if } \psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1, \\ \eta'_\psi & \text{if } \psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1. \end{cases}$$

generates $C^{(\omega\psi^{-1})}$ as a $\mathbb{Z}_p[\Delta]$-module.

Proof. See [R], Chapter 3. □

Again, we have as in Proposition 2.27 that $\langle \zeta_p, \mathcal{C} \rangle_\chi = 0$, so we need only consider the pairing values $\langle \alpha_\psi, \alpha_{\psi^{-1}\chi} \rangle_\chi$.

Proposition 2.54. *If $\psi' \neq \psi^{-1}\chi$ then $\langle \alpha_\psi, \alpha_{\psi'} \rangle_\chi = 0$.*

Proof. Fix an element $\delta \in \Delta$. By definition of the pairing, we have that $\langle \alpha_\psi, \alpha_{\psi'} \rangle_\chi$ is acted on by $\omega^2\chi^{-1}$. Thus $\delta\langle \alpha_\psi, \alpha_{\psi'} \rangle_\chi = \omega^2\chi^{-1}(\delta)\langle \alpha_\psi, \alpha_{\psi'} \rangle_\chi$. On the other hand, by Galois equivariance of the pairing we have that $\delta\langle \alpha_\psi, \alpha_{\psi'} \rangle_\chi = \langle \delta\alpha_\psi, \delta\alpha_{\psi'} \rangle_\chi$ which by definition is equal to $\langle \alpha_\psi^{\omega\psi^{-1}(\delta)}, \alpha_{\psi'}^{\omega\psi'^{-1}(\delta)} \rangle_\chi$. This is the same as $\omega^2\psi^{-1}\psi'^{-1}(\delta)\langle \alpha_\psi, \alpha_{\psi'} \rangle_\chi$. That is,

$$\omega^2\chi^{-1}(\delta)\langle \alpha_\psi, \alpha_{\psi'} \rangle_\chi = \omega^2\psi^{-1}\psi'^{-1}(\delta)\langle \alpha_\psi, \alpha_{\psi'} \rangle_\chi.$$

If $\chi^{-1} \neq \psi^{-1}\psi'^{-1}$; i.e. if $\psi' \neq \psi^{-1}\chi$ then the above equation cannot hold for all δ unless $\langle \alpha_\psi, \alpha_{\psi'} \rangle_\chi = 0$. □

Definition 2.55. *Let $e_{\psi,\chi} = \langle \alpha_\psi, \alpha_{\psi^{-1}\chi} \rangle_\chi$.*

Recall the polynomial $f_a(x)$. We will from now on set $\rho_a = f_a(\zeta_{Np})$, where ζ_{Np} is a fixed primitive Np^{th} root of unity. As we did before, we will derive relations based on the fact that $\langle \rho_a, \rho_{a-1} \rangle_\chi = 0$ for $2 \leq a \leq p-1$.

Before we can do these computations, we need the following facts about our basis for $\mathcal{C}$.

Lemma 2.56.

$$N_{\mathbb{Q}(\mu_{Np})/\mathbb{Q}(\mu_p)}(1 - \zeta_{Np}) = \frac{1 - \zeta_p}{1 - \zeta_p^{N-1}}.$$

Proof. First, we would like to find a and b such that that $\zeta_{Np} = \zeta_p^a \zeta_N^b$. To solve this, recall that we require that $\zeta_{Np}^N = \zeta_p$ and $\zeta_{Np}^p = \zeta_N$. Thus, we have that

$$\zeta_{Np}^N = \zeta_p^{Na} \zeta_N^{Nb}$$

which implies that $\zeta_p = \zeta_p^{Na}$. That is, $Na \equiv 1 \bmod p$; i.e. $a \equiv N^{-1} \bmod p$. Similarly, $b \equiv p^{-1} \bmod N$. Thus, $\zeta_{Np} = \zeta_p^{N^{-1}} \zeta_N^{p^{-1}}$. We may now compute the norm:

$$N_{\mathbb{Q}(\mu_{Np})/\mathbb{Q}(\mu_p)}(1 - \zeta_{Np}) = N_{\mathbb{Q}(\mu_{Np})/\mathbb{Q}(\mu_p)}(1 - \zeta_p^{N^{-1}} \zeta_N^{p^{-1}})$$

$$= \prod_{j=1}^{N-1} (1 - \zeta_p^{N^{-1}} \zeta_N^{p^{-1} j}) = \prod_{j=1}^{N-1} (1 - \zeta_p^{N^{-1}} \zeta_N^{j}) = (-1)^{N-1} \prod_{j=1}^{N-1} (\zeta_p^{N^{-1}} - \zeta_N^{j}) = \Phi(\zeta_p^{N^{-1}})$$

where Φ refers to the N^{th} cyclotomic polynomial. The above is equal to

$$\frac{1 - (\zeta_p^{N^{-1}})^N}{1 - \zeta_p^{N^{-1}}} = \frac{1 - \zeta_p}{1 - \zeta_p^{N^{-1}}}.$$

□

Proposition 2.57. *We have the relationship*

$$\eta_\psi = \eta'^{\,(\frac{1}{N-1})(1-\omega^{-1}\psi(N))}_\psi \text{ whenever } \psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1.$$

Proof.

$$\varepsilon_{\omega\psi^{-1}} = \frac{1}{(N-1)(p-1)} \sum_{\delta \in \Delta} \omega^{-1}\psi(\delta)\delta$$

$$= \left(\frac{1}{N-1} \sum_{\delta \in \mathrm{Gal}(\mathbb{Q}(\mu_{Np})/\mathbb{Q}(\mu_p))} \omega^{-1}\psi(\delta)\delta \right) \left(\frac{1}{p-1} \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_{Np})/\mathbb{Q}(\mu_N))} \omega^{-1}\psi(\sigma)\sigma \right)$$

As $\psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1$ we have that the above is equal to

$$= \left(\frac{1}{N-1} \sum_{\delta \in \mathrm{Gal}(\mathbb{Q}(\mu_{Np})/\mathbb{Q}(\mu_p))} \omega^{-1}(\delta)\delta \right) \left(\frac{1}{p-1} \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_{Np})/\mathbb{Q}(\mu_N))} \omega^{-1}\psi(\sigma)\sigma \right)$$

$$= \left(\frac{1}{N-1}\sum_{\delta\in \mathrm{Gal}(\mathbb{Q}(\mu_{Np})/\mathbb{Q}(\mu_p))}\delta\right)\left(\frac{1}{p-1}\sum_{\sigma\in \mathrm{Gal}(\mathbb{Q}(\mu_{Np})/\mathbb{Q}(\mu_N))}\omega^{-1}\psi(\sigma)\sigma\right)$$

$$= \frac{1}{N-1}\left(\sum_{\delta\in \mathrm{Gal}(\mathbb{Q}(\mu_{Np})/\mathbb{Q}(\mu_p))}\delta\right)\varepsilon'_{\omega\psi^{-1}},$$

where

$$\varepsilon'_{\omega\psi^{-1}} = \frac{1}{p-1}\sum_{\sigma\in \mathrm{Gal}(\mathbb{Q}(\mu_{Np})/\mathbb{Q}(\mu_N)}\omega^{-1}\psi(\sigma)\sigma.$$

Thus, using Lemma 2.56, we have that

$$\eta_\psi = (1-\zeta_{Np})^{\varepsilon_{\omega\psi^{-1}}} = N_{\mathbb{Q}(\mu_{Np})/\mathbb{Q}(\mu_p)}(1-\zeta_{Np})^{\frac{1}{N-1}\varepsilon'_{\omega\psi^{-1}}} =$$

$$\left(\frac{1-\zeta_p}{1-\zeta_p^{N-1}}\right)^{\frac{1}{N-1}\varepsilon'_{\omega\psi^{-1}}}.$$

Notice that

$$(1-\zeta_p)^{\varepsilon_{\omega\psi^{-1}}} = (1-\zeta_p)^{\frac{1}{N-1}(\sum_{\sigma\in \mathrm{Gal}(\mathbb{Q}(\mu_{Np})/\mathbb{Q}(\mu_p)}\sigma)\varepsilon'_{\omega\psi^{-1}}}$$

$$= (1-\zeta_p)^{\frac{N-1}{N-1}\varepsilon'_{\omega\psi^{-1}}} = (1-\zeta_p)^{\varepsilon'_{\omega\psi^{-1}}}.$$

Thus the above is equal to

$$\frac{{\eta'_\psi}^{\frac{1}{N-1}}}{{\eta'_\psi}^{\omega^{-1}\psi(N)\frac{1}{N-1}}} = {\eta'_\psi}^{(\frac{1}{N-1})(1-\omega^{-1}\psi(N))}.$$

□

Proposition 2.58. *If* $\psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$ *then* $(1-\zeta_p)^{\varepsilon_{\omega\psi^{-1}}} = 1$.

Proof. Since $\psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$ for all $\delta \in \mathrm{Gal}(\mathbb{Q}(\mu_{Np})/\mathbb{Q}(\mu_p))$, we have

$$(1-\zeta_p)^{\varepsilon_{\omega\psi^{-1}}} = \delta(1-\zeta_p)^{\varepsilon_{\omega\psi^{-1}}} = (1-\zeta_p)^{\varepsilon_{\omega\psi^{-1}}\omega\psi^{-1}(\delta)} = (1-\zeta_p)^{\varepsilon_{\omega\psi^{-1}}\psi^{-1}(\delta)},$$

which is a contradiction if $(1-\zeta_p)^{\varepsilon_{\omega\psi^{-1}}} \neq 1$. □

Fix notation: ψ always refers to an element of Δ^*, and a sum over ψ means to sum over all such characters; that is, over the entire Dirichlet group modulo Np.

