CENTRAL CRITICAL VALUES OF MODULAR L-FUNCTIONS AND COEFFICIENTS OF HALF-INTEGRAL WEIGHT MODULAR FORMS MODULO ℓ

SCOTT AHLGREN AND MATTHEW BOYLAN

ABSTRACT. If $F(z)$ is a newform of weight 2λ and D is a fundamental discriminant, then let $L(F \otimes \chi_D, s)$ be the usual twisted L-series. We study the algebraic parts of the central critical values of these twisted L-series modulo primes ℓ. We show that if there are two D (subject to some local conditions) for which the algebraic part of $L(F \otimes \chi_D, \lambda)$ is not $0 \pmod{\ell}$, then there are infinitely many such D. These results depend on precise non-vanishing results for the Fourier coefficients of half-integral weight modular forms modulo ℓ, which are of independent interest.

1. INTRODUCTION

Given a normalized newform

$$F(z) := \sum_{n=1}^{\infty} a(n)q^n \in S_{2\lambda}(\Gamma_0(N)),$$

we define the modular L-series

$$L(F, s) := \sum_{n=1}^{\infty} a(n)n^{-s}.$$

The central critical values

$$L(F, \lambda)$$

are of great importance in number theory. Perhaps the most prominent indication of their importance comes from the conjecture of Birch and Swinnerton-Dyer, which relates the analytic properties of the L-function of a weight 2 newform $F(z)$ with integral coefficients to the rank and the order of the Tate-Shafarevich group of the associated elliptic curve $E/\mathbb{Q}$.

More generally, if ψ is a Dirichlet character, then we define the twisted L-series

$$L(F \otimes \psi, s) := \sum_{n=1}^{\infty} \psi(n)a(n)n^{-s}. \tag{1.1}$$

Deep results of Waldspurger [33], of Bump, Friedberg, and Hoffstein [8], of Murty and Murty [22], of Iwaniec [13], and of others (in various cases) establish non-vanishing results for central critical values of quadratic twists of modular L-functions and their derivatives. Combined with work of Gross and Zagier [11] and Kolyvagin [18] these non-vanishing results lead to

Date: June 29, 2005.

2000 *Mathematics Subject Classification.* 11F37, 11F67, 11G40.

The first author thanks the National Science Foundation for its support through grant DMS 01-34577. The second author thanks the National Science Foundation for its support through a VIGRE postdoctoral fellowship.

a proof of the weak Birch and Swinnerton-Dyer conjecture for elliptic curves over $\mathbb{Q}$ with analytic rank ≤ 1 (see, for example, Chapter 3 of [9] for a good expository treatment).

The central critical values themselves are typically transcendental. However, Shimura proved the existence of periods for the values of the twisted L-series given in (1.1) at integral arguments. In particular, if D is the discriminant of a quadratic number field, then let χ_D denote the corresponding Kronecker character. After Theorem 1 of [30] it is known that there exists a period $\Omega \in \mathbb{C}^\times$ such that

$$\frac{L(F \otimes \chi_D, \lambda)|D|^{\lambda-\frac{1}{2}}}{\Omega} \in \overline{\mathbb{Q}} \text{ for all fundamental } D \text{ with } (-1)^\lambda D > 0 \tag{1.2}$$

(in fact, Shimura proves that Ω may be selected so that these values all lie in the number field K_F generated over $\mathbb{Q}$ by the coefficients of F). We note that if ϵ is the sign of the functional equation for $L(F, s)$, then $L(F \otimes \chi_D, \lambda)$ is trivially zero for all D with $\chi_D(-N)\epsilon = -1$.

If $\ell \geq 5$ is prime, then we fix an extension v_ℓ of the usual ℓ-adic valuation on $\mathbb{Q}$ to an algebraic closure $\overline{\mathbb{Q}}$. With this notation, Ono and Skinner ([23], Corollary 1) proved that for all but finitely many primes ℓ there are infinitely many fundamental discriminants D such that

$$\epsilon D > 0 \text{ and } v_\ell\left(\frac{L(F \otimes \chi_D, \lambda)|D|^{\lambda-\frac{1}{2}}}{\Omega}\right) = 0. \tag{1.3}$$

A local version of this result ([23], Corollary 2) is also given.

If N is odd and square-free, Bruinier [5] showed that for all primes ℓ outside of a finite set (which is described in terms of the Hecke eigenvalues of F), there are infinitely many fundamental discriminants D such that

$$(-1)^\lambda D > 0 \text{ and } v_\ell\left(\frac{L(F \otimes \chi_D, \lambda)|D|^{\lambda-\frac{1}{2}}}{\Omega}\right) = 0. \tag{1.4}$$

In this paper we will prove a different type of result. For primes $p \mid N$, let $\epsilon_p \in \{\pm 1\}$ be the eigenvalue of $F(z)$ under the Atkin-Lehner involution w_p^N (see §3 for details). In the next section, we will state a precise non-vanishing theorem (Theorem 2.2) for the coefficients of half-integral weight modular forms modulo ℓ. Combining this with work of Kohnen [16], we will prove the following.

Theorem 1.1. *Suppose that N and λ are positive integers with N odd and square-free, that $F(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{2\lambda}^{\text{new}}(\Gamma_0(N))$ is a normalized newform, and that $\Omega \in \mathbb{C}^\times$ is any period for $F(z)$ satisfying (1.2). Suppose also that $\ell \geq 5$ is a rational prime, and that the minimum*

$$\min\left\{v_\ell\left(\frac{L(F \otimes \chi_D, \lambda)|D|^{\lambda-\frac{1}{2}}}{\Omega}\right)\right\}, \tag{1.5}$$

taken over all fundamental D with $(-1)^\lambda D > 0$ and $\left(\frac{D}{p}\right) = \epsilon_p$ for all $p \mid N$, is attained for two distinct fundamental discriminants D. Then the minimum is attained for infinitely many such D.

Remark. In this paper we employ Kohnen's theory because of its explicit nature. More general results relating coefficients of half-integral weight modular forms to twisted L-values have been proved by Waldspurger [34].

Remark. It will be clear from the proof of Theorem 1.1 that the minimum in (1.5) exists. This is also implied by the fact that it is possible to select a "good" period Ω; in other words, a period for which the relevant L-values are integral at ℓ, but are not all zero $\pmod{\ell}$.

Remark. We make the important remark that Theorem 1.1 is optimal. In particular, there exist forms $F(z)$ for which the minimum in (1.5) is achieved exactly once. Here we give one such example, which has been discussed by Kohnen and Zagier [17] and by Bruinier and Ono [6].

Let $\Delta(z)$ be the unique normalized eigenform of weight 12 on $\Gamma_0(1)$, let $G_4(z) := 1/240 + \sum_{n=1}^{\infty} \sigma_3(n)q^n$ be the usual Eisenstein series of weight 4, and let $\theta(z) := \sum_{n\in\mathbb{Z}} q^{n^2}$. Define

$$g(z) = \sum_{n=1}^{\infty} c(n)q^n := \frac{60}{2\pi i}(2G_4(4z)\theta'(z) - G_4'(4z)\theta(z)).$$

By results of Kohnen and Zagier (see Section 6 below for a complete discussion) there exists a period Ω such that for every positive fundamental discriminant D we have

$$c(D)^2 = \frac{L(\Delta \otimes \chi_D, 6)D^{\frac{11}{2}}}{\Omega}. \tag{1.6}$$

On the other hand, it is easy to verify that

$$g(z) \equiv \sum_{n=1}^{\infty} \left(\tfrac{n}{5}\right) q^{n^2} \pmod{5}. \tag{1.7}$$

By combining (1.6) and (1.7) we see that the minimum in (1.5) is attained only when $D = 1$.

We now consider an application of this theorem to the study of Tate-Shafarevich groups of elliptic curves over $\mathbb{Q}$. Suppose that $E/\mathbb{Q}$ is an elliptic curve with odd, square-free conductor N. Let $f(z)$ be the weight two newform on $\Gamma_0(N)$ associated to E by the work of Wiles [35], and let $L(E, s) = L(f, s)$ be the L-function associated to E. For each fundamental discriminant D let E_D be the D-quadratic twist of E. If ω_D is the invariant differential on E_D, then we define

$$\Omega(E_D) := \int_{E_D(\mathbb{R})} |\omega_D|,$$

and

$$D_0 := \begin{cases} D & \text{if } D \text{ is odd,} \\ D/4 & \text{if } D \text{ is even.} \end{cases}$$

Then, for negative fundamental discriminants D, we find that

$$\Omega(E_D) = \frac{\Omega(E_{-4})}{\sqrt{|D_0|}}. \tag{1.8}$$

Let $Ш(E)$ denote the Tate-Shafarevich group of E and let $\mathrm{Tam}(E)$ denote the Tamagawa number of E. We have $\mathrm{Tam}(E) = \prod_p c_p$, where $c_p := |E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)|$ is the usual local index (see, for example, [31], §16 of Appendix C). The conjecture of Birch and Swinnerton-Dyer predicts that if $L(E_D, 1) \neq 0$, then

$$\frac{L(E_D, 1)}{\Omega(E_D)} = \frac{|Ш(E_D)|}{|E_D(\mathbb{Q})_{\mathrm{tor}}|^2}\,\mathrm{Tam}(E_D). \tag{1.9}$$

For convenience, we let $\mathrm{Sha}(E_D)$ be the order of $Ш(E_D)$ as predicted by Birch and Swinnerton-Dyer.

