Euler systems and Jochnowitz congruences

M. Bertolini*
H. Darmon†

September 9, 2007

Abstract

This article relates the Gross-Zagier formula with a simpler formula of Gross for special values of L-series, via the theory of congruences between modular forms. Given two modular forms f and g (of different levels) which are congruent but whose functional equations have sign -1 and 1 respectively, and an imaginary quadratic field K satisfying certain auxiliary conditions, the main result gives a congruence between the algebraic part of $L'(f/K, 1)$ (expressed in terms of Heegner points) and the algebraic part of the special value $L(g/K, 1)$. Congruences of this type were anticipated by Jochnowitz, and for this reason are referred to as "Jochnowitz congruences".

1 Introduction

Let E be a modular elliptic curve over $\mathbb{Q}$ of conductor N, and let K be a quadratic imaginary field. The L-function $L(E/K, s)$ has a functional equation of the standard kind relating its values at s and $2 - s$. When all the primes dividing N are split in K, then K is said to satisfy the *Heegner hypothesis* relative to E. In that case the sign in the functional equation of $L(E/K, s)$ is -1. Furthermore, a construction of Birch and Heegner based

*Partially supported by GNSAGA (C.N.R.); M.U.R.S.T., progetto nazionale "Geometria algebrica"; Human Capital and Mobility Programme of the European Community, under contract ERBCH RXCT940557.

†Supported by an NSERC grant, an FCAR "Nouveaux Chercheurs" grant, and an Alfred P. Sloan research award.

on the theory of complex multiplication gives a Heegner point $y_K \in E(K)$ coming from the modular parametrization

$$\pi_E : X_0(N) \longrightarrow E.$$

In fact, the Mordell-Weil group $E(K) \otimes \mathbb{Q}$ decomposes into plus and minus eigenspaces $E(K)^+$ and $E(K)^-$ for the action of complex conjugation, and the point y_K belongs to $E(K)^\epsilon$, where $-\epsilon$ is the sign in the functional equation for $L(E/\mathbb{Q}, s)$.

Much deeper is the result of Gross and Zagier [GZ] which expresses the Néron-Tate canonical height of y_K as a non-zero multiple of $L'(E/K, 1)$. In particular, y_K is of infinite order if and only if $L(E/K, s)$ has a simple zero at $s = 1$.

Later, in [Ko], Kolyvagin showed that if y_K is of infinite order, then the rank of $E(K)$ is equal to one, and the Shafarevich-Tate group $\underline{III}(E/K)$ is finite.

The results of Gross-Zagier and Kolyvagin go a long way toward proving the Birch and Swinnerton-Dyer conjecture for (modular) elliptic curves having analytic rank ≤ 1. In particular they imply:

Theorem 1.1 *Suppose that K satisfies the Heegner hypothesis relative to E. If $L'(E/K, 1) \neq 0$, then E has rank one over K, and $\underline{III}(E/K)$ is finite.*

Suppose now that E has a prime q of multiplicative reduction. A quadratic imaginary field is said to satisfy the *modified Heegner hypothesis* relative to E and q if q is inert in K and all other primes dividing N are split. In that case, the sign in the functional equation for $L(E/K, s)$ is 1, so that $L(E/K, s)$ vanishes to *even* order at $s = 1$. Presumably, one often has $L(E/K, 1) \neq 0$. In harmony with that fact, there is no natural Heegner point construction yielding a point on $E(K)$. But there is a variant of the Heegner point construction, explained in [BD2] or [Ro], yielding (for $n \geq 1$) a family of Heegner points $y_n \in E(L^{(n)})$; here $L^{(n)}$ denotes the ring class field of K of conductor q^n. (It is a cyclic extension of the Hilbert class field of K of degree $\frac{2}{\#\mathcal{O}_K^\times}(q+1)q^{n-1}$, which is totally ramified at the primes above q.)

In [BD2], a q-adic analogue of the Gross-Zagier formula was obtained, relating this time the image of y_n in the group of connected components of $E_{/L^{(n)}}$ at q to the special value $L(E/K, 1)$. By applying Kolyvagin's method in this setting, it was then possible to show:

Theorem 1.2 *Suppose that K satisfies the modified Heegner hypothesis relative to q and E. If $L(E/K,1) \neq 0$, then $E(K)$, and the q-primary part of $\underline{III}(E/K)$, are finite.*

The method of descent can also be made to yield (somewhat weaker) information on the p-primary part of $\underline{III}(E/K)$, where p is a prime dividing $q+1$, but a proof of the finiteness of the entire Shafarevich-Tate group still escapes the methods of [BD2].

The principal goal of this paper is to relate the Gross-Zagier formula and the formula of [BD2] (and, thereby, theorems 1.1 and 1.2) via the theory of congruences between modular forms. In the remainder of the introduction, we will state our main result precisely.

Fix a modular elliptic curve E of conductor N, associated to a normalized cusp form of weight 2 for $\Gamma_0(N)$:

$$f = \sum_n a_n q^n, \quad a_n \in \mathbb{Z}, \quad a_1 = 1.$$

Let $\pi_E^* : E \longrightarrow J_0(N)$ and $\pi_{E*} : J_0(N) \longrightarrow E$ be the maps of Jacobians deduced from π_E by contravariant and covariant functoriality respectively. The map π_E is defined over $\mathbb{Q}$, and hence the same is true for π_{E*} and π_E^*. Assume that E is the strong Weil curve in its isogeny class, and that $\deg(\pi_E)$ is minimal. Since N is assumed to be the conductor of E and f is normalized, E is a strong Weil curve if and only if π_E^* is injective, or also if and only if π_{E*} has connected kernel.

Let K be a quadratic imaginary field satisfying the Heegner hypothesis relative to E.

Fix an auxiliary prime p (which will be the "descent prime", i.e., we will perform a p-descent in all that follows) to satisfy the following conditions:

1. the mod p Galois representation $\bar{\rho}_{E,p}$ associated to E is absolutely irreducible.
2. p does not divide $2N$ and the degree of the modular parametrization π_E.

By a result of Serre [Se], all but finitely many primes p satisfy these two conditions.

Let E_p be the module of p-division points of E, and let $K(E_p)$ be the smallest extension of K over which these points are defined. The prime q is called a *Kolyvagin prime* (relative to E, K and p) if it does not divide

$N\mathrm{Disc}(K)p$ – so that in particular it is unramified in $K(E_p)/\mathbb{Q}$ – and its Frobenius element in this extension belongs to the conjugacy class of complex conjugation. This implies that p divides $q+1$ and a_q. There are infinitely many primes q satisfying this condition, by the Chebotarev density theorem.

Let q be a Kolyvagin prime relative to (E, K, p). Let $X_0(Nq)$ be the modular curve of level Nq, and let $\mathbb{T} = \mathbb{T}(Nq)$ be the Hecke algebra of level Nq, generated by the Hecke operators T_ℓ for $\ell \not| Nq$ and U_ℓ for $\ell | Nq$ acting faithfully on $J_0(Nq)$.

Our goal is to study certain modular forms of level Nq which are congruent to f modulo p. Accordingly, let $\mathfrak{m}$ be the maximal ideal of $\mathbb{T}$ defined by

$$\mathfrak{m} = \langle p, \qquad T_\ell - a_\ell \text{ (where } \ell \not| Nq), \qquad U_\ell - a_\ell \text{ (where } \ell | N), \qquad U_q - \epsilon \rangle .$$

Denote by $\mathbb{T}_\mathfrak{m}$ the completion of the Hecke algebra $\mathbb{T}$ at $\mathfrak{m}$:

$$\mathbb{T}_\mathfrak{m} := \lim_{\leftarrow} \mathbb{T}/\mathfrak{m}^n,$$

and let I be the kernel of the natural map $\mathbb{T} \longrightarrow \mathbb{T}_\mathfrak{m}$. Following [Ma1], ch. II (10.4), associate to $\mathfrak{m}$ a quotient J of $J_0(Nq)$ by the rule:

$$J := J_0(Nq)/I.$$

The abelian variety J is analogous to Mazur's Eisenstein quotient, except that the ideal I of $\mathbb{T}$ in this case corresponds to an absolutely irreducible mod p representation, and is not Eisenstein. (This has the effect of simplifying considerably some of the technical features of the study.)

Section 3 invokes a "raising the level" theorem of Ihara and Ribet to establish the following basic fact about the structure of J:

The abelian variety J is isogenous to $E^2 \times J'$, where J' is a non-trivial abelian variety having purely toric reduction at q. More precisely, J' has split toric reduction if $\epsilon = 1$, and non-split toric reduction if $\epsilon = -1$.