Proposition 2.59. *Suppose* $\psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1$. *If* $a \in \mathbb{Z}$ *is prime to* Np, *then*

$$(1-\zeta_p^a)^{\varepsilon_{\omega\psi^{-1}}} = \eta_\psi'^{\omega\psi^{-1}(a)}$$

and

$$(1-\zeta_{Np}^a)^{\varepsilon_{\omega\psi^{-1}}} = \eta_\psi^{\omega\psi^{-1}(a)}.$$

Proof. First we compute that

$$(1-\zeta_p^a)^{\varepsilon_{\omega\psi^{-1}}} = (1-\delta\zeta_p)^{\varepsilon_{\omega\psi^{-1}}}$$

where $\delta \in \Delta$ is an element taking ζ_p to ζ_p^a under the canonical isomorphism $\Delta \cong (\mathbb{Z}/Np\mathbb{Z})^\times$. Then we have that

$$(1-\delta\zeta_p)^{\varepsilon_{\omega\psi^{-1}}} = (1-\zeta_p)^{\omega\psi^{-1}(\delta)\varepsilon_{\omega\psi^{-1}}} \equiv \eta_\psi'^{\omega\psi^{-1}(\delta)} \bmod \mathcal{C}^p$$

by the definition of η_ψ'. Similarly,

$$(1-\zeta_{Np}^a)^{\varepsilon_{\omega\psi^{-1}}} = (1-\sigma\zeta_{Np})^{\varepsilon_{\omega\psi^{-1}}}$$

where $\sigma \in \Delta$ is the element taking ζ_{Np} to ζ_{Np}^a. Then we have that

$$(1-\sigma\zeta_{Np})^{\varepsilon_{\omega\psi^{-1}}} = (1-\zeta_{Np})^{\omega\psi^{-1}(\sigma)\varepsilon_{\omega\psi^{-1}}} \equiv \eta_\psi^{\omega\psi^{-1}(\sigma)} \bmod \mathcal{C}^p$$

by the definition of η_ψ. □

By the eigenspace decomposition, Proposition 2.47, we have that for any $c, c' \in \mathcal{C}$,

$$\langle c, c'\rangle = \langle \prod_\psi c^{\varepsilon_{\omega\psi^{-1}}}, \prod_\psi c'^{\varepsilon_{\omega\psi\chi^{-1}}}\rangle_\chi = \sum_\psi \langle c^{\varepsilon_{\omega\psi^{-1}}}, c'^{\varepsilon_{\omega\psi\chi^{-1}}}\rangle_\chi.$$

Suppose that a is an even integer with a and $a-1$ relatively prime to p and that χ is a fixed even Dirichlet character. Choosing $c = \rho_a$ and $c' = \rho_{a-1}$ we see that

$$\langle \rho_a, \rho_{a-1} \rangle_\chi = \sum_\psi \langle \rho_a^{\varepsilon_{\omega\psi^{-1}}}, \rho_{a-1}^{\varepsilon_{\omega\psi\chi^{-1}}} \rangle_\chi.$$

Since ρ_a is a cyclotomic unit, and by the relationship described in Proposition 2.37, we must have by Proposition 2.35 that

$$\langle \rho_a, \rho_{a-1} \rangle_\chi = 0.$$

To compute the relations arising from this fact, we note that our computation depends on whether or not

$$\psi \mid_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1 \text{ and } \psi^{-1}\chi \mid_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1.$$

Moreover, because of our choice of $\rho_a = \rho_a(\zeta_{Np})$ and similarly with $\rho_{a-1} = \rho_{a-1}(\zeta_{Np})$, by Proposition 2.38 we will be raising ζ_{Np} to powers of a and $a-1$ so we must also consider whether $N \mid a$ and $N \mid a-1$ because if either were the case, our primitive Np^{th} root of unity could be reduced to a primitive p^{th} root of unity, which would affect the computation of the relations.

2.8 The Relations in Case 2

Proposition 2.60. *The following comprise all possible cases necessary to compute the coefficients $c_{\chi,\psi}(a)$ in*

$$0 = \langle \rho_a, \rho_{a-1} \rangle_\chi = \sum_\psi \langle \rho_a^{\varepsilon_{\omega\psi^{-1}}}, \rho_{a-1}^{\varepsilon_{\omega\psi\chi^{-1}}} \rangle_\chi = \sum_\psi c_{\chi,\psi}(a) \langle \alpha_\psi, \alpha_{\chi\psi^{-1}} \rangle_\chi.$$

.

1. $N \mid a-1$ *and* $N \nmid a$ *and* $\psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1$.

2. $N \mid a-1$ *and* $N \nmid a$ *and* $\psi\chi^{-1}\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1$.

3. $N \mid a-1$ *and* $N \nmid a$ *and* $\psi\chi^{-1}\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$ *and* $\psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$.

4. $N \nmid a-1$ *and* $N \mid a$ *and* $\psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1$.

5. $N \nmid a-1$ *and* $N \mid a$ *and* $\psi\chi^{-1}\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1$.

6. $N \nmid a-1$ *and* $N \mid a$ *and* $\psi\chi^{-1}\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$ *and* $\psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$.

7. $N \nmid a-1$ *and* $N \nmid a$ *and* $\psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1$.

8. $N \nmid a-1$ *and* $N \nmid a$ *and* $\psi\chi^{-1}\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1$.

9. $N \nmid a-1$ *and* $N \nmid a$ *and* $\psi\chi^{-1}\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$ *and* $\psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$.

We compute the relations in each of these cases:

1. In the case $N \mid a-1$ and $N \nmid a$, $\psi^{-1}\chi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$ and $\psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1$ we have

$$\rho_a^{\varepsilon_{\omega\psi^{-1}}} = \frac{(1-\zeta_{Np}^a)^{\varepsilon_{\omega\psi^{-1}}}(1-\zeta_{Np})^{\varepsilon_{\omega\psi^{-1}}}}{(1-\zeta_{Np}^2)^{\varepsilon_{\omega\psi^{-1}}}} = \eta_\psi^{\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2)}$$

$$= \eta_\psi'^{\,(\frac{1-\omega^{-1}\psi(N)}{N-1})(\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2))}$$

by Propositions 2.57 and 2.59. Also,

$$\rho_{a-1}^{\varepsilon_{\omega\psi\chi^{-1}}} = \frac{(1-\zeta_p^{\frac{2(a-1)}{N}})^{\varepsilon_{\omega\psi\chi^{-1}}}(1-\zeta_{Np})^{\varepsilon_{\omega\psi\chi^{-1}}}}{(1-\zeta_p^{\frac{(a-1)}{N}})^{\varepsilon_{\omega\psi\chi^{-1}}}(1-\zeta_{Np}^2)^{\varepsilon_{\omega\psi\chi^{-1}}}} = \eta_{\psi^{-1}\chi}^{1-\omega\psi\chi^{-1}(2)},$$

by Propositions 2.58 and 2.59. Because

$$\langle \rho_a^{\varepsilon_{\omega\psi^{-1}}}, \rho_{a-1}^{\varepsilon_{\omega\psi\chi^{-1}}} \rangle_\chi = 0$$

and

$$e_{\psi,\chi} = \langle \alpha_\psi, \alpha_{\psi^{-1}\chi} \rangle_\chi,$$

which in this case is equal to $\langle \eta'_\psi, \eta_{\psi^{-1}\chi} \rangle_\chi$, we have

$$0 = \langle \eta'_\psi {}^{(\frac{1-\omega^{-1}\psi(N)}{N-1})(\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2))}, \eta_{\psi^{-1}\chi}^{1-\omega\psi\chi^{-1}(2)} \rangle_\chi$$

$$= \sum_{\substack{\psi \text{ odd} \\ \psi|_{(\mathbb{Z}/N\mathbb{Z})^\times}=1}} (\frac{1-\omega^{-1}\psi(N)}{N-1})(\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2))(1-\omega\psi\chi^{-1}(2))e_{\psi,\chi}$$

for every a even, $1 < a < Np$ with $N \nmid a$ and $N \mid a-1$.

2. In the case $N \mid a-1$ and $N \nmid a$, $\psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$ and $\psi^{-1}\chi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1$ we have

$$\rho_a^{\varepsilon_{\omega\psi^{-1}}} = \frac{(1-\zeta_{Np}^a)^{\varepsilon_{\omega\psi^{-1}}}(1-\zeta_{Np})^{\varepsilon_{\omega\psi^{-1}}}}{(1-\zeta_{Np}^2)^{\varepsilon_{\omega\psi^{-1}}}} = \eta_\psi^{\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2)}$$

and

$$\begin{aligned}
\rho_{a-1}^{\varepsilon_{\omega\psi\chi^{-1}}} &= \frac{(1-\zeta_p^{\frac{2(a-1)}{N}})^{\varepsilon_{\omega\psi\chi^{-1}}}(1-\zeta_{Np})^{\varepsilon_{\omega\psi\chi^{-1}}}}{(1-\zeta_p^{\frac{(a-1)}{N}})^{\varepsilon_{\omega\psi\chi^{-1}}}(1-\zeta_{Np}^2)^{\varepsilon_{\omega\psi\chi^{-1}}}} \\
&= \eta'^{\omega\psi\chi^{-1}(\frac{2a-2}{N})-\omega\psi\chi^{-1}(\frac{a-1}{N})}_{\psi^{-1}\chi} \eta_{\psi^{-1}\chi}^{1-\omega\psi\chi^{-1}(2)} \\
&= \eta'^{(\frac{1-\omega^{-1}\psi^{-1}\chi(N)}{N-1}-\omega\psi\chi^{-1}(\frac{a-1}{N}))(1-\omega\psi\chi^{-1}(2))}_{\psi^{-1}\chi}.
\end{aligned}$$

Because

$$\langle \rho_a^{\varepsilon_{\omega\psi^{-1}}}, \rho_{a-1}^{\varepsilon_{\omega\psi\chi^{-1}}} \rangle_\chi = 0$$

and

$$e_{\psi,\chi} = \langle \alpha_\psi, \alpha_{\psi^{-1}\chi} \rangle_\chi,$$

which in this case is equal to $\langle \eta_\psi, \eta'_{\psi^{-1}\chi} \rangle_\chi$, we have

$$0 = \langle \eta_\psi^{\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2)}, \eta'^{(\frac{1-\omega^{-1}\psi^{-1}\chi(N)}{N-1}-\omega\psi\chi^{-1}(\frac{a-1}{N}))(1-\omega\psi\chi^{-1}(2))}_{\psi^{-1}\chi} \rangle_\chi$$

$$= \sum_{\substack{\psi \text{ odd} \\ \psi\chi^{-1}|_{(\mathbb{Z}/N\mathbb{Z})^\times}=1}} (\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2))\,(\frac{1-\omega^{-1}\psi^{-1}\chi(N)}{N-1}-\omega\psi\chi^{-1}(\frac{a-1}{N}))(1-\omega\psi\chi^{-1}(2))e_{\psi,\chi}$$

for every a even, $1 < a < Np$ with $N \nmid a$ and $N \mid a-1$.