From (1.9) and (1.8) we obtain, for negative D such that $L(E_D, 1) \neq 0$,

$$\frac{L(E_D, 1) \cdot \sqrt{|D_0|}}{\Omega(E_{-4})} = \frac{\mathrm{Sha}(E_D)}{|E_D(\mathbb{Q})_{\mathrm{tor}}|^2} \mathrm{Tam}(E_D). \tag{1.10}$$

To get a feel for Theorem 1.1 in this context, let ℓ be a fixed odd prime. We consider the issue of replacing the period $\Omega(E_{-4})$ in (1.10) by a period Ω^* with the property that the values

$$\frac{L(E_D, 1) \cdot \sqrt{|D_0|}}{\Omega^*} \tag{1.11}$$

are all integral at ℓ, but are not all divisible by ℓ. Suppose that $\ell = 5$ or 7 and that some twist E_D with $(D, N) = 1$ has ℓ-torsion, but that $v_\ell(\mathrm{Sha}(E_D) \cdot \mathrm{Tam}(E_D)) \leq 1$. It is clear (for example, by considering the Fourier expansions of the associated weight two modular forms) that no other twist E_D with $(D, N) = 1$ can have ℓ-torsion. Therefore, we see that if the period Ω^* has the properties described above, then all but exactly one of the values in (1.11) will be divisible by ℓ. Therefore Theorem 1.1 is natural in this context.

In Conjecture F of [18], Kolyvagin speculates that if $E/\mathbb{Q}$ is an elliptic curve with $L'(E, 1) \neq 0$, then there exists a D (satisfying a "Heegner hypothesis") with

$$L(E_D, 1) \neq 0 \quad \text{and} \quad v_\ell(\mathrm{Sha}(E_D)) = 0. \tag{1.12}$$

Ono and Skinner ([23], Corollaries 2 and 3) prove, given an elliptic curve E, that for all but finitely many primes ℓ, there exist infinitely many D for which (1.12) holds.

An application of Theorem 1.1 gives more information in this direction. As before, let ϵ_p denote the eigenvalue of $f(z)$ under the involution w_p^N.

Theorem 1.2. *Let $E/\mathbb{Q}$ be an elliptic curve with odd, square-free conductor N. Suppose that $\ell \geq 11$ is prime. Suppose further that there exist two negative fundamental discriminants D such that*

1. $\left(\frac{D}{p}\right) = \epsilon_p$ *for all* $p \mid N$.
2. $L(E_D, 1) \neq 0$.
3. $v_\ell(\mathrm{Sha}(E_D)) = 0$.

Then there exist infinitely many negative fundamental discriminants such that (1)–(3) hold.

Remark. It is natural to ask under what conditions we can replace conclusion (3) in Theorem 1.2 with the more desirable conclusion

$$v_\ell(|Ш(E_D)|) = 0. \tag{1.13}$$

In the case when E has complex multiplication, then the work of Rubin [26] implies that, for those D satisfying (2) and (3), (1.13) is true for all $\ell \geq 5$.

Suppose that E is an elliptic curve with conductor N as in the statement of Theorem 1.2, and that E does not have complex multiplication. Suppose further that $\epsilon_p = 1$ for all $p \mid N$. Then every negative fundamental discriminant D which satisfies (1) also satisfies the Heegner hypothesis $D \equiv \square \pmod{4N}$, and so we may apply the results of Kolyvagin [18]. In particular, suppose that

1. D is odd.
2. E has analytic rank equal to one.

(3) ℓ is a prime for which the ℓ-adic representation of the Tate module of E is surjective (this excludes only finitely many ℓ).
(4) $\ell \nmid 2 \cdot \mathrm{Tam}(E) \cdot c(E) \cdot \mathrm{Sha}(E)$ (where $c(E)$ is the Manin constant).

Then Corollary E of [18] guarantees that (1.13) is in fact implied by (2) and (3) of Theorem 1.2. Note that in the simplest case (i.e. when $N = p$ is prime), the condition $\epsilon_p = 1$ is equivalent to the natural condition that $\mathrm{sign}(E, \mathbb{Q}) = -1$.

One would naturally like to weaken the Heegner hypothesis $D \equiv \square \pmod{4N}$, which is restrictive if N is composite. Along these lines, suppose that E is an elliptic curve as in the statement of Theorem 1.2 with the properties that E has analytic rank equal to one and that $\mathrm{sign}(E, \mathbb{Q}) = -1$. Let D be a negative fundamental discriminant which satisfies conditions (1) and (2) of Theorem 1.2 and set $K := \mathbb{Q}(\sqrt{D})$. Then (using, for example, the explicit description in Theorem 3.17 of Darmon's book [9]) we find that $\mathrm{sign}(E, K) = -1$. It follows (see Theorem 4.18 of [9]) that there is a non-trivial Heegner system (arising from a Shimura curve parametrization) attached to the pair (E, K). In this setting, Zhang has proved an analog of the Gross-Zagier formula (see [36] or Theorem 4.19 of [9]). In view of these facts, it seems reasonable to expect that an analog of Kolyvagin's Corollary E should hold for all of the discriminants which satisfy (1) and (2) of Theorem 1.2 (but we do not know of such a statement in the literature). Such a result would, as in the case when all $\epsilon_p = 1$, allow one to replace (3) by the conclusion (1.13) for those primes ℓ outside of an explicit finite set depending on the elliptic curve E.

2. Coefficients of half-integral weight modular forms modulo ℓ

The results in the first section depend on non-vanishing results $\pmod{\ell}$ for the Fourier coefficients of half-integral weight modular forms. The main result in this section, which is of independent interest, gives a precise $\pmod{\ell}$ analogue of a well-known result of Vignéras for half-integral weight modular forms in characteristic zero.

Suppose that N is a positive integer with $4 \mid N$, that χ is a Dirichlet character defined modulo N, that $\lambda \geq 0$ is an integer, and that

$$f(z) = \sum_{n=1}^{\infty} a(n) q^n \in S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi) \tag{2.1}$$

is a half-integral weight cusp form. Partly because of their connections to the issues discussed in the first section, the coefficients $a(n)$ are a central object of study in number theory.

Let $\ell \geq 5$ be prime. Here we will study half-integral weight cusp forms whose reduction modulo ℓ has few non-vanishing coefficients. Cusp forms of this type have been investigated recently by a number of authors, including the present authors [2], [3], Bruinier [5], Bruinier and Ono [6], [7], and Ono and Skinner [23].

The single-variable theta series of weights $1/2$ and $3/2$ provide the simplest examples of modular forms of half-integral weight with few non-vanishing coefficients. If $\epsilon \in \{0, 1\}$, and ϕ is a nontrivial Dirichlet character modulo r which satisfies $\phi(-1) = (-1)^{\epsilon}$, then (see, for example, Section 2 of [29]) these theta series have the form

$$\psi(\phi, z) := \sum_{m=-\infty}^{\infty} m^{\epsilon} \phi(m) q^{m^2} \in M_{\epsilon+\frac{1}{2}}(\Gamma_0(4r^2), \phi\chi_{-1}^{\epsilon}). \tag{2.2}$$

In characteristic zero, a well-known result of Vignéras states that half-integral weight modular forms with many vanishing coefficients must in fact be linear combinations of these theta

series. To be precise, we have the following (a different proof of this result was given by Bruinier [4]).

Theorem 2.1 ([32], Théorème 3)**.** *Suppose that $\lambda \geq 0$ is an integer, that N is a positive integer with $4 \mid N$, and that $F(z) \in M_{\lambda+\frac{1}{2}}(\Gamma_1(N))$. If there are finitely many square-free integers $n_1, n_2, \dots, n_t$ for which*

$$F(z) = \sum_{i=1}^{t} \sum_{m=0}^{\infty} a(n_i m^2) q^{n_i m^2},$$

then $\lambda = 0$ or 1 and $F(z)$ is a linear combination of theta series.

If ℓ is a prime, it is natural to seek $\pmod{\ell}$ analogues of this result. For this purpose, we introduce more notation. Suppose that $f(z)$ is given by (2.1) and has algebraic coefficients. Let $\ell \geq 5$ be a rational prime, let K be a number field containing the coefficients $a(n)$ as well as the values of χ, let v be a place of K over ℓ, and let $\mathcal{O}_v$ denote the corresponding valuation ring. By the principle of "bounded denominators" (see §5 of [28]) we may suppose after normalization that

$$a(n) \in \mathcal{O}_v \quad \text{for all } n. \tag{2.3}$$

If $\mathfrak{m}_v$ is the maximal ideal of $\mathcal{O}_v$ then by a standard abuse of notation we will write $\pmod{v}$ to mean $\pmod{\mathfrak{m}_v}$. We will consider primes v such that there are finitely many distinct square-free integers $n_1, \dots, n_t$ with

$$f(z) \equiv \sum_{i=1}^{t} \sum_{m=1}^{\infty} a(n_i m^2) q^{n_i m^2} \not\equiv 0 \pmod{v}. \tag{2.4}$$

In the representation (2.4) we will always suppose that for each $i \in \{1, \dots t\}$ there is some m_i with $a(n_i m_i^2) \not\equiv 0 \pmod{v}$.

