Jochnowitz Congruences at Residual Primes

by

Brandon M. Carter

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
2018

Doctoral Committee:

Professor Kartik Prasanna, Chair
Professor Kenneth Cadigan
Assistant Professor Wei Ho
Associate Professor Andrew Snowden

Brandon M. Carter

carterbr@umich.edu

ORCID iD: 0000-0002-8848-4729

ACKNOWLEDGEMENTS

I would like to thank my advisor Kartik Prasanna. His advice and support over the past several years were invaluable, and I am certainly a better researcher from having learned under his guidance. I am also grateful to the other members of my committee for their comments and suggestions that improved the quality of this thesis.

I am grateful to the NSF and the Department of Mathematics for their financial support over the years. The work leading to this thesis was partially supported by NSF RTG grant 0943832.

The math department at Michigan was a wonderful place to spend my graduate years. It is impossible to overstate the impact that the faculty, staff, and graduate students here had on my personal and professional development. I especially want to thank Karen Smith for her friendship and advice, especially in my most trying moments. I also want to thank the office staff, including Carrie Berger, Stephanie Carroll, Brenae Smith, Beste Erel Windes, and the irreplaceable Tara McQueen, for all of their help. To my fellow graduate students and friends, I am thankful for all of the times (and in some cases, living situations) we have shared. I am particularly grateful to Jeremy Hoskins, Audra McMillan, Michael Newman, and Derek Wood for their constant friendship through the ups and downs of graduate school. Finally, I would like to thank the students that I had the opportunity to teach at Michigan. I found teaching as an enjoyment rather than an obligation, and that was only because they made the experience as easy and pleasant as possible.

I would also like to thank all those that supported and furthered my mathematical curiosity over the years. In particular, I would like to thank Abby Brown, who convinced me to major in mathematics so many years ago, and Mirela Çiperiani, who patiently entertained my many questions and guided my interests in modern number theory.

I am grateful to my family for their constant positivity and support, and for always picking up the phone when I called, regardless of how infrequent it might have been. Lastly, I would like to thank Emily Bostelmann for her companionship and support. She put up with my countless frustrations, celebrated the triumphs, and kept me grounded over the years. This thesis would never have been completed without her unwavering confidence in me.

TABLE OF CONTENTS

CHAPTER

ABSTRACT

We investigate relationships between the algebraic parts of L-values of weight two eigenforms f and g satisfying a congruence modulo a prime p, but whose signs in the functional equation are -1 and $+1$, respectively. By fixing an imaginary quadratic field satisfying certain hypotheses, we use the formula of Gross-Zagier and an explicit Waldspurger-type formula of Gross to give a certain congruence between Heegner points on GL_2-type abelian varieties and toric periods on definite quaternion algebras. Such a relation may be viewed as a congruence between the algebraic parts of $L'(f/K,1)$ and $L(g/K,1)$, and are known as Jochnowitz congruences. This generalizes earlier work of Bertolini-Darmon and Vatsal to all level raising congruences for which such a sign change occurs.

CHAPTER I

Introduction

1.1 Congruence phenomena

The theory of special values of L-functions suggests that certain values of analytically defined functions should be related to algebraic invariants of geometric Galois representations. Let $\mathrm{G}_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ denote the absolute Galois group of $\mathbf{Q}$. Let $\rho : \mathrm{G}_{\mathbf{Q}} \to \mathrm{GL}_n(\overline{\mathbf{Q}_p})$ be an irreducible p-adic Galois representation coming from the étale cohomology of a smooth projective variety $X/\mathbf{Q}$ with good reduction at p. Let I_ℓ denote the inertia group at a prime ℓ and Frob_ℓ a geometric Frobenius element. Then the L-function of ρ, defined by

$$L(\rho, s) = \prod_{\ell \text{ prime}} (\det(1 - \mathrm{Frob}_\ell \ell^{-s}) \left|_{V^{I_\ell}}\right.)^{-1},$$

converges in some right half plane. Then, adding in certain explicit factors, the Langlands philosophy suggests that the completed L-function $\Lambda(\rho, s)$ should satisfy a functional equation (and thus analytic continuation) of the form

$$\Lambda(\rho, s) = \varepsilon(\rho)\Lambda(\rho^*, k - s)$$

for some integer k, where ρ^* denotes the dual representation, $\varepsilon(\rho) = \pm 1$ is the global root number of ρ.

When ρ is self-dual, for example occurring in the middle-dimensional cohomology of a Shimura variety X, one expects the central value (or more generally, the leading Taylor coefficient at the central point) to encode arithmetic information about algebraic cycles on X.

Fixing a $\mathrm{G}_{\mathbf{Q}}$-stable lattice in V, one can define the mod p representation

$$\overline{\rho} : \mathrm{G}_{\mathbf{Q}} \to \mathrm{GL}(\overline{\mathbf{F}_p}),$$

well-defined up to semisimplification. Suppose now that we have two such self-dual representations ρ, ρ' such that their mod p representations are equivalent. We say that ρ and ρ' are congruent modulo p if such an equivalence holds. In this case, the Euler factors of their L-functions also satisfy a congruence modulo p for almost all primes ℓ. It is then reasonable to expect that the critical values of their L-functions are congruent as well, possibly up to some explicit factors. Morally, one should be able to normalize the values by a transcendental period Ω such that the ***algebraic part***, defined as

$$L^{alg}(\rho, k/2) = \frac{L(\rho, k/2)}{\Omega},$$

of their central critical values satisfy a congruence mod p. Such congruences were suggested by Koblitz for classical modular forms in [22].

When the signs of the functional equations for ρ and ρ' are both equal to $+1$, then this construction suggests the existence of p-adic L-functions interpolating L-values in certain families of representations. When the signs are both -1, one might instead expect congruences between the derivatives of the L-functions. There has been some progress in that direction by Howard [16, 17] on Gross-Zagier type theorems in Hida families. When the signs of the functional equation differ the central L-value of the one with sign -1 vanishes, while we expect the central L-value of the one with sign

+1 to be typically nonzero. In this case, one might predict that the algebraic part of the central L-value with sign +1 should satisfy a congruence with the algebraic part of the central derivative of the one with sign -1. We refer to such congruences as ***Jochnowitz congruences***, as Jochnowitz [20] first predicted such phenomena in general for classical modular forms.

1.2 The 2-dimensional case

Suppose that $\rho = \rho_f$ is the 2-dimensional p-adic representation associated to a weight 2 newform on $\Gamma_0(N)$. For simplicity of exposition, suppose that f has rational Fourier coefficients. Then associated to f is an elliptic curve $E = E_f$ defined over $\mathbf{Q}$ and the rational p-adic Tate module $V = T_p(E) \otimes \mathbf{Q}$ is the geometric realization of ρ. The Birch and Swinnerton-Dyer (BSD) conjecture predicts that

$$\mathrm{ord}_{s=1} L(f, s) = \mathrm{rk}_{\mathbf{Z}}\, E(\mathbf{Q}).$$

1.2.1 The Gross-Zagier formula

Suppose now that the imaginary quadratic field $K = \mathbf{Q}(\sqrt{-D})$ isatisfies the ***Heegner hypothesis*** for N, so all primes dividing N split in K. Then the L-function of base change of ρ to K, denoted by $L(f/K, s)$, satisfies a functional equation of the form

$$L(f/K, s) \doteq \varepsilon(f/K) L(f/K, 2-s),$$

where the dot above the equal sign means up to explicit positive constant.

The sign of the functional equation $\varepsilon(f/K) = \pm 1$ decomposes as a product of local signs

$$\varepsilon(f/K) = \prod_{\nu} \varepsilon_{\nu}(f/K)$$

indexed by the places of K. Explicitly, $\varepsilon_\infty(f/K) = -1$ and $\varepsilon_\nu(f/K) = +1$ for finite ν prime to N. The local sign at a split prime agrees with its conjugate, so the Heegner hypothesis forces the global sign to be -1.

The sign forces the central value $L(f/K, 1)$ to vanish, and so the BSD conjecture predicts that there should be a point of infinite order in $E(K)$. On the other hand, the Heegner hypothesis also implies that there is an ideal $\mathfrak{N}$ of $\mathcal{O}_K$ such that

$$\mathcal{O}_K/\mathfrak{N} \cong \mathbf{Z}/N\mathbf{Z}.$$

Then

$$\frac{\mathbf{C}}{\mathcal{O}_K} \to \frac{\mathbf{C}}{\mathfrak{N}^{-1}\mathcal{O}_K} \tag{1.1}$$

defines a cyclic isogeny of degree N between elliptic curves with complex multiplication by $\mathcal{O}_K$, hence defines a point P on the modular curve $X_0(N)$ parametrizing such isogenies of generalized elliptic curves. The theory of complex multiplication implies that (1.1) is actually defined over the Hilbert class field, H, of K. Then the trace

$$P_K = \sum_{\sigma \in \mathrm{Gal}(H/K)} P^\sigma \in Div(X_0(N))(K)$$

gives a K-rational point on E under the modular parametrization

$$X_0(N) \to E.$$

One might hope that the constructed point, called the ***Heegner point*** associated to K, is such a non-torsion point.

Theorem I.1. (Gross-Zagier)

Let $\langle\, ,\, \rangle_{NT}$ denote the Néron-Tate height pairing on E. Then

$$L'(f/K, 1) \doteq \langle P_K, P_K \rangle_{NT}.$$

The Néron-Tate height pairing is non-degenerate on $E(K) \otimes \mathbf{Q}$, and as a consequence we see that

$$L'(f/K,1) = 0 \quad \Leftrightarrow \quad P_K \text{ is torsion in } E(K).$$

1.2.2 Jochnowitz congruences in $\mathcal{S}_2(\Gamma_0(N))$

On the other hand, suppose that f is congruent to another Hecke eigenform g of weight 2 whose global sign is $+1$. Then, as above, one expects the central L-value $L(g/K,1)$ to be typically nonzero. In this case, as explained above, one should expect to be able to define an algebraic part of $L(g/K,1)$ whose reduction mod p should satisfy a Jochnowitz congruence encoding "mod p" information about the image of the Heegner point P_K on E.

An Eisenstein congruence

Mazur [25] gave the first systematic construction of such congruences for modular forms. For a weight 2 newform f of prime level N and a prime p dividing the numerator of $\frac{N-1}{12}$, earlier work of Mazur [24] implies that f satisfies a congruence with the weight 2 Eisenstein series g of level N. Let χ be the odd quadratic character corresponding to an imaginary quadratic field K of discriminant $-D$ prime to N. Then the central value of the Rankin L-function $L(g,\chi,1)$ divided by an appropriate period is essentially the square of the class number h_K by a result of Waldspurger [42].

When N is inert in K, Mazur uses modular symbols to define the algebraic part of $L(f,\chi,1)$ which satisfies a congruence with h_K. As a consequence, Mazur proves finiteness of the K-rational points on certain p-Eisenstein quotients of $J_0(N)$ and their corresponding Tate-Shafarevich groups.

When N splits in K, the sign of the functional equation for $L(f/K,1)$ is -1. In particular, this forces

$$L(f/K,1) = L(f,1)L(f,\chi,1) = 0.$$

In this case, Mazur instead relates the p-divisibility of h_K to the p-divisibility of the Heegner point on the p-Eisenstein quotient of $J_0(N)$ associated to f.

In fact, Mazur's work was one of the motivations for Jochnowitz to predict the existence of such congruences in general.

The irreducible case

Let $K = \mathbf{Q}(\sqrt{-D})$ be the imaginary quadratic field of discriminant $-D$. Suppose that N satisfies the Heegner hypothesis relative to K, so all primes dividing N split in K. Let $q \nmid ND$ be a prime which is inert in K.

Let $E/\mathbf{Q}$ be an elliptic curve and let

$$f = e^{2\pi i z} + \sum_{n\geq 2} a_n(f)e^{2\pi i n z} \in \mathcal{S}_2(\Gamma_0(N))$$

be the normalized weight 2 newform associated to f by the work of Wiles [43], Taylor-Wiles [38], and Breuil-Conrad-Diamond-Taylor [6].

Let $p \geq 5$ be a prime for which the mod p representation

$$\overline{\rho_{f,p}} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}(E[p]) \cong \mathrm{GL}_2(\mathbf{F}_p)$$

is irreducible.

Suppose that f satisfies a congruence modulo p with a normalized Hecke eigenform

$$g = e^{2\pi i z} + \sum_{n\geq 2} a_n(g)e^{2\pi i n z} \in \mathcal{S}_2(\Gamma_0(Nq))^{q\text{-new}}$$

arising by raising the level of f in the sense of Ribet [28]. Let $F_g = \mathbf{Q}(a_n(g))$ be the number field generated by the Hecke eigenvalues of g. Then for some prime $\mathfrak{P}$ of F_g

lying over p, we have

$$a_\ell(f) \equiv a_\ell(g) \pmod{\mathfrak{P}}, \qquad \text{for all primes } \ell \nmid Nq.$$

Then the local signs for g/K behave similarly to those of f/K except at q, where $\varepsilon_q(g/K) = -1$. In particular, the global root number is $+1$. This is the simplest such setting in which one can expect a Jochnowitz-type congruence to hold.

A special value formula of Gross [10] gives the central value of $L(g/K, 1)$ in terms of a toric period on the definite quaternion algebra B ramified at q and ∞. Let $\mathrm{Cl}(B)$ denote the set of conjugacy classes of oriented Eichler orders of level N in B. Since B is definite, the Jacquet-Langlands correspondence gives rise to a form

$$\psi : \mathrm{Cl}(B) \to \mathbf{C}$$

with the same Hecke eigenvalues as g. One can define the analogue of a Heegner point

$$x_K \in \mathbf{Z}[\mathrm{Cl}(B)]$$

on B, that we refer to as a definite Heegner point.

Theorem I.2. (Gross special value formula)
Extend ψ linearly to $\mathbf{Z}[\mathrm{Cl}(B)]$. Then, up to an appropriate normalization of ψ, one has

$$L(g/K, 1) \doteq (\psi(x_K))^2 \in F_g.$$

When looking at the two special value formulae, one might then expect a relationship between the p-divisibility of the Heegner point P_K in $E(K)$ and the $\mathfrak{P}$-divisibility of $\psi(x_K)$. Instead, since the definite Heegner points depend on the local behavior of B at q, our theorem relates the local p-divisibility of P_K in $E(K_q)$ to that of $\psi(x_K)$.

The main result of this thesis is the following:

Theorem I.3.

Let $P_K \in E(K)$ denote the Heegner point associated to K. Let q be a level-raising prime for f modulo p. If there exists a level-raised form g at q for which $\psi(x_K)$ is a $\mathfrak{P}$-adic unit, then $P_K \notin pE(K_q)$.

Moreover, if either:

- $q \not\equiv 1 \pmod{p}$, *or*
- $q \equiv 1 \pmod{p}$ *and a Frobenius element* Frob_q *of* $\mathrm{G}_{\mathbf{Q}}$ *does not act by a scalar on* $E[p]$,

then the converse holds as well.

Remark I.4. The full strength of our theorem actually implies that one only needs to check the reduction of $\psi(x_K)$ modulo $\mathfrak{P}$ for a single level-raised eigenform. See Section 5.3 for details.

A slightly weaker version of Theorem I.3 was first proven when $q \equiv -1 \pmod{p}$ independently by Bertolini-Darmon [4] and Vatsal [39]. The methods of Bertolini-Darmon in their proof of the anticyclotomic Iwasawa main conjecture for elliptic curves [5] essentially give a proof in the case that $p \nmid q^2 - 1$, and was more explicitly discussed in Zhang's proof of Kolyvagin's conjecture [44]. A related result in the case $p \nmid q^2 - 1$ is discussed in the work of Gross-Parson [11], relating the indivisibility of P_K in $E(K_q)$ instead to the p-Selmer rank of the abelian variety associated to g. The primes q in the first two cases are called Kolyvagin and admissible, respectively. The final case $q \equiv 1 \pmod{p}$ has not been treated before, and so we refer to such primes as residual. The residual case introduces a new difficulty in the failure of a certain mod p multiplicity one theorem (see Prop. IV.4). Our methods closely follow the somewhat simpler argument of Vatsal [39].