3. In the case $N \mid a-1$ and $N \nmid a$ and $\psi^{-1}\chi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$ and $\psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$, we have

$$\rho_a^{\varepsilon_{\omega\psi^{-1}}} = \frac{(1-\zeta_{Np}^a)^{\varepsilon_{\omega\psi^{-1}}}(1-\zeta_{Np})^{\varepsilon_{\omega\psi^{-1}}}}{(1-\zeta_{Np}^2)^{\varepsilon_{\omega\psi^{-1}}}} = \eta_\psi^{\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2)}$$

and

$$\rho_{a-1}^{\varepsilon_{\omega\psi\chi^{-1}}} = \frac{(1-\zeta_p^{2(a-1)/N})^{\varepsilon_{\omega\psi\chi^{-1}}}(1-\zeta_{Np})^{\varepsilon_{\omega\psi\chi^{-1}}}}{(1-\zeta_p^{(a-1)/N})^{\varepsilon_{\omega\psi\chi^{-1}}}(1-\zeta_{Np}^2)^{\varepsilon_{\omega\psi\chi^{-1}}}} = \eta_{\psi^{-1}\chi}^{1-\omega\psi\chi^{-1}(2)}.$$

We have

$$\begin{aligned} 0 &= \langle \eta_\psi^{\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2)}, \eta_{\psi^{-1}\chi}^{1-\omega\psi\chi^{-1}(2)} \rangle_\chi \\ &= \sum_{\substack{\psi \text{ odd} \\ \psi\chi^{-1}|_{(\mathbb{Z}/N\mathbb{Z})^\times}\neq 1}} (\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2))(1-\omega\psi\chi^{-1}(2))e_{\psi,\chi} \end{aligned}$$

for every a even, $1 < a < Np$ with $N \nmid a$ and $N \mid a-1$.

4. In the case $N \nmid a-1$ and $N \mid a$, $\psi^{-1}\chi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$ and $\psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1$, we have

$$\begin{aligned} \rho_a^{\varepsilon_{\omega\psi^{-1}}} &= \frac{(1-\zeta_p^{\frac{a}{N}})^{\varepsilon_{\omega\psi^{-1}}}(1-\zeta_{Np})^{\varepsilon_{\omega\psi^{-1}}}}{(1-\zeta_{Np}^2)^{\varepsilon_{\omega\psi^{-1}}}} \\ &= \eta'_\psi{}^{\omega\psi^{-1}(\frac{a}{N})+(\frac{1}{N-1})(1-\omega^{-1}\psi(N))(1-\omega\psi^{-1}(2))} \end{aligned}$$

and

$$\begin{aligned} \rho_{a-1}^{\varepsilon_{\omega\psi\chi^{-1}}} &= \frac{(1-\zeta_{Np}^{(2a-2)})^{\varepsilon_{\omega\psi\chi^{-1}}}(1-\zeta_{Np})^{\varepsilon_{\omega\psi\chi^{-1}}}}{(1-\zeta_{Np}^{(a-1)})^{\varepsilon_{\omega\psi\chi^{-1}}}(1-\zeta_{Np}^2)^{\varepsilon_{\omega\psi\chi^{-1}}}} \\ &= \eta_{\psi^{-1}\chi}^{\omega\psi\chi^{-1}(2a-2)+1-\omega\psi\chi^{-1}(a-1)-\omega\psi\chi^{-1}(2)}. \end{aligned}$$

We have

$$0 = \langle \eta_\psi^{\omega\psi^{-1}(\frac{a}{N})+(\frac{1}{N-1})(1-\omega^{-1}\psi(N))(1-\omega\psi^{-1}(2))}, \eta_{\psi^{-1}\chi}^{(1-\omega\psi\chi^{-1}(2))(1-\omega\psi\chi^{-1}(a-1))} \rangle_\chi$$

$$= \sum_{\substack{\psi \text{ odd} \\ \psi|_{(\mathbb{Z}/N\mathbb{Z})^\times}=1}} (\omega\psi^{-1}(\frac{a}{N})+(\frac{1-\omega^{-1}\psi(N)}{N-1})(1-\omega\psi^{-1}(2))(1-\omega\psi\chi^{-1}(2))(1-\omega\psi\chi^{-1}(a-1))e_{\psi,\chi}$$

for every a even, $1 < a < Np$ with $N \nmid a-1$ and $N \mid a$.

5. In the case $N \nmid a-1$ and $N \mid a$, $\psi|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$ and $\psi^{-1}\chi|_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1$ we have

$$\rho_a^{\varepsilon_{\omega\psi^{-1}}} = \frac{(1-\zeta_p^{\frac{a}{N}})^{\varepsilon_{\omega\psi^{-1}}}(1-\zeta_{Np})^{\varepsilon_{\omega\psi^{-1}}}}{(1-\zeta_{Np}^2)^{\varepsilon_{\omega\psi^{-1}}}} = \eta_\psi^{1-\omega\psi^{-1}(2)}$$

and

$$\begin{aligned}\rho_{a-1}^{\varepsilon_{\omega\psi\chi^{-1}}} &= \frac{(1-\zeta_{Np}^{(2a-2)})^{\varepsilon_{\omega\psi\chi^{-1}}}(1-\zeta_{Np})^{\varepsilon_{\omega\psi\chi^{-1}}}}{(1-\zeta_{Np}^{(a-1)})^{\varepsilon_{\omega\psi\chi^{-1}}}(1-\zeta_{Np}^2)^{\varepsilon_{\omega\psi\chi^{-1}}}} \\ &= \eta_{\psi^{-1}\chi}^{\omega\psi\chi^{-1}(2a-2)+1-\omega\psi\chi^{-1}(a-1)-\omega\psi\chi^{-1}(2)} \\ &= \eta_{\psi^{-1}\chi}^{\prime\,(\frac{1-\omega^{-1}\psi^{-1}\chi(N)}{N-1})(1-\omega\psi\chi^{-1}(2))(1-\omega\psi\chi^{-1}(a-1))}.\end{aligned}$$

We have

$$0 = \langle \eta_\psi^{1-\omega\psi^{-1}(2)}, \eta_{\psi^{-1}\chi}^{\prime\,(\frac{1-\omega^{-1}\psi^{-1}\chi(N)}{N-1})(1-\omega\psi\chi^{-1}(2))(1-\omega\psi\chi^{-1}(a-1))} \rangle_\chi$$

$$= \sum_{\substack{\psi \text{ odd} \\ \psi\chi^{-1}|_{(\mathbb{Z}/N\mathbb{Z})^\times}=1}} (1-\omega\psi^{-1}(2))(\frac{1-\omega^{-1}\psi^{-1}\chi(N)}{N-1})(1-\omega\psi\chi^{-1}(2))(1-\omega\psi\chi^{-1}(a-1))e_{\psi,\chi}$$

for every a even, $1 < a < Np$ with $N \nmid a-1$ and $N \mid a$.

6. In the case $N \nmid a-1$ and $N \mid a$ and $\psi^{-1}\chi|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$ and $\psi|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$ we have

$$\rho_a^{\varepsilon_{\omega\psi^{-1}}} = \frac{(1-\zeta_p^{\frac{a}{N}})^{\varepsilon_{\omega\psi^{-1}}}(1-\zeta_{Np})^{\varepsilon_{\omega\psi^{-1}}}}{(1-\zeta_{Np}^2)^{\varepsilon_{\omega\psi^{-1}}}} = \eta_\psi^{1-\omega\psi^{-1}(2)}$$

and

$$\rho_{a-1}^{\varepsilon_{\omega\psi\chi^{-1}}} = \frac{(1-\zeta_{Np}^{2a-2})^{\varepsilon_{\omega\psi\chi^{-1}}}(1-\zeta_{Np})^{\varepsilon_{\omega\psi\chi^{-1}}}}{(1-\zeta_{Np}^{a-1})^{\varepsilon_{\omega\psi\chi^{-1}}}(1-\zeta_{Np}^{2})^{\varepsilon_{\omega\psi\chi^{-1}}}} = \eta_{\psi^{-1}\chi}^{(1-\omega\psi\chi^{-1}(2))(1-\omega\psi\chi^{-1}(a-1))}.$$

We have

$$0 = \langle \eta_{\psi}^{1-\omega\psi^{-1}(2)}, \eta_{\psi^{-1}\chi}^{(1-\omega\psi\chi^{-1}(2))(1-\omega\psi\chi^{-1}(a-1))} \rangle_{\chi}$$

$$= \sum_{\substack{\psi \text{ odd} \\ \psi\chi^{-1}|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1}} (1-\omega\psi^{-1}(2))(1-\omega\psi\chi^{-1}(2))(1-\omega\psi\chi^{-1}(a-1))e_{\psi,\chi}$$

for every a even, $1 < a < Np$ with $N \nmid a-1$ and $N \mid a$.

7. In the case $N \nmid a-1$ and $N \nmid a$, $\psi^{-1}\chi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$ and $\psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1$ we have

$$\begin{aligned} \rho_{a}^{\varepsilon_{\omega\psi^{-1}}} &= \frac{(1-\zeta_{Np}^{a})^{\varepsilon_{\omega\psi^{-1}}}(1-\zeta_{Np})^{\varepsilon_{\omega\psi^{-1}}}}{(1-\zeta_{Np}^{2})^{\varepsilon_{\omega\psi^{-1}}}} \\ &= \eta_{\psi}^{\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2)} \\ &= \eta'^{\,(\frac{1-\omega^{-1}\psi(N)}{N-1})(\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2))}_{\psi} \end{aligned}$$

and

$$\begin{aligned} \rho_{a-1}^{\varepsilon_{\omega\psi\chi^{-1}}} &= \frac{(1-\zeta_{Np}^{2a-2})^{\varepsilon_{\omega\psi\chi^{-1}}}(1-\zeta_{Np})^{\varepsilon_{\omega\psi\chi^{-1}}}}{(1-\zeta_{Np}^{a-1})^{\varepsilon_{\omega\psi\chi^{-1}}}(1-\zeta_{Np}^{2})^{\varepsilon_{\omega\psi\chi^{-1}}}} \\ &= \eta_{\psi^{-1}\chi}^{(1-\omega\psi\chi^{-1}(2))(1-\omega\psi\chi^{-1}(a-1))}. \end{aligned}$$

We have

$$0 = \langle \eta'^{\,(\frac{1-\omega^{-1}\psi(N)}{N-1})(\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2))}_{\psi}, \eta_{\psi^{-1}\chi}^{(1-\omega\psi\chi^{-1}(2))(1-\omega\psi\chi^{-1}(a-1))} \rangle_{\chi}$$

$$= \sum_{\substack{\psi \text{ odd} \\ \psi|_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1}} (\frac{1-\omega^{-1}\psi(N)}{N-1})(\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2))(1-\omega\psi\chi^{-1}(2))(1-\omega\psi\chi^{-1}(a-1))e_{\psi,\chi}$$

for every a even, $1 < a < Np$ with $N \nmid a-1$ and $N \nmid a$.