Let g be a normalised eigenform of weight 2 on $\Gamma_0(Nq)$, corresponding to an algebra homomorphism $\phi_g : \mathbb{T} \longrightarrow \mathcal{O}_g$, where $\mathcal{O}_g$ is the ring generated by the Fourier coefficients of g. Let $\mathfrak{m}_g := \phi_g(\mathfrak{m})$. It is a maximal ideal of $\mathcal{O}_g$ (possibly equal to $\mathcal{O}_g$ itself).

The eigenform g is said to be a form on J (resp. J') if the abelian variety A_g associated to g by the Eichler-Shimura construction is a quotient of J

(resp. J'). One can show that g is a form on J' if and only if g is new at q and $\mathfrak{m}_g \neq \mathcal{O}_g$.

A formula of Gross [Gr1] and a generalization of Daghigh [Dag] allows one to define in section 4 the *algebraic part* $\mathbb{L}(g/K,1)$ of the special value $L(g/K,1)$. It can be thought of as (a square root of) the special value $L(g/K,1)$, "divided by the appropriate non-zero period". More precisely, $\mathbb{L}(g/K,1)$ belongs to an $\mathcal{O}_g$-module $\mathcal{M}_g$ (defined in section 4) which is locally free of rank 1 at $\mathfrak{m}_g$, and

$$\mathbb{L}(g/K,1) = 0 \iff L(g/K,1) = 0. \tag{1}$$

Write $\mathbb{L}(g/K,1) = 0 \pmod{\mathfrak{m}_g}$ if $\mathbb{L}(g/K,1)$ belongs to $\mathfrak{m}_g\mathcal{M}_g$.

In section 5 a precise definition of the Heegner point y_K in $E(K)$ is given. Let K_q denote the completion of K at the prime q. The main result, whose proof is the object of section 6, is

Theorem 1.3 *The image of y_K in $E(K_q)/pE(K_q)$ is non-zero if and only if*

$$\mathbb{L}(g/K,1) \neq 0 \pmod{\mathfrak{m}_g},$$

for all forms g on J'.

Since the point y_K encodes the special value of $L'(f/K,1)$ by the Gross-Zagier formula, theorem 1.3 can be viewed as supplying a mod $\mathfrak{m}$ congruence between $L'(f/K,1)$ and $L(g/K,1)$. To even express precisely such a congruence between a special value and a derivative of an L-function requires the machinery of Heegner points and the formula of Gross and Zagier. Congruences of this type were anticipated by Jochnowitz, and for this reason are referred to as "Jochnowitz congruences". The article [J] considered the case of Eisenstein series and of certain modular forms of CM type associated to Hecke L-series, exploiting a formula of Rubin [Ru]. Other instances of this phenomenon, involving congruences at Eisenstein primes, also appear in [Ma2]. Indeed, this work of Mazur is the precursor and one of the main inspirations of the present article.

Let us mention the following corollary of theorem 1.3.

Corollary 1.4 *If the image of y_K in $E(K_q)/pE(K_q)$ is non-zero, then*

$$L(J'/K,1) \neq 0.$$

Proof: By theorem 1.3, $\mathbb{L}(g/K,1) \neq 0 \pmod{\mathfrak{m}_g}$ for all normalised eigenforms g on J'. Hence $\mathbb{L}(g/K,1) \neq 0$, and therefore $L(g/K,1) \neq 0$ by equation (1). But $L(J'/K,1) = \prod_g L(g/K,1)$, where the product is taken over the distinct normalised eigenforms on J'. The result follows.

On the arithmetic side, there is:

Proposition 1.5 *If the image of y_K is non-zero in $E(K_q)/pE(K_q)$, then*

1. *The p-Selmer group of $E(K)$ is one-dimensional over $\mathbb{F}_p$, and is generated by the image of y_K by the connecting homomorphism of Kummer theory.*
2. *The $\mathfrak{m}$-Selmer group of J' is trivial, and hence $J'(K)$ is finite.*

Sketch of Proof: To prove the first part, observe that the hypothesis implies that the image of y_K in $E(K)/pE(K)$ is non zero. The conclusion then follows from a more precise formulation of the theorem of Kolyvagin. (Cf. [Gr2], prop. 2.1). The second part follows from theorem 1.3 and the natural generalization (cf. [BD2]) of theorem 1.2 for eigenforms with non-rational fourier coefficients.

In light of corollary 1.4, part 2 of proposition 1.5 is consistent with the Birch and Swinnerton-Dyer conjecture. This proposition establishes a link (via the theory of congruences between modular forms) between Kolyvagin's descent and the descent of [BD2]. It is worth noting that parts 1 and 2 of proposition 1.5 can be shown to be equivalent, *independently* of any L-function calculation, by a formula for comparing the orders of Selmer groups.

Acknowledgements: The authors would like to thank Fred Diamond and Dino Lorenzini for helpful exchanges related to this paper.

2 Preliminaries

Modular curves:
Let M be a positive integer. If A is an elliptic curve and $C \subset A$ is a cyclic subgroup of order M, then (following Ribet) the pair $\underline{A} := (A, C)$ is called an *enhanced elliptic curve* with $\Gamma_0(M)$-structure. An isogeny between two such enhanced elliptic curves is an isogeny between the underlying curves which induces an isomorphism between the level M structures. The curve $X_0(M)$ is the (coarse) moduli space of enhanced elliptic curves with $\Gamma_0(M)$-structure.

If $M = Nq$ where q is a prime not dividing N, then the modular curve $X_0(M)$ of level Nq can also be viewed as the moduli space for diagrams

$$(\underline{A} \to \underline{A}')$$

where $\underline{A}$ and $\underline{A}'$ are enhanced elliptic curves with $\Gamma_0(N)$-structure, and the arrow is a cyclic q-isogeny between them. The curve $X_0(Nq)$ maps to $X_0(N)$ via the two standard degeneracy maps:

$$\pi_1, \pi_2 : X_0(Nq) \longrightarrow X_0(N),$$

which send the diagram $(\underline{A} \to \underline{A}')$ to $\underline{A}$ and $\underline{A}'$ respectively. The degeneracy maps induce maps between Jacobians by covariant and contravariant functoriality respectively:

$$\pi_{1*}, \pi_{2*} : J_0(Nq) \longrightarrow J_0(N), \qquad \pi_1^*, \pi_2^* : J_0(N) \longrightarrow J_0(Nq).$$

Hecke algebras:
For any $M > 0$, let $\mathbb{T}(M)$ be the full Hecke algebra of level M, i.e., the subring of the endomorphism ring of $J_0(M)$ generated by the Hecke operators T_ℓ with $\ell \nmid M$ and the operators U_ℓ with $\ell | M$. It is a $\mathbb{Z}$-algebra which is finitely generated as a $\mathbb{Z}$-module. For example, the operator T_ℓ acts on $J_0(M)$ via the correspondence on $X_0(M)$:

$$T_\ell(\underline{A}) = \sum_{\underline{A}'} \underline{A}',$$

where the sum is taken over the $\ell + 1$ enhanced elliptic curves which are ℓ-isogenous to $\underline{A}$. The degeneracy maps π_1 and π_2 introduced above satisfy the relations

$$\pi_{1*}\pi_1^* = \pi_{2*}\pi_2^* = q + 1, \qquad \pi_{2*}\pi_1^* = \pi_{1*}\pi_2^* = T_q.$$

The operator U_q acts on $J_0(Nq)$ via the correspondence on $X_0(Nq)$ defined by

$$U_q(\underline{A} \to \underline{B}) = \sum_{\underline{X} \neq \underline{A}} (\underline{B} \to \underline{X}),$$

where the sum is taken over the q distinct cyclic q-isogenies from $\underline{B}$, omitting the dual of $\underline{A} \to \underline{B}$. Define an action of $\mathbb{T} = \mathbb{T}(Nq)$ on $J_0(N)^2$ by letting

T_ℓ and U_ℓ act diagonally on each factor for $\ell \neq q$, and letting U_q act by left multiplication by the matrix $\begin{pmatrix} T_q & q \\ -1 & 0 \end{pmatrix}$. Let

$$\pi_{12}^* : J_0(N)^2 \longrightarrow J_0(Nq), \quad \pi_{12*} : J_0(Nq) \longrightarrow J_0(N)^2$$

be the degeneracy maps formed from the pairs (π_1^*, π_2^*) and (π_{1*}, π_{2*}), and set

$$\tilde{\pi}_{12*} := \begin{pmatrix} 1 & -T_q \\ 0 & 1 \end{pmatrix} \circ \pi_{12*}.$$

Lemma 2.1 *The functions π_{12}^* and $\tilde{\pi}_{12*}$ are compatible with the actions of $\mathbb{T}(Nq)$ on $J_0(Nq)$ and $J_0(N)^2$ defined above.*

Proof: The main point is to check that the maps are compatible with the action of the Hecke operator U_q. From the description of the action of U_q given above, one sees directly that

$$U_q \circ \pi_{12}^* = \pi_{12}^* \circ \begin{pmatrix} T_q & q \\ -1 & 0 \end{pmatrix}, \quad \pi_{12*} \circ U_q = \begin{pmatrix} 0 & q \\ -1 & T_q \end{pmatrix} \pi_{12*}.$$

It follows from this last equation that

$$\tilde{\pi}_{12*} \circ U_q = \begin{pmatrix} T_q & q \\ -1 & 0 \end{pmatrix} \tilde{\pi}_{12*}.$$

Character groups of Jacobians:
Let $\mathcal{J}_0(Nq)$ be the Néron model for $J_0(Nq)$ over $\mathbb{Z}_q$, and let $\mathcal{J}_0(Nq)^0$ be its connected component. The special fiber at q of $\mathcal{J}_0(Nq)^0$ is an extension of the abelian variety $J_0(N) \times J_0(N)$ over $\mathbb{F}_q$ by a torus T. Let $\mathcal{M}$ denote the character group of this torus. It is a free $\mathbb{Z}$-module of finite rank which inherits an action of the Hecke algebra $\mathbb{T}$ from its action on $J_0(Nq)$.