Such congruences have been instrumental in studying the μ-invariants of anticyclotomic p-adic L-functions, as in Vatsal [39] and Pollack-Weston [26]. More recently, Jochnowitz congruences have been used in proving converses to the work of Gross-Zagier [12] and Kolyvagin [23], e.g., Zhang [44] and Skinner-Zhang [37], and in deducing the p-part of the BSD formula in the case of rank 1 from the work of Kato [21] and Skinner-Urban [36] in rank 0. See Zhang [44] and Berti-Bertolini-Venerucci [1] for such examples.

CHAPTER II

Modular forms on quaternion algebras

In this chapter we briefly recall the definition and classification of quaternion algebras and their role in the study of classical modular forms.

2.1 Quaternion algebras

Definition II.1. A ***quaternion algebra*** B over a field F is a four-dimensional central simple algebra over F. That is, the center $Z = Z(B)$ is equal to F and B has no nontrivial two-sided ideals.

Wedderburn's theorem implies that every central simple algebra over a field F is isomorphic to a matrix ring over a division algebra. In particular, by a dimension-counting argument we can conclude that any quaternion algebra B/F must be isomorphic to either the 2×2 matrix algebra $M_2(F)$ or a division algebra over F with center F.

Example II.2.

- Since there are no nontrivial division algebras over an algebraically closed field, the only quaternion algebra over $\mathbf{C}$ is $M_2(\mathbf{C})$.
- Over $\mathbf{R}$, as is well-known, the only two quaternion algebras are $M_2(\mathbf{R})$ and the Hamiltonian quaternion algebra $\mathbf{H} := \mathbf{R} \oplus \mathbf{R}i \oplus \mathbf{R}j \oplus \mathbf{R}k$ with the multiplication

determined by $ij = -ji = k$ and $i^2 = j^2 = -1$.

- Let F be a nonarchimedean local field with uniformizer π and residue field of order q. Then there are only 2 isomorphism classes of quaternion algebras: the ***split*** quaternion algebra $M_2(F)$ and the ***nonsplit*** quaternion algebra B given by $B = F(\zeta) \oplus F(\zeta)x$ with center F and multiplication determined by the identities $x^2 = \pi$ and $x\zeta = -\zeta x$, where ζ is a nontrivial trace zero element of the unique unramified quadratic extension of F.

For a quaternion algebra B over a number field F, we can consider the quaternion algebra $B \otimes F_\nu$ for each place ν of F. We say that B ***ramifies*** at ν if $B \otimes_F F_\nu$ is nonsplit (i.e., not isomorphic to $M_2(F_\nu)$) and ***split*** otherwise.

Class field theory implies that B ramifies at only finitely many places, and in fact the isomorphism class of B is completely determined by the set of ramified places. Moreover, B must be ramified at an even number of places. Define the ***discriminant*** $\Delta = \Delta_B$ to be the (formal) product of all places at which B ramifies, so Δ is a squarefree product of an even number of finite and/or real infinite places. Given such a product Δ there is a unique quaternion algebra B over F ramified at exactly those places. We will denote this quaternion algebra by $B(\Delta)$.

Define the ***absolute discriminant*** $D = D_B$ of B to be the product of all finite primes dividing Δ. For a quaternion algebra $B/\mathbf{Q}$, we say that B is ***definite*** if B is ramified at ∞ and is ***indefinite*** otherwise. In particular, B is definite or indefinite depending on whether D is divisible by an odd or even number of primes, respectively.

Nonsplit quaternion algebras may become split after passing to an extension of the base field. The following theorems allow us to recognize precisely when this happens in the case of a quadratic extension.

Theorem II.3. (Albert-Brauer-Hasse-Noether)

Let F be a number field and B a quaternion algebra over F. Suppose K is a quadratic extension of F. There is an embedding of K into F if and only if all primes ramified in B are inert or ramified in K.

Proposition II.4. *Let F, B, and K be as in the above theorem. K splits B, i.e., $B \otimes_F K \cong M_2(K)$, if and only if K embeds in B.*

2.1.1 Orders and class groups

Similar to the ring of integers inside of a number field, a quaternion algebra also admits certain integral structures.

Definition II.5. Let F be a number field or nonarchimedean local field. An ***order*** $\mathcal{O}$ of a quaternion algebra B/F is an $\mathcal{O}_F$-submodule of B such that $\mathcal{O}$ is a subring of B and $\mathcal{O} \otimes \mathbf{Q} = B$.

A ***maximal order*** is an order that is not properly contained in any other order. In general, there are many maximal orders for a given quaternion algebra.

For a simple example, the subring $M_2(\mathbf{Z})$ of the split quaternion algebra $M_2(\mathbf{Q})$ over $\mathbf{Q}$ is a maximal order. A key example that will be used later in this thesis is the following:

Example II.6. The endomorphism ring of a supersingular elliptic curve $E/\overline{\mathbf{F}}_p$ is a maximal order in a quaternion algebra over $\mathbf{Q}$. More specifically, $\mathrm{End}^0(E) := \mathrm{End}(E) \otimes \mathbf{Q}$ is the (unique) definite quaternion algebra ramified at p and ∞.

Definition II.7. An ***Eichler order*** of B is an intersection of any two maximal orders. The ***level*** of an Eichler order is its index in either of the maximal orders containing it.

Example II.8. In the split quaternion algebra $M_2(\mathbf{Q})$, the order

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}$$

is an Eichler order of level N. It is, in fact, the unique Eichler order of level N up to conjugation.

Definition II.9. For any order $\mathcal{O}$ of B, let I and J be two right fractional ideals of $\mathcal{O}$. We say that I and J are in the same ***right ideal class*** of $\mathcal{O}$ if there exists an element $\alpha \in B^\times$ with $\alpha I = J$. The set of right ideal classes of $\mathcal{O}$ is denoted by $\mathrm{Cl}(\mathcal{O})$.

Lemma II.10. [41, III.5]

The set of right ideal classes of $\mathcal{O}$ is naturally in bijection with

$$B^\times \backslash B^\times(\mathbf{A}_f)/\widehat{\mathcal{O}}^\times. \tag{2.1}$$

When B is definite and R is an Eichler order of level N with N prime to Δ, the set $\mathrm{Cl}(R)$ admits an alternate description.

Definition II.11. Let B, R, and N be as above. An ***orientation*** on R is a choice of surjective homomorphism

$$\phi : R \to \mathbf{Z}/N\mathbf{Z}.$$

The pair (R, ϕ) is referred to as an ***oriented Eichler order***.

Remark II.12. We note that an orientation on R can equivalently be described as a collection of local orientations

$$\phi_\ell : R \otimes \mathbf{Z}_\ell \to \mathbf{Z}/\ell^{v_\ell(N)}\mathbf{Z}, \quad \ell \mid N. \tag{2.2}$$

In this setting we may also describe $\mathrm{Cl}(R)$ in terms of the structure of oriented Eichler orders.

Lemma II.13. $\mathrm{Cl}(R)$ *is in natural bijection with the set of conjugacy classes of oriented Eichler orders of level* N*.*

Proof. The bijection is obtained via the map

$$\begin{aligned} B^\times(\mathbf{A}_f) &\to \{\text{conjugacy classes of oriented Eichler orders of level } N\} \\ b &\mapsto (b\widehat{R}^\times b^{-1} \cap B), \end{aligned}$$

noting that the orientation on R naturally induces an orientation on $b\widehat{R}^\times b^{-1} \cap B$ via the local orientations described above, cf. [2, Section 1]. □

As a consequence of the above lemma, the set $\mathrm{Cl}(R)$ does not depend on the choice of Eichler order R, but rather only on B and N. When the value of N is clear, we will take the convention of writing $\mathrm{Cl}(B)$ rather than $\mathrm{Cl}(R)$.

2.2 Modular forms on GL_2

We briefly recall the fundamentals of classical modular forms and modular curves. Readers already familiar with the theory should feel free to skip ahead to the next section. Due to the variety of comprehensive resources on the topic, e.g., [9], any proofs will be short and/or omitted.

Let $\mathcal{H}$ denote the upper half-plane, and let $\mathrm{SL}_2(\mathbf{Z})$ denote the group of 2×2 matrices with integer entries and determinant 1. We note that $\mathrm{SL}_2(\mathbf{Z})$ acts on $\mathcal{H}$ by fractional linear transformations.

Definition II.14. A subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbf{Z})$ is called a ***congruence subgroup*** if it contains $\Gamma(N)$ for some positive integer N, where

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod N \right\}.$$

The subgroup $\Gamma(N)$ is called the ***principal congruence subgroup of level*** N.

We will generally only concern ourselves with specific congruence subgroups. Consider the families of congruence subgroups

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod N \right\}$$

and

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N \right\}$$

Definition II.15. For any integer k and $\gamma \in \mathrm{SL}_2(\mathbf{Z})$, the ***weight k operator*** $[\gamma]_k$ acts on a complex valued function $f : \mathcal{H} \to \mathbf{C}$ via

$$f|[\gamma]_k = (cz+d)^{-k} f(\gamma z),$$

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

Throughout this thesis, we will be interested in certain functions on the upper half-plane that are invariant under this operator for a fixed k and all $\gamma \in \Gamma$, for some congruence subgroup Γ. In particular, we will only consider congruence subgroups of the form $\Gamma_0(N)$ for certain N, so from this point onwards we will always assume Γ denotes such a congruence subgroup unless otherwise stated.

Note that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma$ and the weight k operator $\left[\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right]_k$ sends $f(z)$ to $f(z+1)$. Hence every function $f : \mathcal{H} \to \mathbf{C}$ invariant under the action the action of $[\gamma]_k$ for all $\gamma \in \Gamma$ admits a Fourier expansion of the form

$$f(q) = \sum_{n=-\infty}^{\infty} a_n(f) q^n, \qquad q = e^{2\pi i z}. \tag{2.3}$$

We note there is similarly an action of $\mathrm{SL}_2(\mathbf{Z})$ on $\mathbf{P}^1(\mathbf{Q})$, again via fractional linear transformations.

Definition II.16. A ***cusp*** for Γ is an orbit Γs for the action of Γ on $s \in \mathbf{P}^1(\mathbf{Q})$. We will often denote a cusp by a distinguished element of the orbit.

Example II.17. The only cusp for the action of $\Gamma = \mathrm{SL}_2(\mathbf{Z})$ on $\mathbf{P}^1(\mathbf{Q})$ is ∞.

Since every congruence subgroup is of finite index in $\mathrm{SL}_2(\mathbf{Z})$, we see from the example above that there are always finitely many cusps.

If s is a cusp other than ∞, let $\gamma \in \mathrm{SL}_2(\mathbf{Z})$ such that $\gamma\infty = s$. Then $f|[\gamma]_k$ also admits a Fourier expansion similar to (2.3). We refer to this q-expansion as the Fourier expansion at the cusp s.

We say that f is holomorphic at a cusp s if the Fourier coefficients of the expansion at s are zero for all $n < 0$. In particular, f is holomorphic at s if the Fourier expansion converges at $q = 0$.

Definition II.18. For any congruence subgroup Γ, we define the space of ***modular forms*** of level Γ and weight k, denoted $\mathcal{M}_k(\Gamma)$, by the space of functions $f : \mathcal{H} \to \mathbf{C}$ satisfying:

- f is holomorphic on $\mathcal{H}$,
- $f|[\gamma]_k = f$ for all $\gamma \in \Gamma$,
- f is holomorphic at all cusps.

The space of ***cusp forms*** of level Γ and weight k, denoted $\mathcal{S}_k(\Gamma)$, is the subspace of $\mathcal{M}_k(\Gamma)$ consisting of forms that vanish at the cusp, i.e., $a_0(f) = 0$. A cusp form is ***normalized*** if $a_1(f) = 1$.

2.2.1 Hecke algebra and eigenforms

Spaces of modular forms of a fixed weight and level come naturally equipped with the action of a particular algebra of operators. Let Γ denote a congruence subgroup of the form $\Gamma_0(N)$.

Let p be a prime not dividing N. Let α_p denote the element $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$. The double coset $\Gamma\alpha_p\Gamma$ decomposes as a disjoint union

$$\Gamma\alpha\Gamma = \bigsqcup_i \Gamma\beta_i$$

of right cosets. Then we can define the action of the $p^{\boldsymbol{th}}$ ***Hecke operator***, T_p on $\mathcal{M}_k(\Gamma)$

$$T_p f = \sum_i f[\beta_i]_k.$$

For any prime power p^r we may define the Hecke operator T_{p^r} inductively by

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

with the convention that $T_1 = 1$ and $\langle p\rangle = 0$ if $p \mid N$.

By explicit computation, one can check that the Hecke operators and diamond operators all commute with one another. As a consequence, we may define a Hecke operator T_n for any positive integer n via

$$T_n = \prod_{p^r || N} T_{p^r}.$$

Definition II.19. The ***Hecke algebra*** $\mathbf{T} = \mathbf{T}(N)$ of level N is the $\mathbf{Z}$-algebra generated by all of the T_n.

There is an additional operator on $\mathcal{S}_k(\Gamma)$. Let $w_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$. The double coset decomposition

$$\Gamma w_N \Gamma = \bigsqcup_i \Gamma w_i$$

gives rise to the ***Atkin-Lehner operator***, denoted W_N. Explicitly,

$$W_N f = N^{1-k/2} \sum_i f[w_i]_k.$$

It can be checked that $W_N^2 = (-1)^k$, and so W_N is an involution when k is even. W_N commutes with the Hecke operators T_n for n with $(n, N) = 1$, but not with all Hecke operators in general.

We say that a cusp form $f \in \mathcal{S}_k(\Gamma_0(N))$ is an ***eigenform*** if it is an eigenfunction for the action of all Hecke operators.

We define an inner product on $\mathcal{S}_k(\Gamma_0(N))$ by

$$\langle f, g\rangle = \int_{\mathcal{H}\backslash\Gamma_0(N)} f(z)\overline{g(z)}\frac{dxdy}{y^{k-2}}, \tag{2.4}$$

where $z = x + iy$.

The ***Petersson inner product*** of (2.4) is self-adjoint under the action of the Hecke operators, and so $S_k(\Gamma_0(N))$ has a basis of eigenforms.

Fix a positive integer N. For any positive integer $M \mid N$ such that $(N, N/M) = 1$ and $d \mid M$, there is a degeneracy map

$$\iota_{d,M,N} : \mathcal{S}_k(\Gamma_0(N/M)) \to \mathcal{S}_k(\Gamma_0(N))$$

given by

$$\iota_{d,M,N}(f(z)) = f(dz).$$

We say that a cusp form in the space spanned by the image of all such degeneracy maps is ***old*** at M, and denote the space of such forms by $\mathcal{S}_k(\Gamma_0(N))^{M-\text{old}}$. The orthogonal complement of the forms that are old at M under the Petersson inner product (2.4) is the space of forms that are ***new*** at M and denote it by $\mathcal{S}_k(\Gamma_0(N))^{M-\text{new}}$. Both subspaces are preserved by the action of $\mathbf{T}$.

Of particular interest is the case when $M = N$. In this case, we drop the M from the notation and simply refer to the subspaces as the old and new subspaces of $\mathcal{S}_k(\Gamma_0(N))$.

We say that a cusp form f is a ***newform*** if it is an eigenform for all Hecke operators and new at all divisors of N.

For any normalized cusp form $f \in \mathcal{S}_k(\Gamma_1(N))$, its ***L-function***, denoted $L(f,s)$ is the complex-valued function defined by the Dirichlet series

$$L(f,s) = \sum_{n=1} \frac{a_n(f)}{n^s}. \tag{2.5}$$

It is known (cf. [9, Section 5]) that the Fourier coefficients of f satisfy

$$a_n(f) = \mathcal{O}(n^{k/2}) \tag{2.6}$$

and so $L(f,s)$ converges absolutely and uniformly in the right half-plane $\Re(s) > k/2+1$.

We define the completed L-function of f to be (essentially) the Mellin transform of f. Explicitly, we define it to be

$$\Lambda(f,s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(f,s). \tag{2.7}$$

The completed L-function satisfies a simple functional equation.