8. In the case $N \nmid a-1$ and $N \nmid a$, $\psi\mid_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$ and $\psi^{-1}\chi\mid_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1$ we have

$$\rho_a^{\varepsilon_{\omega\psi^{-1}}} = \frac{(1-\zeta_{Np}^a)^{\varepsilon_{\omega\psi^{-1}}}(1-\zeta_{Np})^{\varepsilon_{\omega\psi^{-1}}}}{(1-\zeta_{Np}^2)^{\varepsilon_{\omega\psi^{-1}}}} = \eta_\psi^{\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2)}$$

and

$$\begin{aligned}\rho_{a-1}^{\varepsilon_{\omega\psi\chi^{-1}}} &= \frac{(1-\zeta_{Np}^{2a-2})^{\varepsilon_{\omega\psi\chi^{-1}}}(1-\zeta_{Np})^{\varepsilon_{\omega\psi\chi^{-1}}}}{(1-\zeta_{Np}^{a-1})^{\varepsilon_{\omega\psi\chi^{-1}}}(1-\zeta_{Np}^2)^{\varepsilon_{\omega\psi\chi^{-1}}}} \\ &= \eta_{\psi^{-1}\chi}^{(1-\omega\psi\chi^{-1}(2))(1-\omega\psi\chi^{-1}(a-1))} \\ &= \eta_{\psi^{-1}\chi}^{\prime\,(\frac{1-\omega^{-1}\psi^{-1}\chi(N)}{N-1})(1-\omega\psi\chi^{-1}(2))(1-\omega\psi\chi^{-1}(a-1))}.\end{aligned}$$

We have

$$0 = \langle \eta_\psi^{\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2)}, \eta_{\psi^{-1}\chi}^{\prime\,(\frac{1-\omega^{-1}\psi^{-1}\chi(N)}{N-1})(1-\omega\psi\chi^{-1}(2))(1-\omega\psi\chi^{-1}(a-1))} \rangle_\chi$$

$$= \sum_{\substack{\psi \text{ odd} \\ \psi\mid_{(\mathbb{Z}/N\mathbb{Z})^\times}\neq 1}} (\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2))(\frac{1-\omega^{-1}\psi^{-1}\chi(N)}{N-1})(1-\omega\psi\chi^{-1}(2))(1-\omega\psi\chi^{-1}(a-1))e_{\psi,\chi}$$

for every a even, $1 < a < Np$ with $N \nmid a-1$ and $N \nmid a$.

9. In the case $N \nmid a-1$ and $N \nmid a$ and $\psi^{-1}\chi\mid_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$ and $\psi\mid_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$ we have

$$\rho_a^{\varepsilon_{\omega\psi^{-1}}} = \frac{(1-\zeta_{Np}^a)^{\varepsilon_{\omega\psi^{-1}}}(1-\zeta_{Np})^{\varepsilon_{\omega\psi^{-1}}}}{(1-\zeta_{Np}^2)^{\varepsilon_{\omega\psi^{-1}}}} = \eta_\psi^{\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2)}$$

and

$$\begin{aligned}\rho_{a-1}^{\varepsilon_{\omega\psi\chi^{-1}}} &= \frac{(1-\zeta_{Np}^{2a-2})^{\varepsilon_{\omega\psi\chi^{-1}}}(1-\zeta_{Np})^{\varepsilon_{\omega\psi\chi^{-1}}}}{(1-\zeta_{Np}^{a-1})^{\varepsilon_{\omega\psi\chi^{-1}}}(1-\zeta_{Np}^2)^{\varepsilon_{\omega\psi\chi^{-1}}}} \\ &= \eta_{\psi^{-1}\chi}^{(1-\omega\psi\chi^{-1}(2))(1-\omega\psi\chi^{-1}(a-1))}.\end{aligned}$$

We have

$$0 = \langle \eta_\psi^{\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2)}, \eta_{\psi^{-1}\chi}^{(1-\omega\psi\chi^{-1}(2))(1-\omega\psi\chi^{-1}(a-1))} \rangle_\chi$$

$$= \sum_{\substack{\psi \text{ odd} \\ \psi\chi^{-1}|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1}} (\omega\psi^{-1}(a) + 1 - \omega\psi^{-1}(2))(1 - \omega\psi\chi^{-1}(2))(1 - \omega\psi\chi^{-1}(a-1))e_{\psi,\chi}$$

for every a even, $1 < a < Np$ with $N \nmid a - 1$ and $N \nmid a$.

In addition to these nine relations, we also have the following property which follows from the antisymmetry of the cup product.

Proposition 2.61. *We have that*

$$\langle \alpha_\psi, \alpha_{\psi^{-1}\chi} \rangle_\chi = -\langle \alpha_{\psi^{-1}\chi}, \alpha_\psi \rangle_\chi.$$

This implies

i. If $\psi = \psi^{-1}\chi$, then $e_\psi = 0$.

ii. If $\psi \neq \psi^{-1}\chi$, then $e_\psi + e_{\psi^{-1}\chi} = 0$.

We now state the results of our computations. Refer to the table of Appendix B to see all values tested.

Theorem 2.62. *For all triples N, p, χ as above with $N = 3, p < 822$ and $5 \leq N \leq 1000$ and $5 \leq p \leq \lceil \frac{1000}{N} \rceil$ except for one value of χ in the cases $N = 3, p = 683$; $N = 5, p = 17$; $N = 7, p = 73$; $N = 7, p = 97$; $N = 7, p = 103$; $N = 11, p = 31$; $N = 13, p = 61$; $N = 23, p = 199$ and two values of χ in the case of $N = 23, p = 89$, the dimension of the nullspace of coefficients of relations computed in cases 1 through 9 of this section together with those of Proposition 2.61 is equal to one. That is, the $e_{\psi,\chi}$ with ψ odd determine a unique possibility for the pairing values up to a single possibly zero scalar in $\mathbb{Z}/p\mathbb{Z}$.*

Proof. We wrote a routine in Magma which directly computes the nullspace of the matrix containing all the relations in each of the cases above. More precisely, we first compute four matrices. We have that M_1 is the matrix of the key relations $1, 2$ and 3 in the case $N \mid a-1$. Then M_2 is computed as the matrix of the key relations $4, 5$ and 6 in the case $N \mid a$, and M_3 is the matrix of the key relations $7, 8$ and 9 in the case $N \nmid a$ and $N \nmid a-1$. Finally, we compute the matrix M_4 of antisymmetry relations. Then we compute the nullspace of the first matrix. Next, we compute the nullspace of M_2 on the nullspace determined by M_1. Similarly, we compute the nullspace of M_3 and M_4 on the nullspaces determined by M_2 and M_1, respectively. Finally, we end up with a nullspace which takes into account all the necessary relations. □

Example 2.63. *For example, one matrix is*

$$M_3 = (c_{\psi,\chi}(a))_{a,\chi}$$

corresponding to relations numbered 7,8 and 9, where $2 \leq a \leq Np-1$, *for* a *even, where* $N \nmid a, a-1$, *where* ψ *odd with* $\psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1$ *and where, for any* ψ, a, *we have that* $c_{\psi,\chi}(a)$ *is equal to*

$$\begin{cases} (\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2))(1-\omega\psi\chi^{-1}(2))(1-\omega\psi\chi^{-1}(a-1)), & \text{if } \psi\chi^{-1}\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} \neq 1 \\ (\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2))(\frac{1-\omega^{-1}\psi^{-1}\chi(N)}{N-1})(1-\omega\psi\chi^{-1}(2))(1-\omega\psi\chi^{-1}(a-1)), & \text{if } \psi\chi^{-1}\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1 \\ (\frac{1-\omega^{-1}\psi(N)}{N-1})(\omega\psi^{-1}(a)+1-\omega\psi^{-1}(2))(1-\omega\psi\chi^{-1}(2))(1-\omega\psi\chi^{-1}(a-1)), & \text{if } \psi\,|_{(\mathbb{Z}/N\mathbb{Z})^\times} = 1. \end{cases}$$

3 Connections Between the Eisenstein Ideal and the Pairing

3.1 The Key Theorem

Let $N \geq 3$ and $p \geq 5$ be odd prime numbers which are relatively prime to each other and with the property that $\varphi(N) \mid \varphi(p)$. Let χ be a nontrivial even Dirichlet character modulo Np. Suppose that $\chi\,|_{(\mathbb{Z}/p\mathbb{Z})^\times} \neq \omega\,|_{(\mathbb{Z}/p\mathbb{Z})^\times}$.

We will provide in the following theorem the essential key to understanding the objects of our study.