The work of Grothendieck [SGA], Raynaud [Ra], Deligne and Rapoport [DR] provides an explicit description of the $\mathbb{T}$-module $\mathcal{M}$. Here in fact are two equivalent descriptions:

1. The module $\mathcal{M}$ is isomorphic to the group of degree 0 divisors supported on the supersingular points of $X_0(N)_{\bar{\mathbb{F}}_q}$. (Cf. for example [Ri2], prop. 3.1.) In other words, $\mathcal{M}$ consists of the formal degree zero $\mathbb{Z}$-linear combinations $\sum_i n_i \underline{A}_i$, where the $\underline{A}_i$ are enhanced elliptic curves with $\Gamma_0(N)$-structure

defined over $\bar{\mathbb{F}}_q$, which are *supersingular* (in the sense that the underlying elliptic curve is.)

2. Let B be the definite quaternion algebra which is ramified at q and ∞. An Eichler order R in B of level N is said to be *oriented* if it is equipped with a surjective algebra homomorphism $\iota : R \longrightarrow \mathbb{Z}/N\mathbb{Z}$. The set of conjugacy classes of oriented Eichler orders of level N is in natural bijection with the set of supersingular points described in 1. (Cf. [Gr1].) Choose a system of representatives $R_1, \ldots, R_t$ for the conjugacy classes of oriented Eichler orders of level N. Thus each R_j is an Eichler order of level N equipped with an orientation

$$\iota_j : R_j \longrightarrow \mathbb{Z}/N\mathbb{Z}. \tag{2}$$

An element in $\mathcal{M}$ will sometimes be written as a formal $\mathbb{Z}$-linear combination $\sum_j n_j[R_j]$ with $\sum_j n_j = 0$.

The module $\mathcal{M}$ also comes equipped with a natural positive-definite inner product defined by

$$\langle [R_i], [R_j] \rangle := \frac{1}{2}\delta_{ij} \# R_j^{\times}. \tag{3}$$

In other words, $\langle [R_i], [R_j] \rangle$ is the number of isomorphisms between R_i and R_j. The Hecke operators T_ℓ with $\ell \not| N$ are self-adjoint for this inner product. (Cf. for example [Gr1], prop. 4.6).

Component groups of Néron Models:
Let F be a finite extension of $\mathbb{Q}_q$ with ramification index e, and let $\mathcal{J}_0(Nq)_F$ be the Néron model of the Jacobian $J_0(Nq)$ over the ring of integers of F. Denote by $\Phi(J_0(Nq)/F)$ the group of connected components of the special fiber of $\mathcal{J}_0(Nq)_F$. This group can be described canonically as the cokernel of the composition

$$\mathcal{M} \stackrel{e}{\longrightarrow} \mathcal{M} \longrightarrow \mathcal{M}^{\vee},$$

where the first map is multiplication by e and the second is the natural inclusion of $\mathcal{M}$ into $\mathcal{M}^{\vee} := \mathrm{Hom}(\mathcal{M}, \mathbb{Z})$ arising from the pairing $\langle\ ,\ \rangle$. Hence, there is an exact sequence:

$$0 \longrightarrow \mathcal{M} \otimes (\mathbb{Z}/e\mathbb{Z}) \longrightarrow \Phi(J_0(Nq)/F) \longrightarrow \Phi(J_0(Nq)/\mathbb{Q}_q) \longrightarrow 0,$$

where the last map is induced from the norm if $F/\mathbb{Q}_q$ is totally ramified. The group $\Phi(J_0(Nq)/\mathbb{Q}_q)$ is *Eisenstein* in the sense of [Ri2], thm. 3.12. In particular, taking the completion at a non-Eisenstein maximal ideal $\mathfrak{m}$ of the Hecke algebra, one obtains:

Proposition 2.2 *The completion of* $\Phi(J_0(Nq)/F)$ *at a non-Eisenstein ideal* $\mathfrak{m}$ *is isomorphic as a Hecke module to the completion of* $\mathcal{M} \otimes (\mathbb{Z}/e\mathbb{Z})$ *at* $\mathfrak{m}$.

Multiplicity one:
Let $\mathfrak{m}$ be a maximal ideal of the Hecke algebra $\mathbb{T}$ whose residue characteristic is prime to $2Nq(q-1)$, associated to an absolutely irreducible Galois representation. The following multiplicity one theorem of Mazur (cf. [Ri2], th. 6.4) will be crucial in our later study:

Theorem 2.3 *The group* $\mathcal{M}/\mathfrak{m}$ *is a one-dimensional vector space over the field* $\mathbb{T}/\mathfrak{m}\mathbb{T}$. *(And hence, the completion* $\mathcal{M} \otimes_{\mathbb{T}} \mathbb{T}_{\mathfrak{m}}$ *is free of rank one over* $\mathbb{T}_{\mathfrak{m}}$.*)*

3 The abelian variety J

We now turn to a detailed study of the abelian variety J defined in the introduction. In particular, the integers N, p and q satisfy all the assumptions stated there, namely:

1. The quadratic imaginary field K satisfies the Heegner hypothesis relative to E.
2. The mod p representation attached to E is absolutely irreducible and p does not divide $2N$ or $\deg(\pi_E)$.
3. The prime q is a Kolyvagin prime relative to E, K and p.

The ideal $\mathfrak{m}$:
The normalised eigenform f of weight 2 on $\Gamma_0(N)$

$$f = \sum_{n=1}^{\infty} a_n q^n, \qquad a_1 = 1, \quad q = e^{2\pi i \tau},$$

can also be viewed as a modular form on $\Gamma_0(Nq)$, but it is not an eigenform for the Hecke algebra $\mathbb{T} = \mathbb{T}(Nq)$, because it fails to be an eigenform for the Hecke operator U_q. Choose a root α of the polynomial

$$x^2 - a_q x + q,$$

and define the modular form f_q with coefficients in the ring $\mathbb{Z}[\alpha]$ by

$$f_q := f(\tau) - q/\alpha f(q\tau).$$

Its L-function factorizes as the following Euler product:

$$L(f_q, s) = (1 - \alpha q^{-s})^{-1} \prod_{p|N} (1 - a_p p^{-s})^{-1} \prod_{p \not| Nq} (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

The form f_q is an eigenform for $\mathbb{T}$ of level Nq which is in the same old-class as f, and the eigenvalue of U_q acting on it is α. By the assumption that q is a Kolyvagin prime, the eigenvalues of the Frobenius element at q acting on E_p are 1 and -1, i.e.,

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

Since p is odd, it splits in the quadratic imaginary order $\mathbb{Z}[\alpha]$, and is equal to $(p, \alpha - 1)(p, \alpha + 1)$.

Recall that $-\epsilon$ is the sign in the functional equation for $L(E/\mathbb{Q}, s)$. Let $\mathfrak{m}_f$ be the ideal $(p, \alpha - \epsilon)$ of $\mathbb{Z}[\alpha]$, and let $\mathfrak{m}$ be the inverse image of $\mathfrak{m}_f$ in $\mathbb{T}$ for the homomorphism $\mathbb{T} \longrightarrow \mathbb{Z}[\alpha]$ determined by f_q. Specifically, the ideal $\mathfrak{m}$ is equal to

$$\mathfrak{m} = \langle p, \qquad T_\ell - a_\ell \text{ (where } \ell \not| Nq), \qquad U_\ell - a_\ell \text{ (where } \ell | N), \qquad U_q - \epsilon \rangle,$$

as defined in the introduction.

If M is any $\mathbb{T}$-module, denote by

$$M_{\mathfrak{m}} := \lim_{\leftarrow} M/\mathfrak{m}^n M$$

the completion of M at $\mathfrak{m}$. The ideal $\mathfrak{m}$ is said to be in the *support* of M if this completion is non-zero.