Bruinier [5] and Ono and Skinner [23] obtained $\pmod{\ell}$ analogues of the result of Vignéras. Suppose that $f(z)$ is a half-integral weight eigenform. Ono and Skinner showed (under the additional assumption that $f(z)$ is "good", which was later removed by McGraw [21] and Jimenez-Urroz and Ono [14]) that if $f(z)$ satisfies (2.1) and (2.3) and is an eigenform of the half-integral weight Hecke operators, then it can have the form (2.4) for only finitely many primes ℓ. Using different methods, Bruinier [5] proved the same result (with no additional assumption). In addition, Bruinier's method gives a description of the exceptional finite set of primes ℓ in terms of the Hecke eigenvalues of $f(z)$. These results lead to statements (1.3) and (1.4) discussed in the last section. Bruinier and Ono (see [6] or Proposition 4.1 below) later refined Bruinier's result.

More recently, the present authors [2] have placed restrictions on the weight of modular forms $f(z)$ which can satisfy (2.4). To be precise, write

$$\lambda = \overline{\lambda} + i_\lambda(\ell - 1), \tag{2.5}$$

where $\overline{\lambda} \in \{0, \dots, \ell - 2\}$ and $i_\lambda \geq 0$. If, for example, $\ell \nmid n_i$ for some i, then Theorem 2 of [2] implies that

$$\overline{\lambda} \leq 2i_\lambda + 1. \tag{2.6}$$

We remark that Theorem 2 of [2] is stated only for rational primes ℓ. However, the proof can be extended to treat arbitrary primes v. We also remark that the inequality (2.6) plays a vital role in the resolution of many cases of a classical conjecture of Newman regarding

the distribution modulo ℓ^j of values of the ordinary partition function (see Theorem 5 of [2]). In a brief addendum [3] we note that the inequality (2.6) is sharp for certain modular forms. For example, let $E_k(z)$ denote the usual Eisenstein series of weight k, let $\eta(z)$ denote the Dedekind eta-function, and let $\Theta := q\frac{d}{dq}$ be Ramanujan's differential operator. Then for each prime $\ell \geq 5$, the cusp form

$$E_{\ell+1}(8z)\eta^3(8z) \equiv \Theta\eta^3(8z) \equiv \sum_{n=0}^{\infty}(-1)^n(2n+1)^3q^{(2n+1)^2} \pmod{\ell} \tag{2.7}$$

has $\overline{\lambda} = 3$ and $i_\lambda = 1$, so that the inequality (2.6) reads $3 \leq 3$.

Our main result in this section is a precise $\pmod{\ell}$ version of the theorem of Vignéras in the following sense. Suppose that $f(z)$ is a modular form satisfying (2.1), (2.3), and (2.4), and suppose further that f is an eigenform modulo v. Our result states that, just as in the example (2.7), $f(z) \pmod{v}$ arises from the image of a single-variable theta series under iterated application of the theta-operator.

We now fix some notation. Suppose that $f(z)$ is a half-integral weight modular form which satisfies (2.1), (2.3), and (2.4) with $\lambda \geq 1$. If $\lambda = 1$, we also require that $f(z)$ be in the orthogonal complement (with respect to the Petersson inner product) of the subspace of $S_{\frac{3}{2}}(\Gamma_0(N), \chi)$ spanned by single-variable theta series. We further suppose that $f(z)$ is a Hecke eigenform modulo v; in other words, that, for each prime p with $p \nmid N\ell$, there is an algebraic integer λ_p such that

$$f(z)\big|T(p^2, \lambda + \tfrac{1}{2}, \chi) \equiv \lambda_p f(z) \pmod{v} \tag{2.8}$$

(we enlarge K if necessary to ensure that it contains the eigenvalues λ_p).

If $t \in \mathbb{Z}$, and the discriminant of $\mathbb{Q}(\sqrt{t})$ is D, then we denote by $\chi_t := \left(\frac{D}{\bullet}\right)$ the Kronecker character of conductor $|D|$. If χ is a Dirichlet character, we let χ^* be the Dirichlet character defined by $\chi^* := \chi_{-1}^{\lambda}\chi$ (the value of λ will always be clear from context).

We will prove the following analogue of the theorem of Vignéras.

Theorem 2.2. *Suppose that $f(z)$ satisfies* (2.1), (2.3), (2.4), *and* (2.8). *Then the following are true.*

(1) *The form $f(z)$ is supported on a single square class modulo v. In other words, we have $t = 1$ and*
$$f(z) \equiv \sum_{m=1}^{\infty} a(n_1m^2)q^{n_1m^2} \pmod{v}.$$

(2) *For every integer $m_0 \geq 1$, we have*
$$\sum_{\gcd(m, Nn_1m_0\ell)=1} a(n_1m_0^2m^2)q^{n_1m^2} \equiv a(n_1m_0^2) \sum_{\gcd(m,m_0)=1} \chi_{n_1}(m)\chi^*(m)m^{\lambda}q^{n_1m^2} \pmod{v}.$$

Remark. Here we do not assume that $\ell \nmid N$. We stress that if we are in the case when $\ell \nmid N$, then the weight inequalities given in Theorem 2 of [2] hold for every modular form $f(z)$ satisfying the hypotheses of Theorem 2.2.

Remark. Define $\epsilon_\lambda \in \{0, 1\}$ by

$$\epsilon_\lambda := \lambda \pmod{2}. \tag{2.9}$$

If $M \geq 1$ is an integer, we denote by χ_M^{triv} the trivial character modulo M. Using the notation from (2.2), (2.5), and (2.9), we define

$$g_{m_0}(z) := \frac{1}{2}\Theta^{\frac{\overline{\lambda}-\epsilon_\lambda}{2}}\psi(\chi_{m_0}^{\text{triv}}\chi_{n_1}\chi^*, z).$$

Note that $g_{m_0}(z)$ is not itself a half-integral weight modular form. It is, however, congruent modulo v to a form in the space $M_{\epsilon_\lambda+\frac{1}{2}+\frac{\overline{\lambda}-\epsilon_\lambda}{2}(\ell+1)}(\Gamma_0(N^2n_1^2m_0^2), \chi\chi_{n_1})$. We may restate the second conclusion of Theorem 2.2 in the following way (see Section 3 for precise definitions of the operators involved):

$$(f(z) \mid U_{n_1m_0^2}) \otimes \chi_{Nn_1\ell m_0}^{\text{triv}} \equiv a(n_1m_0^2)g_{m_0}(z) \pmod{v}. \tag{2.10}$$

This is the most natural way to construct forms satisfying (2.1), (2.3), (2.4), and (2.8). The main thrust of Theorem 2.2 is that every form of this type arises via such a construction.

Remark. A calculation shows that the image of a form as in Theorem 2.2 under the Shimura lift (see (3.14)) is congruent $\pmod{v}$ to the image of a weight two Eisenstein series under the operator $\Theta^{\lambda-1}$.

In the third section we pause to describe some of the objects and operators which we require. In Section 4 we prove Theorem 2.2 in the case when $\ell \nmid N$. The proof involves several theoretical tools. In particular, it requires the q-expansion principle (which is important in the work of Bruinier and Ono on the partial determination of the action of the half-integral weight Hecke algebra on forms satisfying (2.1), (2.3), and (2.4)), Shimura's theory of half-integral weight modular forms, the theory (due to Deligne and Serre) of residual Galois representations attached to integer weight eigenforms, and the work of Ribet and Swinnerton-Dyer on the determination of the possible images of these representations. In Section 5 we reduce the general case to the case when $\ell \nmid N$. Finally, in the last section we use Theorem 2.2 together with results of Kohnen in order to prove the results stated in the first section.

3. Background on modular forms

Here we briefly collect some of the facts which we will require regarding modular forms (see, for example, [15], [28], or [29] for details). Suppose that λ is a non-negative integer, that N is a positive integer with $4 \mid N$, and that χ is a Dirichlet character defined modulo N. Suppose that

$$f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi).$$

For each prime $p \nmid N$, there is a Hecke operator

$$T(p^2, \lambda+\tfrac{1}{2}, \chi) \ : \ S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi) \to S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi)$$

whose action is given by

$$f(z) \mid T(p^2, \lambda+\tfrac{1}{2}, \chi) = \sum_{n=1}^{\infty}\left(a(p^2n) + \left(\tfrac{n}{p}\right)\chi^*(p)p^{\lambda-1}a(n) + \chi^*(p^2)p^{2\lambda-1}a(n/p^2)\right)q^n. \tag{3.1}$$

We denote this operator simply by $T(p^2, \lambda+\frac{1}{2})$ when the character χ is trivial. Additionally, for each prime p, there are operators V_p and U_p whose actions are given by

$$f(z) \mid V_p = \sum_{n=1}^{\infty} a(n) q^{np} = f(pz),$$

$$f(z) \mid U_p = \sum_{n=1}^{\infty} a(np) q^n = \frac{1}{p} \sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right). \tag{3.2}$$

We have

$$V_p \ : \ S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi) \to S_{\lambda+\frac{1}{2}}(\Gamma_0(Np), \chi\chi_p). \tag{3.3}$$

If $4p \mid N$, then we have

$$U_p \ : \ S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi) \to S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi\chi_p). \tag{3.4}$$