Theorem II.20. [9, Section 5]

Let k be a positive even integer. Suppose $f \in \mathcal{S}_k(\Gamma_0(N))$ is an eigenform for the Atkin-Lehner involution W_N with eigenvalue ε. Let $\varepsilon(f) = \varepsilon \cdot i^k$. Then $\Lambda(f,s)$ satisfies the functional equation

$$\Lambda(f,s) = \varepsilon(f)\Lambda(f,k-s). \tag{2.8}$$

Since the Atkin-Lehner involution W_N commutes with the Hecke operators T_ℓ for ℓ prime to N, we can see that an eigenform for all of the Hecke operators is automatically an eigenform for W_N. In particular, the L-function of any eigenform satisfies a functional equation of the form (2.8).

We will study the sign $\varepsilon(f)$ of the functional equation more carefully in Chapter III.

2.2.2 Modular curves and the Eichler-Shimura construction

The connection between modular forms and elliptic curves arises from the former's connection to certain moduli spaces of elliptic curves. Let $\Gamma = \Gamma_0(N)$, and let

$$\mathcal{H}^* = \mathcal{H} \cup \mathbf{P}^1(\mathbf{Q}).$$

Definition II.21. The ***open modular curve of level*** Γ is

$$Y_\Gamma := \Gamma \backslash \mathcal{H}.$$

It is a smooth Riemann surface and admits a canonical compactification

$$X_\Gamma := \Gamma \backslash \mathcal{H}^*,$$

called the ***modular curve of level*** Γ. X_Γ is a smooth, compact Riemann surface and admits an algebraic structure, hence is an algebraic curve over $\mathbf{C}$.

For $\Gamma = \Gamma(N)$, $\Gamma_1(N)$, or $\Gamma_0(N)$, respectively, we will denote the (compactified) modular curve of level Γ by $X(N)$, $X_1(N)$, or $X_0(N)$, respectively.

An ***enhanced elliptic curve of level*** $\Gamma_0(N)$ defined over a field F is an elliptic curve E/F together with a cyclic N-isogeny

$$E \to E' \tag{2.9}$$

defined over F. The open modular curve $Y_0(N)$ is a coarse moduli space for enhanced elliptic curves of level $\Gamma_0(N)$. Its compactification $X_0(N)$ similarly admits a moduli interpretation as a moduli space of generalized enhanced elliptic curves. Using this moduli interpretation, one can see that $X_0(N)$ is defined over $\mathbf{Q}$ and admits a smooth, proper model over $\mathbf{Z}\left[\frac{1}{N}\right]$.

$X_0(N)$ admits an action of the Hecke algebra $\mathbf{T}$. We could equivalently describe a point (2.9) on the open curve $Y_0(N)$ by the pair

$$(E, C) \tag{2.10}$$

where $C = \ker(E \to E')$. Then the action of the Hecke operator T_p is given by

$$T_p(E, C) = \sum_D (E/C, (C + D)/D) \tag{2.11}$$

where the sum is indexed over cyclic subgroups D of $E[p]$ such that $C \cap D = 0$. One can extend the action the cusps of $X_0(N)$ in order to give a correspondence

$$T_p : E \to \mathrm{Div}(E). \tag{2.12}$$

This correspondence in turn gives rise to an endomorphism of the Jacobian, $J_0(N)$, of $X_0(N)$ via Albanese or Picard functoriality. The choice differs by the action of an Atkin-Lehner involution. Since we will primarily concern ourselves with newforms, we note that the choice only differs by a sign, so we take the convention of Albanese functoriality.

Let f be a weight 2 newform in $\mathcal{S}_2(\Gamma_0(N))$. We define the prime ideal associated to f to be

$$I_f = \ker(\mathbf{T} \to \mathbf{C}) \tag{2.13}$$

where $\mathbf{T} \to \mathbf{C}$ is the map sending a Hecke operator T_p to its eigenvalue $a_p(f)$.

The abelian variety associated to f is

$$A_f = J_0(N)/I_f J_0(N) \tag{2.14}$$

where

$$I_f J_0(N) = \sum_T T J_0(N)$$

for all $T \in I_f$. We say that A_f is the ***optimal quotient*** of $J_0(N)$ attached to f via ***Eichler-Shimura*** construction.

It is known that A_f is an abelian variety defined over $\mathbf{Q}$ of dimension

$$[\mathbf{Q}(a_n(f)) : \mathbf{Q}]$$

with an embedding $\mathbf{T}/I_f \hookrightarrow \mathrm{End}(A_f)$. In particular, when f has rational coefficients A_f is an elliptic curve over $\mathbf{Q}$.

We say that an abelian variety defined over $\mathbf{Q}$ is ***modular*** if it is isogenous to some A_f. By work of Wiles [43], Taylor-Wiles [38], and Breuil-Conrad-Diamond-Taylor [6] it is now known that all abelian varieties of GL_2-type are modular. In particular, all elliptic curves over $\mathbf{Q}$ have an associated newform f with rational coefficients such that E is isogenous to A_f. Let $\mathrm{cond}(E)$ denote the conductor of E. For a prime p, we define

$$a_p = \begin{cases} p+1-\#E(\mathbf{F}_p) & \text{if } E \text{ has good reduction at } p \\ 1 & \text{if } E \text{ has split multiplicative reduction at } p \\ -1 & \text{if } E \text{ has nonsplit multiplicative reduction at } p \\ 0 & \text{if } E \text{ has additive reduction at } p \end{cases}.$$

As a corollary, we have

$$L(E,s) = L(f,s), \tag{2.15}$$

where

$$L(E,s) = \prod_{p \mid \mathrm{cond}(E)} (1 - a_p p^{-s})^{-1} \prod_{p \nmid \mathrm{cond}(E)} (1 - a_p p^{-s} + p^{1-2s}), \tag{2.16}$$

It follows from Theorem II.20 that we also have analytic continuation and a functional equation of $L(E,s)$.

2.2.3 Galois representations associated to modular forms

Let $f \in \mathcal{S}_2(\Gamma_0(N))$ be a normalized eigenform. Then a construction of Shimura [35] gives rise to a compatible family of semisimple 2-dimensional p-adic representations

$$\rho_{f,p} : \mathrm{G}_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{Q}_p}) \tag{2.17}$$

such that

- $\rho_{f,p}$ is unramified away from Np,
- $\mathrm{tr}(\rho_{f,p}(\mathrm{Frob}_\ell)) = a_\ell(f)$ for primes $\ell \nmid Np$,
- $\det(\rho_{f,p}) = \chi_p$, where χ_p is the p-adic cyclotomic character.

Let $T_p(J_0(N))$ denote the p-adic Tate module of $J_0(N)$. Let $F_f = \mathbf{Q}(a_n(f))$ be the number field generated by the Fourier coefficients of f and let $\mathfrak{p}$ be a prime of F_f above p. Let $F_{f,\mathfrak{p}}$ denote the corresponding $\mathfrak{p}$-adic completion.

The action of $\mathbf{T}$ on $J_0(N)$ gives rise to an action on $T_p(J_0(N))$. Then we define $\rho_{f,\mathfrak{p}}$ to be the semisimplification of

$$\{x \in T_p(J_0(N)) \otimes F_{f,\mathfrak{p}} \,|\, T_\ell x = a_\ell(f)x \text{ for all primes } \ell \nmid Np\}.$$

We note that the image of $\rho_{f,p}$ actually lies in $\mathrm{GL}_2(F_{f,\mathfrak{p}})$ by construction. Let V be the underlying space of the representation $\rho = \rho_{f,\mathfrak{p}}$. By choosing a $\mathrm{G}_{\mathbf{Q}}$-stable lattice inside V it is also possible to define a residual representation

$$\overline{\rho_{f,\mathfrak{p}}} : \mathrm{G}_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}_p}).$$

We may define the L-function associated to ρ by

$$L(\rho, s) = \prod_p \det(1 - \rho(\mathrm{Frob}_p)p^{-s}\,|_{V^{I_p}})$$

where I_p denotes the inertia group at p. It can be checked that if f has rational coefficients, so $E = A_f$ is an elliptic curve over $\mathbf{Q}$, that

$$L(\rho_{f,p}, s) = L(E, s) = L(f, s).$$

2.3 Modular forms on definite quaternion algebras

Let $\mathbf{A}$ denote the ring of adeles over $\mathbf{Q}$ and let $\mathbf{A}_f$ be the ring of finite adeles.

Let B be a definite quaternion algebra $B/\mathbf{Q}$ of absolute discriminant D. We can define an algebraic group, also denoted by $B^\times$, over $\mathbf{Q}$ defined by its functor of points as follows: given a $\mathbf{Q}$-algebra A, $B^\times(A) = (B \otimes_{\mathbf{Q}} A)^\times$.

For any integer S, let $\mathbf{A}_f^{(S)} := \prod'_{\ell \nmid S} \mathbf{Q}_\ell$ be the ring of prime-to-S adeles. For any prime $\ell \nmid D$, we have $B \otimes \mathbf{Z}_\ell \simeq M_2(\mathbf{Q}_\ell)$. Let $\mathcal{O}$ be a maximal order in B. Then, up to conjugation, we have $\mathcal{O} \otimes \mathbf{Z}_\ell = M_2(\mathbf{Z}_\ell)$ for each $\ell \nmid D$. Fix isomorphisms

$$\iota_\ell : B \otimes \mathbf{Z}_\ell = M_2(\mathbf{Q}_\ell)$$

such that $\iota_\ell(\mathcal{O} \otimes \mathbf{Z}_\ell) = M_2(\mathbf{Z}_\ell)$ for each such ℓ. We will, in general, omit ι_ℓ and simply use this fixed identification throughout.

For any compact open subgroup $K \subset \widehat{\mathcal{O}}^\times$, we can consider the double coset space

$$B^\times \backslash B^\times(\mathbf{A}_f)/K. \tag{2.18}$$

We will often work with compact open subgroups of the form $K = \prod_\ell K_\ell$. For any positive integers N with $(N, D) = 1$, one can consider the following compact open subgroups:

$$\begin{aligned} K_0(N) &= \left\{ (x_\ell) \in \widehat{\mathcal{O}}^\times \mid x_\ell \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \text{ for all } \ell \mid N \right\}, \\ K_1(N) &= \left\{ (x_\ell) \in \widehat{\mathcal{O}}^\times \mid x_\ell \equiv \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \pmod{N} \text{ for all } \ell \mid N \right\}. \end{aligned} \tag{2.19}$$

These are the quaternionic analogues of the congruence subgroups $\Gamma_0(N)$ and $\Gamma_1(N)$, respectively.

When B is definite and $K = K_0(N)$, the double coset space (2.18), sometimes referred to as the ***Gross curve of level*** N in the literature, is the analogue of a modular curve in the classical modular form setting. However, unlike the classical case, the following lemma implies that this space is finite.

Remark II.22. Some authors use the term Gross curve to refer to a certain disjoint union X of genus 0 curves indexed by the elements of X_K. Then we have the identification $\mathrm{Pic}(X) \cong \mathbf{Z}[X_K]$.

Lemma II.23 ([15, Thm 2.8])**.**
For any compact open subgroup K*,* $B^\times \backslash B^\times(\mathbf{A}_f)/K$ *is finite.*

If R is the order of $\mathcal{O}$ determined by the same local congruence conditions as $K_0(N)$ in (2.19), then R is an Eichler order of level N in B with $\widehat{R}^\times = K_0(N)$. Then the Gross curve of level N is precisely the class group $\mathrm{Cl}(B)$ by Lemma II.10.

For a compact open subgroup K of B, we can now define ***quaternionic modular forms of level*** K as certain functions on X_K. A ***modular form of weight 2 and level*** K ***on*** B is a function

$$\phi : B^\times \backslash B^\times(\mathbf{A}_f)/K \to \mathbf{C}.$$

The $\mathbf{C}$-vector space of such functions is denoted by $\mathcal{M}_2^B(K)$. The space of ***cusp forms of weight 2 and level*** K ***on*** B is the subspace of $\mathcal{M}_2^B(K)$ that is orthogonal to the constant functions, and is denoted $\mathcal{S}_2^B(K)$.

The space $\mathcal{S}_2^B(K_0(N))$ also has an inner product on it, that we again call the Petersson inner product. Let R be an Eichler order of level N in B, and $\mathrm{Cl}(B) =$

$\mathrm{Cl}(R)$ the set of conjugacy classes of Eichler orders of level N, so

$$\mathcal{S}_2^B(K_0(N)) \hookrightarrow \mathrm{Hom}(\mathrm{Cl}(B), \mathbf{C}).$$

Pick representatives $\{x_i\}$ of $\widehat{B}^\times$ for the elements of $\mathrm{Cl}(B)$. Let

$$\Gamma_i = \frac{x_i \widehat{R}^\times x_i^{-1} \cap B^\times}{\{\pm 1\}} \tag{2.20}$$

and set $w_i = \#\Gamma_i$. Then for any two forms $g_1, g_2 \in \mathcal{S}_2^B(K_0(N))$, we define the ***Petersson inner product*** on B by

$$\langle g_1, g_2 \rangle = \sum_i w_i g_1(x_i) g_2(x_i). \tag{2.21}$$

2.4 The Jacquet-Langlands correspondence

As in the case of classical modular forms, we can define the action of Hecke operators on quaternionic modular forms. Let K be an open compact subgroup of the form $K_0(N)$.

Let π_q denote the element of $B^\times(\mathbf{A}_f)$ that is the identity at all places except at q, where it is $\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}$. Let $z_q \in B^\times(\mathbf{A}_f)$ be the identity at all places except at q, where it is $\begin{pmatrix} q & 0 \\ 0 & q \end{pmatrix}$.

We first define the operators T_q for primes $q \nmid D$. The double coset space $K\pi_q K$ breaks up as a finite disjoint union of left cosets

$$K\pi_q K = \bigsqcup_i g_{i,q} K.$$

Then we can define the action of T_q on $\mathcal{M}_2^B(K)$ via

$$(T_q f)(x) = \sum_i f(x g_{i,q}).$$

The Hecke operators T_q for $q \mid D$ are defined similarly, replacing π_q with an element of reduced norm q in $B \otimes \mathbf{Q}_q$.

The $\mathbf{Z}$-algebra generated by the Hecke operators T_q is the ***Hecke algebra of level*** K for B, denoted $\mathbf{T}_B = \mathbf{T}_B(N)$. We can then define eigenforms in the quaternionic setting to be those that are eigenfunctions for all of the Hecke operators.

Theorem II.24. (Jacquet-Langlands correspondence, [2, Theorem 1.2])
Let B be a definite quaternion algebra over $\mathbf{Q}$ of absolute discriminant D and N a positive integer with $(D, N) = 1$. Then there is an injective map of Hecke modules

$$\mathcal{S}_2^B(K_0(N)) \hookrightarrow \mathcal{S}_2(\Gamma_0(DN), \mathbf{C})$$

whose image is the subspace consisting of forms which are new at all primes dividing D.

Let $\psi \in \mathcal{S}_2^B(K_0(N))$, and let $F = F_\psi$ denote the number field generated by all of the Hecke eigenvalues of ψ. Consider the space $\mathcal{S}_2^B(K_0(N), F)$ of quaternionic modular forms whose image lies in $F^\times$. The subspace

$$\mathcal{S}_2^B(K_0(N), F)^\psi \subset \mathcal{S}_2^B(K_0(N), F)$$

on which the Hecke operators act via the eigenvalues of ψ is preserved by the action of the Hecke operators. This gives an F-structure on this subspace, and so there must be a nontrivial element of $\mathcal{S}_2^B(K_0(N), F)^\psi$. This gives us the following corollary to the above theorem:

Corollary II.25. *Let f be a weight 2 eigenform of level $\Gamma_0(N)$ and q a prime dividing N such that f is new at q. Let F_f be the number field generated by all of the Hecke eigenvalues of f. Then there is an eigenform $\psi \in \mathcal{S}_2^{B(q\infty)}(K_0(N/q), F_f)$ with the same Hecke eigenvalues as f.*

Due to the lack of a Fourier expansion in the quaternionic setting, there is no canonical normalization for the eigenform ψ. Instead, ψ is well-defined up to scaling by an element of $F_f^\times$. We will take a fixed normalization later, but we hold off on this for now.

CHAPTER III

Heegner points and special value formulae

We briefly recall certain special points on the modular and Gross curves from the previous chapter, and their role in special value formulae for the L-functions of weight 2 modular forms.