The ring $\mathbb{T}_{\mathfrak{m}}$ is a direct factor of the semi-local ring $\mathbb{T} \otimes \mathbb{Z}_p$:

$$\mathbb{T} \otimes \mathbb{Z}_p = \mathbb{T}_{\mathfrak{m}} \times \mathbb{T}', \tag{4}$$

where $(\mathbb{T}')_{\mathfrak{m}} = 0$ (cf. [Ma1], sec. II.7). Let I be the kernel of the natural map $\mathbb{T} \longrightarrow \mathbb{T}_{\mathfrak{m}}$ (so that $\mathbb{T}/\mathrm{Ann}_{\mathbb{T}} I$ injects into $\mathbb{T}'$).

The abelian variety J:
As in the introduction, let

$$J = J_0(Nq)/IJ_0(Nq).$$

If g is any normalised eigenform on $\Gamma_0(Nq)$ and $\mathcal{O}_g$ is the ring generated by its Fourier coefficients, recall that $\phi_g : \mathbb{T} \longrightarrow \mathcal{O}_g$ is the algebra homomorphism

associated to g, and that I_g is its kernel. Following the introduction, we say that g is a form on J if the following three equivalent conditions are satisfied:

1. The abelian variety quotient $A_g := J_0(Nq)/I_g$ associated to g by the Eichler-Shimura construction is a quotient of J. (Note that A_g depends only on the Galois orbit $[g]$ of g.)

2. $I \subset I_g$;

3. The ideal $\mathfrak{m}_g := \phi_g(\mathfrak{m})$ is a maximal ideal of $\mathcal{O}_g$ which is not equal to $\mathcal{O}_g$ itself, and
$$a_n(f_q) \pmod{\mathfrak{m}_f} = a_n(g) \pmod{\mathfrak{m}_g}. \tag{5}$$

The absolute Galois group of $\mathbb{Q}$ acts on the normalised eigenforms via its action on Fourier expansions. If g is any normalised eigenform, let $[g]$ denote its orbit under this action. We may write
$$J \sim \prod_{[g]} A_g,$$
where the symbol $\sim$ denotes isogeny and the product is taken over the distinct Galois orbits of normalised eigenforms g on J. Because of the assumption in the introduction that p does not divide the degree of the modular parametrization π_E, there is only one oldform (up to the Galois action) which is congruent to f_q, namely f_q itself. The ring $\mathcal{O}_{f_q} = \mathbb{T}/I_{f_q}$ is equal to $\mathbb{Z}[\alpha]$. Finally, the abelian variety $A_{f_q} := J_0(Nq)/I_{f_q}$ is isogenous to $E \times E$. Hence, J is isogenous to the abelian variety
$$J \sim E^2 \times \prod_{[g]} A_g, \tag{6}$$
where the product now is taken over the Galois orbits of normalised eigenforms on J which are new at q.

Here is a precise description of such an isogeny. Let $\pi_E^* : E \longrightarrow J_0(N)$ be the map deduced from π_E by contravariant functoriality. It induces a homomorphism $E^2 \longrightarrow J_0(N)^2$, which will also be denoted π_E^* by abuse of notation. Let
$$\varphi_E : E^2 \longrightarrow J \tag{7}$$
be the composition of the maps
$$E^2 \xrightarrow{\pi_E^*} J_0(N)^2 \xrightarrow{\pi_{12}^*} J_0(Nq) \xrightarrow{\pi_J} J. \tag{8}$$

By lemma 2.1, the map φ_E is $\mathbb{T}$-equivariant for the action of $\mathbb{T}$ on E^2 defined by making the Hecke operators T_ℓ for $\ell \not| Nq$ and U_ℓ for $\ell | N$ act by multiplication by a_ℓ, and letting U_q act by left multiplication by the matrix

$$\begin{pmatrix} a_q & q \\ -1 & 0 \end{pmatrix}. \tag{9}$$

Let $J_0'(Nq)$ be the q-new subvariety of $J_0(Nq)$, i.e., the kernel of the map

$$\pi_{12*} : J_0(Nq) \longrightarrow J_0(N)^2.$$

(Note that we may also replace π_{12*} by $\tilde{\pi}_{12*}$ in this definition.) Let J' be the image of $J_0'(Nq)$ in J, and let

$$\varphi' : J' \longrightarrow J$$

be the natural inclusion map. Define an isogeny φ by

$$\varphi := \varphi_E + \varphi' : E^2 \times J' \longrightarrow J.$$

Proposition 3.1 *The abelian variety J' is non-trivial, and has purely multiplicative reduction at q. This reduction is split if $\epsilon = 1$, and is non-split if $\epsilon = -1$.*

Proof: By equation (6),

$$J' \sim \prod_{[g]} A_g,$$

where the product is taken over the Galois orbits of normalised eigenforms of level Nq which are new at q and satisfy $\mathfrak{m}_g \neq \mathcal{O}_g$. Such eigenforms satisfy the congruence

$$a_n(g) \pmod{\mathfrak{m}_g} = a_n(f_q) \pmod{\mathfrak{m}_f} \qquad \text{for all } n.$$

But a raising the level theorem of Ribet [Ri1] states that there exists such an eigenform g if and only if $\alpha \equiv \pm 1 \pmod{\mathfrak{m}_f}$. Furthermore, $a_q(g) = 1$ (resp. -1) if and only if A_g has split (resp. non-split) multiplicative reduction at q. Since $a_q(g) \equiv \epsilon \pmod{\mathfrak{m}_g}$, and since $p \neq 2$, the result follows.

Corollary 3.2 *1. There is an exact sequence*

$$0 \longrightarrow \Lambda \longrightarrow (K_q^\times)^d \longrightarrow J'(K_q) \longrightarrow 0,$$

where Λ is a lattice in $(K_q^\times)^d$, (and d is the dimension of J').

2. Denote by $z \mapsto \bar{z}$ the usual complex conjugation acting on K_q, and make $Gal(K_q/\mathbb{Q}_q) = \langle\tau\rangle$ act on $K_q^\times$ by setting $\tau(z) := \bar{z}^\epsilon$. Then the exact sequence of 1 is $Gal(K_q/\mathbb{Q}_q)$-equivariant.

Lemma 3.3 *The ideal $\mathfrak{m}$ is not in the support of the kernel of φ_E. (In other words, φ_E is "injective at $\mathfrak{m}$".)*

Proof: The map $\pi_E^* : E^2 \longrightarrow J_0(N)^2$ is injective, by our assumption that π_E is the strong Weil parametrization associated to f. The map π_{12}^* has a kernel (related to the *Shimura subgroup* of $J_0(N)$) whose support consists entirely of Eisenstein primes (cf. [Ri1]). Finally, any submodule M of $IJ_0(Nq)(\bar{\mathbb{Q}})$ has support disjoint from $\mathfrak{m}$ by the construction of J. This is because the action of $\mathbb{T} \otimes \mathbb{Z}_p$ on $M \otimes \mathbb{Z}_p$ factors through the ring $\mathbb{T}'$ of equation (4).

If M is any module on which complex conjugation in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts, write M^+ and M^- for the submodules of M on which this involution acts by 1 and -1 respectively.

Lemma 3.4 *Let V denote the kernel of the isogeny φ. Then*

1. *The map $V \longrightarrow E^2$ induced by projection onto the first factor is injective, so that $V_{/K_q}$ extends to a finite flat group scheme over the ring of integers $\mathcal{O}_q$ of K_q.*
2. *The map $V(K_q)_\mathfrak{m}^\epsilon \longrightarrow E^2(K_q)_\mathfrak{m}^\epsilon$ is an isomorphism.*

Proof: Part 1 is a consequence of the injectivity of the map $J' \longrightarrow J$. Projection onto E^2 now allows us to view V as a finite subgroup scheme $\underline{V}$ of E^2 over $\mathcal{O}_q$. In order to prove part 2, we describe $\underline{V}$ more explicitly. Begin by noting that x belongs to $\underline{V}(K_q)$ if and only if $\varphi_E(x)$ belongs to $\varphi'(J')$, i.e., if and only if $\pi_{12}^*\pi_E^*(x)$ belongs to the q-new subvariety $J_0'(Nq)$, which is the kernel of $\tilde{\pi}_{12*}$. Hence $\underline{V}_\mathfrak{m}$ is equal to the completion at $\mathfrak{m}$ of the kernel of the endomorphism

$$\pi_{E*}\tilde{\pi}_{12*}\pi_{12}^*\pi_E^* = \deg(\pi_E) \begin{pmatrix} q+1-a_q^2 & -a_q q \\ a_q & q+1 \end{pmatrix}. \tag{10}$$