Suppose that r is a positive integer, that ϕ is a Dirichlet character defined modulo r, and that χ has conductor s. Set $M := \operatorname{lcm}(N, r^2, rs)$. Then by Lemma 3.6 of [29], the twist $f(z) \otimes \phi := \sum_{n=1}^{\infty} \phi(n) a(n) q^n$ has

$$f(z) \otimes \phi \in S_{\lambda+\frac{1}{2}}(\Gamma_0(M), \chi\phi^2). \tag{3.5}$$

We next record some commutation relations between these operators (see §3 of [28] for some of these). Suppose as above that $f(z) = \sum_{n=1}^{\infty} a(n) q^n \in S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi)$. If p and p' are primes with $p \nmid N$, then we have

$$(f(z) \mid V_{p'}) \mid T(p^2, \lambda+\tfrac{1}{2}, \chi\chi_{p'}) = \big(f(z) \mid T(p^2, \lambda+\tfrac{1}{2}, \chi)\big) \mid V_{p'}. \tag{3.6}$$

If also $4p' \mid N$, then we have

$$(f(z) \mid U_{p'}) \mid T(p^2, \lambda+\tfrac{1}{2}, \chi\chi_{p'}) = \big(f(z) \mid T(p^2, \lambda+\tfrac{1}{2}, \chi)\big) \mid U_{p'}. \tag{3.7}$$

Finally, if ϕ is a trivial or quadratic character defined modulo r, and $p \nmid Nr$ is prime, then we have

$$(f(z) \otimes \phi) \mid T(p^2, \lambda+\tfrac{1}{2}, \chi) = \big(f(z) \mid T(p^2, \lambda+\tfrac{1}{2}, \chi)\big) \otimes \phi. \tag{3.8}$$

We define G to be the group extension of $\mathrm{GL}_2^+(\mathbb{R})$ whose elements are pairs $(M, \phi(z))$, where $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R})$ and $\phi(z)^2 = \alpha \det(M)^{-\frac{1}{2}}(tz+u)$, with $|\alpha| = 1$. Then the slash operator is given by

$$(f \mid_{\lambda+\frac{1}{2}} (M, \phi))(z) := \phi(z)^{-(2\lambda+1)} f(Mz). \tag{3.9}$$

If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4)$, then we define

$$\varepsilon_d := \begin{cases} 1 & \text{if } d \equiv 1 \pmod 4, \\ i & \text{if } d \equiv 3 \pmod 4, \end{cases}$$

and

$$j(A, z) := \varepsilon_d^{-1} \left(\tfrac{c}{d}\right) (cz+d)^{\frac{1}{2}},$$

and we set $A^* := (A, j(A, z)) \in G$.

If $p \mid N$ is a prime such that $\gcd(p, N/p) = 1$, then there are integers a and b for which $pb - (N/p)a = 1$, and we define

$$W_p^N := \left(\begin{pmatrix} p & a \\ N & pb \end{pmatrix}, \chi_{-1}(p)^{-\frac{1}{2}} p^{-\frac{1}{4}} (Nz + pb)^{\frac{1}{2}} \right) \in G. \tag{3.10}$$

The Fricke (or Atkin-Lehner) involution (see [15], p. 39) is defined by

$$f \to f \mid_{\lambda+\frac{1}{2}} W_p^N.$$

It takes $S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi)$ to $S_{\lambda+\frac{1}{2}}\left(\Gamma_0(N), \chi\left(\frac{\cdot}{p}\right)\right)$.

If p is a prime with $4p \mid N$, then write $\Gamma_0(N/p)$ as the disjoint union

$$\Gamma_0(N/p) = \bigcup_{j=1}^{\mu} \Gamma_0(N) A_j. \tag{3.11}$$

If we assume that the character χ is definable modulo N/p, then (see, for example, [28], §3) we have the trace operator

$$\mathrm{Tr}_{N/p}^N \ : \ S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi) \to S_{\lambda+\frac{1}{2}}(\Gamma_0(N/p), \chi)$$

defined by

$$\mathrm{Tr}_{N/p}^N := \sum_{j=1}^{\mu} \chi(a_j) A_j^*. \tag{3.12}$$

If in addition we assume that $p^2 \nmid N$, then $\mu = p + 1$, and we may take

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix} \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix} \right\}_{j=0}^{p-1}$$

as the complete set of coset representatives in (3.11). Using (3.2), (3.9), (3.10), (3.11), and (3.12), a calculation shows that the trace operator may be written as

$$\mathrm{Tr}_{N/p}^N(f) = f + \chi_{-1}(p)^{-(\lambda+\frac{1}{2})} p^{-\frac{\lambda}{2}+\frac{3}{4}} \left(f \mid_{\lambda+\frac{1}{2}} W_p^N \right) \mid U_p. \tag{3.13}$$

Note that formula (3.13) is derived in [15] (on pages 66 and 67) in the case when $N/4$ is odd and square-free. The proof in this case is the same.

We briefly recall some facts about the Shimura correspondence (see [29] for details). If $\lambda \geq 2$, then for every square-free integer $t \geq 1$, we have the Shimura lift

$$\mathrm{Sh}_t \ : \ S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi) \to S_{2\lambda}(\Gamma_0(N), \chi^2).$$

If $f(z) = \sum a(n) q^n$, then the Shimura lift is defined by $\mathrm{Sh}_t(f(z)) := \sum_{n=1}^{\infty} A_t(n) q^n$, where the coefficients $A_t(n)$ are given by

$$\sum_{n=1}^{\infty} A_t(n) n^{-s} = L(s - \lambda + 1, \chi \chi_t \chi_{-1}^{\lambda}) \cdot \sum_{n=1}^{\infty} a(tn^2) n^{-s}. \tag{3.14}$$

The most important fact for our purposes is that each Shimura lift commutes with the actions of the Hecke operators of index p^2 and p on the respective spaces. If $\lambda = 1$, the situation is slightly different: the lift Sh_t takes the orthogonal complement (with respect to the Petersson inner product) of the subspace of $S_{\frac{3}{2}}(\Gamma_0(N), \chi)$ spanned by single-variable theta series to the space $S_2(\Gamma_0(N), \chi^2)$.

We briefly discuss integral weight modular forms; we do not suppose here that $4 \mid N$. If $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R})$, then we define the integral weight slash operator by

$$(f \mid_k \gamma)(z) := (\det \gamma)^{\frac{k}{2}}(cz+d)^{-k} f(\gamma z).$$

If a prime $p \mid N$ has $\gcd(p, N/p) = 1$, then there are integers a and b for which $bp - (N/p)a = 1$, and we define

$$w_p^N := \begin{pmatrix} p & a \\ N & pb \end{pmatrix}. \tag{3.15}$$

If χ is a real character, then the Atkin-Lehner involution

$$F \to F \mid_k w_p^N$$

sends $M_k(\Gamma_0(N), \chi)$ to itself. In the case where $N = p$, we may write the matrix in (3.15) simply as

$$w_p = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$$

If N is square-free, and $F(z) \in S_k(\Gamma_0(N))$ is a newform, then for each $p \mid N$ there is an integer $\epsilon_p \in \{\pm 1\}$ for which

$$F(z) \mid_k w_p^N = \epsilon_p F(z). \tag{3.16}$$

4. The proof of Theorem 2.2 when $\ell \nmid N$

In this section we prove Theorem 2.2 in the case when $\ell \nmid N$. Using an argument of Bruinier [5], the next result was proved by Bruinier and Ono ([6], Theorem 3.1) in the case when χ is a real character and $K = \mathbb{Q}$. Since the proof in the general case follows the arguments in these two works, we will not include the details here. The proof relies in a crucial way on the q-expansion principle of arithmetic geometry.

Proposition 4.1. *Suppose that*

$$f(z) = \sum_{n=1}^{\infty} a(n) q^n \in S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi)$$

has coefficients in the ring of integers $\mathcal{O}_K$ of a number field K, that $\mathfrak{m}$ is an ideal of $\mathcal{O}_K$ coprime to N, and that p is a rational prime coprime to N and $\mathfrak{m}$. If there is an $\epsilon_p \in \{\pm 1\}$ such that

$$f(z) \equiv \sum_{\left(\frac{n}{p}\right) \in \{0, \epsilon_p\}} a(n) q^n \pmod{\mathfrak{m}},$$

then

$$(p-1) f(z) \mid T(p^2, \lambda + \tfrac{1}{2}, \chi) \equiv \epsilon_p \chi^*(p)(p^\lambda + p^{\lambda-1})(p-1) f(z) \pmod{\mathfrak{m}}.$$

Theorem 2.2 in the case when $\ell \nmid N$ follows from the next two propositions.

