CRITICAL L-VALUES OF LEVEL p NEWFORMS $\pmod p$

SCOTT AHLGREN AND JEREMY ROUSE

Abstract. Suppose that $p \geq 5$ is prime, that $\mathcal{F}(z) \in S_{2k}(\Gamma_0(p))$ is a newform, that v is a prime above p in the field generated by the coefficients of $\mathcal{F}$, and that D is a fundamental discriminant. We prove non-vanishing theorems modulo v for the twisted central critical values $L(\mathcal{F} \otimes \chi_D, k)$. For example, we show that if k is odd and not too large compared to p, then infinitely many of these twisted L-values are nonzero $\pmod v$. We give applications for elliptic curves. For example, we prove that if $E/\mathbb{Q}$ is an elliptic curve of conductor p, where p is a sufficiently large prime, there there are infinitely many twists D with $\text{Ш}(E_D/\mathbb{Q})[p] = 0$, assuming the Birch and Swinnerton-Dyer conjecture for curves of rank zero as well as a weak form of Hall's conjecture. The results depend on a careful study of the coefficients of half-integral weight newforms of level $4p$, which is of independent interest.

1. Introduction and statement of results

Let $k \geq 1$ be an integer and let

$$f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{k+\frac{1}{2}}(\Gamma_0(4N)), \quad q = e^{2\pi i z},$$

be a cusp form of weight $k + \frac{1}{2}$ for the group $\Gamma_0(4N)$. If $f(z)$ is orthogonal to the space of single-variable theta series then the Shimura correspondence [37] associates to $f(z)$ a cusp form $\mathcal{F}(z)$. If $f(z)$ is an eigenform for the Hecke operators T_{p^2}, then famous theorems of Kohnen [20], Kohnen and Zagier [17], and Waldspurger [42] relate the numbers $a(|D|)^2$ and $L(\mathcal{F} \otimes \chi_D, k)$ for fundamental discriminants D (see below for precise statements). Using these results, a number of recent papers have studied the Fourier coefficients of such forms in connection with values of modular L-functions ([8], [32], [31], [3]), ranks and Tate-Shafarevich groups of elliptic curves ([9], [22]), ternary quadratic forms ([33], [16]), and combinatorial generating functions ([7], [1], [2]).

An important non-vanishing result in characteristic zero is due to Vignéras [41], who proved that if

$$f(z) = \sum_{i=1}^{m} \sum_{n=1}^{\infty} a(t_i n^2) q^{t_i n^2},$$

then $k = 0$ or 1 and $f(z)$ is a linear combination of single-variable theta series. Suppose now that $f(z)$ is normalized to have Fourier coefficients that are algebraic integers, and that v is a prime ideal in the ring of integers of the coefficient field of $f(z)$. In [7], [8] and [31], it is

Date: October 9, 2009.

2000 *Mathematics Subject Classification.* 11F33, 11F37, 11G05.

The second author was supported by NSF grant DMS-0901090.

shown that if $f(z)$ is not a linear combination of theta series, then a congruence of the form

$$f(z) \equiv \sum_{i=1}^{m} \sum_{n=1}^{\infty} a(t_i n^2) q^{t_i n^2} \pmod{v} \tag{1.1}$$

can occur for only finitely many v. Precise information about the action of the Hecke algebra on the form f mod v is determined when a congruence does occur, and this is used to obtain information about the distribution of the Fourier coefficients $a(n)$ in residue classes mod v.

Theorem 2.2 of [3] shows that if $f(z)$ is a Hecke eigenform modulo v, and (1.1) occurs, then $f(z)$ is essentially congruent to a single-variable theta series under repeated iteration of the Θ-operator defined by

$$\Theta\left(\sum a(n)q^n\right) := \sum na(n)q^n.$$

As a consequence, a precise description of the coefficients of f are obtained outside of those arithmetic progressions which share a factor with the level.