Lemma 3.1. *Let p and χ be as above. Then $B_{1,\chi\omega^{-1}} \equiv \frac{B_{n,\chi\omega^{-n}}}{n} \bmod p$. In particular, $p \mid B_{1,\chi\omega^{-1}}$ if and only if $p \mid B_{2,\chi\omega^{-2}}$.*

Proof. See [W], Chapter 5. In particular, this follows from Theorem 5.11 and Corollary 5.13, as in Corollary 5.15. □

Remark 3.2. *For the computations regarding the Eisenstein ideal, we assumed that $p \mid B_{2,\chi\omega^{-2}}$ in order that $\mathbf{I} \neq h$. For our study of the pairing we assumed that $p \mid B_{1,\chi\omega^{-1}}$ so that $A_K^{(\omega\chi^{-1})} \neq 0$. Then Lemma 3.1 ensures us that these hypotheses are actually the same.*

Theorem 3.3. *Suppose that $\chi\,|_{(\mathbb{Z}/p\mathbb{Z})^\times} \neq \omega\,|_{(\mathbb{Z}/p\mathbb{Z})^\times}, \chi^2\,|_{(\mathbb{Z}/p\mathbb{Z})^\times} \neq \omega^2\,|_{(\mathbb{Z}/p\mathbb{Z})^\times}$, $p \mid B_{1,\chi\omega^{-1}}$ and $p \nmid B_{1,\omega\chi^{-1}}$ The pairing with p is surjective (i.e., $\langle p, \rangle_\chi$ is*

surjective) if and only if the Hecke operator $U_p - 1$ generates the Eisenstein ideal $\mathbf{I}$.

Proof. See [S2], Theorem 5.6. □

When we know that $U_p - 1$ generates $\mathbf{I}$ and we know $\langle\ ,\ \rangle_\chi$ up to a scalar, then Theorem 3.3 tells us that the pairing and hence the scalar must be nonzero. That is, in these cases we know the whole pairing up to a nonzero scalar.

3.2 Final Comments

We have proved that it is not always the case that the Eisenstein ideal is generated by $U_p - 1$, and thus that the pairing with p is not always surjective. We also found many examples where we were able to understand the pairing completely to within a single scalar multiple, and many examples of cases in which the element $U_p - 1$ does generate $\mathbf{I}$. We continue running the Magma routines in search of more such interesting examples.

We fix some notation. For any N and p, we define the character ψ as the unique Dirichlet character on $(\mathbb{Z}/Np\mathbb{Z})^\times \cong (\mathbb{Z}/N\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times$ factoring through $(\mathbb{Z}/N\mathbb{Z})^\times$ and taking the smallest positive primitive root modulo N to the $(\frac{p-1}{N-1})^{th}$ power of the smallest positive primitive root modulo p.

We note that there are also several cases in which the nullspace of the matrix of relations we computed was larger than 1-dimensional. For instance, for the case $N = 7$, $p = 73$ and $\chi = \psi^3\omega^{11}$ we have a 13-dimensional nullspace. In the case $N = 23$, $p = 89$, $\chi = \psi^{10}\omega^{30}$, we have a nullspace of dimension 45. These are just two concrete examples, but there are many more. This

does not in itself prove or disprove anything, as it is possible to impose more linear relations, such as those found in [S1] arising from K-theory, which may lead us to discover that in these cases there is a unique nontrivial possibility for the pairing after all.

There were some cases in which the hypothesis that $p \nmid B_{1,\omega\chi^{-1}}$ on Bernoulli numbers fails, and in these cases Theorem 3.3 no longer applies. For example, this occured for the triples $(N, p, \chi) = (23, 67, \psi\omega^{49}), (23, 89, \psi^{12}\omega^{60})$ and $(31, 61, \psi^4\omega^{22})$, just to name a few. Moreover, because the Eisenstein ideal program has the additional restriction that $p^2 \nmid B_{2,\chi\omega^{-2}}$ but the pairing program does not require this, there were some cases where we actually computed the nullspace of the relations but not whether $U_p - 1$ generates $\mathbf{I}$.

There were also some cases in which the hypothesis on Dirichlet characters that $\chi^2 \mid_{(\mathbb{Z}/p\mathbb{Z})^\times} \neq \omega^2 \mid_{(\mathbb{Z}/p\mathbb{Z})^\times}$ fails, and in these cases Theorem 3.3 no longer applies. For example, this occured for the triples $(N, p, \chi) = (11, 31, \psi^8\omega^{16}), (13, 73, \psi^5\omega^{37}), (19, 37, \psi^5\omega^{19})$ and $(23, 67, \psi^{12}\omega^{34})$. Note that in these cases it is true that $\chi \mid_{(\mathbb{Z}/p\mathbb{Z})^\times} \neq \omega \mid_{(\mathbb{Z}/p\mathbb{Z})^\times}$.

Moreover, we found four examples in which the nullspace has dimension one, but the computed basis vector of this nullspace shows that the pairing with p is not surjective. The four triples found are as follows: $(N, p, \chi) = (3, 331, \psi\omega^{149}), (23, 67, \psi^{14}\omega^{44}), (23, 89, \psi^{10}\omega^{54})$ and $(31, 61, \psi^8\omega^{36})$. We are currently running the other program to verify whether in these cases $U_p - 1$ generates $\mathbf{I}$ but have only produced results in the case $(3, 331, \psi\omega^{149})$.

It is also of interest to notice that in each of the cases $N = 3, p = 257, \chi = \psi\omega^{21}$ and $N = 19, p = 37, \chi = \psi\omega^{101}$ we know that $p^2 \mid B_{1,\chi\omega^{-1}}$ and that $U_p - 1$ generates $\mathbf{I}$. This leads to the following result.

Proposition 3.4. *If χ satisfies the hypotheses of Theorem 3.3, $p^2 \mid B_{1,\chi\omega^{-1}}$ and $U_p - 1$ generates $\boldsymbol{I}$ then $A_K^{(\omega\psi^{-1})} \cong \mathbb{Z}/p^2\mathbb{Z}$.*

Proof. By the results of [S2], we have that the p-rank of $A_K^{(\omega\psi^{-1})}$, that is, $\dim_{\mathbb{F}_p} A^{(\omega\psi^{-1})}/p$ is equal to the p-rank of $\mathbf{I}/\mathbf{I}^2$. Because of the hypothesis that $U_p - 1$ generates $\mathbf{I}/\mathbf{I}^2$, the p-ranks are forced to be one, which in turn forces $A_K^{(\omega\psi^{-1})} \cong \mathbb{Z}/p^2\mathbb{Z}$. □

Ultimately our goal has been to obtain some understand of the pairing arising from the cup product, the Eisenstein ideal, and the structure of the eigenspaces, all three of which are related. This thesis has explained how we went about studying these objects, what we have found, and what still remains mysterious.

4 Appendix A: Computations

4.1 The program for computing whether $U_p - 1$ generates the Eisenstein ideal

```
function conv(V,phi,A)
seq := ElementToSequence(A); //converts matrix to a sequence
seq := [phi(seq[i]) : i in [1..#seq] ]; /*applies the map phi
to each element in the sequence.*/
return V!seq;
end function;

function alggens(V,L,phi) /*used to find vector space basis
of Hecke algebra.*/
nums := [1];
M := sub< V | conv(V,phi,L[1]) >;
for i in [j : j in [2..#L]] do
v := conv(V,phi,L[i]);
if not v in M then
Append(~nums,i);
```

```
M := M + sub<V|v>;
end if;
end for;
return M,nums;
end function;

function idealeq(V,L,I,phi,Up1) /* used to compute I^2
+ (U_p-1) & compare w/ I */
M := sub< V | conv(V,phi,Up1) >;
//M := sub< V | 0>;
for i in [1..#L] do
for j in [i..#L] do
v := conv(V,phi,L[i]*L[j]);  //product of two Hecke operators
if not v in M then
M := M + sub<V|v>;   //create M = I^2 + (U_p-1)
end if;
if M eq I then
return true,M;
break;
end if;
end for;
end for;
return false,M;
end function;
```

```
function rootofunity(p,prec)  //a primitive root mod p^prec
g := PrimitiveRoot(p);
for i in [2..prec] do
g := (IntegerRing(p^i)!g)^p;
end for;
return Integers()!g;
end function;

function Uptest(N, p, char : prec := 2, val := 1);
K := CyclotomicField(p-1);
G<a, b> := DirichletGroup(N*p,K);
M := ModularSymbols(char,2,1);
DisownChildren(M);
C := CuspidalSubspace(M);
n := ((N*p)/6)*(&*[1+1/q : q in [x : x in [2..N*p] |
IsDivisibleBy(N*p,x) and IsPrime(x)]]); /*number of
Hecke operators needed to generate C */
ls := [l : l in [1..Ceiling(n)]];
L := [HeckeOperator(C,l) : l in ls]; /*create the matrices
representing Hecke operators */
d := Dimension(C);
R := IntegerRing(p^prec);
g := R!rootofunity(p,prec);
phi := hom<K->R|g>;
V := RModule(R,d^2);
```

```
T,nums := alggens(V,L,phi); /* find gens. of Hecke algebra
as module over Z_p */
T2 := sub<V | [ p^val*T.i : i in [1..Rank(T)]] >;
while Rank(T2) lt d do
printf "error dim T = %o, dim C = %o, dim pT = %o\n",
Rank(T), d, Rank(T2); /* these lines check what mod p^?
is good enough */
prec +:= 1;
R := IntegerRing(p^prec);
g := R!rootofunity(p,prec);
phi := hom<K->R | g>;
V := RModule(R,d^2);
T,nums := alggens(V,L,phi);
T2 := sub<V | [p^val*T.i : i in [1..Rank(T)]] >;
end while;
L1 := [ L[n]-&+[m^(k-1)*Evaluate(char,m): m in Divisors(n)]
: n in nums | n ne 1] cat [p*L[1]]; /* generators of I over
zp */
  I := sub< V | [conv(V,phi,i) : i in L1] >;  /* find
Eisenstein ideal */
if T eq I then printf "T = I\n";
end if;   // test if working so far here
Up1 := HeckeOperator(C,p)-1;
ans, I2 := idealeq(V,L1,I,phi,Up1); /* test if I^2 +
(U_p-1) = I */
```

```
return ans;
end function;

function Bern(N,p);    //finds allowable characters
K := CyclotomicField(p-1);
G<a, b> := DirichletGroup(N*p,K);
R := IntegerRing(p^2);
g := PrimitiveRoot(p);
g := (IntegerRing(p^2)!g)^p;
phi := hom<K->R|g>;
chars := [];  /* creates list of all even Dirichlet
characters modulo Np with conductor N or Np */
for i in [1..Order(a)] do
for j in [1..Order(b)] do
w:= a^i*b^j;
if w(-1) eq 1 and IsDivisibleBy(Conductor(w), N) then
Append(~chars,w);
end if;
end for;
end for;
L := #chars;
C :=[];
i := 1;
while i le L do
w := chars[i];
```

```
B:= &+[w(k)*((k^2)/(N*p)-k+(N*p)/6) : k in [0..((N*p)-1)]];
/* The Bernoulli  number B_2,char for each even character
of conductor N or Np */
b:=phi(B);
if GF(p)!b eq GF(p)!0 and not b eq R!0 then
Append(~C,w); //tests the Bernoulli divisibility condition
end if;
i := i+1;
end while;
return C;
end function;

function BTest()
for N in [y : y in [3..1000] | IsPrime(y)] do
for p in [x : x in [5..Ceiling(5000/N)] | IsPrime(x) and
Gcd(x,N) eq 1] do
S := [];
if IsDivisibleBy(EulerPhi(p),EulerPhi(N)) then /* check
divisibility */
C := Bern(N , p); //the list of all the allowable characters
if #C ge 1 then
T:=[* *];
Append(~T,N);
Append(~T,p);
for i in [1..#C] do
```

```
bool := Uptest(N,p,C[i]); //test whether U_p-1 generates I
Append(~T,C[i]);
Append(~T,bool);
end for;
Append(S,T);
print S;
end if;
end if;
end for;
end for;
return [];
end function;
```