Let $\underline{V}_{p^\infty} := \cup_n \underline{V}_{p^n}$, and let E_{p^∞} be the p-divisible group over $\mathcal{O}_q$ attached to E. For the purpose of this proof, denote by α the root of $x^2 - a_q x + q$ in $\mathbb{Z}_p$ which is congruent to 1 mod p, and let $\bar{\alpha}$ be the root which is congruent to -1. By diagonalizing the matrix in equation (10), we find that (since $\deg(\pi_E)$ is a unit at p) the module $\underline{V}_{p^\infty}$ is equal to the kernel of the endomorphism of $E^2_{p^\infty}$:

$$\begin{pmatrix} 1 & \bar{\alpha} \\ -1 & -\alpha \end{pmatrix}^{-1} \begin{pmatrix} 1-\alpha^2 & 0 \\ 0 & 1-\bar{\alpha}^2 \end{pmatrix} \begin{pmatrix} 1 & \bar{\alpha} \\ -1 & -\alpha \end{pmatrix}. \tag{11}$$

Let

$$n^+ := \mathrm{ord}_p(1-\alpha^2), \qquad n^- := \mathrm{ord}_p(1-\bar{\alpha}^2).$$

By (11), the isomorphism $E^2_{p^\infty} \longrightarrow E^2_{p^\infty}$ sending (x, y) to $(x + \bar{\alpha}y, -x - \alpha y)$ induces an isomorphism

$$\kappa : \underline{V}_{p^\infty} \longrightarrow E_{p^{n^+}} \times E_{p^{n^-}}.$$

Note that

$$n^+ = \mathrm{ord}_p(q + 1 - a_q), \quad n^- = \mathrm{ord}_p(q + 1 + a_q).$$

The isomorphism κ is equivariant for the Hecke operators T_ℓ for $\ell \not| Nq$, and satisfies the relation

$$\kappa U_q = \begin{pmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{pmatrix} \kappa,$$

so that it "diagonalizes" the action of U_q. In other words, the Hecke operator U_q acts on $E_{p^{n^+}} \times E_{p^{n^-}}$ with eigenvalue α and $\bar{\alpha}$ on the first and second component. Hence completing at the ideal $\mathfrak{m}$ gives an isomorphism

$$\kappa_{\mathfrak{m}} : \underline{V}_{\mathfrak{m}} \longrightarrow E_{p^{n^\epsilon}}.$$

It follows that $\underline{V}^\epsilon_{\mathfrak{m}}$ is a cyclic group of order p^{n^ϵ}. The same is true of $E^2(K_q)^\epsilon_{\mathfrak{m}}$, as can be seen from a direct calculation using (9). Hence the map of part 2 is an isomorphism.

If F is any finite extension of K_q with ring of integers $\mathcal{O}_F$, denote by $\mathcal{J}_0(Nq)_{/\mathcal{O}_F}$, (resp. $\mathcal{J}_{/\mathcal{O}_F}$, $\mathcal{J}'_{/\mathcal{O}_F}$) the Néron model of $J_0(Nq)$ (resp. J, J') over $\mathcal{O}_F$, and let $\Phi(J_0(Nq)/F)$, (resp. $\Phi(J/F)$, $\Phi(J'/F)$) denote the component groups of these Néron models. Since we will be working exclusively with

the Néron models from now on, we will make an abuse of notation and write $J_0(Nq)(F)$ (resp. $J(F)$, $J'(F)$) instead of $\mathcal{J}_0(Nq)(\mathcal{O}_F)$ (resp. $\mathcal{J}(\mathcal{O}_F)$, $\mathcal{J}'(\mathcal{O}_F)$). In particular, $J^0(F)$ will denote the connected component of the identity in $\mathcal{J}(\mathcal{O}_F)$, etc.

Lemma 3.5 *The natural map*

$$\Phi(J_0(Nq)/F)_{\mathfrak{m}} \longrightarrow \Phi(J/F)_{\mathfrak{m}}$$

is an isomorphism.

Proof: Let $I^{\perp} := \mathrm{Ann}_{\mathbb{T}}(I)$, and let $J^{\perp} = J_0(Nq)/I^{\perp}$. Then the natural isogeny

$$J_0(Nq) \longrightarrow J \times J^{\perp}$$

has a kernel which is contained in $IJ_0(Nq)$, and hence its support is disjoint from $\mathfrak{m}$. (Cf. the proof of lemma 3.3.) Therefore this isogeny induces an isomorphism

$$\Phi(J_0(Nq)/F)_{\mathfrak{m}} \longrightarrow \Phi(J/F)_{\mathfrak{m}} \times \Phi(J^{\perp}/F)_{\mathfrak{m}}.$$

But the action of $\mathbb{T}\otimes\mathbb{Z}_p$ on $\Phi(J^{\perp})\otimes\mathbb{Z}_p$ factors through the ring $\mathbb{T}'$ of equation (4). Hence $\Phi(J^{\perp}/F)_{\mathfrak{m}} = 0$, and the result follows.

Lemma 3.6 *The natural map $V(K_q) \longrightarrow \Phi(J'/K_q)_{\mathfrak{m}}$ is surjective.*

Proof: Consider the commutative diagram

$$\begin{array}{ccccc} V(K_q) & \longrightarrow & E^2(K_q)\times J'(K_q) & \longrightarrow & J(K_q) \\ & & \big| & & \big| \\ & \searrow & \downarrow & & \downarrow \\ & & \Phi(J'/K_q)_{\mathfrak{m}} & \longrightarrow & \Phi(J/K_q)_{\mathfrak{m}}. \end{array}$$

By lemma 3.5, the group $\Phi(J/K_q)_{\mathfrak{m}}$ is isomorphic to $\Phi(J_0(Nq)/K_q)_{\mathfrak{m}}$. The latter group is trivial, because the group of connected components in $J_0(Nq)$ over an unramified extension of $\mathbb{Q}_q$ is Eisenstein. But it follows from [BLR] th. 4 (ii) that the cokernel of the diagonal map above injects into $\Phi(J/K_q)_{\mathfrak{m}}$.

Proposition 3.7 *The map*

$$\mathbf{i} : E^2(K_q)^{\epsilon}_{\mathfrak{m}} \longrightarrow J(K_q)^{\epsilon}_{\mathfrak{m}}$$

induced by the map φ_E of equation (7) is an isomorphism.

Proof: By lemma 3.3, the map $\mathbf{i}$ is injective. To prove surjectivity, consider the diagram

$$\begin{array}{ccccc} & & 0 & & 0 \\ & & \downarrow & & \downarrow \\ & & E^2(K_q)^\epsilon_{\mathfrak{m}} & = & E^2(K_q)^\epsilon_{\mathfrak{m}} \\ & & \downarrow & & \downarrow \mathbf{i} \\ V(K_q)^\epsilon_{\mathfrak{m}} & \longrightarrow & (E^2(K_q) \times J'(K_q))^\epsilon_{\mathfrak{m}} & \xrightarrow{\varphi_{\mathfrak{m}}} & J(K_q)^\epsilon_{\mathfrak{m}} \\ & \searrow & \downarrow & & \\ & & \Phi(J'/K_q)^\epsilon_{\mathfrak{m}} & & \end{array} \tag{12}$$

Note that:
1. The leftmost vertical sequence is exact. Indeed, the kernel of the map $J'(K_q)^\epsilon \longrightarrow \Phi(J'/K_q)$ is isomorphic to an extension of a group of exponent $q-1$ by a pro-q group, by proposition 3.1; hence the support of this kernel is disjoint from $\mathfrak{m}$, as p does not divide $q(q-1)$.

2. The map $\varphi_{\mathfrak{m}}$ is surjective. Indeed, taking K_q-rational points in the exact sequence

$$0 \longrightarrow V \longrightarrow E^2 \times J' \longrightarrow J \longrightarrow 0$$

gives the long exact cohomology sequence

$$E^2(K_q) \times J'(K_q) \longrightarrow J(K_q) \longrightarrow H^1(K_q, V) \longrightarrow H^1(K_q, E^2) \times H^1(K_q, J').$$

Note that since q does not divide pN, the Galois representation V (over K_q) is unramified. Using lemma 3.4, we see that the kernel of $H^1(K_q, V) \longrightarrow H^1(K_q, E^2)$ is the finite part $H^1_f(K_q, V)$ of the cohomology, since the curve E has good reduction at q. Let V^0 be the kernel of the natural map $V \longrightarrow \Phi(J'/K_q)$. The kernel of $H^1_f(K_q, V) \longrightarrow H^1(K_q, J')$ is contained in the image of $H^1_f(K_q, V^0)$. Hence, the cokernel of $\phi_{\mathfrak{m}}$ is a quotient of $H^1_f(K_q, V^0)^\epsilon_{\mathfrak{m}}$. But this group is trivial, since complex conjugation acts by $-\epsilon$ on $(V^0)_{\mathfrak{m}}$ and trivially on $\mathrm{Gal}(K_q^{nr}/K_q)$.