3.1 Heegner points on $X_0(N)$

The moduli interpretation of the open modular curve $Y_0(N)$ allows us to construct points defined over certain extensions of imaginary quadratic fields.

Definition III.1. A ***Heegner point*** on $X_0(N)$ is a point corresponding, via the moduli interpretation, to an isogeny between elliptic curves with complex multiplication by the same order in an imaginary quadratic field.

Let K be an imaginary quadratic field of discriminant $-D$ with ring of integers $\mathcal{O}_K$, and let $\mathcal{O}_c \subset \mathcal{O}_K$ be the order of conductor c, with c prime to N. Then Heegner points corresponding to elliptic curves with complex multiplication by $\mathcal{O}_c$ exist if and only if N satisfies the so-called ***Heegner hypothesis*** relative to K. We say that the Heegner point is of conductor c if it corresponds to an isogeny between elliptic curves with complex multiplication by $\mathcal{O}_c$.

Definition III.2. We say that N satisfies the ***Heegner hypothesis*** relative to K

if every prime dividing N splits or is ramified in K, and every prime p with $p^2 \mid N$ splits in K.

In particular, N satisfies the Heegner hypothesis relative to K if and only if there exists an ideal $\mathfrak{N}$ of $\mathcal{O}_K$ with $\mathcal{O}_K/\mathfrak{N} \cong \mathbf{Z}/N\mathbf{Z}$.

Fix such an $\mathfrak{N}$ and let $\mathfrak{N}_c = \mathfrak{N} \cap \mathcal{O}_c$. Since N is prime to the conductor of $\mathcal{O}_c$, we have $\mathcal{O}_c/\mathfrak{N}_c \cong \mathbf{Z}/N\mathbf{Z}$. Then, for any projective $\mathcal{O}_c$-module $\mathfrak{a} \subset K$, the cyclic isogeny

$$\mathbf{C}/\mathfrak{a} \to \mathbf{C}/\mathfrak{N}^{-1}\mathfrak{a} \tag{3.1}$$

of complex elliptic curves determines a $\mathbf{C}$-point on $X_0(N)$. Since $\mathrm{End}(\mathbf{C}/\mathfrak{a}) = \mathrm{End}(\mathbf{C}/\mathfrak{N}^{-1}\mathfrak{a}) = \mathcal{O}_c$, this is in fact a Heegner point. The isomorphism class of the Heegner point depends only on the class of $\mathfrak{a}$ in $\mathrm{Pic}(\mathcal{O}_c)$, so for a fixed ideal $\mathfrak{N}$ there are precisely $\#\mathrm{Pic}(\mathcal{O}_c)$ such points. The theory of complex multiplication implies that these points are actually defined over certain abelian extensions of K.

Let $\hat{\mathcal{O}}_c = \mathcal{O}_c \otimes \hat{\mathbf{Z}}$ denote the profinite completion of $\mathcal{O}_c$. Then the ***ring class field of conductor*** c, denoted K_c is the abelian extension of K associated to the subgroup $K^\times \hat{\mathcal{O}}_c^\times \mathbf{C}^\times \subset \mathbf{A}_K^\times$ by class field theory. We have a canonical isomorphism

$$\mathrm{Gal}(K_c/K) \cong \mathrm{Pic}(\mathcal{O}_c). \tag{3.2}$$

Theorem III.3. (Main theorem of complex multiplication)
Let $\mathfrak{a}, \mathfrak{b}$ be projective $\mathcal{O}_c$-submodules of K. Let $\sigma_{\mathfrak{b}} \in \mathrm{Gal}(K_c/K)$ denote the corresponding automorphism of K_c under the isomorphism (3.2)*. Then the following hold:*

1. *$K_c = K(j(\mathbf{C}/\mathfrak{a}))$.*

2. *Any elliptic curve with complex multiplication by $\mathcal{O}_c$ is of the form $\mathbf{C}/\mathfrak{a}$ for some projective $\mathcal{O}_c$-submodule $\mathfrak{a} \subset K$.*

3. $\sigma_{\mathfrak{b}}(j(\mathbf{C}/\mathfrak{a})) = j(\mathbf{C}/\mathfrak{b}^{-1}\mathfrak{a})$.

Since the function field of $X_0(N)$ is generated by $j(z)$ and $j(Nz)$, we obtain the following corollary.

Corollary III.4. *All Heegner points of conductor c are of the form* (3.1) *and are defined over K_c.*

Throughout this thesis, we will primarily be concerned with Heegner points of conductor 1. Let H be the Hilbert class field of K. Let

$$P_K = \sum_{\sigma \in \mathrm{Gal}(H/K)} P^\sigma \in \mathrm{Div}(X_0(N))(K) \tag{3.3}$$

for any Heegner point P of conductor 1. We will refer to P_K as the Heegner point for K.

Remark III.5. It should be noted that P_K is well-defined as long as the ideal $\mathfrak{N}$ is fixed. Changing $\mathfrak{N}$ has the effect of possibly changing P_K by the action of an Atkin-Lehner involution on $J_0(N)$. The image of P_K on a modular abelian variety associated to a weight 2 newform of level N is thus well-defined up to ±1. Since this is the case of interest to us, and the sign is unimportant in our situation, we ignore the subtlety here and fix an ideal $\mathfrak{N}$ once and for all.

We will also use P_K to denote the image of the Heegner point on $J_0(N)$ under the embedding

$$\begin{aligned} X_0(N) &\to J_0(N) \\ x &\mapsto (x) - (\infty). \end{aligned}$$

3.2 Heegner points on definite quaternion algebras

Definite quaternion algebras, like their indefinite counterpart, also admit certain special points, following [2].

Let B be a definite quaternion algebra and N a positive integer prime to the discriminant of B. Let $R \subset B$ be an oriented Eichler order of level N.

Let K be an imaginary quadratic field of discriminant prime to N and $\Delta(B)$ such that all primes dividing $\Delta(B)$ are nonsplit in K. Then we have an embedding $K \hookrightarrow B$ by Theorem II.3.

Definition III.6. Let $\mathcal{O}_c$ denote the order of $\mathcal{O}_K$ of conductor c. We say that an embedding $f : K \hookrightarrow B$ is ***optimal*** relative to $\mathcal{O}_c$ if

$$f(K) \cap R = f(\mathcal{O}_c).$$

If K satisfies the Heegner hypothesis (Definition III.2), then $\mathcal{O}_K$ has a surjection $\mathcal{O}_K \twoheadrightarrow \mathbf{Z}/N\mathbf{Z}$ that we will also refer to as an orientation on $\mathcal{O}_K$. Our choice of ideal $\mathfrak{N}$ of the previous section thus fixes an orientation on $\mathcal{O}_K$, and thus on all orders $\mathcal{O}_c$ of K.

An optimal embedding $f : K \to B$ relative to $\mathcal{O}_c$ is said to be ***oriented*** if the orientation on $\mathcal{O}_c$ induces the fixed orientation on R. That is, if the diagram

$$\begin{tikzcd}
K \arrow[r, hook] & B \\
\mathcal{O}_c \arrow[u, hook] \arrow[r, hook] \arrow[dr] & R \arrow[u, hook] \arrow[d] \\
& \mathbf{Z}/N\mathbf{Z}
\end{tikzcd} \tag{3.4}$$

commutes, where the bottom two arrows are the orientations on $\mathcal{O}_c$ and R.

Definition III.7. A ***definite Heegner point on*** B of conductor c is an optimal oriented embedding relative to $\mathcal{O}_c$ for some oriented Eichler order R. We put an equivalence relation on the set of definite Heegner points on B by identifying two optimal oriented embeddings if they differ by conjugation by an element of $B^\times$.

Remark III.8. Heegner points on definite quaternion algebras are known by several names in the literature, including Gross points and special points.

Let H_c denote the set of Heegner points on B of conductor c. Then it is known [2, Lemma 2.5] that H_c is a principal homogeneous space for $\mathrm{Pic}(\mathcal{O}_c)$, noting that we have fixed our orientation on K. Hence $\#H_c = \#\mathrm{Pic}(\mathcal{O}_c)$, and so there is an abstract (non-canonical) bijection between Heegner points of conductor c on $X_0(N)$ and on definite quaternion algebras.

As in the case of Heegner points on $X_0(N)$, given a Heegner point x of conductor 1 on B we can define the definite Heegner point of K by

$$x_K = \sum_{\sigma \in \mathrm{Gal}(H/K)} x^\sigma \in \mathbf{Z}[H] \tag{3.5}$$

where the action of $\mathrm{Gal}(H/K)$ is given by the action of $\mathrm{Pic}(\mathcal{O}_K) \cong \mathrm{Gal}(H/K)$ when viewing H_1 as a principal homogeneous space.

There is also a degeneracy map

$$H_c \to \mathrm{Cl}(B) \tag{3.6}$$

sending a Heegner point to the conjugacy class of the oriented Eichler order defining it. The size of the fiber in H over a class in $\mathrm{Cl}(B)$ under (3.6) is precisely $\#\Gamma$, where Γ is as in (2.20).

3.3 The central sign of $L(f/K, s)$

Before we can give special value formulae for the L-functions associated to a weight 2 eigenform $f \in \mathcal{S}_2(\Gamma_0(N))$, we determine the sign $\varepsilon(f)$ of the functional equation (2.8) in terms of N and K.

The sign $\varepsilon(f)$ decomposes as a product of local signs

$$\varepsilon(f) = \prod_{p \leq \infty} \varepsilon_p(f) \tag{3.7}$$

over all places p.

The local sign at ∞ is always -1 [32, Prop. 1], and the sign $\varepsilon_p(f) = \pm 1$ for p is determined by the local behavior of ρ_f at p. In particular, if ρ_f is unramified at p then $\varepsilon_p(f) = 1$. See [32] for explicit computations of the signs when f has rational coefficients.

We may also consider the ***base change L-function*** $L(f/K, s)$, defined by

$$L(f/K, s) = L(\rho_f|_{G_K}, s), \tag{3.8}$$

where $G_K = \mathrm{Gal}(\overline{K}/K)$ is considered as a subgroup of $\mathrm{G}_{\mathbf{Q}}$.

If f has rational coefficients, so $E = A_f$ is an elliptic curve, then $L(f/K, s) = L(E/K, s)$ is nothing more than the Hasse-Weil L-function of the base change of E to K. In particular, we have a factorization

$$L(E/K, s) = L(E, s)L(E^K, s), \tag{3.9}$$

where E^K denotes the quadratic twist of E by K.

A careful study of Rankin L-series gives the following, cf. [12, Ch. IV].

Theorem III.9. [19, Thm. 19.14]
Assume $(N, D) = 1$. Let

$$\Lambda(f/K, s) = N^2 D^2 (2\pi)^{-2s} \Gamma(s)^2 L(f/K, s).$$

Then $\Lambda(f/K, s)$ converges absolutely in a right half plane and admits an analytic continuation to all of $\mathbf{C}$. In particular, it satisfies the functional equation

$$\Lambda(f/K, s) = \varepsilon(f/K)\Lambda(f/K, 2 - s), \tag{3.10}$$

where $\varepsilon(f/K) = \pm 1$.

The sign $\varepsilon(f/K)$ of (3.10) similarly decomposes as a product of local signs

$$\varepsilon(f/K) = \prod_{\nu \leq \infty} \varepsilon_\nu(f/K),$$

where the product is taken over the places of K. We again have $\varepsilon_\infty(f/K) = -1$, and the classification of local signs at finite primes is similar to the above. In particular, $\varepsilon_\nu(f/K) = 1$ for all finite $\nu \nmid N$.

Proposition III.10. *Suppose that either:*

1. *all primes dividing N split in K, or*
2. *$N = Mq$, where all primes dividing M split in K and q is inert in K.*

Then $\varepsilon(f/K) = -1$ or $\varepsilon(f/K) = 1$, respectively.

Proof. (Sketch)
Let $p \mid N$ be a prime that splits in K. Write $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ in K. Then the local behavior of $\rho_f|_{G_K}$ at $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ is the same, as ρ_f is defined over $\mathbf{Q}$ and the corresponding decomposition groups are conjugate in $\mathrm{G}_{\mathbf{Q}}$. Hence

$$\varepsilon_{\mathfrak{p}}(f/K) = \varepsilon_{\overline{\mathfrak{p}}}(f/K).$$

If $q \parallel N$, then the abelian variety A_f associated to f has toric reduction at q over $\mathbf{Q}$. If q is inert in K, then the reduction at q becomes split over K, which implies that $\varepsilon_q(f/K) = -1$, cf. [32, Prop. 3]. □

3.4 Special value formulae for $L(f/K, s)$

Let f be a weight 2 eigenform on $\Gamma_0(N)$ and $K = \mathbf{Q}(\sqrt{-D})$ an imaginary quadratic field of discriminant $-D$. Write $N = N^+N^-$, where N^+ is divisible by the primes which split in K and N^- is split by the primes which are inert in K. Assume N^- is squarefree. Then the general theory of special values of L-functions suggests that the leading term of the Taylor expansion of $L(f/K, s)$ at $s = 1$ should be related to the arithmetic of certain level N^+ structures in the quaternion algebra ramified at N^- (and possibly ∞, depending on whether N^- is divisible by an even or odd number of primes).

The cases we will be primarily interested in are when N satisfies either of the conditions of Proposition III.10.

3.4.1 The Gross-Zagier theorem

Suppose all primes dividing N split in K. Then N satisfies the Heegner hypothesis relative to K and, using our notation above, we have $N^- = 1$. Since the sign of the functional equation for $L(f/K, s)$ is -1, we have

$$L(f/K, 1) = -L(f/K, 1). \tag{3.11}$$

In particular the central L-value $L(f/K, 1)$ must vanish. By the philosophy above one expects to understand the central derivative $L'(f/K, 1)$ in terms of level N structure on the split quaternion algebra GL_2. This is precisely what the results of Gross-Zagier [12] provide.

Let A_f be the abelian variety associated to f. There is a canonical height pairing

$$\langle\, ,\, \rangle_{NT} : E(K) \times E(K) \to \mathbf{C} \tag{3.12}$$

called the ***canonical Néron-Tate height pairing***. On the restriction to the diagonal, the pairing satisfies

$$\langle P, P \rangle_{NT} = 0 \qquad \Leftrightarrow \qquad P \text{ is torsion in } E(K).$$

Then the main theorem of [12] relates the canonical Néron-Tate height of the image of the Heegner point (3.3) on A_f under the modular parametrization to the central derivative $L'(f/K, 1)$.

Theorem III.11. (Gross-Zagier formula)

Let f be a weight 2 newform on $\Gamma_0(N)$. Let $K = \mathbf{Q}(\sqrt{-D})$ be an imaginary quadratic field of discriminant $-D$. Suppose that all primes dividing N split in K. Then

$$L'(f/K, 1) = \frac{8\pi^2 \langle f, f\rangle_{\Gamma_0(N)}}{h_K u_K^2 \sqrt{D}} \langle P_K, P_K\rangle_{NT}$$

where $\langle\, ,\, \rangle_{\Gamma_0(N)}$ denotes the Petersson inner product on $X_0(N)$, $h_K = \#\mathrm{Cl}(K)$, and $u_K = \frac{1}{2}\#\mathcal{O}_K^\times$.

Corollary III.12. *Let f, N, and K be as above. Then*

$$L'(f/K, 1) \neq 0 \qquad \Leftrightarrow \qquad P_K \textit{ is non-torsion in } E(K).$$

3.4.2 The Gross formula

We now let g be an eigenform of level N satisfying the second condition of Proposition III.10. We write $N = Mq$, where all primes dividing M split in K and q is inert in K. In this case, the sign of the functional equation is $+1$, and so expects the central L-value $L(g/K, 1)$ to be related to some quantity on the quaternion algebra $B = B(q\infty)$ ramified at q and ∞.

The following theorem, due originally to Gross when $N = 1$ [10] and generalized to arbitray N by Daghigh [7], gives a precise formula for $L(g/K, 1)$. It may be viewed as an explicit Waldspurger formula [42] for the associated automorphic representation.