4.2 The program for computing the dimension of the nullspace of relations of the pairing

```
function psi(a,b,m,n,N)
/* this will return a sequence T consisting of all odd
Dirichlet characters. Recall that b is the Teichmuller
character, a is  the "real" other generator of the
Dirichlet group and chi is a^n*b^m.*/
assert b(-1) eq -1;
assert a(-1) eq -1;
T:=[];
T1:=[]; /* trivial on psi (so nontrivial on psi chi^-1) */
T2:=[]; /* trivial on psi chi^-1 (so nontrivial on psi) */
```

```
/* The complement T-T1-T2 will constitute the other case:
psi chi^-1 nontrivial (and psi nontrivial). */
for i in [0..Order(a)-1] do
for j in [0..Order(b)-1] do
if IsOdd(i+j) then
Append(~T,a^i*b^j);
if i mod (N-1) eq 0 then
Append(~T1,a^i*b^j);
else if n-i mod (N-1) eq 0 then
Append(~T2,a^i*b^j);
end if;
end if;
end if;
end for;
end for;
return T,T1,T2;
end function;

function rel1(c,d,a,N,H); /* N divides a-1, a < *Np even,
use zeta_N*p. The restriction of psi to z/Nz* is trivial. */
return (1/(N-1))*(1-((H!c)^(-1))(N))*(c(a)+1-c(2))*(1-d(2));
end function;

function rel2(c,d,a,N,H); /* N divides a-1, a < *Np even,
use zeta_N*p. The restriction of psi*chi^-1 to z/Nz*
```

```
is trivial. */
return (c(a)+1-c(2))*((H!d)((2*a-2) div N) - (H!d)((a-1)
div N) + (1/(N-1))*(1-((H!d)^(-1))(N))*(1-d(2)));
end function;

function rel3(c,d,a); /* N divides a-1, a < *Np even,
use zeta_N*p. The restriction of psi*chi^-1 to z/Nz*
is non-trivial. */
return (c(a)+1-c(2))*(1-d(2));
end function;

function rel4(c,d,a,N,H); /* N divides a, a < *Np
even, use zeta_N*p.The restriction of psi to
z/Nz* is trivial. */
return ((H!c)( a div N) + (1/(N-1))*(1-((H!c)^(-1))(N))
*(1-c(2)))*(d(2*a-2)+1-d(a-1)-d(2));
end function;

function rel5(c,d,a,N,H); /* N divides a, a < *Np
even, use zeta_N*p. The restriction of psi*chi^-1
to z/Nz* is trivial.  */
return (1-c(2))*(1/(N-1))*(1-((H!d)^(-1))(N))*
(d(2*a-2)+1-d(a-1)-d(2));
end function;
```

```
function rel6(c,d,a); /* N divides a, a < *Np even,
use zeta_N*p. The restriction of psi*chi^-1 to z/Nz*
is non-trivial. */
return (1-c(2))*(d(2*a-2)+1-d(a-1)-d(2));
end function;

function rel7(c,d,a,N,H) /* N does not divide a
or a-1, a < *Np even, use zeta_N*p. The
restriction of psi to z/Nz* is trivial. */
return (1/(N-1))*(1-((H!c)^(-1))(N))*(c(a)+1-c(2))
*(d(2*a-2)+1-d(a-1)-d(2));
end function;

function rel8(c,d,a,N,H); /* N does not divide a
or a-1, a < *Np even, use zeta_N*p. The restriction
of psi*chi^-1 to z/Nz* is trivial. */
return (c(a)+1-c(2))*(1/(N-1))*(1-((H!d)^(-1))(N))
*(d(2*a-2)+1-d(a-1)-d(2));
end function;

function rel9(c,d,a); /* N does not divide a or a-1,
a < *Np even, use zeta_N*p. The restriction of
psi*chi^-1 to z/Nz* is non-trivial. */
return (c(a)+1-c(2))*(d(2*a-2)+1-d(a-1)-d(2));
end function;
```

```
function reltab1(R,T,T1,T2,w,chi,S1,f,N,H)
/*a matrix of 3 key relations in the case N divides a-1 */
nr := #T;
nc:=#S1;
M1:=RMatrixSpace(R,nr,nc)!0;
for i in [1..nr] do
for j in [1..nc] do
if (T[i] in T1) then /* restriction of psi trivial */
M1[i,j] := f(rel1(w*((T[i])^(-1)),
(w*(T[i])*((chi)^(-1))),S1[j],N,H));
else if (T[i] in T2) then /* restriction of
psi*chi^-1 trivial */
M1[i,j] := f(rel2(w*((T[i])^(-1)),
(w*(T[i])*((chi)^(-1))),S1[j],N,H));
else /* restriction of psi*chi^-1 non-trivial */
M1[i,j] := f(rel3(w*((T[i])^(-1)),
w*(T[i])*((chi)^(-1)),S1[j]));
end if;
end if;
end for;
end for;
return M1;
end function;
```

```
function reltab2(R,T,T1,T2,w,chi,S2,f,N,H) /* a matrix of 3
key relations in the case N divides a */
nr := #T;
nc:=#S2;
M2:=RMatrixSpace(R,nr,nc)!0;
for i in [1..nr] do
for j in [1..nc] do
if (T[i] in T1) then /* restriction of psi trivial */
M2[i,j] := f(rel4(w*((T[i])^(-1)),w*(T[i])*((chi)^(-1)),
S2[j],N,H));
else if (T[i] in T2) then /* restriction of psi*chi^-1
trivial */
M2[i,j] := f(rel5(w*((T[i])^(-1)),(w*(T[i])*((chi)^(-1))),
S2[j],N,H));
else /* restriction of psi*chi^-1 non-trivial */
M2[i,j] := f(rel6(w*((T[i])^(-1)),w*(T[i])*((chi)^(-1)),
S2[j]));
end if;
end if;
end for;
end for;
return M2;
end function;

function reltab3(R,T,T1,T2,w,chi,S3,f,N,H) /* a matrix of
```

```
3 key relations  in the case where N divides neither a
nor a-1 */
nr := #T;
nc:=#S3;
M3:=RMatrixSpace(R,nr,nc)!0;
for i in [1..nr] do
for j in [1..nc] do
if (T[i] in T1) then /* restriction of psi trivial */
M3[i,j] := f(rel7(w*((T[i])^(-1)),w*(T[i])*((chi)^(-1)),
S3[j],N,H));
else if (T[i] in T2) then /* restriction of psi*chi^-1
trivial */
M3[i,j] := f(rel8(w*((T[i])^(-1)),(w*(T[i])*((chi)^(-1))),
S3[j],N,H));
else /*restriction of psi*chi^-1 non-trivial */
M3[i,j] := f(rel9(w*((T[i])^(-1)),w*(T[i])*((chi)^(-1)),
 S3[j]));
end if;
end if;
end for;
end for;
return M3;
end function;

function antientry(i,j,T,chi,p)
```

```
if (j eq i) or (T[i] eq (T[j]^(-1))*(chi)) then
return 1;
else
return 0;
end if;
end function;

function antitab(T,chi,p) /* the matrix of antisymmetry
relations. */
R:=GF(p);
nr := #T;
nc := nr;
M := RMatrixSpace(R,nr,nc)!0;
for i in [1..nc] do
for j in [1..nr] do
M[j,i] := antientry(i,j,T,chi,p);
end for;
end for;
return M;
end function;

function null(N,p,n,m,a,b,chi,f,H); /* finds the null space
with all the relations */
assert IsDivisibleBy(p-1,N-1);
R:=GF(p);
```

```
T, T1, T2 := psi(a,b,m,n,N);
nr := #T;
S1:=[x : x in [2..N*p by 2] | x mod N ne 0 and x mod N eq
1 and x mod p ne 0 and x mod p ne 1];
S2:=[x : x in [2..N*p by 2] | x mod N eq 0 and x mod N
ne 1 and x mod p ne 0 and x mod p ne 1];
S3:=[x : x in [2..N*p by 2] | x mod N ne 0 and x mod N
ne 1 and x mod p ne 0 and x mod p ne 1];
nc1:=#S1;
nc2:=#S2;
nc3:=#S3;
V := RSpace(R,nr);
W := sub<V|V>;
W := NullSpace(Hom(W,RSpace(R,nc1))!reltab1(R,T,T1,T2,b,
chi,S1,f,N,H));
W := NullSpace(Hom(W,RSpace(R,nc2))!reltab2(R,T,T1,T2,b,
chi,S2,f,N,H));
W := NullSpace(Hom(W,RSpace(R,nc3))!reltab3(R,T,T1,T2,b,
chi,S3,f,N,H));
W := NullSpace(Hom(W,RSpace(R,nr))!antitab(T,chi,p));
return W;
end function;

function setup(N,p)
F:=CyclotomicField(p-1);
```

```
y:=PrimitiveElement(GF(p));
G:=DirichletGroup(N*p,F);
a:=G!DirichletGroup(N,F).1;
b:=G!DirichletGroup(p,F).1;
f:=hom<F->GF(p) | y>;
x:=CRT([Integers()!y,1],[p,N]);
assert f(b(x)) eq GF(p)!y; //tests that b is the Teichmuller
w:=PrimitiveRoot(N);
z:=f(Evaluate(a,w));
assert #[u : u in [2..w-1] | IsPrimitive(u,N)] eq 0; /* w
is the smallest
primitive root mod N */
assert #[v : v in [2..Integers()!(y-1)] | IsPrimitive(v,p)]
eq 0; /* y is the smallest primitive root mod p */
assert f(a(w)) eq f(b(x))^((p-1) div (N-1)); /* a is what
we think it is */
return a,b,y,f;
end function;

function berndiv(N,p,char,b,f,y)
char1:=char*b^-1;
F:=Conductor(char1);
Bern:=&+[(char1)(k)*(k/F) : k in [1..(F-1)]]; /* This is
the Bernoulli number B_{1, chi omega^-1} */
bern:=f(Bern);
```

```
if bern eq 0 then
if f(&+[(char1^(-1))(k)*(k/F) : k in [1..(F-1)]]) eq 0
then printf "p | B_{1, omega^{-1}*chi}!";
end if;
phi:=hom<CyclotomicField(p-1) -> IntegerRing(p^2) |
(IntegerRing(p^2)!(Integers()!y))^p>;
if IntegerRing(p^2)!phi(Bern) eq 0 then
printf "p^2 | B_{1, chi*omega^{-1}}!";
end if;
char2:=char*b^-2;
Bern2:=&+[(char2)(k)*((k^2)/(N*p)-k+(N*p)/6) : k in
[0..(N*p-1)]];
assert f(Bern2) eq 0; /*tests that p divides
B_{2,chi*omega^-2} as it should */
if IntegerRing(p^2)!phi(Bern2) eq 0 then
printf "p^2 | B_{2, chi*omega^(-2)}!";
end if;
return true;
else return false;
end if;
end function;

procedure run()
for N in [y : y in [3] | IsPrime(y)] do
for p in [x : x in [547..661] | (IsPrime(x) and x
```

```
gt N and IsDivisibleBy(x-1,N-1)) and Gcd(x,N) eq 1] do
assert IsPrime(N);
assert IsPrime(p) and IsDivisibleBy(p-1,N-1) and Gcd(p,N)
eq 1;
a,b,y,f := setup(N,p);
for n in [1..N-2] do
for m in [0..p-2] do
chi:=a^n*b^m;
if IsDivisibleBy(Conductor(chi),N) and IsEven(chi)
and Conductor(chi) ne 1 then
if berndiv(N,p,chi,b,f,y) then
W := null(N,p,n,m,a,b,chi,hom<CyclotomicField(p-1) ->
IntegerRing(p)|
CRT([PrimitiveRoot(p),1],[p,N])>,
DirichletGroup(p,CyclotomicField(p-1)));
printf "N = %o, p = %o, chi = %o, dim = %o,\n%o\n", N, p,
chi, Dimension(W), Basis(W);
end if;
end if;
end for;
end for;
end for;
end for;
end procedure;
```