3. The diagonal map in the diagram of equation (12) is surjective, by lemma 3.6.

The surjectivity of the map $\mathbf{i}$ now follows from combining these three facts with a diagram chase.

Let H be the Hilbert class field of K, and let L denote the ring class field of K of conductor q. It is a cyclic extension of H of degree $(q+1)/u$, where $u = \frac{1}{2}\#\mathcal{O}_K^\times$.

The prime q is inert in $K/\mathbb{Q}$, and hence splits completely in H/K. Furthermore, any prime of H above q is totally ramified in L/H. Let L_q be the completion of L at any such prime above q. The extension L_q is a totally ramified cyclic extension of K_q of degree $(q+1)/u$. Let σ be a generator for $\mathrm{Gal}(L_q/K_q)$. Note that $\mathrm{Gal}(L_q/\mathbb{Q}_q)$ is isomorphic to a dihedral group of order $2(q+1)/u$, and that complex conjugation in $\mathrm{Gal}(K_q/\mathbb{Q}_q)$ conjugates σ to σ^{-1}.

Let $\tilde{J}$ be the group

$$\tilde{J} = \frac{J(L_q)}{\varphi_E(E^2(L_q)) + (\sigma - 1)J(L_q)}.$$

The module $\tilde{J}$ is equipped with a natural action of the Hecke operators and of complex conjugation. Since $\varphi_E(E^2)$ is contained in the connected component of the identity of J, and since $\mathrm{Gal}(L_q/K_q)$ acts trivially on $\Phi(J/L_q)$ (because it acts trivially on $\Phi(J_0(Nq)/L_q)$), projection onto the group of connected components gives a well-defined map

$$\mathbf{p} : \tilde{J}^\epsilon_{\mathfrak{m}} \longrightarrow \Phi(J/L_q)_{\mathfrak{m}}.$$

Proposition 3.8 *The map* $\mathbf{p}$ *is an isomorphism.*

Proof: The surjectivity of $\mathbf{p}$ follows directly from its definition. To prove the injectivity, choose an element $\tau \in \mathrm{Gal}(L_q/\mathbb{Q}_q)$ whose image in $\mathrm{Gal}(K_q/\mathbb{Q}_q)$ is complex conjugation. (Such a τ is necessarily an involution.) If M is any $\mathrm{Gal}(L_q/\mathbb{Q}_q)$-module, write M^+ and M^- for the submodules of M on which τ acts by 1 and -1 respectively. By the same reasoning as in part 2 of the proof of proposition 3.7, the map $\varphi_{\mathfrak{m}} : (E^2(L_q) \times J'(L_q))^\epsilon_{\mathfrak{m}} \longrightarrow J(L_q)^\epsilon_{\mathfrak{m}}$ is surjective. Recall that $J'(L_q)^0$ denotes the connected component of the identity of Néron model of J' over the ring of integers of L_q. Let $\bar{V}^\epsilon_{\mathfrak{m}}$ be the image of $V(L_q)^\epsilon_{\mathfrak{m}}$ in $\Phi(J'/L_q)^\epsilon_{\mathfrak{m}}$. Then the rows and columns in the following

diagram are exact:

$$\begin{array}{ccccccc} & & V(L_q)^\epsilon_{\mathfrak{m}} & \longrightarrow & \bar{V}(L_q)^\epsilon_{\mathfrak{m}} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \\ (E^2(L_q)\times J'(L_q)^0)^\epsilon_{\mathfrak{m}} & \longrightarrow & (E^2(L_q)\times J'(L_q))^\epsilon_{\mathfrak{m}} & \longrightarrow & \Phi(J'/L_q)^\epsilon_{\mathfrak{m}} & \longrightarrow & 0 \\ \varphi^0_{\mathfrak{m}}\downarrow & & \varphi_{\mathfrak{m}}\downarrow & & \downarrow & & \\ J^0(L_q)^\epsilon_{\mathfrak{m}} & \longrightarrow & J(L_q)^\epsilon_{\mathfrak{m}} & \longrightarrow & \Phi(J/L_q)^\epsilon_{\mathfrak{m}} & \longrightarrow & 0 \\ & & \downarrow & & & & \\ & & 0 & & & & \end{array}$$

A straightforward diagram chase show that the map $\varphi^0_{\mathfrak{m}}$ is surjective, so that we have an exact sequence

$$(E^2(L_q)\times J'(L_q)^0)^\epsilon_{\mathfrak{m}} \longrightarrow J(L_q)^\epsilon_{\mathfrak{m}} \longrightarrow \Phi(J/L_q)^\epsilon_{\mathfrak{m}} \longrightarrow 1.$$

But by corollary 3.2, $(J'(L_q)^0)^\epsilon$ is an extension of a group of exponent $q-1$ by a pro-q-group, and so its completion at $\mathfrak{m}$ is zero. Hence, the group $(J^0(L_q)_{\mathfrak{m}})^\epsilon$ is generated by the image of $\varphi_E(E^2(L_q)^\epsilon_{\mathfrak{m}})$. The injectivity of $\mathbf{p}$ follows.

Corollary 3.9 *The group $(\tilde{J}/\mathfrak{m}\tilde{J})^\epsilon$ is a one-dimensional $\mathbb{T}/\mathfrak{m}\mathbb{T}$-vector space.*

Proof: The one-dimensionality of the group $\Phi(J/L_q)/\mathfrak{m}\Phi(J/L_q)$ follows directly from theorem 2.3 in light of proposition 2.2. The corollary is now a consequence of proposition 3.8.

Let $\mathrm{N}_{L_q/K_q} = \sum_{j=1}^{(q+1)/u}\sigma^j$ denote the norm map of L_q over K_q. Since the extension L_q/K_q is totally ramified of degree $(q+1)/u$ prime to q, we have $\mathrm{N}_{L_q/K_q}(E(L_q)) = \frac{q+1}{u}E(K_q)$, and hence

$$\mathrm{N}_{L_q/K_q}(\varphi_E(E^2(L_q)) = \varphi_E(\mathrm{N}_{L_q/K_q}(E^2(L_q))) = \varphi_E((q+1)E^2(K_q)) \subset \mathfrak{m}J(K_q).$$

It follows that N_{L_q/K_q} induces a well-defined map

$$\mathbf{n} : \tilde{J}/\mathfrak{m}\tilde{J} \longrightarrow J(K_q)/\mathfrak{m}J(K_q)$$

which commutes with the action of complex conjugation on these two groups.

Proposition 3.10 *The map*

$$\mathbf{n} : (\tilde{J}/\mathfrak{m}\tilde{J})^\epsilon \longrightarrow (J(K_q)/\mathfrak{m}J(K_q))^\epsilon$$

obtained by restricting $\mathbf{n}$ *to ϵ-eigencomponents is an isomorphism.*

Proof: We begin by proving the surjectivity of $\mathbf{n}$. For this, consider the diagram

$$\begin{array}{ccccc} & & (J'(L_q)/\mathfrak{m}J'(L_q))^\epsilon & \longrightarrow & (\tilde{J}/\mathfrak{m}\tilde{J})^\epsilon \\ & & \downarrow & & \downarrow \mathbf{n} \\ V(K_q)^\epsilon_{\mathfrak{m}} & \longrightarrow & ((E^2(K_q)\times J'(K_q))/\mathfrak{m})^\epsilon & \xrightarrow{\varphi_{\mathfrak{m}}} & (J(K_q)/\mathfrak{m}J(K_q))^\epsilon \\ & \searrow & \downarrow & & \\ & & (E^2(K_q)/\mathfrak{m})^\epsilon, & & \end{array}$$

where the topmost vertical arrows are induced by the norm maps, and the bottom vertical arrow is the natural projection onto the first component. Observe that:

1. The leftmost vertical sequence is exact. Indeed, since $J'(L_q)$ is isomorphic to a quotient of $(L_q^\times)^r$ by a discrete subgroup, it follows from local class field theory that the image of the norm map contains $J'(K_q)^\epsilon$.

2. As in part 2 in the proof of prop. 3.7, the map $\varphi_{\mathfrak{m}}$ is surjective.

3. The map $V(K_q)^\epsilon_{\mathfrak{m}} \longrightarrow (E^2(K_q)/\mathfrak{m})^\epsilon$ is surjective, by part 2 of lemma 3.4.

The surjectivity of $\mathbf{n}$ follows directly from these three remarks by a diagram chase.

Now, to prove injectivity, observe that $(\tilde{J}/\mathfrak{m}\tilde{J})^\epsilon$ is a one-dimensional $\mathbb{F}_p$-vector space, by corollary 3.9, and that $(J(K_q)/\mathfrak{m}J(K_q))^\epsilon$ has dimension one as well, by proposition 3.7 (cf. the proof of lemma 3.4). It follows that $\mathbf{n}$ is an isomorphism.