Theorem III.13. (Gross formula)

Let x_K be the image of the definite Heegner point (3.5) *in* $\mathrm{Cl}(B)$ *under the map* (3.6). *Let $\psi : \mathrm{Cl}(B) \to \mathbf{C}$ be the Jacquet-Langlands transfer of g to B (cf. Corollary II.25). Then*

$$L(g/K, 1) = \frac{(\psi(x_K))^2}{u_K^2\sqrt{D}} \, \frac{8\pi^2 \langle g\, ,\, g\rangle_{\Gamma_0(N)}}{\langle \psi\, ,\, \psi\rangle_B},$$

where $\langle\, ,\, \rangle_{\Gamma_0(N)}$ and $\langle\, ,\, \rangle_B$ denote the Petersson inner products on $X_0(N)$ and B, respectively.

We define the ***algebraic part*** of $L(g/K,1)$ to be

$$L^{alg}(g/K,1) = \frac{(\psi(x_K))^2}{u_K^2\sqrt{D}}.$$

Note that $L^{alg}(g/K,1)$ is nonzero if and only if $L(g/K,1)$ is.

$L^{alg}(g/K,1)$ is only defined up to a nonzero scalar, as ψ is. Since we will be interested in the reduction of $L^{alg}(g/K,1)$ at a prime $\mathfrak{P}$ of $\overline{\mathbf{Q}}$, we will take a fixed normalization; we normalize ψ to be $\mathfrak{P}$-adically integral and containing a $\mathfrak{P}$-adic unit. As an immediate consequence of our choice, we have the following:

Lemma III.14. *Suppose $\mathfrak{P} \cap \mathbf{Z} = p\mathbf{Z}$ and $p \nmid 6D$. Then $L^{alg}(g/K,1) \equiv 0 \pmod{\mathfrak{P}}$ if and only if $\psi(x_K) \equiv 0 \pmod{\mathfrak{P}}$.*

Remark III.15. The choice of transcendental period used to define $L^{alg}(g/K,1)$ may seem a bit unusual in light of the availability of Hida's canonical period Ω_g^{can} [14]. Our choice differs from Ω_g^{can} by the ratio of $\langle\psi,\psi\rangle_B$ and a congruence number for g on $\Gamma_0(N)$. This choice is more natural from the point of view of Iwasawa theory, as our definition of $L^{alg}(g/K,1)$ resembles the theta elements used to define an anticyclotomic p-adic L-function for g, cf. [39, Section 3].

CHAPTER IV

Congruences and multiplicity one theorems

We briefly review some results of Mazur and Ribet regarding congruences between eigenforms and mod p multiplicity one results.

4.1 Reduction of CM points on $X_0(N)$

We briefly recall the behavior of the reduction of the Heegner points on $X_0(N)$. Suppose K is an imaginary quadratic field satisfying the Heegner hypothesis relative to N, so all primes dividing N split in K. Let $q \nmid N$ be an inert prime in K. Recall that we have fixed an ideal $\mathfrak{N} \subset \mathcal{O}_K$ of index N with cyclic quotient.

The following result of Ribet will allow us to view these reduced points in terms of definite Heegner points, following [39, Section 6.8]. We omit the proof, though we will recall one direction of the bijection below in the case of a supersingular point coming from the reduction of a Heegner point.

Proposition IV.1. ([30, Prop. 3.3])

Let $\Sigma \subset X_0(N)(\mathbf{F}_{q^2})$ denote the set of points on $X_0(N)$ coming from supersingular elliptic curves via the moduli interpretation. Let B denote the definite quaternion algebra ramified at q and ∞. Then there is a bijection between Σ and the set of conjugacy classes of oriented Eichler orders of level N in B.

Let c be prime to N and let $\mathcal{O}_c$ be the order of conductor c in $\mathcal{O}_K$. Let E be an elliptic curve with CM by $\mathcal{O}_c$. Since we have fixed $\mathfrak{N}$, the ideal $\mathfrak{N}_c = \mathfrak{N} \cap \mathcal{O}_c$ is of index N and has cyclic quotient. The reduction $\widetilde{E}$ of E at q is supersingular since q is inert in K and prime to N. Recall that the endomorphism ring $\mathrm{End}(\widetilde{E})$ is a maximal order in the definite quaternion algebra $B = B(q\infty)$ ramified at q and ∞.

Let $C \subset E$ be the kernel of the multiplication by $\mathfrak{N}_c$ map $[\mathfrak{N}_c]$ on E. Since all supersingular points modulo q are defined over $\mathbf{F}_{q^2}$, the reduction of the pair (E, C) gives rise to a point in $X_0(N)(\mathbf{F}_{q^2})$. Conjugation by $[\mathfrak{N}_c]$ gives rise to an embedding

$$\mathrm{End}(\widetilde{E/C}) \hookrightarrow \mathrm{End}^0(\widetilde{E}) = B.$$

Then $R = \mathrm{End}(\widetilde{E/C}) \cap \mathrm{End}(\widetilde{E})$ is an Eichler order of level N in B and the reduction map gives rise to an embedding $\mathcal{O}_c = \mathrm{End}(E) \hookrightarrow R$. This, in turn, induces an optimal embedding $K \hookrightarrow B$ relative to $\mathcal{O}_c$. We may then define an orientation on R so that the optimal embedding is compatible with the orientation on $\mathcal{O}_c$ determined by $\mathfrak{N}_c$.

This construction is somewhat unsatisfying, as we have an constructed an Eichler order $R \subset B$ that depends on the choice of isomorphism $\mathrm{End}^0(\widetilde{E}) \cong B$. By fixing a single Heegner point $(E_0, E_0[\mathfrak{N}])$ of conductor 1, for any other Heegner point (E, C) as above we can choose an isogeny $E \to E_0$. Conjugating by the isogeny gives an embedding $\mathrm{End}(\widetilde{E}) \hookrightarrow \mathrm{End}^0(\widetilde{E_0}) \cong B$, and so we may compare the various Eichler orders constructed above. In particular, since the embedding of each Eichler order is only defined up to conjugation, the reduction of (E, C) gives a construction of a definite Heegner point on B in the sense of Definition III.7.

4.2 Raising the level

As alluded to in the introduction, given a weight 2 newform f of level N and a prime $q \nmid N$ we are interested in weight 2 eigenforms of level Nq that are congruent to f. The seminal theorem of Ribet [28] gives necessary and sufficient conditions for such a prime to exist:

Theorem IV.2. ([28])

Let $\mathfrak{P}$ be a prime of $\overline{\mathbf{Q}}$ lying above p. If $p \nmid Nq$ and $\overline{\rho_{f,p}}$ is irreducible, then there is a modular form

$$g = q + \sum_{n \geq 2} a_n(g) q^n \in S_2(\Gamma_0(Nq))^{q-new}$$

satisfying

$$a_n(f) \equiv a_n(g) \pmod{\mathfrak{P}}, \quad \textit{for all } n \textit{ with } (n,q) = 1,$$

if and only if

$$a_q(f) \equiv \pm(q+1) \pmod{\mathfrak{P}}.$$

Moreover, g is new at all primes exactly dividing N and $a_q(g) = \varepsilon$ where $\varepsilon = \pm 1$ is such that

$$q + 1 - \varepsilon a_q(f) \in \mathfrak{P}.$$

Remark IV.3. It should be noted that if $q \not\equiv -1 \pmod{p}$, then there is a unique choice of ε that satisfies the congruence. When $q \equiv -1 \pmod{p}$, each choice of $\varepsilon = \pm 1$ gives rise to a different level-raised form. This ambiguity will be of importance in Chapter V.

Due to the well-known nature of the result, we opt to highlight the key ingredients of the proof. For an in-depth treatment, see [31].

Proof. (Sketch)

Let $\mathbf{T}(Nq)$ be the Hecke algebra of level Nq. The subspace $\mathcal{S}_2(\Gamma_0(Nq))^{q-\text{new}}$ of cuspforms that are new at q is stable under the action of $\mathbf{T}(Nq) \subset \mathrm{End}(\mathcal{S}_2(\Gamma_0(Nq)))$. Let $\overline{\mathbf{T}(Nq)}$ denote the image of $\mathbf{T}(Nq)$ in $\mathrm{End}(\mathcal{S}_2(\Gamma_0(Nq)))^{q-\text{new}}$.

One has two degeneracy maps

$$X_0(Nq) \rightrightarrows X_0(N)$$

induced by duality by from the degeneracy maps

$$\mathcal{S}_2(\Gamma_0(N)) \rightrightarrows \mathcal{S}_2(\Gamma_0(Nq)).$$

Correspondingly, the degeneracy maps induce a map

$$\alpha : J_0(N)^2 \to J_0(Nq) \tag{4.1}$$

by Albanese functoriality whose image is, by definition, the q-old subvariety $J_0(Nq)^{q-\text{old}}$ of $J_0(Nq)$.

In turn, using the principal polarization on $J_0(Nq)$, one can define the abelian subvariety $J_0(Nq)^{q-\text{new}}$ by

$$J_0(Nq)^{q-\text{new}} = \left(\ker(J_0(Nq) \to J_0(Nq)^{q-\text{old}})\right)^{\vee} \subset J_0(Nq).$$

The q-new and q-old subvarieties are complementary in the sense that their internal sum generates $J_0(Nq)$ and they have finite intersection.

Let $\mathfrak{m}_f \subset \mathbf{T}(N)$ be the maximal ideal associated to f modulo $\mathfrak{P}$, and let $V_f = J_0(N)[\mathfrak{m}_f]$. Then V_f^2 is a subgroup scheme of $J_0(N)^2$. One checks that the kernel of α is supported at Eisenstein primes of $\mathbf{T}(N)$, and so $V_f^2 \cap \ker(\alpha) = 0$. As a result, we may view V_f^2 as a subgroup scheme of the q-old subvariety of $J_0(Nq)$.

Embedding V_f in its square under the embedding

$$v \mapsto (v, -\varepsilon v)$$

thus allows us to embed V_f in the q-old subvariety of $J_0(Nq)$. By explicit computation, one can check that the Hecke operators of level Nq then act on V_f via the morphism

$$\begin{aligned} \chi : \mathbf{T}(Nq) &\to k \\ T_\ell &\mapsto t_\ell \quad , \ell \nmid q \\ T_q &\mapsto \varepsilon \end{aligned}$$

where t_ℓ denotes the reduction modulo $\mathfrak{P}$ of the Hecke eigenvalue at ℓ for f.

This gives a construction of a form of level Nq congruent to f, but one needs to then check that the form is new at q. It is enough to show that the image of V_f embedded in $J_0(Nq)^{q-\text{old}}$ actually lies in the intersection with the q-new subvariety, as this then implies that χ factors through $\overline{\mathbf{T}(Nq)}$ and is thus the reduction of a form new at q. This can be done by explicit computation of the image, see [31, Lemma 2] for details. □

4.3 A mod p multiplicity theorem

We next turn to a related result on the dimension of a certain space of mod p modular forms. Let N be a positive integer, and q a prime number not dividing N. Let $J_0(Nq)^0$ denote the connected component of the identity in the special fiber of the Néron model of $J_0(Nq)$ over $\mathbf{Q}_q$. Then work of Raynaud [27] and Deligne-Rapoport [8] gives an exact sequence

$$0 \to T \to J_0(Nq)^0 \xrightarrow{\pi} J_0(N)^2 \to 0, \tag{4.2}$$

where $T/\mathbf{F}_q$ is a torus. Then the character group

$$X = \mathrm{Hom}(T, \mathbf{G}_m)$$

can be identified with the set of degree 0 divisors supported on the supersingular locus of $X_0(N)(\mathbf{F}_{q^2})$ [30, Prop. 3.1]. Our primary goal is then to compute the dimension of the g-isotypic part of X, where g is a Hecke eigenform of level Nq. The following result of Ribet computes the dimension in the cases of interest to us. It is a generalization of an earlier result of Mazur [30, Theorem 6.4] that showed that handled certain cases when the dimension is at most 1.

The theorem below implies that the dimension essentially behaves on the local behavior of the residual $\mathfrak{P}$-adic representation $\overline{\rho_g}$ at q.

Proposition IV.4. ([29, Prop. 1])

Suppose that $p \nmid 2N$, g is new at q, and ρ_g is irreducible modulo a prime $\mathfrak{P}$ of $\overline{\mathbf{Q}}$. Let $\mathfrak{m}$ denote the maximal ideal of $\mathbf{T}(Nq)$ determined by g modulo $\mathfrak{P}$. Let $k = \mathbf{T}(Nq)/\mathfrak{m}$. Then $\dim_k(X/\mathfrak{m}X) = 1$ unless $\overline{\rho_g}$ is unramified at q and $\overline{\rho_g}(\mathrm{Frob}_q) = \pm 1$. In the latter case, $\dim_k(X/\mathfrak{m}X) = 2$.

Proof. (Sketch)

Since g is new at q, the Jacquet-Langlands correspondence (Corollary II.25) and Proposition IV.1 combine to give a map

$$\psi : X \to F_g$$

where F_g is the field generated by the Hecke eigenvalues of g. Normalizing ψ to be $\mathfrak{P}$-adically integral and containing a $\mathfrak{P}$-adic unit, its reduction gives a nonzero map

$$\psi : X \to k$$

which factors through the g-isotypic part of X. In particular, we have $\dim_k(X/\mathfrak{m}X) \geq 1$.

On the other hand, Grothendieck [13] showed that there is an inclusion

$$\mathrm{Hom}(X/\mathfrak{m}X, \mu_p) \hookrightarrow J_0(Nq)[\mathfrak{m}] \tag{4.3}$$

of $k[\mathrm{Gal}(\overline{\mathbf{Q}_q}/\mathbf{Q})]$-modules. Since $p > 2$, $J_0(Nq)[\mathfrak{m}] \cong \overline{\rho_g}$ is 2-dimensional (cf. [24, Ch. II, Prop. 14.2]). Thus the dimension of $X/\mathfrak{m}X$ is at most 2.

Suppose $\dim_k(X/\mathfrak{m}X) = 2$, so (4.3) is an isomorphism. $\mathrm{Hom}(X/\mathfrak{m}X, \mu_p)$ is unramified at q, hence $\overline{\rho_g}$ is as well, with Frob_q acting via qT_q. Since g is new at q, T_q acts via the negative of the Atkin-Lehner involution w_q on T, hence Frob_q acts on $\mathrm{Hom}(X/\mathfrak{m}X, \mu_p)$ via $\pm q$. If the dimension is 2, then the determinant of Frob_q acts via q^2 on the left side of (4.3), while $\det(\overline{\rho_g}(\mathrm{Frob}_q)) = q$. Thus $q \equiv 1 \pmod{p}$.

Conversely if $\overline{\rho_g}$ is unramified at q, then comparing determinants again implies that $q \equiv 1 \pmod{p}$. Since $\overline{\rho_g}$ is unramified at q, Ribet's results on level-lowering [30, Theorem 8.2] imply that there is form of level N congruent modulo $\mathfrak{P}$ to g. In particular, viewing $J_0(N)^2$ as isogenous to a subvariety of $J_0(Nq)$ by (4.1), we have $J_0(N)^2[\mathfrak{m}] \neq 0$. Since the kernel of α is Eisenstein and $\overline{\rho_g}$ irreducible, we get an identification

$$J_0(N)^2[\mathfrak{m}] \cong J_0(Nq)[\mathfrak{m}].$$

Let $\varepsilon = \pm 1$ be such that $\overline{\rho_g}(\mathrm{Frob}_q) = \varepsilon$. It can be checked that $J_0(N)^2[\mathfrak{m}]$ lies in the subspace

$$\{(x, -\varepsilon x) \mid x \in J_0(N)\} \subset J_0(N)^2.$$

Then one can define a subgroup $W \subset J_0(N)[p]$ whose image under the diagonal or antidiagonal embedding (chosen to be compatible with the embedding above) is precisely $J_0(N)[\mathfrak{m}]$. Then Frob_q acts on W by ε, which forces both the Frobenius and Verschiebung endomorphisms on the reduction of $J_0(N)$ to act via ε.