5 Appendix B: Table of Program Output

We must fix some notation before presenting the table of computed values. For any N and p, where as before $\Delta^* = \mathrm{Hom}(\mathrm{Gal}(\mathbb{Q}(\mu_{Np})/\mathbb{Q}), \mathbb{Z}_p^\times)$, let b be the Teichmüller character, and let a be the unique Dirichlet character on $(\mathbb{Z}/Np\mathbb{Z})^\times \cong (\mathbb{Z}/N\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times$ factoring through $(\mathbb{Z}/N\mathbb{Z})^\times$ and taking the smallest positive primitive root modulo N to the $(\frac{p-1}{N-1})^{th}$ power of the smallest positive primitive root modulo p. Then a and b generate Δ^*.

Table 1: Output from the programs

N	p	χ	Nullity	$U_p - 1$	$p^2 \mid B_{1,\chi\omega^{-1}}$	$p \mid B_{1,\omega\chi^{-1}}$	$p^2 \mid B_{2,\chi\omega^{-2}}$
3	23	ab^{17}	1	true	false	false	false
3	47	ab^{13}	1	true	false	false	false
3	53	ab^{29}	1	true	false	false	false
3	53	ab^{45}	1	true	false	false	false
3	67	ab^{47}	1	true	false	false	false
3	103	ab^{93}	1	true	false	false	false

Continued on the Next Page

Table 1 – Continued

N	p	χ	Nullity	$U_p - 1$	$p^2 \mid B_{1,\chi\omega^{-1}}$	$p \mid B_{1,\omega\chi^{-1}}$	$p^2 \mid B_{2,\chi\omega^{-2}}$
3	113	ab^{55}	1		false	false	**true**
3	139	ab^{99}	1	true	false	false	false
3	197	ab^{179}	1	true	false	false	false
3	197	ab^{183}	1	true	false	false	false
3	199	ab^{161}	1	true	false	false	false
3	241	ab^{21}	1	true	false	false	false
3	257	ab^{101}	1	true	**true**	false	false
3	263	ab^{81}	1	true	false	false	false
3	271	ab^{89}	1	true	false	false	false
3	281	ab^{131}	1	true	false	false	false
3	281	ab^{261}	1	true	false	false	false
3	317	ab^{101}	1	true	false	**true**	false
3	317	ab^{217}	1	true	false	**true**	false
3	317	ab^{265}	1	true	false	false	false
3	331	ab^{149}	1	**false**	false	false	false
3	337	ab^{201}	1	true	false	false	false
3	337	ab^{207}	1	true	false	false	false
3	347	ab^{295}	1	true	false	false	false
3	353	ab^{291}	1		false	false	false
3	401	ab^{17}	1		false	false	false
3	409	ab^{61}	1		false	false	false

Continued on the Next Page

Table 1 – Continued

N	p	χ	Nullity	$U_p - 1$	$p^2 \mid B_{1,\chi\omega^{-1}}$	$p \mid B_{1,\omega\chi^{-1}}$	$p^2 \mid B_{2,\chi\omega^{-2}}$
3	419	ab^{15}	1		false	false	false
3	421	ab^{73}	1		false	false	false
3	457	ab^{95}	1		false	false	false
3	467	ab^{271}	1		false	false	false
3	491	ab^{403}	1		false	false	false
3	521	ab^{263}	1		false	false	false
3	547	ab^{303}	1		false	false	false
3	577	ab^{473}	1		false	false	false
3	577	ab^{527}	1		false	false	false
3	601	ab^{103}	1		false	false	false
3	673	ab^{363}	1		false	false	false
3	677	ab^{331}	1		false	false	false
3	683	ab^{651}	32		false	false	false
3	691	ab^{641}	1		false	false	false
3	809	ab^{9}	1		false	false	false
3	811	ab^{529}	1		false	false	false
3	811	ab^{731}	1		false	false	false
3	821	ab^{721}	1		false	false	false
5	17	a^2b^{14}	3	true	false	false	false
5	37	ab^{31}	1	true	false	false	false
5	41	a^2b^{18}	1	true	false	false	false

Continued on the Next Page

Table 1 – Continued

N	p	χ	Nullity	$U_p - 1$	$p^2 \mid B_{1,\chi\omega^{-1}}$	$p \mid B_{1,\omega\chi^{-1}}$	$p^2 \mid B_{2,\chi\omega^{-2}}$
5	53	ab^{47}	1	true	false	false	false
5	61	ab^{27}	1	true	false	false	false
5	61	a^2b^{42}	1	true	false	false	false
5	61	a^3b^{51}	1		false	false	**true**
5	73	ab^{47}	1	true	false	false	false
5	73	a^2b^{70}	1	true	false	false	false
5	73	a^3b^{45}	1	true	false	false	false
5	73	a^3b^{49}	1	true	false	false	false
5	89	a^3b^{37}	1	true	false	false	false
5	97	a^3b^{69}	1	true	false	false	false
5	101	ab^{9}	1	true	false	false	false
5	137	ab^{25}	1	true	false	false	false
5	137	a^2b^{84}	1	true	false	false	false
5	149	ab^{119}	1	true	false	false	false
5	149	a^2b^{22}	1	true	false	false	false
5	149	a^3b^{61}	1	true	false	false	false
5	157	ab^{113}	1	true	false	false	false
5	181	a^3b^{43}	1	true	false	false	false
5	181	a^3b^{77}	1	true	false	false	false
5	193	ab^{185}	1	true	false	false	false
5	193	a^3b^{27}	1	true	false	false	false

Continued on the Next Page

Table 1 – Continued

N	p	χ	Nullity	$U_p - 1$	$p^2 \mid B_{1,\chi\omega^{-1}}$	$p \mid B_{1,\omega\chi^{-1}}$	$p^2 \mid B_{2,\chi\omega^{-2}}$
5	197	ab^{29}	1	true	false	false	false
5	197	a^3b^{15}	1	true	false	false	false
7	13	a^5b^5	1	true	false	false	false
7	19	ab^{11}	1	true	false	false	false
7	43	a^5b^7	1	true	false	false	false
7	43	a^5b^9	1	true	false	false	false
7	61	a^2	1	true	false	false	false
7	61	a^2b^{42}	1	true	false	false	false
7	61	a^5b^{17}	1	true	false	false	false
7	67	a^5b^{13}	1	true	false	false	false
7	73	a^3b^7	1	true	false	false	false
7	73	a^3b^{11}	13	true	false	false	false
7	79	a^2b^4	1	true	false	false	false
7	79	a^5b^{73}	1	true	false	false	false
7	97	ab^7	1	true	false	false	false
7	97	a^4b^{18}	4	true	false	false	false
7	97	a^4b^{92}	1	true	false	false	false
7	103	ab^{15}	1	true	false	false	false
7	103	ab^{35}	1	true	false	false	false
7	103	ab^{53}	2	true	false	false	false
7	103	ab^{93}	1	true	false	false	false