If N is an odd, square-free integer and k is an integer, then we denote by $S_{k+\frac{1}{2}}(4N)$ the *Kohnen plus-space* of forms of weight $k+\frac{1}{2}$ on $\Gamma_0(4N)$. Kohnen [19] showed that these spaces are isomorphic as Hecke modules to the spaces $S_{2k}(\Gamma_0(N))$, and that they possess a theory of newforms analogous to that in the integer weight case (definitions and more details can be found in the next section). In [4], assuming that $f(z) \in S_{k+\frac{1}{2}}(4)$ satisfies (1.1) (but is not necessarily a Hecke eigenform), it is shown that if v is a prime above ℓ and $k+\frac{1}{2} < \ell(\ell+1+\frac{1}{2})$, then k is even and $f(z) \equiv a(1)\sum n^k q^{n^2} \pmod{v}$ (the bound on the weight is sharp).

In this paper we obtain results of this type for Kohnen newforms of level $4p$ modulo primes above p, and we give applications to modular L-values and to the arithmetic of elliptic curves of conductor p modulo p. This situation (in which the level and the characteristic are the same) is quite interesting, and it produces phenomena which do not typically occur. Our first result is the following.

Theorem 1.1. *Suppose that k is a positive integer, that $p \geq 5$ is a prime with $p > \frac{2k-1}{3}$, that K is a number field, and that v is a prime of K above p. Suppose that*

$$f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S^{\text{new}}_{k+\frac{1}{2}}(4p)$$

is a Kohnen newform normalized to have Fourier coefficients which are algebraic integers in K, and suppose that f has the form

$$f(z) \equiv \sum_{i=1}^{r} \sum_{n=1}^{\infty} a(t_i n^2) q^{t_i n^2} \not\equiv 0 \pmod{v}.$$

Then k is even and

$$f(z) \equiv a(1) \sum_{n=1}^{\infty} n^k q^{n^2} \pmod{v}.$$

Remark. There are many Kohnen newforms of the type described in the theorem. For example, in the space $S^{\text{new}}_{2+\frac{1}{2}}(20)$ there is a single Kohnen newform

$$f(z) = q - 6q^4 + 5q^5 - q^9 + 16q^{16} - 10q^{20} - 30q^{21} + 20q^{24} - 5q^{25} + 20q^{29} + \cdots$$

which visibly satisfies the congruence

$$f(z) \equiv \sum_{n=1}^{\infty} n^2 q^{n^2} \pmod{5}.$$

We now discuss the connection to the L-values of integer weight newforms. Suppose that k is a positive integer, that N is an odd, positive, square-free integer, and that

$$\mathcal{F}(z) = \sum_{n=1}^{\infty} A(n) q^n \in S_{2k}^{\mathrm{new}}(\Gamma_0(N))$$

is a normalized newform. There is a Kohnen newform

$$f(z) = \sum_{n=1}^{\infty} a(n) q^n \in S_{k+\frac{1}{2}}^{\mathrm{new}}(4N)$$

which corresponds to $\mathcal{F}$ via the Shimura correspondence. We normalize f so that its Fourier coefficients are relatively prime algebraic integers.

For fundamental discriminants D we will study the central critical values $L(\mathcal{F}, D, k)$ of the twisted modular L-function

$$L(\mathcal{F}, D, s) := \sum_{n=1}^{\infty} \left(\tfrac{D}{n}\right) A(n) n^{-s}.$$

In order to study congruences, we require a slight modification of a fundamental result of Kohnen [20]. Following the argument used to prove Corollary 1 in that paper gives the next result (see Section 6 below for a brief discussion). Here $\langle f, f \rangle$ and $\langle \mathcal{F}, \mathcal{F} \rangle$ denote the Petersson norms of f and $\mathcal{F}$, respectively.

Theorem 1.2. *Let the notation be as above. For each $p \mid N$, let $\lambda_p \in \{\pm 1\}$ be the eigenvalue of $\mathcal{F}$ under the Atkin-Lehner involution W_p^N. Suppose that D is a fundamental discriminant with $(-1)^k D > 0$. Then we have*

$$a(|D|)^2 = \prod_{p \mid N} \left(1 + \lambda_p \left(\tfrac{D}{p}\right)\right) \cdot \frac{|D|^{k-1/2} \langle f, f \rangle (k-1)!}{\langle \mathcal{F}, \mathcal{F} \rangle \pi^k} \cdot L(\mathcal{F}, D, k). \tag{1.2}$$

Remark. The statement of Corollary 1 of [20] involves $|a(|D|)|^2$. However, Proposition 2.3.1 of [39] implies that (with the normalization specified above), the coefficients of f lie in the field generated by those of $\mathcal{F}$. Since $\mathcal{F}$ is a normalized newform for $\Gamma_0(N)$, its coefficients are totally real algebraic integers, and hence $|a(|D|)|^2 = a(|D|)^2$.