To summarize the main results of this section, all the arrows in the following diagram are isomorphisms of one-dimensional $\mathbb{F}_p$-vector spaces.

$$\begin{array}{ccccc} & & & & \Phi(J_0(Nq)/L_q)/\mathfrak{m} \\ & & & & \downarrow \mathbf{j} \\ & & (\tilde{J}/\mathfrak{m}\tilde{J})^\epsilon & \xrightarrow{\mathbf{p}} & \Phi(J/L_q)/\mathfrak{m} \\ & & \downarrow \mathbf{n} & & \\ (E^2(K_q)/\mathfrak{m})^\epsilon & \xrightarrow{\mathbf{i}} & (J(K_q)/\mathfrak{m}J(K_q))^\epsilon & & \end{array}$$

(We have applied lemma 3.5 to conclude that $\mathbf{j}$ is an isomorphism.) Recall from proposition 2.2 that $\Phi(J_0(Nq)/L_q)/\mathfrak{m}$ can be identified with $\mathcal{M}/\mathfrak{m}\mathcal{M}$, where $\mathcal{M}$ is the module introduced in section 2. Let

$$\eta : (E^2(K_q)/\mathfrak{m})^\epsilon \longrightarrow \mathcal{M}/\mathfrak{m}\mathcal{M}$$

be the isomorphism defined by $\eta = \mathbf{j}^{-1}\mathbf{p}\mathbf{n}^{-1}\mathbf{i}$. It will play an important role later on.

4 Special values of L-functions

The module $\mathcal{M}_g$:
We view the module $\mathcal{M}$ introduced in section 2 as the set of formal degree zero $\mathbb{Z}$-linear combinations of $[R_1], \ldots, [R_t]$, where $R_1, \ldots, R_t$ are the (distinct, up to conjugacy) oriented Eichler orders of level N. It will also be convenient to work with the module $\tilde{\mathcal{M}}$ of all formal $\mathbb{Z}$-linear combinations of the $[R_i]$, which sits in an exact sequence

$$0 \longrightarrow \mathcal{M} \longrightarrow \tilde{\mathcal{M}} \longrightarrow \mathbb{Z} \longrightarrow 0. \tag{13}$$

The module $\tilde{\mathcal{M}}$ is endowed with a natural Hecke action compatible with the inclusion $\mathcal{M} \longrightarrow \tilde{\mathcal{M}}$.

If g is any form on J', let I_g be the kernel of the natural map $\phi_g : \mathbb{T} \longrightarrow \mathcal{O}_g$ as before, and let $\mathcal{O}_{g,\mathfrak{m}}$ be the completion of $\mathcal{O}_g$ at $\mathfrak{m}_g$. Finally, let

$$\mathcal{M}_g := (\mathcal{M}/I_g) \otimes_{\mathbb{T}} \mathcal{O}_{g,\mathfrak{m}}, \qquad \tilde{\mathcal{M}}_g := (\tilde{\mathcal{M}}/I_g) \otimes_{\mathbb{T}} \mathcal{O}_{g,\mathfrak{m}}.$$

Proposition 4.1 *The natural map $\mathcal{M}_g \longrightarrow \tilde{\mathcal{M}}_g$ is an isomorphism, and $\mathcal{M}_g$ is free of rank one over $\mathcal{O}_{g,\mathfrak{m}}$.*

Proof: The first statement follows upon tensoring the exact sequence (13) with $\mathcal{O}_{g,\mathfrak{m}}$, and noting that the action of the Hecke algebra on $\tilde{\mathcal{M}}/\mathcal{M} = \mathbb{Z}$ is Eisenstein. The second statement follows from theorem 2.3.

Algebraic parts of special values:
By the Heegner hypothesis, there exists an ideal $\mathcal{N} \subset \mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \simeq \mathbb{Z}/N\mathbb{Z}$. Fix such an ideal $\mathcal{N}$ of $\mathcal{O}_K$. An embedding $(\psi : \mathcal{O}_K \longrightarrow R)$ is called *oriented* relative to this fixed choice of $\mathcal{N}$ if the kernel of $\iota \circ \psi$ is equal to $\mathcal{N}$ (where ι is the orientation provided to R, as in equation (2) of section 2). There are exactly $h = \#Pic(\mathcal{O}_K)$ distinct oriented embeddings $\psi_1, \ldots, \psi_h$ of $\mathcal{O}_K$ into some oriented Eichler order, taken modulo conjugation. (Cf. [Gr1], sec. 3. In fact, the group $\mathrm{Pic}(\mathcal{O}_K)$ acts simply transitively on the ψ_j.)

Each $(\psi_j : \mathcal{O}_K \longrightarrow R_j)$ gives rise to the element $[R_j] \in \tilde{\mathcal{M}}$. Let ψ_K be the formal sum

$$\psi_K := \psi_1 + \cdots + \psi_h,$$

viewed as an element of $\tilde{\mathcal{M}}$.

Definition 4.2 *The* algebraic part *of* $L(g/K,1)$*, denoted* $\mathbb{L}(g/K,1)$*, is the image of* ψ_K *in the rank one* $\mathcal{O}_{g,\mathfrak{m}}$*-module* $\mathcal{M}_g = \tilde{\mathcal{M}}_g$*.*

Remark: Although we view $\mathbb{L}(g/K,1)$ as the "algebraic part" of $L(g/K,1)$, it might perhaps be more appropriate to view it as the "square root" of this algebraic part; cf. formula (15) below.

The main justification for this definition is the following theorem of Gross (generalized to cover our situation by Daghigh [Dag]).

Theorem 4.3 $L(g/K,1) = 0$ *if and only if* $\mathbb{L}(g/K,1) = 0$*.*

Proof: Viewing ψ_K as an element of $\tilde{\mathcal{M}} \otimes \mathbb{C}$, and g as a complex normalised eigenform, let $\psi_{K,g}$ be the projection of ψ_K onto the g-isotypic component of $\tilde{\mathcal{M}} \otimes \mathbb{C}$. Then

$$\psi_{K,g} = 0 \text{ if and only if } \mathbb{L}(g/K,1) = 0. \tag{14}$$

The g-isotypic component of $\tilde{\mathcal{M}} \otimes \mathbb{C}$ is a one-dimensional complex vector space and the pairing $\langle\ ,\ \rangle$ on $\tilde{\mathcal{M}}$ defined by equation (3) gives rise to a perfect non-degenerate pairing on it. By a formula of Gross [Gr1], prop. 11.2, and a generalization by Daghigh for modular forms of arbitrary level [Dag],

$$\frac{L(g/K,1)}{(g,g)} = \frac{\langle \psi_{K,g}, \psi_{K,g} \rangle}{u^2\sqrt{D}}, \tag{15}$$

where (g,g) is the Petersson scalar product of g with itself, u is equal to $\#\mathcal{O}_K^\times/2$, and D is the discriminant of K. The result follows at once from (14) and (15).

The main advantage of having defined $\mathbb{L}(g/K,1)$ in this way is that it allows us to talk of congruences for $\mathbb{L}(g/K,1)$ modulo ideals in the Hecke algebra. For example, say that $\mathbb{L}(g/K,1)$ is *congruent to* 0 *mod* $\mathfrak{m}_g$, and write $\mathbb{L}(g/K,1) \equiv 0 \pmod{\mathfrak{m}_g}$, if $\mathbb{L}(g/K,1)$ belongs to $\mathfrak{m}_g\mathcal{M}_g$.

5 Heegner points

Let K be as before a quadratic imaginary field satisfying the Heegner hypothesis relative to E. Choose a Kolyvagin prime q (relative to E, K and p) as in the introduction. Recall that H and L denote the Hilbert class field of K and the ring class field of K of conductor q respectively. Finally, note

$$G_q := \mathrm{Gal}(L/H), \quad \tilde{G}_q = \mathrm{Gal}(L/K), \quad \Delta = \mathrm{Gal}(H/K).$$

Heegner points:
By the theory of complex multiplication, there are h distinct elliptic curves $A_1, \ldots, A_h$ up to isomorphism satisfying $\mathrm{End}(A_j) \simeq \mathcal{O}_K$. They are defined over the Hilbert class field H and are permuted transitively by Δ. Recall the ideal $\mathcal{N}$ of $\mathcal{O}_K$ which was fixed in the previous section. Letting C_j be the group $A_j[\mathcal{N}]$ of $\mathcal{N}$-torsion points of A_j, one obtains enhanced elliptic curves $\underline{A}_j = (A_j, C_j)$ with $\Gamma_0(N)$-structure, which are *also* defined over H. Let

$$P_j \in X_0(N)(H)$$

be the algebraic point corresponding to the modulus $\underline{A}_j$.