Proposition 4.2. *Suppose that $f(z)$ satisfies hypotheses* (2.1), (2.3), (2.4), (2.8), *and that $\ell \nmid N$. Then $t = 1$.*

Proof. Since f has bounded denominators, we may suppose without loss of generality under these hypotheses that $f \in \mathcal{O}_K[[q]]$. Recall that for each i there is an integer $m_i \geq 1$ such that $a(n_i m_i^2) \not\equiv 0 \pmod{v}$. Suppose that $i \in \{1, \dots, t\}$. Then, following the argument of Lemma 4.1 of [2], we can find primes $p_{i,1}, \dots, p_{i,s_i}$, each greater than ℓ, and a modular form $f_i(z) \in S_{\lambda+\frac{1}{2}}(\Gamma_0(Np_{i,1}^2 \dots p_{i,s_i}^2), \chi) \cap \mathcal{O}_K[[q]]$ with the property that

$$f_i(z) \equiv \sum_{\gcd(m, \prod_j p_{i,j})=1} a(n_i m^2) q^{n_i m^2} \not\equiv 0 \pmod{v}. \tag{4.1}$$

Each form $f_i(z)$ can be constructed from $f(z)$ by iteratively taking twists of linear combinations of twists by trivial and quadratic characters defined modulo the primes $p_{i,j}$. Let N_0 be the least common multiple of N and all of the $p_{i,j}^2$. Then we have $\ell \nmid N_0$ and $f_i(z) \in S_{\lambda+\frac{1}{2}}(\Gamma_0(N_0), \chi)$ for each i. Moreover, using (3.8) together with (2.8), we see that for each i, and for all $p \nmid N_0\ell$, we have

$$f_i(z) \big| T(p^2, \lambda + \tfrac{1}{2}, \chi) \equiv \lambda_p f_i(z) \pmod{v}. \tag{4.2}$$

In view of (4.1), Proposition 4.1 implies that for each p with $p \nmid N_0\ell$, $p > \max\{n_i\}$, and $p \not\equiv 1 \pmod{\ell}$, we have

$$f_i(z) \big| T(p^2, \lambda + \tfrac{1}{2}, \chi) \equiv \left(\tfrac{n_i}{p}\right) \chi^*(p)(p^\lambda + p^{\lambda-1}) f_i(z) \pmod{v}. \tag{4.3}$$

Combining (4.2) and (4.3), we see that

$$\left(\tfrac{n_i}{p}\right) = \left(\tfrac{n_j}{p}\right) \quad \text{for } 1 \leq i, j \leq t \text{ and for } p \nmid N_0\ell,\ p \not\equiv \pm 1 \pmod{\ell},\ p > \max\{n_i\}. \tag{4.4}$$

From (4.4) we deduce that $t = 1$. If not, then let $n_i = p_1 \cdots p_r$ and $n_j = q_1 \cdots q_s$ be two distinct elements of $\{n_1, \dots, n_t\}$. We may suppose without loss of generality that n_i and n_j are coprime and that $s \geq 1$. If $n_j = 2$, then any large p such that $p \not\equiv \pm 1 \pmod{\ell}$ (recall that $\ell \geq 5$), $p \equiv 5 \pmod{8}$, and such that p is a quadratic residue modulo each of $p_1, \dots, p_r$ gives a contradiction to (4.4). If $n_j \neq 2$ then suppose that q_1 is odd. Let p be a large prime such that $p \not\equiv \pm 1 \pmod{\ell}$, $p \equiv 1 \pmod{8}$, such that p is a quadratic residue modulo each of $p_1, \dots, p_r$ and modulo each of the odd primes among $q_2, \dots, q_s$, and such that p is a quadratic non-residue modulo q_1. With this choice of p, (4.4) fails to hold (note that this argument works also when $q_1 = \ell$). □

The next proposition is the main step towards the second assertion of Theorem 2.2 in the case when $\ell \nmid N$.

Proposition 4.3. *Suppose that $f(z)$ satisfies hypotheses* (2.1), (2.3), (2.4), *and* (2.8), *and that $\ell \nmid N$. Let n_1 be the square-free integer given by Proposition 4.2, so that we have*

$$f(z) \equiv \sum_{m=1}^{\infty} a(n_1 m^2) q^{n_1 m^2} \not\equiv 0 \pmod{v}.$$

Then for all $p \nmid N n_1 \ell$ we have

$$f(z) \big| T(p^2, \lambda + \tfrac{1}{2}, \chi) \equiv \lambda_p f(z) \pmod{v},$$

where

$$\lambda_p \equiv \left(\tfrac{n_1}{p}\right) \chi^*(p)(p^\lambda + p^{\lambda-1}) \pmod{v}. \tag{4.5}$$

Remark. Proposition 4.1 implies that (4.5) holds for $p \nmid Nn_1\ell$ and $p \not\equiv 1 \pmod{\ell}$. Therefore the content of Proposition 4.3 is to make the same assertion for primes in this residue class.

Proof. Recalling from Section 3 the definition of the Shimura lifting, we define $F(z) := \mathrm{Sh}_{n_1}(f(z)) \in S_{2\lambda}(\Gamma_0(N), \chi^2) \cap \mathcal{O}_v[[q]]$. Using the fact that the Shimura correspondence commutes with the action of the Hecke operators, we find from (2.8) that

$$F(z)\big|T(p, 2\lambda, \chi^2) \equiv \lambda_p F(z) \pmod{v} \text{ for } p \nmid N\ell.$$

Let m_v be the maximal ideal of $\mathcal{O}_v$, and let $\mathbb{F}_v := \mathcal{O}_v/m_v$ be the residue field. By Théorème 6.7 of [10], there exists a continuous semisimple representation

$$\rho \ : \ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_v),$$

unramified outside of $N\ell$, and such that for primes $p \nmid N\ell$ we have

$$\mathrm{Tr}(\rho(\mathrm{Frob}_p)) \equiv \lambda_p \pmod{v}, \tag{4.6}$$

$$\mathrm{Det}(\rho(\mathrm{Frob}_p)) \equiv \chi^2(p)p^{2\lambda-1} \pmod{v}. \tag{4.7}$$

Following the arguments of Section 4 of [2] (see in particular (4.9)-(4.17) of that work), we conclude from (4.6) and the remark above that the representation ρ is reducible. Since ρ is semisimple, it follows (as in the proof of Theorem 2.1 of [24]) that ρ can be written as a direct sum

$$\rho = \psi_1\chi_\ell^{m'} \oplus \psi_2\chi_\ell^{m} \tag{4.8}$$

where ψ_1 and ψ_2 are Dirichlet characters unramified outside N (viewed as characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in the usual way), $\chi_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\ell^\times$ is the mod ℓ cyclotomic character, and m and m' are integers defined modulo $\ell - 1$. Comparing (4.7) and (4.8) for sufficiently many primes p, we conclude that $m' + m \equiv 2\lambda - 1 \pmod{\ell - 1}$ and that $\psi_1\psi_2 = \chi^2$. We may suppose that $0 \le m < m' \le \ell - 2$.

Writing $\psi := \psi_1$ and using the remark above together with (4.6) and (4.8), we conclude that, for $p \nmid Nn_1\ell$ and $p \not\equiv 1 \pmod{\ell}$, we have

$$\mathrm{Tr}(\rho(\mathrm{Frob}_p)) \equiv \psi(p)p^{m'} + \overline{\psi}(p)\chi^2(p)p^m \equiv \left(\tfrac{n_1}{p}\right)\chi^*(p)(p^\lambda + p^{\lambda-1}) \pmod{v}. \tag{4.9}$$

Suppose that $p \equiv -1 \pmod{\ell}$. Then, since m and m' have opposite parity, (4.9) becomes

$$\psi(p) - \overline{\psi}(p)\chi^2(p) \equiv 0 \pmod{v}.$$

Therefore, $\psi(p) = \overline{\psi}(p)\chi^2(p)$ for some p in every residue class of $(\mathbb{Z}/N\mathbb{Z})^*$; it follows that $\psi = \overline{\psi}\chi^2$. Hence, if $p \nmid Nn_1\ell$ and $p \not\equiv 1 \pmod{\ell}$, (4.9) becomes

$$\mathrm{Tr}(\rho(\mathrm{Frob}_p)) \equiv \psi(p)(p^{m'} + p^m) \equiv \left(\tfrac{n_1}{p}\right)\chi^*(p)(p^\lambda + p^{\lambda-1}) \pmod{v}. \tag{4.10}$$

To finish the proof, suppose first that $\ell \nmid n_1$. It suffices to establish (4.10) for primes $p \nmid Nn_1\ell$ and $p \equiv 1 \pmod{\ell}$; for this it is enough to show that for these primes we have

$$\psi(p) = \left(\tfrac{n_1}{p}\right)\chi^*(p). \tag{4.11}$$

If $p \nmid Nn_1\ell$ has $p \equiv 1 \pmod{Nn_1}$ and $p \not\equiv 1 \pmod{\ell}$, then (4.10) yields

$$p^{m'} + p^m \equiv p^\lambda + p^{\lambda-1} \pmod{\ell}. \tag{4.12}$$

If n is a non-negative integer, then we define the integer $\overline{n} \in \{0, \dots, \ell-2\}$ by $\overline{n} := n \pmod{\ell-1}$. Since we can find a prime p satisfying (4.12) in each residue class modulo ℓ, it follows that

$$\{m,\, m'\} = \{\overline{\lambda},\, \overline{\lambda-1}\}. \tag{4.13}$$

From (4.10) and (4.13) we see that (4.11) holds for $p \nmid Nn_1\ell$ and $p \not\equiv \pm 1 \pmod{\ell}$. It follows that (4.11) holds for all $p \nmid Nn_1\ell$, which proves the proposition in this case.