Remark. In [20] it is assumed that $\left(\frac{D}{p}\right) = \lambda_p$ for each $p \mid N$. This produces the term $2^{\nu(N)}$ which appears in the statement of Corollary 1 loc. cit..

Remark. Working directly from (1.2), it is possible to obtain analogous formulas relating the values of $L(\mathcal{F}, D, k)$ to the coefficients of newforms $f(z) \in S_{k+\frac{1}{2}}^{\mathrm{new}}(4N, \chi)$, where χ is any quadratic character modulo N. For completeness, we state a general result in this direction in Section 6 below.

Theorem 1.2 provides a convenient normalization of the algebraic parts of the values $L(\mathcal{F}, D, k)$. We now specialize to the case when

$$N = p \quad \text{is an odd prime} \geq 5.$$

Following Theorem 1.2, for a normalized newform $\mathcal{F}(z) \in S^{\text{new}}_{k+\frac{1}{2}}(\Gamma_0(p))$ we define

$$L^{\text{alg}}(\mathcal{F}, D, k) = \left(1 + \lambda_p \left(\tfrac{D}{p}\right)\right) \cdot \frac{|D|^{k-1/2}\langle f, f\rangle (k-1)!}{\langle \mathcal{F}, \mathcal{F}\rangle \pi^k} \cdot L(\mathcal{F}, D, k). \tag{1.3}$$

With this definition, and recalling some basic facts (see the discussion on pages 242-243 of [20]), we have

$$a(|D|) = L(\mathcal{F}, D, k) = L^{\text{alg}}(\mathcal{F}, D, k) = 0 \quad \text{when} \quad \left(\tfrac{D}{p}\right) = -\lambda_p \text{ and } (-1)^k D > 0. \tag{1.4}$$

Theorem 1.2 gives the fundamental identity

$$a(|D|)^2 = L_{\text{alg}}(\mathcal{F}, D, k) \quad \text{for} \quad (-1)^k D > 0. \tag{1.5}$$

In the next two corollaries, we will suppose that

(1) $p \geq 5$ is prime, and v is a prime of $\overline{\mathbb{Q}}$ above p.
(2) $\mathcal{F} \in S^{\text{new}}_{2k}(\Gamma_0(p))$ is a normalized newform.
(3) $p > \frac{2k-1}{3}$.

Corollary 1.3. *With assumptions (1)–(3) above, suppose also that k is odd. Then there are infinitely many fundamental discriminants $D < 0$ such that*

$$L^{\text{alg}}(\mathcal{F}, D, k) \not\equiv 0 \pmod{v}.$$

Corollary 1.4. *With assumptions (1)–(3) above, suppose also that k is even. Suppose that there are only finitely many fundamental discriminants $D > 0$ such that*

$$L^{\text{alg}}(\mathcal{F}, D, k) \not\equiv 0 \pmod{v}.$$

Then $L^{\text{alg}}(\mathcal{F}, 1, k) \not\equiv 0 \pmod{v}$, and $L^{\text{alg}}(\mathcal{F}, D, k) \equiv 0 \pmod{v}$ for all other fundamental discriminants $D > 0$.

Remark. It is clear that a form as in the conclusion of Corollary 1.4 has eigenvalue 1 under the Aktin-Lehner involution W_p.

Remark. The newform $\mathcal{F} \in S_4(\Gamma_0(5))$ corresponding to the newform $f \in S_{2+\frac{1}{2}}(20)$ described after Theorem 1.1 gives an example of the phenomenon described in Corollary 1.4.