By an explicit description [29, Lemma 1] of the map π in terms of the Frobenius and Verschiebung endomorphisms, we have $J_0(Nq)[\mathfrak{m}] \in \ker(\pi \circ \widetilde{\alpha})$, where $\widetilde{\alpha}$ denotes the reduction of α. Since the image of $\widetilde{\alpha}$ lands in the connected component of the identity, this gives an inclusion

$$J_0(Nq)[\mathfrak{m}] \subset T$$

which implies that $\dim_k(X/\mathfrak{m}X) = 2$. □

CHAPTER V

Jochnowitz congruences

We are now prepared to give the proof of the Jochnowitz congruence for a weight 2 newform of level $\Gamma_0(N)$. Let $f = \sum a_n(f)e^{2\pi inz}$ be a normalized weight 2 newform on $\Gamma_0(N)$. Suppose that $g = \sum a_n(g)e^{2\pi inz}$ is a normalized weight 2 eigenform on $\Gamma_0(Nq)$ that is new at q and congruent modulo p to f for some prime q. Explicitly, suppose there is a prime $\mathfrak{P}$ of $\overline{\mathbf{Q}}$ lying over p such that

$$a_\ell(f) \equiv a_\ell(g) \pmod{\mathfrak{P}}, \quad \text{for all primes } \ell \nmid pq.$$

As explained in Chapter I, one expects a congruence between the special values of the L-functions of f and g at their central critical points. Let K be an imaginary quadratic field satisfying the Heegner hypothesis for N. Suppose further that q is inert in K. Then the global root number of f/K is -1, while that of g/K is $+1$. Then $L(f/K, 1) = 0$ while $L(g/K, 1)$ should typically be nonzero. The Jochnowitz perspective then predicts a congruence between the algebraic parts of $L'(f/K, 1)$ and $L(g/K, 1)$. In light of the special value formulae of Chapter III, we may view this as a relation between the Heegner point on the f-isotypic part of $J_0(N)$ and the algebraic part of $L(g/K, 1)$.

5.1 Preliminaries

Let $E = E_f$ denote the optimal quotient of $J_0(N)$ associated to f via the Eichler-Shimura construction, and let $\pi : X_0(N) \to E$ be a modular parametrization of minimal degree. For ease of exposition we assume f has rational Fourier coefficients, so E is an elliptic curve. We do remark that all results in this chapter have analogues for modular GL_2-type abelian varieties with the same proofs, cf. [44, Section 6]. Let $k = \mathbf{F}_p$, and let ρ_f denote the two-dimensional p-adic Galois representation attached to f. Recall that $\rho_f = \rho_{f,p} : \mathrm{G}_{\mathbf{Q}} \to \mathrm{GL}(T_p(E)) \cong \mathrm{GL}_2(\mathbf{Z}_p)$ satisfies

- ρ_f is unramified away from Np.
- $\mathrm{tr}(\rho_f(\mathrm{Frob}_\ell)) = a_\ell(f)$ for primes $\ell \nmid Np$.
- $\det(\rho_f) = \chi_p$, where χ_p is the p-adic cyclotomic character.

Let $V_f = E[p]$, so $\overline{\rho_f} : \mathrm{G}_{\mathbf{Q}} \to \mathrm{GL}(V_f)$. Let K be an imaginary quadratic field of discriminant $-D$. Let $\mathbf{T} = \mathbf{T}(N)$ denote the Hecke algebra of level N, and let $\mathfrak{m}$ denote the maximal ideal of $\mathbf{T}$ cut out by f modulo p. Thus $\mathbf{T}/\mathfrak{m} \cong k$. The following theorem of Mazur implies that the representation occurs in $J_0(N)$ with multiplicity one. See also the discussion in Section 5 of [30].

Theorem V.1. [24, Ch. II, Prop. 14.2]
Let V_f be the mod p representation associated to f as above. Assume that V_f is irreducible and $p \nmid 2N$. Then

$$J_0(N)[\mathfrak{m}] \cong V_f \cong E[p],$$

where $J_0(N)[\mathfrak{m}] = \{x \in J_0(N) \,|\, x \in \ker(\phi)$ for all $\phi \in \mathfrak{m}\}$.

We will make the following assumptions:

Assumption V.2. *The triple (f, K, p) satisfies:*

- (Heegner hypothesis) *All primes dividing N split in K.*
- *$p \nmid 2ND$.*
- *$\overline{\rho_f}$ is irreducible.*
- *p does not divide the order of the* **Shimura subgroup**

$$\ker(J_1(N) \to J_0(N)).$$

Theorem V.3. (Jochnowitz congruence, informal version) *Let P_K denote the trace of the Heegner point of level N in $E(K)$. Then*

$$P_K \in pE(K_q) \quad \Leftrightarrow \quad \mathfrak{P} \mid L^{alg}(g/K, 1).$$

In view of Theorem IV.2 on raising the level of ρ_f, we divide the level-raising primes into three distinct classes.

Definition V.4. Let q be a level-raising prime which is inert in K.

- We say q is ***admissible*** if $q \not\equiv \pm 1 \pmod{p}$.
- We say q is ***Kolyvagin*** if $q \equiv -1 \pmod{p}$.
- We say q is ***residual*** if $q \equiv 1 \pmod{p}$.

Under our hypotheses, the following lemma shows that testing the divisibility of a rational point locally is equivalent to testing the divisibility over the residue field.

Proposition V.5. *Let L be a finite unramified extension of $\mathbf{Q}_q$. Let $\mathfrak{m}$ denote the maximal ideal of the ring of integers of L. Let κ denote the residue field.*

Suppose E_1, E_2 are elliptic curves over L with good reduction. For any isogeny $\phi : E_1 \to E_2$ defined over L of degree prime to q, we have

$$\frac{E_2(L)}{\phi(E_1(L))} \cong \frac{E_2(\kappa)}{\widetilde{\phi}(E_1(\kappa))},$$

where $\widetilde{\phi}$ denotes the reduction of ϕ.

Proof. One has the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \widehat{E_1}(\mathfrak{m}) \arrow[r] \arrow[d, "\widehat{\phi}"] & E_1(L) \arrow[r] \arrow[d, "\phi"] & E_1(\kappa) \arrow[r] \arrow[d, "\widetilde{\phi}"] & 0 \\
0 \arrow[r] & \widehat{E_2}(\mathfrak{m}) \arrow[r] & E_2(L) \arrow[r] & E_2(\kappa) \arrow[r] & 0
\end{tikzcd} \tag{5.1}$$

where $\widehat{E_i}$ denotes the formal group associated to E_i and $\widehat{\phi}$ denotes the induced isogeny on formal groups.

An application of the snake lemma gives the exact sequence

$$\operatorname{coker}\left(\widehat{\phi}\right) \longrightarrow \frac{E_2(L)}{\phi(E_1(L))} \longrightarrow \frac{E_2(\kappa)}{\widetilde{\phi}(E_1(\kappa))} \longrightarrow 0. \tag{5.2}$$

Since $\phi^\vee \circ \phi$ and $\phi \circ \phi^\vee$ give the multiplication by $\deg(\phi)$ maps on E_1 and E_2, respectively, it follows that $\widehat{\phi^\vee} \circ \widehat{\phi}$ and $\widehat{\phi} \circ \widehat{\phi^\vee}$ give the multiplication by $\deg(\phi)$ maps on $\widehat{E_1}(\mathfrak{m})$ and $\widehat{E_2}(\mathfrak{m})$, respectively. But $L/\mathbf{Q}_q$ is unramified, hence the formal logarithm gives isomorphisms

$$\widehat{E_i}(\mathfrak{m}) \xrightarrow{\sim} \mathcal{O}_L, \quad i = 1, 2.$$

The latter is a pro-q group, hence multiplication by $\deg(\phi)$ is an isomorphism. In particular, $\widehat{\phi}$ is an isomorphism and (5.2) gives the result. □

The strategy of the proof is to construct two nontrivial maps

$$\mathbf{Z}[\Sigma]^0 \to k,$$

where $\Sigma \subset X_0(N)(\mathbf{F}_{q^2})$ denotes the points on the modular curve arising from supersingular elliptic curves and the superscript denotes the degree zero divisors. The first map essentially comes from Kummer theory and the second from the Jacquet-Langlands transfer of g to the definite quaternion algebra ramified at q and ∞. After checking that both maps are equivariant for the action of the Hecke algebra, we may then conclude that the maps are nonzero multiples of one another by Proposition IV.4. When the mod p multiplicity one fails, we must take a slightly more careful approach.

5.2 Galois cohomology and the Kummer map

Let F be a number field, and let V be a finite dimensional p-adic vector space admitting a geometric action of G_F. Let $\rho : G_F \to \mathrm{GL}(V)$ be the aforementioned Galois representation, so ρ is unramified outside a finite set of places. Fix a G_F-stable lattice $T \subset V$ with $T \otimes \mathbf{Q} \simeq V$, and define

$$T_\pi := T/\pi T,$$

where π is a uniformizer of the p-adic field underlying V. Let N be the conductor of ρ. Let $\ell \neq p$ be a prime not dividing N, and let λ be a prime of F lying above ℓ. Let F_λ denote the completion of F at λ, and k_λ the residue field of F_λ.

With $B = V, T$, or T_π, the ***singular*** quotient of $H^1(F_\lambda, B)$ is

$$H^1_s(F_\lambda, B) = H^1(I_\lambda, B)^{I_\lambda},$$

where I_λ denotes the inertia subgroup of G_{F_λ}.

Similarly, we define the ***finite*** part of $H^1(F_\lambda, B)$ to be

$$H^1_f(F_\lambda, B) = \ker\left(H^1(F_\lambda, B) \to H^1_s(F_\lambda, B)\right).$$

The following lemma provides a simple method to compute the finite part in terms of coinvariants of B.

Lemma V.6. [33, Lemma B.2.8]

Let $\mathrm{Frob}_\lambda \in \mathrm{Gal}(F_\lambda^{nr}/F_\lambda)$ *denote the Frobenius automorphism. For any* $\mathbf{Z}_p[G_{F_\lambda}]$*-module that is a discrete torsion* $\mathbf{Z}_p$*-module, we have*

$$H^1_f(F_\lambda, B) \cong B^{I_\lambda}/(\mathrm{Frob}_\lambda - 1)B^{I_\lambda}.$$

Proof. It follows from the inflation-restriction sequence that

$$H^1_f(F_\lambda, B) \cong H^1(F_\lambda^{ur}/F_\lambda, B^{I_\lambda}). \tag{5.3}$$

Since $\mathrm{Gal}(F_\lambda^{ur}/F_\lambda)$ is pro-cyclic with topological generator Frob_λ, one can check easily that evaluating a cocycle at Frob_λ gives rise to the isomorphism

$$H^1(F_\lambda^{ur}/F_\lambda, B^{I_\lambda}) \cong B^{I_\lambda}/(\mathrm{Frob}_\lambda - 1)B^{I_\lambda}.$$

□

We now consider the case where $(\rho, V) = (\rho_f, T_p(E) \otimes \mathbf{Q})$ is the representation considered above. Then, using our notation above, we can let $T = T_p(E)$, $\pi = p$, and $T_\pi \cong V_f$. Let Frob_q denote the Frobenius element of $\mathrm{Gal}(\mathbf{Q}_q^{nr}/\mathbf{Q}_q) \cong \mathrm{Gal}(\overline{\mathbf{F}_q}/\mathbf{F}_q)$, so Frob_q^2 is the corresponding Frobenius element for $\mathrm{Gal}(K_q^{nr}/K_q) \cong \mathrm{Gal}(\overline{\mathbf{F}_q}/\mathbf{F}_{q^2})$.

Lemma V.7. *Let q be a level raising prime for $\overline{\rho_f}$ such that q is inert in K. Then*

$$H^1_f(K_q, V_f) \cong \begin{cases} k & \text{if } q \text{ admissible} \\ k \oplus k & \text{if } q \text{ Kolyvagin} \\ k & \text{if } q \text{ residual and } \overline{\rho_f}(\mathrm{Frob}_q) \neq \pm 1 \\ k \oplus k & \text{if } q \text{ residual and } \overline{\rho_f}(\mathrm{Frob}_q) = \pm 1. \end{cases}$$

Proof. By Assumption V.2, $\overline{\rho_f}$ is unramified at q. Hence there is a filtration

$$0 \subset k(1) \subset V_f, \tag{5.4}$$

with $V_f/k(1) \cong k$.

If q is admissible, so $p \nmid (q^2 - 1)$, then k and $k(1)$ have distinct Galois actions, so there is a canonical decomposition

$$V_f \cong k \oplus k(1) \tag{5.5}$$

as G_{K_q}-modules. Hence

$$\begin{aligned} H^1_f(K_q, V_f) &\cong H^1_f(K_q, k) \oplus H^1_f(K_q, k(1)) \\ &\cong k \oplus 0 \qquad\qquad \text{by Lemma } V.6 \\ &\cong k. \end{aligned}$$

If q is Kolyvagin, then the characteristic polynomial of Frob_q acting on V_f is

$$x^2 - a_q(f)x + q \equiv x^2 - 1 \pmod{p}. \tag{5.6}$$

Hence V_f decomposes as

$$V_f \cong k_+ \oplus k_- \tag{5.7}$$

where $k_\pm$ denotes the ±1-eigenspaces of V_f for the action of Frob_q. Using a similar computation as above, we obtain

$$H^1_f(K_q, V_f) \cong H^1_f(K_q, k_+) \oplus H^1_f(K_q, k_-) \cong k \oplus k.$$

Finally, if q is residual, then the characteristic polynomial of Frob_q on V_f is

$$x^2 - a_q(f)x + q \equiv (x - \varepsilon)^2 \pmod{p}, \tag{5.8}$$

where $\varepsilon = \pm1$ is such that $p \mid (q + 1 - \varepsilon a_q(f))$. Hence

$$\overline{\rho_f}(\mathrm{Frob}_q) = \begin{pmatrix} \varepsilon & * \\ 0 & \varepsilon \end{pmatrix}. \tag{5.9}$$

Using Lemma V.6, we see that $H^1_f(K_q, V_f)$ is isomorphic to k if and only $\overline{\rho_f}(\mathrm{Frob}_q) \neq \pm1$, and is isomorphic to k^2 otherwise. □

For any isogeny $\psi : E' \to E$ of defined over K_q, one has the local Kummer map

$$\frac{E(K_q)}{\psi(E'(K_q))} \hookrightarrow H^1(K_q, \ker(\psi)). \tag{5.10}$$

If ψ is of degree prime to q, then $\ker(\psi)$ is unramified at q and the image of the Kummer map is precisely the finite part of $H^1(K_q, \ker(\psi))$. That is,

$$\frac{E(K_q)}{\psi(E'(K_q))} \xrightarrow{\sim} H^1_f(K_q, \ker(\psi)) \subset H^1(K_q, \ker(\psi)). \tag{5.11}$$

In this case, the map (5.11) can be described explicitly. Let $P \in E(K_q)$ and let $Q \in E'(\overline{K_q})$ such that $\psi(Q) = P$. Then the image of P is the cocycle

$$\sigma \mapsto (\sigma - 1)Q \in H^1(K_q, \ker(\psi)), \tag{5.12}$$

noting that the cocycle does not depend on the choice of Q. The identification

$$H^1_f(K_q, \ker(\psi)) \cong \frac{\ker(\psi)}{(\mathrm{Frob}_q^2 - 1)\ker(\psi)}$$

of Lemma V.6 sends a cocycle to its evaluation on a topological generator, thus (5.11) can be written

$$P \mapsto (\mathrm{Frob}_q^2 - 1)Q. \tag{5.13}$$

Let $W = k(1) \subset V_f$ be the subspace in the filtration (5.4). Let $E_W = E/W$ and

$$\phi : E_W \to E \tag{5.14}$$

be the dual of the natural isogeny $E \to E_W$. Both W and its Cartier dual $W^\vee \cong \ker(\phi)$ are finite flat group schemes defined over K_q, hence ϕ and its dual are similarly defined over K_q. There is a commutative diagram

$$\begin{tikzcd} \frac{E(K_q)}{pE(K_q)} \arrow[r, two heads] \arrow[d, "\wr"] & \frac{E(K_q)}{\phi(E_W(K_q))} \arrow[d, "\wr"] \\ H^1_f(K_q, V_f) \arrow[r, two heads] & H^1_f(K_q, k), \end{tikzcd} \tag{5.15}$$

noting that the Weil pairing shows that $W^\vee$ is constant and isomorphic to k over K_q.