Next, suppose that $\ell \mid n_1$. Write $n_1 = \ell n_1'$ with $\ell \nmid n_1'$. In this case, for $p \nmid Nn_1'\ell$ and $p \not\equiv 1 \pmod{\ell}$, (4.10) becomes

$$\mathrm{Tr}(\rho(\mathrm{Frob}_p)) \equiv \psi(p)(p^{m'} + p^m) \equiv \left(\frac{(-1)^{\frac{\ell-1}{2}} n_1'}{p}\right) \chi^*(p)(p^{\lambda+\frac{\ell-1}{2}} + p^{\lambda+\frac{\ell-3}{2}}) \pmod{v}. \tag{4.14}$$

As in the previous case, it suffices to show for all primes $p \nmid Nn_1'\ell$ and $p \equiv 1 \pmod{\ell}$ that

$$\psi(p) = \left(\frac{(-1)^{\frac{\ell-1}{2}} n_1'}{p}\right) \chi^*(p). \tag{4.15}$$

If $p \nmid Nn_1'\ell$ has $p \equiv 1 \pmod{Nn_1'}$ and $p \not\equiv 1 \pmod{\ell}$, then (4.14) becomes

$$p^{m'} + p^m \equiv p^{\lambda+\frac{\ell-1}{2}} + p^{\lambda+\frac{\ell-3}{2}} \pmod{\ell}.$$

It follows that

$$\{m, m'\} = \{\overline{\lambda+\tfrac{\ell-1}{2}},\, \overline{\lambda+\tfrac{\ell-3}{2}}\}. \tag{4.16}$$

From (4.14) and (4.16) we find that (4.15) holds for $p \nmid Nn_1'\ell$ and $p \not\equiv \pm 1 \pmod{\ell}$. The characters involved in (4.15) are defined modulo Nn_1'; it follows that (4.15) holds for all $p \nmid Nn_1'\ell$, which proves the proposition in this case. □

We now turn to the proof of Theorem 2.2 under the assumption that $\ell \nmid N$. Suppose that $f(z)$ satisfies hypotheses (2.1), (2.3), (2.4), and (2.8). The first assertion in the theorem follows immediately from Proposition 4.2. We may therefore suppose that

$$f(z) \equiv \sum_{m=1}^{\infty} a(n_1m^2) q^{n_1m^2} \not\equiv 0 \pmod{v}.$$

Using Proposition 4.3 and (3.1), we conclude for every prime $p \nmid Nn_1\ell$ and for every positive integer m_0 that

$$\begin{aligned} a(n_1m_0^2p^2) + \chi^*(p)\left(\tfrac{n_1m_0^2}{p}\right) p^{\lambda-1} a(n_1m_0^2) + \chi(p^2)p^{2\lambda-1} a\left(\frac{n_1m_0^2}{p^2}\right) \\ \equiv \chi^*(p)\left(\tfrac{n_1}{p}\right)(p^\lambda + p^{\lambda-1}) a(n_1m_0^2) \pmod{v}. \end{aligned} \tag{4.17}$$

For every $p \nmid Nn_1m_0\ell$, a straightforward induction on j using (4.17) yields

$$a(n_1m_0^2p^{2j}) \equiv a(n_1m_0^2)\chi^*(p^j)\left(\tfrac{n_1}{p^j}\right) p^{j\lambda} \pmod{v}. \tag{4.18}$$

Using (4.18) repeatedly, we obtain, for all integers $m \geq 1$ with $\gcd(m, Nn_1m_0\ell) = 1$,

$$a(n_1m_0^2m^2) \equiv a(n_1m_0^2)\chi^*(m)\left(\tfrac{n_1}{m}\right) m^\lambda \pmod{v}.$$

This concludes the proof in the case when $\ell \nmid N$. □

5. Reduction to the case when $\ell \nmid N$.

The general statement of Theorem 2.2 follows directly from the results of the last section together with the next proposition. We adapt the proof of the analogous result in the integral weight setting (see Theorem 2.1 of [25]).

Proposition 5.1. *Suppose that $\ell \geq 5$ is prime, that K is a number field, that v is a place of K over ℓ, and that $\mathcal{O}_v$ is the associated valuation ring. Suppose that $\ell \nmid N$, that $j \geq 1$ is an integer, and that*

$$f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{\lambda+\frac{1}{2}}(\Gamma_0(N\ell^j), \chi) \cap \mathcal{O}_v[[q]].$$

Suppose for each $p \nmid N\ell$ that $f(z)$ is an eigenform modulo v of the Hecke operator $T(p^2, \lambda + \frac{1}{2}, \chi)$. Then there is an integer λ', a character χ' modulo N, and a cusp form $f'(z) \in S_{\lambda'+\frac{1}{2}}(\Gamma_0(N), \chi') \cap \mathcal{O}_v[[q]]$ such that

$$f'(z) \equiv f(z) \pmod{v}$$

and such that, for each $p \nmid N\ell$, $f'(z)$ is an eigenform modulo v of the Hecke operator $T(p^2, \lambda' + \frac{1}{2}, \chi')$.

Proof. Let $\mathbb{F}_v := \mathcal{O}_v/m_v$ as before, and let $r \geq 1$ be the integer for which $\#\mathbb{F}_v = \ell^r$. Note that for all $u \in \mathbb{F}_v$, we have

$$u^{\ell^r} = u. \tag{5.1}$$

We first decompose the character χ into a suitable form. Let ω denote the Teichmüller character with conductor ℓ, so that ω has order $\ell - 1$ and coincides with the identity map on $\mathbb{F}_\ell$. There is a character η of ℓ-power order and ℓ-power conductor, a character ϵ of conductor dividing N, and an integer $i \geq 1$ such that

$$\chi = \epsilon\eta\omega^i.$$

We define the Eisenstein series (see, for example [12], Proposition 5.1.2)

$$E_{\overline{\omega}^i}(z) := 1 - \frac{2i}{B_{i,\overline{\omega}^i}} \sum_{n=1}^{\infty} \sum_{d|n} \overline{\omega}^i(d) d^{i-1} q^n \in M_i(\Gamma_0(\ell), \overline{\omega}^i),$$

where $B_{i,\overline{\omega}^i}$ is the ith generalized Bernoulli number attached to $\overline{\omega}^i$. This series has v-integral coefficients and satisfies

$$E_{\overline{\omega}^i}(z) \equiv 1 \pmod{v}. \tag{5.2}$$

We let $a \geq 2$ be an even integer for which $ar \geq j$ and we set

$$\tilde{\lambda} := \lambda\ell^{ar} + \frac{\ell^{ar} - 1}{2} + i \quad \text{and} \quad \tilde{\epsilon} := \epsilon^{\ell^{ar}}.$$

Using (5.1), (5.2), and (3.3), we deduce that

$$f(z)^{\ell^{ar}} E_{\overline{\omega}^i}(z) \equiv f(\ell^{ar} z) \equiv f(z) \mid V_{\ell^{ar}} \pmod{v} \tag{5.3}$$

is a modular form in $S_{\tilde{\lambda}+\frac{1}{2}}(\Gamma_0(N\ell^j), \tilde{\epsilon}\chi_{-1}^i)$ (to compute the character, recall that in order to consider a form of integral weight k as a form of half-integral weight, one must twist the character by χ_{-1}^k).

Next, we define the modular forms

$$\theta(z) := 1 + 2\sum_{n=1}^{\infty} q^{n^2} \in M_{\frac{1}{2}}(\Gamma_0(4))$$

and

$$h(z) := \left(f(z)^{\ell^{ar}} E_{\overline{\omega}^i}(z)\theta(\ell^{ar}z)\right) \mid U_{\ell^{ar}} = \left(f(z)^{\ell^{ar}} E_{\overline{\omega}^i}(z)\right) \mid U_{\ell^{ar}} \cdot \theta(z).$$

Since the modular form

$$f(z)^{\ell^{ar}} E_{\overline{\omega}^i}(z)\theta(\ell^{ar}z) \in S_{\tilde{\lambda}+1}(\Gamma_0(N\ell^{ar}), \tilde{\epsilon}\chi_{-1}^{i+\tilde{\lambda}+1})$$

has integral weight and character defined modulo N, Lemma 1 of [19] implies that $h(z) \in S_{\tilde{\lambda}+1}(\Gamma_0(N\ell), \tilde{\epsilon}\chi_{-1}^{i+\tilde{\lambda}+1})$. Therefore, we find that $\frac{h(z)}{\theta(z)}$ is a meromorphic modular form of weight $\tilde{\lambda}+\frac{1}{2}$ and character $\tilde{\epsilon}\chi_{-1}^{i}$ with respect to $\Gamma_0(N\ell)$.