Continued on the Next Page

Table 1 – Continued

N	p	χ	Nullity	$U_p - 1$	$p^2 \mid B_{1,\chi\omega^{-1}}$	$p \mid B_{1,\omega\chi^{-1}}$	$p^2 \mid B_{2,\chi\omega^{-2}}$
7	103	a^2b^{34}	1	true	false	false	false
7	103	a^2b^{100}	1	true	false	false	false
7	109	ab^9	1	true	false	false	false
7	109	a^3b^{105}	1	true	false	false	false
7	109	a^4b^{36}	1	true	false	false	false
7	109	a^5b^{21}	1	true	false	false	false
7	109	a^5b^{57}	1	true	false	false	false
7	127	ab^5	1	true	false	false	false
7	127	ab^{11}	1	true	false	false	false
7	127	ab^{17}	1	true	false	false	false
7	127	a^5b^{91}	1	true	false	false	false
7	139	ab^{13}	1	true	false	false	false
7	139	ab^{123}	1	true	false	false	false
7	139	a^3b^{21}	1	true	false	false	false
7	139	a^5b^{61}	1	true	false	false	false
11	31	a^6b^{14}	1	true	false	false	false
11	31	a^8b^{16}	8	true	false	false	false
11	31	a^8b^{22}	1	true	false	false	false
11	41	a^2b^{30}	1	true	false	false	false
11	41	a^3b^{35}	1	true	false	false	false
11	41	a^9b^5	1	true	false	false	false

Continued on the Next Page

Table 1 – Continued

N	p	χ	Nullity	$U_p - 1$	$p^2 \mid B_{1,\chi\omega^{-1}}$	$p \mid B_{1,\omega\chi^{-1}}$	$p^2 \mid B_{2,\chi\omega^{-2}}$
11	61	ab^{57}	1	true	false	false	false
11	61	a^3b^{39}	1	true	false	false	false
11	61	a^6b^{36}	1	true	false	false	false
11	71	a^2b^{42}	1	true	false	false	false
11	71	a^4b^{14}	1	true	false	false	false
11	71	a^5b^7	1	true	false	false	false
11	71	a^6b^4	1	true	false	false	false
11	71	a^6b^{24}	1	true	false	false	false
11	71	a^7b^{35}	1	true	false	false	false
13	37	a^3b^3	1	true	false	false	false
13	37	a^6b^{34}	1	true	false	false	false
13	37	a^7b^{29}	1	true	false	false	false
13	37	a^8b^{34}	1	true	false	false	false
13	37	$a^{10}b^{24}$	1	true	false	false	false
13	37	$a^{11}b^{31}$	1	true	false	false	false
13	61	ab^{33}	1	true	false	false	false
13	61	a^2b^{46}	1	true	false	false	false
13	61	a^2b^{52}	6	true	false	false	false
13	61	a^6b^{48}	1	true	false	false	false
13	61	a^9b^{13}	1	true	false	false	false
13	61	$a^{10}b^{38}$	1	true	false	false	false

Continued on the Next Page

Table 1 – Continued

N	p	χ	Nullity	$U_p - 1$	$p^2 \mid B_{1,\chi\omega^{-1}}$	$p \mid B_{1,\omega\chi^{-1}}$	$p^2 \mid B_{2,\chi\omega^{-2}}$
13	61	$a^{11}b^3$	1	true	false	false	false
13	73	ab^{63}	1	true	false	false	false
13	73	a^2b^{38}	1	true	false	false	false
13	73	a^2b^{48}	1	true	false	false	false
13	73	a^3b^7	1	true	false	false	false
13	73	a^5b^{37}	1	true	false	false	false
13	73	a^8b^6	1	true	false	false	false
13	73	a^9b^{31}	1	true	false	false	false
13	73	$a^{11}b^{49}$	1	true	false	false	false
19	37	a^5b^{19}	1	true	false	false	false
19	37	a^5b^{27}	1	true	false	false	false
19	37	a^6b^8	1	true	false	false	false
19	37	a^8b^{28}	1	true	false	false	false
19	37	a^9b^{17}	1	true	false	false	false
19	37	$a^{10}b^{12}$	1	true	false	false	false
19	37	$a^{10}b^{32}$	1	true	false	false	false
19	37	$a^{11}b^{21}$	1	true	**true**	false	false
19	37	$a^{11}b^{27}$	1	true	false	false	false
19	37	$a^{14}b^{22}$	1	true	false	false	false
19	37	$a^{16}b^{18}$	1	true	false	false	false
19	37	$a^{17}b^7$	1		false	false	**true**

Continued on the Next Page

Table 1 – Continued

N	p	χ	Nullity	$U_p - 1$	$p^2 \mid B_{1,\chi\omega^{-1}}$	$p \mid B_{1,\omega\chi^{-1}}$	$p^2 \mid B_{2,\chi\omega^{-2}}$
23	67	ab^{49}	1		false	**true**	false
23	67	a^2b^{50}	1		false	false	false
23	67	a^7b^{11}	1		false	false	false
23	67	a^8b^{50}	1		false	false	false
23	67	a^9b^{41}	1		false	false	false
23	67	$a^{11}b^{39}$	1		false	false	false
23	67	$a^{12}b^{34}$	1		false	false	false
23	67	$a^{12}b^{54}$	1		false	false	false
23	67	$a^{13}b^{37}$	1		false	false	false
23	67	$a^{14}b^{36}$	1		false	false	false
23	67	$a^{14}b^{44}$	1		false	false	false
23	67	$a^{14}b^{56}$	1		false	false	false
23	67	$a^{17}b^{55}$	1		false	false	false
23	67	$a^{18}b^{46}$	1		false	false	false
23	67	$a^{19}b^{33}$	1		false	false	false
23	67	$a^{21}b^{19}$	1		false	**true**	false
23	89	a^2b^{40}	1		false	false	false
23	89	a^3b^{15}	1		false	false	false
23	89	a^4b^8	1		false	false	false
23	89	a^5b^{59}	1		false	false	false
23	89	a^6b^{66}	1		false	false	false

Continued on the Next Page

Table 1 – Continued

N	p	χ	Nullity	$U_p - 1$	$p^2 \mid B_{1,\chi\omega^{-1}}$	$p \mid B_{1,\omega\chi^{-1}}$	$p^2 \mid B_{2,\chi\omega^{-2}}$
23	89	a^6b^{74}	1		false	false	false
23	89	$a^{10}b^{30}$	45		false	**true**	false
23	89	$a^{10}b^{54}$	1		false	false	false
23	89	$a^{12}b^{30}$	1		false	false	false
23	89	$a^{12}b^{60}$	1		false	**true**	false
23	89	$a^{12}b^{64}$	1		false	false	false
23	89	$a^{16}b^{8}$	1		false	false	false
23	89	$a^{18}b^{46}$	1		false	false	false
23	89	$a^{18}b^{64}$	1		false	false	false
23	89	$a^{19}b^{9}$	47		false	false	false
23	89	$a^{19}b^{43}$	1		false	false	false
23	89	$a^{20}b^{28}$	1		false	false	false
23	89	$a^{20}b^{68}$	1		false	false	false
23	199	$a^{3}b^{65}$	101		false	false	false
23	199	$a^{4}b^{144}$	1		false	false	false
23	199	$a^{5}b^{107}$	1		false	false	false
23	199	$a^{13}b^{163}$	1		false	false	false
23	199	$a^{16}b^{168}$	1		false	false	false
23	199	$a^{19}b^{179}$	1		false	false	false
31	61	$a^{4}b^{22}$	1		false	**true**	false
31	61	$a^{6}b^{16}$	1		false	false	false

Continued on the Next Page

Table 1 – Continued

N	p	χ	Nullity	$U_p - 1$	$p^2 \mid B_{1,\chi\omega^{-1}}$	$p \mid B_{1,\omega\chi^{-1}}$	$p^2 \mid B_{2,\chi\omega^{-2}}$
31	61	a^5b^{55}	1		false	false	false
31	61	a^6b^{16}	1		false	false	false
31	61	a^8b^{10}	1		false	false	false
31	61	a^8b^{12}	1		false	false	false
31	61	a^8b^{36}	1		false	false	false
31	61	a^9b^{27}	1		false	false	false
31	61	$a^{10}b^{16}$	1		false	false	**true**
31	61	$a^{11}b^{11}$	1		false	false	false
31	61	$a^{11}b^{15}$	1		false	false	false
31	61	$a^{11}b^{59}$	1		false	false	false
31	61	$a^{12}b^{52}$	1		false	false	false
31	61	$a^{15}b^{27}$	1		false	false	false
31	61	$a^{16}b^{34}$	1		false	false	false
31	61	$a^{17}b^{17}$	1		false	false	false
31	61	$a^{18}b^{8}$	1		false	false	false
31	61	$a^{20}b^{10}$	1		false	false	false
31	61	$a^{22}b^{54}$	1		false	false	false
31	61	$a^{26}b^{40}$	1		false	**true**	false
31	61	$a^{27}b^{53}$	1		false	false	false
31	61	$a^{28}b^{24}$	1		false	false	false

References

[AS] Agashe, Amod and Stein, William, Appedix to Lario, J.-C. and Schoof, R., Some Computations with Hecke Rings and Deformation Rings, *Experiment. Math.* **11** no. 2, 2002, 310-311.

[C] Cremona, John, Algorithms for Modular Elliptic Curves, Cambridge University Press, 1997.

[DS] Diamond, Fred and Shurman, Jerry, A., First Course in Modular Forms, Graduate Texts in Mathematics **228**, Springer, 2005.

[K] Kurihara, Masato, Ideal Class Groups of Cyclotomic fields and Modular Forms of Level 1, *J. Number Theory* **45** (1993), 281-294.

[McS] McCallum, William and Sharifi, Romyar, A Cup Product in the Galois Cohomology of Number Fields, *Duke Math. J.* **120** (2003), 270-284.

[M] Merel, Loic, Universal Fourier Expansions of Modular Forms, On Artin's Conjecture for Odd 2-Dimensional Representations, Lecture Notes in Math. **1585**, Springer, 1994, 59-94.

[R] Rubin, Karl, Euler Systems, Annals of Mathematical Studies **127**, Princeton University Press, 2000.

[S1] Sharifi, Romyar, Computations on Milnor K_2 of Integer Rings, slides from a talk given at Schloss Dagstuhl, 2004.

[S2] Sharifi, Romyar, Iwasawa Theory and the Eisenstein Ideal, to appear in *Duke Math. J.*

[St] Stein, William, Explicitly Computing Modular Forms, online at: `http://modular.washington.edu/msri06/refs/stein-book-on-modular-forms.pdf`.

[W] Washington, Lawrence C., Introduction to Cyclotomic Fields, Springer, 1997.