Recall that $u = \#(\mathcal{O}_K^\times)/2$. There are $(q+1)/u$ possible cyclic q-isogenies $\underline{A}_j \to \underline{A}'_j$, up to composition on the left by $\mathcal{O}_K^\times/\langle \pm 1 \rangle$. The assumption that q is inert in K implies that the possible isomorphism classes of diagrams $(\underline{A}_j \to \underline{A}'_j)$ are defined over the ring class field L, and are permuted transitively by G_q. The endomorphism ring of $\underline{A}'_j$ is isomorphic to the order of K of conductor q. For each $j = 1, \ldots, h$, choose any q-isogeny $(\underline{A}_j \to \underline{A}'_j)$, and let

$$P'_j \in X_0(Nq)(L)$$

be the algebraic point corresponding to the diagram of enhanced elliptic curves $(\underline{A}_j \to \underline{A}'_j)$.

Write ∞ for the cusp of $X_0(Nq)$ corresponding to the point $i\infty$ in the completed upper half plane. Let P_K and P'_L be the elements of $J_0(N)(K)$ and $J_0(Nq)(L)$ respectively represented by the degree 0 divisors:

$$P_K := (P_1) + \cdots (P_h) - h(\infty), \quad P'_L = (P'_1) + \cdots + (P'_h) - h(\infty).$$

Let $C(Nq)$ be the cuspidal subgroup of $J_0(Nq)$. It is a finite subgroup of $J_0(Nq)$ which is Eisenstein as a $\mathbb{T}$-module. We write $x \equiv y \pmod{C(Nq)}$ if the difference $x - y$ belongs to $C(Nq)$.

Proposition 5.1 *Let $N_{L/H}$ be the norm map $\sum_{\sigma \in G_q} \sigma$. Then*

$$\pi_{1*}(P'_L) = P_K, \qquad \pi_1^*(P_K) \equiv u N_{L/H}(P'_L) \pmod{C(Nq)}.$$

Proof: A direct calculation.

Now, define the Heegner point $y_K \in E(K)$ by the formula:

$$y_K := \pi_{E*}(P_K).$$

6 Jochnowitz Congruences

Recall the isomorphism $\eta : (E^2(K_q)/\mathfrak{m})^\epsilon \longrightarrow \mathcal{M}/\mathfrak{m}\mathcal{M} = \mathcal{M}_g/\mathfrak{m}_g\mathcal{M}_g$ constructed in section 3. The following is our main result, which is the Jochnowitz congruence alluded to in the title. It directly implies theorem 1.3.

Theorem 6.1 *If g is a normalised eigenform on J', then*

$$\eta((y_K, 0)) \equiv u \deg(\pi_E) \cdot \mathbb{L}(g/K, 1) \pmod{\mathfrak{m}}.$$

Proof: Let π_J be the natural projection $J_0(Nq) \longrightarrow J$, and let $\tilde{\pi}_J$ be the induced map from $J_0(Nq)(L_q)$ to $\tilde{J}/\mathfrak{m}\tilde{J}$. Let $J_0(Nq)(L_q)^\epsilon$ denote the module of points in $J_0(Nq)(L_q)$ whose natural image in $J_0(Nq)(L_q)/(\sigma_q - 1)J_0(Nq)(L_q)$ belongs to the ϵ-eigenspace for the action of complex conjugation on this module. Consider the commutative diagram

$$\begin{array}{ccc} J_0(Nq)(L_q)^\epsilon & \xrightarrow{\Psi_q} & \mathcal{M}/\mathfrak{m}\mathcal{M} \\ \tilde{\pi}_J \downarrow & & \downarrow \mathbf{j} \\ (\tilde{J}/\mathfrak{m}\tilde{J})^\epsilon & \xrightarrow{\mathbf{p}} & \Phi(J/L_q)/\mathfrak{m} \\ \downarrow \mathbf{n} & & \\ (E^2(K_q)/\mathfrak{m})^\epsilon & \xrightarrow{\mathbf{i}} & (J(K_q)/\mathfrak{m})^\epsilon. \end{array} \tag{16}$$

The proof of theorem 6.1 rests on the following two lemmas:

Lemma 6.2 $\mathbf{p}(\tilde{\pi}_J(P'_L)) = \mathbf{j}(\mathbb{L}(g/K, 1)) \pmod{\mathfrak{m}_g}$.

Proof: See [BD2], sec. 3, theorem 3.2.

Lemma 6.3 $u \deg(\pi_E) \cdot \mathbf{n}(\tilde{\pi}_J(P'_L)) = \mathbf{i}(y_K, 0)$.

Proof: By proposition 5.1, we have

$$u \cdot \mathbf{n}(\tilde{\pi}_J(P'_L)) = \pi_J(\pi_1^*(P_K)) \pmod{\mathfrak{m}}.$$

But the following equality holds in $J(K_q)/\mathfrak{m}$:

$$\deg(\pi_E) P_K = \pi_E^*(y_K).$$

Hence

$$u \deg(\pi_E) \cdot \mathbf{n}(\tilde{\pi}_J(P'_L)) = \pi_J \pi_1^* \pi_E^*(y_K) = \pi_J \pi_{12}^* \pi_E^*(y_K, 0) = \mathbf{i}(y_K, 0),$$

where the last equality follows from the definition of φ_E (and hence, of $\mathbf{i}$) given in equation (7) of section 3. The lemma follows.

Combining lemmas 6.2 and 6.3 and using the commutativity of the diagram (16) yields theorem 6.1.

References

[BD1] M. Bertolini and H. Darmon, *Heegner points on Mumford-Tate curves*. Invent. Math **126** 413–456 (1996).

[BD2] M. Bertolini and H. Darmon, *A rigid-analytic Gross-Zagier formula and arithmetic applications*. Annals of Math **146** (1997) 111-147.

[BD3] M. Bertolini and H. Darmon, *Heegner points, p-adic L-functions, and the Cerednik-Drinfeld uniformization*. Invent. Math, to appear.

[BD4] M. Bertolini and H. Darmon, *p-adic periods, p-adic L-functions and the p-adic uniformization of Shimura curves*, Duke Math J., to appear..

[BLR] S. Bosch, W. Lütkebohmert, and M. Raynaud, Néron Models, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3 Folge - Band 21, Springer-Verlag, 1990.

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

[DDT] H. Darmon, F. Diamond, and R. Taylor, *Fermat's Last Theorem*, Current Developments in Mathematics Vol. **1**, International Press, 1995, pp. 1–154.

[DR] P. Deligne, M. Rapoport, *Les schémas de modules de courbes elliptiques* (LNM vol. **349**, pp. 143–316). Berlin-Heidelberg-New York: Springer 1973.

[Gr1] B.H. Gross, *Heights and special values of L-series*. CMS conference proceedings, vol. **7**, 1987.

[Gr2] B.H. Gross, *Kolyvagin's work on modular elliptic curves*. L-functions and arithmetic (Durham, 1989), 235–256, London Math. Soc. Lecture Note Ser., **153**, Cambridge Univ. Press, Cambridge, 1991.

[GZ] B.H. Gross, D. Zagier, *Heegner points and derivatives of L-series*. Invent. Math. **84** (1986), no. 2, 225–320.

[J] N. Jochnowitz, *A p-adic conjecture about derivatives of L-series attached to modular forms*. p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991), 239–263, Contemp. Math., **165**, Amer. Math. Soc., Providence, RI, 1994.

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

[Ma1] B. Mazur, *Modular curves and the Eisenstein ideal.* Inst. Hautes Études Sci. Publ. Math. No. **47** (1977), 33–186 (1978).

[Ma2] B. Mazur *On the arithmetic of special values of L functions*. Invent. Math. **55** (1979), no. 3, 207–240.

[Ra] M. Raynaud, *Spécialisation du foncteur de Picard*, Publ. Math, IHES **38**, 27-76 (1970).

[Ri1] K. Ribet, *Congruence relations between modular forms*. Proceedings of the International Congress of Mathematicians, Vol. **1**, 2 (Warsaw, 1983), 503–514, PWN, Warsaw, 1984.

[Ri2] K. Ribet, *On modular representations of Gal*$(\bar{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100**, 431–476 (1990).

[Ro] D. Roberts, Shimura curves analogous to $X_0(N)$, Harvard PhD thesis, 1990.

[Ru] K. Rubin, *p-adic L-functions and rational points on elliptic curves with complex multiplication*, Invent. Math. **107** (1992), 323-350.

[Se] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. **15** (1972), no. 4, 259–331.

[SGA] A. Grothendieck, SGA 7 I, Exposé IX. (Lecture notes in Math. vol. **288** pp. 313-523.) Berlin-Heidelberg-New York: Springer 1972.