On the other hand, by (3.4), we have

$$\frac{h(z)}{\theta(z)} = \left(f(z)^{\ell^{ar}} E_{\overline{\omega}^i}(z)\right) \mid U_{\ell^{ar}} \in S_{\tilde{\lambda}+\frac{1}{2}}(\Gamma_0(N\ell^j), \tilde{\epsilon}\chi_{-1}^{i}).$$

Combining these facts, it follows that

$$\frac{h(z)}{\theta(z)} \in S_{\tilde{\lambda}+\frac{1}{2}}(\Gamma_0(N\ell), \tilde{\epsilon}\chi_{-1}^{i}).$$

Furthermore, using (5.3), we see that

$$\frac{h(z)}{\theta(z)} = \left(f(z)^{\ell^{ar}} E_{\overline{\omega}^i}(z)\right) \mid U_{\ell^{ar}} \equiv f(z) \mid V_{\ell^{ar}} \mid U_{\ell^{ar}} \equiv f(z) \pmod{v}.$$

It remains to lower the level from $N\ell$ to N. For this purpose we adapt the argument of Serre ([27], §3.2). As in that work, we define modular forms

$$E_{\ell-1}(z) := 1 - \frac{2(\ell-1)}{B_{\ell-1}} \sum_{n=1}^{\infty}\sum_{d|n} d^{\ell-2}q^n \in M_{\ell-1}(\Gamma_0(1)), \tag{5.4}$$

$$g(z) := E_{\ell-1}(z) - \ell^{\frac{\ell-1}{2}} E_{\ell-1} \mid_{\ell-1} w_\ell \in M_{\ell-1}(\Gamma_0(\ell)), \tag{5.5}$$

where $B_{\ell-1}$ is the usual Bernoulli number. From (5.4) and (5.5), it follows that, for all integers $m \geq 1$, $g(z)$ satisfies

$$g(z)^{\ell^m} \equiv 1 \pmod{\ell^{m+1}}, \tag{5.6}$$

$$g(z) \mid_{\ell-1} w_\ell \equiv 0 \pmod{\ell^{\frac{\ell+1}{2}}}. \tag{5.7}$$

If $m \geq 1$ is an integer, we set

$$\lambda_m := \tilde{\lambda} + \ell^m(\ell-1) \text{ and } f_m(z) := \frac{h(z)}{\theta(z)} \cdot g(z)^{\ell^m} \in S_{\lambda_m+\frac{1}{2}}(\Gamma_0(N\ell), \tilde{\epsilon}\chi_{-1}^{i}).$$

By (3.13), we have

$$\mathrm{Tr}_N^{N\ell}(f_m(z)) \in S_{\lambda_m+\frac{1}{2}}(\Gamma_0(N), \tilde{\epsilon}\chi_{-1}^{i}).$$

Using (3.13), (5.6), and (5.7), and adapting the argument of [27], §3.2 to the half-integral weight setting (we omit the details), we conclude that if m is large enough, then

$$\mathrm{Tr}_N^{N\ell}(f_m(z)) \equiv f(z) \pmod{v}. \tag{5.8}$$

Hence, if m is an integer for which (5.8) holds, we see that the conclusion of the proposition holds with $\lambda' = \lambda_m$, $\chi' = \tilde{\epsilon}\chi_{-1}^i$, and $f'(z) = \mathrm{Tr}_N^{N\ell}(f_m(z))$. A calculation using (3.1) shows that the modular form $f'(z)$ obtained this way is an eigenform modulo v for the Hecke operators $T(p^2, \lambda_m + \frac{1}{2}, \tilde{\epsilon}\chi_{-1}^i)$ for all primes $p \nmid N\ell$.

□

6. The proof of Theorem 1.1

In this section, we use Theorem 2.2 together with work of Kohnen to prove Theorem 1.1. Let $N \geq 1$ be an odd square-free integer, and let

$$F(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{2\lambda}^{\mathrm{new}}(\Gamma_0(N)) \tag{6.1}$$

be a normalized newform as in the hypotheses of Theorem 1.1.

By work of Kohnen [15] it is known that the new subspaces $S_{2\lambda}^{\mathrm{new}}(\Gamma_0(N))$ and $S_{\lambda+\frac{1}{2}}^{\mathrm{new}}(\Gamma_0(4N))$ are isomorphic as Hecke modules. In particular, there is a non-zero (and unique up to scalar multiplication) eigenform

$$g(z) = \sum_{(-1)^\lambda n \equiv 0,1 \pmod 4} c(n)q^n \in S_{\lambda+\frac{1}{2}}^{\mathrm{new}}(\Gamma_0(4N)) \tag{6.2}$$

with the same Hecke eigenvalues as F. For every prime $p \mid N$, let $\epsilon_p \in \{\pm 1\}$ denote the eigenvalue of $F(z)$ for the Fricke involution w_p^N (see (3.16)). If D is coprime to N, $(-1)^\lambda D > 0$, and $c(|D|) \neq 0$, then (see, for example, the remark following Corollary 1 of [16]), we have

$$\left(\frac{D}{p}\right) = \epsilon_p \quad \text{for all } p \mid N. \tag{6.3}$$

By equation (11) of [16], we find that, for every D with $(-1)^\lambda D > 0$ and every integer $n \geq 1$, the coefficients of $g(z)$ and $F(z)$ are related by

$$c(n^2|D|) = c(|D|) \sum_{\substack{d \mid n \\ \gcd(d,N)=1}} \mu(d) \left(\frac{D}{d}\right) d^{\lambda-1} a\left(\frac{n}{d}\right). \tag{6.4}$$

Let $\langle \cdot\,, \cdot \rangle$ denote the Petersson inner product, and let $\nu(N)$ denote the number of distinct prime divisors of N. Kohnen proved the following.

Theorem 6.1 ([16], Corollary 1)**.** *Suppose that $F(z)$ and $g(z)$ are as in* (6.1) *and* (6.2)*, respectively. Suppose that D is a fundamental discriminant with $(-1)^\lambda D > 0$ which satisfies* (6.3)*. Then*

$$\frac{|c(|D|)|^2}{\langle g, g \rangle} = 2^{\nu(N)} \frac{(\lambda-1)!}{\pi^\lambda} |D|^{\lambda-\frac{1}{2}} \frac{L(F \otimes \chi_D, \lambda)}{\langle F, F \rangle}. \tag{6.5}$$

The appearance of the absolute value on the coefficients $c(|D|)$ creates some technical difficulty when working modulo ℓ. To circumvent this difficulty, we will use the following lemma[1].

[1]We are grateful to W. Kohnen for suggesting this approach.

Lemma 6.2. *Suppose that $f(z) = \sum a(n)q^n \in S^{\text{new}}_{\lambda+\frac{1}{2}}(\Gamma_0(4N))$ is a newform, and that $a(n_0)$ is a non-zero coefficient of f. Then the form $\frac{1}{a(n_0)}f(z)$ has real Fourier coefficients.*

Proof of Lemma 6.2. If $f(z) = \sum a(n)q^n$, then set $f^c(z) := \sum \overline{a(n)}q^n$. We have $f^c(z) = \overline{f(-\overline{z})}$. A direct computation using this fact together with the transformation law in half-integral weight shows that the map $f \mapsto f^c$ preserves the space $S^+_{\lambda+\frac{1}{2}}(\Gamma_0(4N))$ (the "plus space" is the space of forms having expansions as in (6.2)).

We claim that this map also preserves the space $S^{\text{new}}_{\lambda+\frac{1}{2}}(\Gamma_0(4N))$. Suppose for the moment that this has been established. The eigenvalues for f under the operators $T(p^2, \lambda+\frac{1}{2})$ and $U(p^2)$ are real (since they are also eigenvalues for some newform in $S_{2\lambda}(\Gamma_0(N))$). Examining Fourier expansions and using the claim, we see that f^c is a newform with the same eigenvalues as f; by "multiplicity one" we conclude that f^c is a constant multiple of f. If some coefficient of f equals one then $f^c = f$; the lemma follows.

It remains to prove the claim. Kohnen ([15], §5, Theorem 2) proved the decomposition

$$S^+_{\lambda+\frac{1}{2}}(\Gamma_0(4N)) = S^{\text{new}}_{\lambda+\frac{1}{2}}(\Gamma_0(4N)) \oplus \bigoplus_{r\geq 1,\ d<N,\ rd|N} S^{\text{new}}_{\lambda+\frac{1}{2}}(\Gamma_0(4d))\big|U(r^2). \tag{6.6}$$

For each $p \nmid N$ let λ_p be the eigenvalue of f under $T(p^2, \lambda+\frac{1}{2})$. If f^c is not new at level N, then it follows from this decomposition that there exists a proper divisor d of N and a newform $g(z) \in S^{\text{new}}_{\lambda+\frac{1}{2}}(\Gamma_0(4d))$ with eigenvalues $\overline{\lambda_p}$ for $p \nmid N$. From the theorem of Kohnen just mentioned, we conclude that there is a modular form $G(z) \in S_{2\lambda}(\Gamma_0(d))$ with the same eigenvalues. On the other hand, f^c is an eigenform for all operators $T(p^2, \lambda+\frac{1}{2})$ and $U(p^2)$. Again by Kohnen's theorem, there exists a modular form $G_1(z) \in S_{2\lambda}(\Gamma_0(N))$ which is an eigenform for all $T(p)$ (for $p \nmid N$) and $U(p)$ (for $p \mid N$) with the same eigenvalues as f^c. By the theory of integral weight newforms (see Theorem 5 of [1]), $G_1(z)$ is a newform at level N. However, the form $G(z)$ has level d and the same eigenvalues as $G_1(z)$ for $p \nmid N$. This contradicts the last mentioned theorem; it follows that f^c is new at level N. □

Proof of Theorem 1.1. Let $g(z)$ be as in (6.2). After normalizing, we may assume after Lemma 6.2 that all of the coefficients $c(n)$ are real, and that $c(|D_0|) = 1$ for some fundamental discriminant D_0. Set

$$\Omega^* := \frac{\langle F, F\rangle \pi^\lambda}{\langle g, g\rangle 2^{\nu(N)}(\lambda-1)!}.$$

Then, for D such that $(-1)^\lambda D > 0$ and $\left(\frac{D}{p}\right) = \epsilon_p$ for all $p \mid N$, (6.5) becomes

$$c(|D|)^2 = \frac{L(F\otimes\chi_D, \lambda)|D|^{\lambda-\frac{1}{2}}}{\Omega^*}. \tag{6.7}$$