Since ϕ and $[p]$ have degree prime to q, we may use Proposition V.5 to rewrite the above diagram as

$$\begin{tikzcd}
\frac{E(\mathbf{F}_{q^2})}{pE(\mathbf{F}_{q^2})} \arrow[r, two heads] \arrow[d, "\wr"] & \frac{E(\mathbf{F}_{q^2})}{\phi(E_W(\mathbf{F}_{q^2}))} \arrow[d, "\wr"] \\
H^1_f(K_q, V_f) \arrow[r, two heads] & H^1_f(K_q, k).
\end{tikzcd} \tag{5.16}$$

Remark V.8. We note that since V_f is unramified at p, (5.3) gives a canonical identification

$$H^1_f(K_q, W) \cong H^1(\mathbf{F}_{q^2}, W). \tag{5.17}$$

for any G_{K_q}-submodule $W \subset V_f$. As a consequence, one may think of Proposition V.5 as giving a canonical identification of the Kummer map over K_q and the analogous map on the reduced curve. In particular, we could have written (5.16) purely in terms of the geometry of the reduction $E/\mathbf{F}_{q^2}$.

When V_f is decomposable, we can actually say something stronger.

Lemma V.9. *If V_f admits a decomposition of G_{K_q}-modules*

$$V_f \cong W_1 \oplus W_2, \tag{5.18}$$

then, for $i = 1, 2$, let $E_i = E/W_i$ and $\phi_i : E_i \to E$ be the isogenies defined similarly to the above. Then there is a commutative diagram

$$\begin{tikzcd}
\frac{E(\mathbf{F}_{q^2})}{pE(\mathbf{F}_{q^2})} \arrow[r, "\sim"] \arrow[d, "\wr"] & \frac{E(\mathbf{F}_{q^2})}{\phi_1(E_1(\mathbf{F}_{q^2}))} \oplus \frac{E(\mathbf{F}_{q^2})}{\phi_2(E_2(\mathbf{F}_{q^2})} \arrow[d, "\wr"] \\
H^1_f(K_q, V_f) \arrow[r, "\sim"] & H^1_f(K_q, W_1^\vee) \oplus H^1_f(K_q, W_2^\vee)
\end{tikzcd} \tag{5.19}$$

Proof. The top row is the only map that is not obviously an isomorphism. It is enough to show

$$\phi_1(E_1(\mathbf{F}_{q^2})) \cap \phi_2(E_2(\mathbf{F}_{q^2})) \subset pE(\mathbf{F}_{q^2}),$$

but this is an immediate consequence of $E \xrightarrow{[p]} E$ being the pullback of the two covers $E_i \to E$. □

5.3 The main theorem

Let $\varepsilon = \pm 1$ be the value such that

$$p \mid (q + 1 - \varepsilon a_q(f)). \tag{5.20}$$

Let $g \in S_2(\Gamma_0(Nq))$ be the level-raised form of Theorem IV.2 satisfying

$$a_\ell(g) \equiv a_\ell(f) \pmod{\mathfrak{P}} \text{ for } \ell \nmid q, \qquad a_q(g) = \varepsilon. \tag{5.21}$$

We note that there is a unique choice of ε if $p \nmid (q+1)$. If $p \mid (q+1)$, so q is Kolyvagin, then each choice of sign gives rise to a different level-raised form.

Let W_ε be the maximal G_{K_q}-submodule of V_f whose Cartier dual is constant over K_q and such that Frob_q acts on $W_\varepsilon^\vee$ by ε. Let $E_{W_\varepsilon} := E/W_\varepsilon$ and $\phi : E_{W_\varepsilon} \to E$ be the dual of the natural isogeny $E \to E_{W_\varepsilon}$, as in (5.14).

Explicitly, if q is admissible or is residual and $\overline{\rho_f}(\mathrm{Frob}_q) \neq \pm 1$, then W_ε is the subspace $k(1)$ of (5.4). If q is Kolyvagin, then W_ε is the $-\varepsilon$-eigenspace of V_f. Finally, if q is residual and $\overline{\rho_f}(\mathrm{Frob}_q) = \varepsilon$, then $W_\varepsilon = V_f$.

The Kummer map for the reduced isogeny $\widetilde{\phi}$ over $\mathbf{F}_{q^2}$ is best understood via geometric class field theory, particularly using the method of Frobenius substitution (cf. [34], [39]). Since $W_\varepsilon^\vee$ is constant over $\mathbf{F}_{q^2}$, the map $\widetilde{\phi}$ is Galois with group $W_\varepsilon^\vee$. Hence Frobenius substitution gives a map

$$E(\mathbf{F}_{q^2}) \longrightarrow W_\varepsilon^\vee. \tag{5.22}$$

This map can be viewed as the "reduced" Kummer map in light of Remark V.8.

By pulling (5.22) back along the modular parametrization $\pi : X_0(N) \to E$, we get a map

$$X_0(N)(\mathbf{F}_{q^2}) \to W_\varepsilon^\vee.$$

As discussed at the beginning of the chapter, let $\Sigma \subset X_0(N)(\mathbf{F}_{q^2})$ denote the points on the modular curve arising from supersingular elliptic curves. Restricting the above map to Σ and extending linearly, we obtain a map

$$F : \mathbf{Z}[\Sigma] \to W_\varepsilon^\vee.$$

Remark V.10. We emphasize that, by construction, the evaluation of (5.22) on a point of E in the image of Σ under the modular parametrization agrees with the evaluation of F on any point in its preimage under π.

Before we discuss this further, we must briefly recall some basic results of geometric class field theory.

Theorem V.11 ([40, Thm 1.17])**.**
Let X be a smooth projective curve over a finite field $\mathbf{F}$. Then there is a bijective correspondence between geometrically connected Galois covers of X and finite $\mathbf{F}$-rational subgroup schemes of $\mathrm{Jac}(X)(\overline{\mathbf{F}})$ whose Cartier duals are constant.

Under this correspondence, pullback of a finite Galois cover along a nonconstant map of curves can be described in terms of the above theorem. Let $X_1 \to X_2$ be a nonconstant map of curves and let $X_2' \to X_2$ be a finite connected Galois cover. Then the above theorem gives a subgroup scheme $Z \subset \mathrm{Jac}(X_2)$ that corresponds to this cover. Then the pullback, X_1', of the cover to X_1 corresponds to the image of Z under the natural map $\mathrm{Jac}(X_2) \to \mathrm{Jac}(X_1)$ induced from Picard functoriality. Under this construction, X_1' is connected if and only if $Z \cap \ker(\mathrm{Jac}(X_2) \to \mathrm{Jac}(X_1)) = 0$.

We can define a cover X_ε of $X_0(N)$ by pulling back the cover $E_{W_\varepsilon} \to E$ along the modular parametrization. X_ε is only well-defined up to fixing an embedding $X_0(N) \to J_0(N)$, so we take the natural embedding $P \mapsto (P) - (\infty)$, where ∞ is the cusp at infinity on $X_0(N)$. Then $X_\varepsilon \to X_0(N)$ is a Galois cover with $\mathrm{Gal}(X_\varepsilon/X_0(N))$

canonically isomorphic to $\mathrm{Gal}(E_{W_\varepsilon}/E) \cong W_\varepsilon^\vee$. Moreover, X_ε is connected since E is the optimal quotient associated to f.

By functoriality, it follows immediately that using the Frobenius reciprocity map from the cover $X_\varepsilon/X_0(N)$ gives the same map $\mathbf{Z}[\Sigma] \to W_\varepsilon^\vee$ as the cover E_{W_ε}/E.

In order to apply the mod p multiplicity results of Mazur and Ribet, we must first verify the Hecke equivariance of the map F. Let $\mathbf{T}(N)$ denote the Hecke algebra (of level N), and let T_ℓ denote the ℓ^{th} Hecke operator for each rational prime ℓ.

Proposition V.12. *Let $P \in X_0(N)(\mathbf{F}_{q^2})$. The map F satisfies the following properties:*

1. *For any Hecke operator T_ℓ with $(\ell, q) = 1$, one has*

$$F(T_\ell P) = t_\ell F(P),$$

   where t_ℓ denotes the image of T_ℓ in $\mathbf{T}/\mathfrak{m} \cong k$.

2. *F commutes with the action of the Frobenius element* Frob_q. *Explicitly,*

$$F(\mathrm{Frob}_q P) = \mathrm{Frob}_q F(P) = \varepsilon F(P).$$

3. *F is surjective.*

Proof. The first two statements follow from the explicit description (5.13) of the map F and the fact that T_ℓ and ϕ are defined over $\mathbf{F}_q$, respectively (cf. [39, Lemma 6.13]).

For the last, we need to use a theorem of Ihara [18] that states that the fundamental group of the modular curve $X(N)/\mathbf{F}_{q^2}$ is generated by the Frobenius elements of supersingular points. In particular, let $\Sigma(N) \subset X(N)(\mathbf{F}_{q^2})$ denote the supersingular points on $X(N)(\overline{\mathbf{F}_q})$. Theorem 1 of [18] implies that for any finite connected unramified Galois cover $X \to X(N)$, the corresponding Frobenius reciprocity map, extended linearly and restricted to $\mathbf{Z}[\Sigma(N)]$, is surjective. Let X'_ε denote the pullback of the cover X_ε to $X(N)$. Then X'_ε is an unramified Galois cover of $X(N)$, which is connected if $\ker(J_0(N) \to J(N))$ does not contain an element of order p. But $J_0(N) \to J(N)$ factors as

$$J_0(N) \to J_1(N) \to J(N)$$

and the kernel of the first map is the Shimura subgroup, which p does not divide by assumption, while the second map is known to be injective since $X(N) \to X_1(N)$ is totally ramified at ∞. Hence X'_ε is a connected unramified Galois cover, and so

$$\mathbf{Z}[\Sigma(N)] \to \mathrm{Gal}(X'_\varepsilon/X(N)) \cong \mathrm{Gal}(X_\varepsilon/X_0(N)) \cong W_\varepsilon^\vee \tag{5.23}$$

is surjective. Since the image of $\Sigma(N)$ under the natural map $X(N) \to X_0(N)$ is Σ, the functorial properties of the reciprocity map give the surjectivity of F. □

Let $B = B(q\infty)$ denote the definite quaternion algebra ramified at q and ∞. Since g is new at q, the Jacquet-Langlands correspondence (see Corollary II.25) gives rise to a map

$$\mathrm{Cl}(B) \to F_g \tag{5.24}$$

with an equivariant action of the Hecke algebra $\mathbf{T}(Nq)$ of level Nq factoring through the maximal ideal $\mathfrak{m}_g$ associated to g modulo $\mathfrak{P}$. As in Chapter III, we normalize ψ so that the image is $\mathfrak{P}$-adically integral and contains a $\mathfrak{P}$-adic unit. Let $\overline{\psi}$ be the reduction of ψ modulo $\mathfrak{P}$.

Proposition V.13. *Let $\widetilde{P_K}$ denote the reduction of the Heegner point P_K modulo q. Let x_K be the image of the definite Heegner point 3.5 in* $\mathrm{Cl}(B)$*. If q is not residual or $\overline{\rho_f}(\mathrm{Frob}_q) \neq \pm 1$, then*

$$F(\widetilde{P_K}) = \overline{\psi}(x_K)$$

up to a unit in k.

Proof. Let $X = \mathbf{Z}[\Sigma]^0 \cong \mathbf{Z}[\mathrm{Cl}(B)]^0$, where the isomorphism is given by Proposition IV.1. In order to apply Proposition IV.4, we need to show that $\mathbf{T}(Nq)$, rather than $\mathbf{T}(N)$, acts compatibly on F. For Hecke operators $T_\ell \in \mathbf{T}(Nq)$ with $(\ell, q) \neq 1$, the action of T_ℓ is induced from the action of the corresponding Hecke operator in $\mathbf{T}(N)$ (cf. p. 444-445 of [30]). By [30, Prop. 3.8], the q^{th} Hecke operator T_q of $\mathbf{T}(Nq)$ acts on a point of X by Frob_q, hence

$$F(T_q x) = F(\mathrm{Frob}_q x)$$

for all $x \in X$. It follows from Proposition V.12 that the restriction of F to the degree 0 divisors factors through $X/\mathfrak{m}_g X$. Since g is not Eisenstein modulo $\mathfrak{P}$ (equivalently, $\mathfrak{m}_g$ is not Eisenstein), we have an isomorphism

$$\frac{\mathbf{Z}[\Sigma]}{\mathfrak{m}_g \mathbf{Z}[\Sigma]} \cong \frac{\mathbf{Z}[\Sigma]^0}{\mathfrak{m}_g \mathbf{Z}[\Sigma]^0} = X/\mathfrak{m}_g X.$$

Hence F factors as

$$\begin{tikzcd}
\mathbf{Z}[\Sigma] \arrow[r] \arrow[d, two heads] & W_\varepsilon^\vee \\
\frac{\mathbf{Z}[\Sigma]}{\mathfrak{m}_g \mathbf{Z}[\Sigma]} \arrow[r, "\sim"] & X/\mathfrak{m}_g X \arrow[u, two heads]
\end{tikzcd} \tag{5.25}$$

$\overline{\psi}$ similarly factors through $X/\mathfrak{m}_g X$ as in (5.25). Then $W_\varepsilon^\vee$ is constant over $\mathbf{F}_{q^2}$, and by the assumption that either q is not residual or $\overline{\rho_f}(\mathrm{Frob}_q) \neq \pm 1$, we have an isomorphism $W_\varepsilon^\vee \cong k$ over $\mathbf{F}_{q^2}$. Fix such an isomorphism. Then, as F and $\overline{\psi}$ factor through the $\mathfrak{m}_g$-isotypic part of the degree 0 divisors, Proposition IV.4 implies that F and $\overline{\psi}$ must be nonzero multiples of one another.

Let P be a Heegner point of conductor 1 for K on $X_0(N)$. Recall that P_K is defined as

$$P_K = \sum_{\sigma \in \mathrm{Gal}(H/K)} P^\sigma.$$

The reduction of P modulo q gives rise to a definite Heegner point on B of conductor 1 as in Section 4.1. Let $\overline{P}$ be the image of the definite Heegner point under the map (3.6). Both P and $\overline{P}$ admit an action of $\mathrm{Gal}(H/K)$, the first being the natural Galois action and the latter being the action on the definite Heegner points as a principal homogeneous space. These actions are equivariant with respect to the reduction map by [3, Lemma 4.2], and so extending linearly, the reduction of P_K corresponds to the image of the definite Heegner point x_K of (3.5). In particular, up to a unit in k, we have

$$\begin{aligned} F(\widetilde{P_K}) &= F\left(\sum_{\sigma \in \mathrm{Gal}(H/K)} \widetilde{P}^{\sigma}\right) \\ &= \overline{\psi}\left(\sum_{\sigma \in \mathrm{Gal}(H/K)} \overline{P}^{\sigma}\right) \\ &= \overline{\psi}(x_K). \end{aligned}$$

□

Recall that $\overline{\psi}(x_K)$ is nonzero if and only if $L^{alg}(g/K, 1) \equiv 0 \pmod{\mathfrak{P}}$ by Lemma III.14. On the other hand, recall that F is defined as the mod p Kummer map (5.22). Since $W_\varepsilon^\vee$ is constant over $\mathbf{F}_{q^2}$ and of the same dimension as $H^1_f(K_q, W_\varepsilon^\vee)$, we may fix an isomorphism

$$H^1_f(K_q, W_\varepsilon^\vee) \cong W_\varepsilon^\vee$$

of k-modules. In particular, we have a commutative diagram

$$\begin{tikzcd} \mathbf{Z}[\Sigma] \arrow[r] \arrow[d, two heads, "F"] & \frac{E(\mathbf{F}_{q^2})}{\phi_{W_\varepsilon}(E_{W_\varepsilon}(\mathbf{F}_{q^2}))} \arrow[d, "\wr"] \\ W_\varepsilon^\vee \arrow[r, "\sim"] & H^1_f(K_q, W_\varepsilon^\vee) \end{tikzcd} \tag{5.26}$$

Then from the above we see that $F(\widetilde{P_K})$ is nonzero if and only if $\widetilde{P_K}$ is nonzero in $H^1(\mathbf{F}_{q^2}, W_\varepsilon^\vee)$. But by (5.16) and Remark V.8, this happens if and only if the image of $\widetilde{\pi(P_K)}$ is zero in

$$\frac{E(\mathbf{F}_{q^2})}{\phi(E_{W_\varepsilon}(\mathbf{F}_{q^2}))}.$$

Remark V.14. The following diagram may be helpful to summarize much of the above.

$$\begin{tikzcd}
 & & P_K \arrow[d, mapsto] & \in & J_0(N)(K_q) \arrow[r] \arrow[d] & \frac{E(K_q)}{pE(K_q)} \arrow[r, "\sim"] \arrow[d, two heads] & H^1_f(K_q, E[p]) \arrow[d, two heads] \\
 & & P_K \arrow[dll, mapsto] & \in & J_0(N)(K_q) \arrow[r] \arrow[d] & \frac{E(K_q)}{\phi(E_{W_\varepsilon}(K_q))} \arrow[r, "\sim"] \arrow[d, "\wr"] & H^1_f(K_q, W_\varepsilon^\vee) \arrow[d, "\wr"] \\
\widetilde{P_K} & \in & \mathbf{Z}[\Sigma] \arrow[rr, hook] \arrow[rrrr, bend right, "F"'] & & J_0(N)(\mathbf{F}_{q^2}) \arrow[r] & \frac{E(\mathbf{F}_{q^2})}{\phi(E_{W_\varepsilon}(\mathbf{F}_{q^2}))} \arrow[r, "\sim"] & H^1(\mathbf{F}_{q^2}, W_\varepsilon^\vee)
\end{tikzcd}$$

If $p \nmid q+1$, then our choice of W_ε gives that all vertical maps in the two rightmost columns are isomorphisms. If $p \mid q+1$, then there are two such maps F depending on the choice of ε, and may decompose the diagram in terms of direct sums as in the decomposition (5.7).