Next we will consider the particular case when $k = 1$ and $\mathcal{F}$ is a modular form corresponding to an elliptic curve. We recall the famous conjecture of Birch and Swinnerton-Dyer, which asserts that if $E/\mathbb{Q}$ is an elliptic curve and $L(E, s)$ is the L-series of E, then

$$\text{ord}_{s=1} L(E, s) = \text{rank}\, E(\mathbb{Q})$$

and

$$\lim_{s \to 1} \frac{L(E, s)}{(s-1)^{\text{rank}\, E(\mathbb{Q})}} = \frac{\Omega(E/\mathbb{Q}) 2^{\text{rank}\, E(\mathbb{Q})} R(E/\mathbb{Q}) \# Ш(E/\mathbb{Q}) \prod_p c_p}{(\# E(\mathbb{Q})_{\text{tors}})^2}.$$

Here $\Omega(E/\mathbb{Q})$ is the real period or twice the real period, depending on whether or not $E(\mathbb{R})$ is connected, $R(E/\mathbb{Q})$ denotes the elliptic regulator, c_p denotes the index in $E(\mathbb{Q}_p)$ of the subgroup of points that reduce mod p to a singular point of $E(\mathbb{F}_p)$, and $Ш(E/\mathbb{Q})$ denotes the Tate-Shafarevich group.

The most notable result in this direction is due to Kolyvagin [24], building on the work of Gross-Zagier [12]. It states that if $E/\mathbb{Q}$ is an elliptic curve and $\text{ord}_{s=1} L(E, s) = 0$ or 1, then $\text{ord}_{s=1} L(E, s) = \text{rank}\, E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ is finite.

In [25], Kolyvagin computes explicit upper bounds on the order of $Ш(E/\mathbb{Q})$ under various hypotheses, and conjectures that for each elliptic curve $E/\mathbb{Q}$ with analytic rank zero or one and each prime ℓ, there is a twist E_D of analytic rank zero so that $Ш(E_D/\mathbb{Q})[\ell] = 0$. This work of Kolyvagin was used in [15] to prove that if $E/\mathbb{Q}$ is a fixed elliptic curve and ℓ is a sufficiently large prime (depending on E), then

$$\#\{|D| < x : L(E_D, 1) \neq 0, Ш(E_D/\mathbb{Q})[\ell] = 0\} \gg \frac{x^{1/2}}{\log x}.$$

We give two corollaries of Theorem 1.1 regarding the triviality of $Ш(E_D/\mathbb{Q})[p]$ for an elliptic curve $E/\mathbb{Q}$ of conductor p.

Theorem 1.5. *Assume that the Birch and Swinnerton-Dyer conjecture is true for elliptic curves with rank zero. Suppose that $E/\mathbb{Q}$ is an elliptic curve of prime conductor p, and that there exists one fundamental discriminant D such that*

1. *$D < 0$,*
2. *$L(E_D, 1) \neq 0$,*
3. *$Ш(E_D/\mathbb{Q})[p] = 0$.*

Then there are infinitely many D which satisfy these three conditions.

Of course, one would like to remove the hypothesis of the existence of one suitable discriminant D from this result. With some work, this is possible under the assumption of a well-known Diophantine inequality. In particular, we recall a conjecture of Hall [26], which states that for any $\epsilon > 0$ and $x, y \in \mathbb{Z}$ with $x^3 - y^2 \neq 0$, we have

$$|x^3 - y^2| \gg \max\{|x|^{1/2-\epsilon}, |y|^{1/3-\epsilon}\}$$

(this is known to follow from the ABC conjecture). We will assume a slightly weaker form of Hall's conjecture; namely that there exists some $\delta > 0$ such that for x, $y \in \mathbb{Z}$ with $x^3 - y^2 \neq 0$ we have

$$|x^3 - y^2| \gg \max\{|x|^{1/3+\delta}, |y|^{2/9+\delta}\}. \tag{1.6}$$

Combining (1.6) with a result of Serre and the convexity bound for degree 2 L-functions, we obtain the following.