Let Ω be the period given in the statement of Theorem 1.1, and define

$$b(n) := c(n)\sqrt{\tfrac{\Omega^*}{\Omega}}. \tag{6.8}$$

Set $h(z) := \sum b(n)q^n$. From (6.7), (6.8), (6.4), and (1.2) we see that the coefficients of h and g are all algebraic (recall that $c(|D_0|) = 1$ for some D_0). Moreover, the hypothesis (1.5) in Theorem 1.1 implies that the minimum

$$M := \min_D \{v_\ell(b(|D|))\} \tag{6.9}$$

is attained for two distinct fundamental discriminants D. Applying Theorem 2.2 to a suitable normalization of $h(z)$, we conclude that there are infinitely many distinct square-free n_i such that there exists m_i with $v_\ell\left(b(n_i m_i^2)\right) = M$. It follows from (6.4) that there are infinitely many distinct fundamental discriminants D such that $v_\ell\left(b(|D|)\right) = M$. Theorem 1.1 follows from this fact together with (6.7) and (6.8). (With regard to the remark following the statement of Theorem 1.1, note that the principle of bounded denominators applied to the form $h(z)$ shows that the minimum in (1.5) indeed exists.) □

Proof of Theorem 1.2. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N as in the statement of the theorem, and let f be the associated weight two modular form. For primes $p \mid N$, let ϵ_p be the eigenvalue of $f(z)$ under the involution w_p^N. If D is a fundamental discriminant with $(D, N) = 1$ then let E_D be the D-quadratic twist of E. Recall from (1.10) that, for negative D such that $L(E_D, 1) \neq 0$, we have

$$\frac{L(f \otimes \chi_D, 1) \cdot \sqrt{|D_0|}}{\Omega(E_{-4})} = \frac{L(E_D, 1) \cdot \sqrt{|D_0|}}{\Omega(E_{-4})} = \frac{\mathrm{Sha}(E_D)}{|E_D(\mathbb{Q})_{\mathrm{tor}}|^2} \mathrm{Tam}(E_D). \tag{6.10}$$

Mazur [20] proved that only primes ≤ 7 can divide $|E_D(\mathbb{Q})_{\mathrm{tor}}|$. We conclude that for each prime $\ell \geq 11$ and for each negative fundamental discriminant D with $L(E_D, 1) \neq 0$, we have

$$v_\ell\left(\frac{L(f \otimes \chi_D, 1)\sqrt{|D_0|}}{\Omega(E_{-4})}\right) \geq 0. \tag{6.11}$$

We require the following lemma.

Lemma 6.3. *With all notation as above, suppose that* $\left(\frac{D}{p}\right) = \epsilon_p$ *for all* $p \mid N$. *Then* $\mathrm{Tam}(E_D)$ *is divisible only by the primes* 2 *and* 3.

Proof of Lemma 6.3. Using a result of Kodaira and Néron (see Theorem 6.1 of Chapter VII of [31]), it suffices to show, under these hypotheses, that E_D does not have split multiplicative reduction for any prime p. Let $f_E(z) = \sum a(n)q^n$ and $f_{E_D}(z) = \sum b(n)q^n$ be the weight two newforms associated to E and E_D. Then we have

$$b(n) = \left(\tfrac{D}{n}\right) a(n) \quad \text{for all } n. \tag{6.12}$$

Using the description of the Euler factor of the L-series of an elliptic curve at a prime of bad reduction (see §16 of Appendix C of [31]) it will suffice to show that for all $p \mid DN$ we have $b(p) \neq 1$. From (6.12) this is obvious if $p \mid D$.

We may therefore suppose that $p \mid N$. By Theorem 3 of [1] we have $\epsilon_p = -a(p)$. However, we also have $\epsilon_p = \left(\frac{D}{p}\right)$. Combining these facts with (6.12) we see that it is impossible to have $b(p) = 1$; the lemma follows. □

To finish we notice that, together with Lemma 6.3, the assumption in Theorem 1.2 implies that equality is achieved in (6.11) for two distinct negative fundamental discriminants D satisfying (6.3). By Theorem 1.1 it follows that equality is achieved for infinitely many such D. Theorem 1.2 now follows from (6.10). □

Acknowledgments. We are grateful to W. Kohnen for helpful discussions and to K. Ono for helpful comments on an earlier draft of this paper.

References

[1] A.O.L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(M)$, Math. Ann. **185** (1970), 134-160.

[2] S. Ahlgren and M. Boylan, *Coefficients of half-integral weight modular forms modulo* ℓ^j, Math. Ann. **331** (2005), 219-239.

[3] S. Ahlgren and M. Boylan, *Coefficients of half-integral weight modular forms modulo* ℓ^j *(addendum)*, Math. Ann. **331** (2005), 241-242.

[4] J. Bruinier, *On a theorem of Vignéras*, Abh. Math. Sem. Univ. Hamburg **68** (1998), pages 163-168.

[5] J. Bruinier, *Non-vanishing modulo* ℓ *of Fourier coefficients of half-integral weight modular forms*, Duke Math. J. **98** (1999), 595-611.

[6] J. Bruinier and K. Ono, *Coefficients of half-integral weight modular forms*, J. Number Theory **99** (2003), 164-179.

[7] J. Bruinier and K. Ono, *Coefficients of half-integral weight modular forms (corrigendum)*, J. Number Theory **104** (2004), 378-379.

[8] D. Bump, S. Friedberg, and J. Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. **102** (1990), 543-618.

[9] H. Darmon, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Mathematics, Number 101 (2004), American Mathematical Society, Providence, RI.

[10] P. Deligne and J.-P. Serre, *Formes modulaires de poids* 1, Ann. Sci. École Normale Sup. 4^e sér. 7 (1974), 507-530.

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

[12] H. Hida, *Elementary theory of L-functions and Eisenstein series*, London Math. Soc. Student Texts **26**, Cambridge Univ. Press, (1993).

[13] H. Iwaniec, *On the order of vanishing of modular L-functions at the critical point*, Séminaire de Théorie des Nombres, Bordeaux **2** (1990), 365-376.

[14] J. Jimenez-Urroz and K. Ono, *On "good" half-integral weight modular forms*, Math. Res. Lett. **7** (2000), no. 2-3, 205-212.

[15] W. Kohnen, *Newforms of half-integral weight*, J. Reine Angew. Math. **333** (1982), 32-72.

[16] W. Kohnen, *Fourier coefficients of modular forms of half-integral weight*, Math. Ann. **271** (1985), 237-268.

[17] W. Kohnen and D. Zagier, *Values of L-series of modular forms at the center of the critical strip*, Invent. Math. **64** (1981), 173-198.

[18] V. Kolyvagin, *Euler Systems*, in The Grothendieck Festschrift, Vol. II, Prog. Math. **87**, Birkhäuser, Boston, MA (1990), 435-483.

[19] W.-C. Li, *Newforms and functional equations*, Math. Ann. **212** (1975), 285-315.

[20] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33-186.

[21] W. McGraw, *On a theorem of Ono and Skinner*, J. Number Theory **86** (2001), 244-252.

[22] M. R. Murty and V. K. Murty, *Mean values of derivatives of modular L-series*, Ann. of Math. **133** (1991), 447-475.

[23] K. Ono and C. Skinner, *Fourier coefficients of half-integral weight modular forms modulo* ℓ, Ann. of Math. **147** (1998), 453-470.

[24] K. Ribet, *On* ℓ*-adic representations attached to modular forms II*, Glasgow Math. J. **27** (1985), 185-194.

[25] K. Ribet, *Report on mod* ℓ *representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Proc. Sympos. Pure Math. vol. 55 Part 2, Amer. Math. Soc. (1994), 639-676.

[26] K. Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), 527-559.

[27] J.-P. Serre, *Formes modulaires et fonctions zêta p-adiques*, Lect. Notes in Math. **350** (Modular functions of one variable III), Springer-Verlag Berlin, (1973), 191-268.

[28] J.-P. Serre and H. Stark, *Modular forms of weight* $\frac{1}{2}$, Lect. Notes in Math. **627** (Modular functions of one variable VI), Springer-Verlag Berlin, (1977), 29-68.

[29] G. Shimura, *On modular forms of half-integral weight*, Ann. of Math. **97** (1973), 440-481.

[30] G. Shimura, *On the periods of modular forms*, Math. Ann. **229** (1977), 211-221.

[31] J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York Berlin Heidelberg (1986).
[32] M. F. Vignéras, *Facteurs gamma et équations fonctionelles*, Lect. Notes in Math. **627** (Modular functions of one variable VI), Springer-Verlag Berlin, (1977), 79-103.
[33] J.-L. Waldspurger, *Sur les valeurs de certaines fonctions L automorphe en leur centre de symétrie*, Compositio Math. **54** (1985), no 2, 173-242.
[34] J.-L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures et Appl. **60** (1981), pages 375-484.
[35] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995), no. 3, 443-551.
[36] S. Zhang, *Heights of points on Shimura curves*, Ann. of Math. (2) **153** (2001), no. 1, 27-147.

Department of Mathematics, University of Illinois, Urbana, IL 61801
E-mail address: ahlgren@math.uiuc.edu

Department of Mathematics, University of Illinois, Urbana, IL 61801
E-mail address: boylan@math.uiuc.edu