We are now prepared to state and prove the main result. To maximize readability we break it into three pieces, each corresponding to one class of primes in the trichotomy of level-raising primes introduced in Definition V.4. For the rest of the thesis, let $X = \mathbf{Z}[\Sigma]^0 \cong \mathbf{Z}[\mathrm{Cl}(B)]^0$ be as in the proof of Proposition V.13.

Theorem V.15. (Jochnowitz congruence, admissible case)
Let q be an admissible prime relative to (f, K, p) and let g be a level-raised form at q. Then P_K is locally divisible by p in $E(K_q)$ if and only if $L^{alg}(g/K, 1) \equiv 0 \pmod{\mathfrak{P}}$.

Proof. Applying the procedure above gives rise to a map

$$F : X \to k$$

that realizes the right vertical map of (5.16). Since q is admissible, $H^1_f(K_q, V_f) \cong k$ by Lemma V.7, and so all arrows in (5.16) are isomorphisms. Since $F(\widetilde{P_K}) = 0$ if and only if $P_K \in pE(K_q)$ and $L^{alg}(g/K, 1) \equiv 0 \pmod{\mathfrak{P}}$ if and only if $\overline{\psi}(x_K)) = 0$, the result follows from Proposition V.13. □

Theorem V.16. (Jochnowitz congruence, Kolyvagin case)
Let q be a Kolyvagin prime relative to (f, K, p). Let $\varepsilon = \pm 1$ be such that the sign of $E/\mathbf{Q}$ is $-\varepsilon$. Let g be a level-raised form at q whose Hecke eigenvalue at q is ε. Then P_K is locally divisible by p in $E(K_q)$ if and only if $L^{alg}(g/K, 1) \equiv 0 \pmod{\mathfrak{P}}$.

Proof. Recall that f has two distinct level-raised forms of level Nq when q is Kolyvagin. Let $g_\pm \in \mathcal{S}_2(\Gamma_0(Nq))^{q-\text{new}}$ be two level-raised forms whose Hecke eigenvalues at q are ± 1, respectively. Let

$$V_f = k_+ \oplus k_-$$

be the decomposition into ± 1-eigenspaces. Then applying the procedure of this section for each of the two subspaces $k_\pm$ gives rise to two distinct maps

$$F_\pm : X \to H^1_f(K_q, k_\mp).$$

We note that we are using the natural isomorphism $k_\pm^\vee \cong k_\mp$ over $\mathbf{Q}_q$ induced by the autoduality of V_f under the Weil pairing. Let $E_\pm = E/k_\pm$ and let $\phi_\pm : E_\pm \to E$ be the corresponding isogenies. Then Lemma V.9 gives the diagram

$$\begin{tikzcd}
\frac{E(\mathbf{F}_{q^2})}{pE(\mathbf{F}_{q^2})} \arrow[r, "\sim"] \arrow[d, "\wr"] & \frac{E(\mathbf{F}_{q^2})}{\phi_+(E_+(\mathbf{F}_{q^2}))} \oplus \frac{E(\mathbf{F}_{q^2})}{\phi_-(E_-(\mathbf{F}_{q^2})} \arrow[d, "\wr"] \\
H^1_f(K_q, V_f) \arrow[r, "\sim"] & H^1_f(K_q, k_-) \oplus H^1_f(K_q, k_+)
\end{tikzcd} \tag{5.27}$$

where the right vertical map is essentially determined by $F_- \oplus F_+$ in light of (5.26). Proposition V.13 then implies that $F_\pm(\widetilde{P_K}) = 0$ if and only if $L^{alg}(g_+/K, 1) \equiv L^{alg}(g_-/K, 1) \equiv 0 \pmod{\mathfrak{P}}$. The result then follows from the following lemma:

Lemma V.17. $L^{alg}(g_{-\varepsilon}/K, 1) \equiv 0 \pmod{\mathfrak{P}}$.

Proof. (Proof of the lemma)

By the work of Kolyvagin [23], the Heegner point lies in the ε-eigenspace of $E(K) \otimes \mathbf{Z}/p\mathbf{Z}$ for the action of complex conjugation. Since q is Kolyvagin, Frob_q lies in the conjugacy class of complex conjugation, and hence Frob_q acts on the image of P_K in $E(K) \otimes \mathbf{Z}/p\mathbf{Z}$ by ε.

In particular, again recalling that F factors through $\mathfrak{m}_g \ni p$, we have

$$\begin{aligned} F_{-\varepsilon}(\widetilde{P_K}) &= F_{-\varepsilon}(\varepsilon \mathrm{Frob}_q(\widetilde{P_K})) \\ &= \mathrm{Frob}_q \cdot F_{-\varepsilon}(\varepsilon \widetilde{P_K}) \quad \text{by Prop. } V.12 \\ &= -\varepsilon F_{-\varepsilon}(\varepsilon \widetilde{P_K}) \\ &= -\varepsilon^2 F_{-\varepsilon}(\widetilde{P_K}) \\ &= -F_{-\varepsilon}(\widetilde{P_K}). \end{aligned}$$

Since p is odd, this forces $F_{-\varepsilon}(\widetilde{P_K})$ to vanish. Then $L^{alg}(g_{-\varepsilon}/K, 1) \equiv 0 \pmod{\mathfrak{P}}$ by Prop. V.13.

□

Theorem V.18. (Jochnowitz congruence, residual case)

Let q be a residual prime relative to (f, K, p) and let g be a level-raised form at q. Then P_K is locally divisible by p in $E(K_q)$ only if $L^{alg}(g/K, 1) \equiv 0 \pmod{\mathfrak{P}}$. If $\overline{\rho_f}(\mathrm{Frob}_q) \neq \pm 1$, then the converse holds as well.

Proof. If $\overline{\rho_f}(\mathrm{Frob}_q) \neq \pm 1$, then the result follows from an argument identical to that of Theorem V.15.

Assume that q is residual and $\overline{\rho_f}(\mathrm{Frob}_q) = \pm 1$. In this setting, since g comes from level raising a newform at level prime to q, the mod $\mathfrak{P}$ representation $\overline{\rho_g}$ is equivalent to $\overline{\rho_f}$ and thus is unramified at q. Hence Proposition IV.4 implies that $X/\mathfrak{m}_g X$ is 2-dimensional over k. In particular, there are $\#k+1$ distinct nonzero maps

$$X/\mathfrak{m}_g X \to k$$

up to multiplication by a scalar. Since V_f is constant over K_q, applying the procedure above with $W_\varepsilon = V_f$ gives a surjective map

$$F : X/\mathfrak{m}_g X \twoheadrightarrow V_f \cong k^2. \tag{5.28}$$

For any one-dimensional subspaces $W \subset V_f$ (noting again that W is constant over K_q and stable under Frob_q and the action of the Hecke algebra), we can apply the process to W to obtain a surjective map

$$F_W : X/\mathfrak{m}_g X \twoheadrightarrow W \cong k. \tag{5.29}$$

Moreover, for any two distinct such subspaces W_1 and W_2, F_{W_1} and F_{W_2} cannot be scalar multiples of one another by Lemma V.9, as this would contradict the surjectivity of (5.28). Since there are $\#k+1$ distinct one-dimensional subspaces of V_f, it follows that any nonzero map $X/\mathfrak{m}_g X \to k$ must be a constant multiple of the map F_W for some one dimensional subspace $W \subset V_f$. Hence $\overline{\psi}$ is, up to unit, equal to F_W for some W. In particular, $L^{alg}(g/K,1) \neq 0 \pmod{\mathfrak{P}}$ if and only if the image of the reduction of the Heegner point under F_W is nonzero. But by (5.16), we see that $F_W(\widetilde{P_K}) \neq 0$ implies that P_K is indivisible by p in $E(K_q)$. □

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] A. Berti, M. Bertolini, and R. Venerucci. Congruences between modular forms and the Birch and Swinnerton-Dyer conjecture. In *Elliptic curves, modular forms and Iwasawa theory*, volume 188 of *Springer Proc. Math. Stat.*, pages 1–31. Springer, Cham, 2016.

[2] M. Bertolini and H. Darmon. Heegner points on Mumford-Tate curves. *Inventiones Mathematicae*, 126(3):413–456, 1996.

[3] M. Bertolini and H. Darmon. A rigid analytic Gross-Zagier formula and artihmetic applications. *Annals of Mathematics. Second Series*, 146(1):111–147, 1997. With an appendix by Bas Edixhoven.

[4] M. Bertolini and H. Darmon. Euler Systems and Jochnowitz Congruences. *American Journal of Mathematics*, 121(2):259–281, 1999.

[5] M. Bertolini and H. Darmon. Iwasawa's Main Conjecture for elliptic curves over anticyclotomic $\mathbf{Z}_p$-extensions. *Annals of Mathematics*, 162(1):1–64, 2005.

[6] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *Journal of the American Mathematical Society*, 14(4):843–939, 2001.

[7] H. Daghigh. *Modular forms, quaternion algebras, and special values of L-functions.* PhD thesis, McGill University, 1997.

[8] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, volume 349 of *Lecture Notes in Math.*, pages 143–316. Springer, Berlin, 1973.

[9] F. Diamond and J. Im. Modular forms and modular curves. *CMS Conf. Proc.*, 17(Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994)):39–133, 1995.

[10] B. H. Gross. Heights and the special values of L-series. In *Number theory (Montreal, Que., 1985)*, volume 7 of *CMS Conf. Proc.*, pages 115–187. Amer. Math. Soc., Providence, RI, 1987.

[11] B. H. Gross and J. A. Parson. On the local divisibility of Heegner points. In *Number theory, analysis and geometry*, pages 215–241. Springer, New York, 2012.

[12] B. H. Gross and D. B. Zagier. Heegner points and derivatives of L-series. *Inventiones Mathematicae*, 84(2):225–320, 1986.

[13] A. Grothendieck. *Groupes de monodromie en géométrie algébrique, SGA 7 I*, volume 288 of *Lecture Notes in Mathematics.* Springer, Berlin-Heidelberg-New York, 1972.

[14] H. Hida. Modules of congruence of Hecke algebras and L-functions associated with cusp forms. *Amer. J. Math.*, 110(2):323–382, 1988.

[15] H. Hida. *Hilbert Modular Forms and Iwasawa Theory.* Oxford University Press, 2006.

[16] B. Howard. Central derivatives of L-functions in Hida families. *Mathematische Annalen*, 339(4):803–818, 2007.

[17] B. Howard. Twisted Gross-Zagier theorems. *Canada J. Math*, 61(4):828–887, 2009.

[18] Y. Ihara. On modular curves over finite fields. In *Discrete subgroups of Lie groups and applications to moduli.* Oxford University Press, 1975.

[19] H. Jacquet. *Automorphic forms on* GL(2). *Part II.* Lecture Notes in Mathematics, Vol. 278. Springer-Verlag, Berlin-New York, 1972.

[20] N. Jochnowitz. A p-adic conjecture about derivatives of L-series attached to modular forms. *Contemporary Mathematics*, 165:239–263, 1994.

[21] K. Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, (295):ix, 117–290, 2004. Cohomologies p-adiques et applications arithmétiques. III.

[22] N. Koblitz. Congruences for periods of modular forms. *Duke Mathematical Journal*, 54(2):361–373, 1987.

[23] V. A. Kolyvagin. Euler systems. In *The Grothendieck Festschrift, Vol. II*, volume 87 of *Progr. Math.*, pages 435–483. Birkhäuser Boston, Boston, MA, 1990.

[24] B. Mazur. Modular curves and the Eisenstein ideal. *Institut des Hautes Études Scientifiques. Publications Mathématiques*, 47:33–186, 1977.

[25] B. Mazur. On the Arithmetic of Special Values of L Functions. *Inventiones Mathematicae*, 55(3):207–240, 1979.

[26] R. Pollack and T. Weston. On anticyclotomic μ-invariants of modular forms. *Compos. Math.*, 147(5):1353–1381, 2011.

[27] M. Raynaud. Spécialisation du foncteur de Picard. *Institut des Hautes Études Scientifiques. Publications Mathématiques*, 38:27–76, 1970.

[28] K. A. Ribet. Congruence relations between modular forms. *Proceedings of the International Congress of Mathematicians*, 1(2):503–514, 1983.

[29] K. A. Ribet. Multiplicities of Galois representations in Jacobians of Shimura curves. *Israel Math. Conf. Proc*, 3:221–236, 1990.

[30] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Inventiones mathematicae*, 100:431–476, 1990.

[31] K. A. Ribet. Raising the levels of modular representations. In *Séminaire de Théorie des Nombres, Paris 1987–88*, volume 81 of *Progr. Math.*, pages 259–271. Birkhäuser Boston, Boston, MA, 1990.

[32] D. E. Rohrlich. Variation of the root number in families of elliptic curves. *Compositio Mathematica*, 87(2):119–151, 1993.

[33] K. Rubin. *Euler Systems*, volume 147 of *Annals of Mathematics Studies.* Princeton University Press, Princeton, NJ, 2000.

[34] J.-P. Serre. *Algebraic groups and class fields*, volume 117 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1988.

[35] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 1 of *Kanô Memorial Lectures.* Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971.

[36] C. Skinner and E. Urban. The Iwasawa main conjectures for GL_2. *Inventiones mathematicae*, 195(1):1–277, 2014.

[37] C. Skinner and W. Zhang. Indivisibility of Heegner points in the multiplicative case. *preprint*, 2014.

[38] R. Taylor and A. Wiles. Ring-Theoretic Properties of Certain Hecke Algebras. *Annals of Mathematics*, 141(3):553, 1995.

[39] V. Vatsal. Special values of anticyclotomic L-functions. *Duke Mathematical Journal*, 116(2):219–261, 2003.

[40] V. Vatsal. Multiplicative subgroups of $J_0(N)$ and applications to elliptic curves. *Journal of the Institute of Mathematics of Jussieu*, 4(2):281–316, 2005.

[41] M.-F. Vignéras. *Arithmétique des algèbres de quaternions*, volume 800. Springer, Berlin, lecture no edition, 1980.

[42] J.-L. Waldspurger. Correspondances de Shimura et quaternions. *Forum Mathematicum*, 3:219–307, 1991.

[43] A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Annals of Mathematics*, 141:443–551, 1995.

[44] W. Zhang. Selmer groups and the indivisibility of Heegner points. *Cambridge Journal of Mathematics*, 2(2):191–253, 2014.