Theorem 1.6. *Assume the Birch and Swinnerton-Dyer conjecture for elliptic curves with rank zero and the weak Hall conjecture* (1.6). *Then there is an absolute constant C so that if $p > C$ is prime and $E/\mathbb{Q}$ is an elliptic curve of conductor p, then there are infinitely many discriminants $D < 0$ such that $L(E_D, 1) \neq 0$ and $Ш(E_D/\mathbb{Q})[p] = 0$.*

Remark. It would be of interest to remove the assumption of the Birch and Swinnerton-Dyer conjecture in the above result. A number of bounds on the order of $Ш(E/K)$ in terms of the conjectured order have been given by Kolyvagin and others when $E/\mathbb{Q}$ is an elliptic curve and $K = \mathbb{Q}(\sqrt{D})$ is a quadratic field satisfying the standard Heegner hypotheses. In order to apply these results it would be necessary for $E/\mathbb{Q}$ to have analytic rank one and to have some control over $Ш(E/\mathbb{Q})[p]$.

In the next section we will provide some of the background which is required. In Section 3 we will consider mod p congruences between Kohnen newforms f of level $4Np$ and cusp forms of level $4N$ (these are related to work of Dummigan [11] and McGraw and Ono [28]). We simultaneously consider congruences for f and $f|U(p)$; the results we obtain are of independent interest. Corollary 3.3 describes the implications of these results in regard to congruences for L-values. In Section 4 we prove Theorem 1.1, and in Section 5 we prove the two results regarding elliptic curves. In Section 6 we discuss Theorem 1.2 and state a general version for forms with quadratic character.

2. Preliminaries

If f is a function on the upper half-plane, $k \in \mathbb{Z}$, and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R})$, then we define

$$(f|_k\gamma)(z) := \det(\gamma)^{\frac{k}{2}}(cz+d)^{-k}f(\gamma z). \tag{2.1}$$

If k is an integer, N is a natural number, and χ is a Dirichlet character defined modulo N, then we denote by $M_k(N,\chi)$ and $S_k(N,\chi)$ the usual spaces of holomorphic modular forms and cusp forms of weight k and character χ on $\Gamma_0(N)$.

To define the relevant spaces of half-integral weight forms, we follow the exposition in [19]. If k is an integer, we let $\mathfrak{G}_{k+\frac{1}{2}}$ be the group consisting of pairs $(\gamma, \phi(z))$, where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R})$ and $\phi(z)$ is a holomorphic function on $\mathbb{H}$ such that

$$|\phi(z)| = \det(\gamma)^{-\frac{k}{2}-\frac{1}{4}}|cz+d|^{k+\frac{1}{2}}.$$

If f is a function on the upper half-plane and $(\gamma,\phi) \in \mathfrak{G}_{k+\frac{1}{2}}$, we define

$$f|(\gamma,\phi) := \phi(z)^{-1}f(\gamma z). \tag{2.2}$$

Suppose that N is a natural number and that ω is an even Dirichlet character modulo $4N$. Then the group $\widetilde{\Gamma}_0(4N,\omega)_{k+\frac{1}{2}} \subseteq \mathfrak{G}_{k+\frac{1}{2}}$ consists of pairs $(\gamma, \phi(z))$ with $\gamma \in \Gamma_0(4N)$ and

$$\phi(z) = \omega(d)\left(\tfrac{c}{d}\right)\left(\tfrac{-4}{d}\right)^{-k-\frac{1}{2}}(cz+d)^{k+\frac{1}{2}}.$$

We denote by $\mathfrak{G}_{k+\frac{1}{2}}(4N,\omega)$ the space of weight $k+\frac{1}{2}$ modular forms on $\Gamma_0(4N)$ in the sense of Shimura [37]. In particular, such forms satisfy

$$f|\tilde{\gamma} = f \quad \text{for all} \quad \tilde{\gamma} \in \widetilde{\Gamma}_0(4N,\omega)_{k+\frac{1}{2}}.$$

For the duration, N will denote an odd square-free natural number, and χ will be a real Dirichlet character modulo N. Define

$$\epsilon_\chi := \chi(-1).$$

Then the *Kohnen plus-space* $S_{k+\frac{1}{2}}(4N,\chi)$ is the subspace of $\mathfrak{G}_{k+\frac{1}{2}}\left(4N, \left(\frac{4\epsilon_\chi}{\bullet}\right)\chi\right)$ consisting of those cusp forms $f(z)$ with a Fourier expansion of the form

$$f(z) = \sum_{\epsilon_\chi(-1)^k n \equiv 0,1 \pmod 4} a(n)q^n. \tag{2.3}$$

For natural numbers t we define the operator $U(t)$ on power series via

$$\left(\sum a(n)q^n\right)|U(t) := \sum a(nt)q^n. \tag{2.4}$$

Proposition 3 of [19] shows that if $\mathfrak{f}$ is the conductor of χ, then $U(\mathfrak{f})$ gives an isomorphism

$$U(\mathfrak{f}) \ : \ S_{k+\frac{1}{2}}(4N) \to S_{k+\frac{1}{2}}(4N,\chi). \tag{2.5}$$

We will now consider levels $4Np$, where N is odd and square-free. We will assume throughout that

$$p \geq 5 \quad \text{and} \quad p \nmid N.$$

Until the sixth section, χ will be one of the two characters

$$\chi = \chi_{\text{triv}} \quad \text{or} \quad \chi := \left(\frac{\bullet}{p}\right). \tag{2.6}$$

For such a level, define $W(p)^{4Np}_{k+\frac{1}{2}} \in \mathfrak{G}_{k+\frac{1}{2}}$ by

$$W(p)^{4Np}_{k+\frac{1}{2}} := \left(\begin{pmatrix} p & a \\ 4Np & pb \end{pmatrix}, \left(\frac{-4}{p}\right)^{-k-\frac{1}{2}} p^{-\frac{k}{2}-\frac{1}{4}}(4Npz+pb)^{k+\frac{1}{2}}\right), \tag{2.7}$$

where a and b are integers such that $p^2b - 4Npa = p$. Kohnen (Proposition 2 of [19]) proved that $W(p)^{4Np}_{k+\frac{1}{2}}$ maps $S_{k+\frac{1}{2}}(4Np)$ isomorphically to $S_{k+\frac{1}{2}}\left(4Np, \left(\frac{\bullet}{p}\right)\right)$. Moreover,

$$\left(\frac{-4}{p}\right)^{-\frac{k}{2}-\frac{1}{4}} W(p)^{4Np}_{k+\frac{1}{2}} \tag{2.8}$$

is an involution on the sum of these spaces.

We define

$$w^{4Np}_{p,k+\frac{1}{2}} := p^{-\frac{k}{2}+\frac{1}{4}} U(p) W(p)^{4Np}_{k+\frac{1}{2}}. \tag{2.9}$$

Proposition 4 of [19] shows that $w^{4Np}_{p,k+\frac{1}{2}}$ is an involution on $S_{k+\frac{1}{2}}(4Np)$ and that there is a decomposition

$$S_{k+\frac{1}{2}}(4Np) = S^{+,p}_{k+\frac{1}{2}}(4Np) \oplus S^{-,p}_{k+\frac{1}{2}}(4Np)$$

where the two summands are the $+1$, -1 eigenspaces of $w^{4Np}_{p,k+\frac{1}{2}}$, respectively. If $\epsilon \in \{\pm 1\}$ and $f \in S^{\epsilon,p}_{k+\frac{1}{2}}(4Np)$ then using (2.8) and (2.9) we find that

$$f|W(p)^{4Np}_{k+\frac{1}{2}} = \epsilon \left(\frac{-4}{p}\right)^{k+\frac{1}{2}} p^{-\frac{k}{2}+\frac{1}{4}} f|U(p). \tag{2.10}$$

We will study the new subspace $S^{\text{new}}_{k+\frac{1}{2}}(4Np, \chi)$ (as in the integral weight case, this is defined as the orthogonal complement of the space of old forms; see Section 5 of [19] for details). Theorem 2 of [19] shows that this space maps isomorphically to $S^{\text{new}}_{2k}(Np)$ through the Shimura correspondence, while Theorem 1 of [19] asserts that

$$U(p^2) = -p^{k-1} w^{4Np}_{p,k+\frac{1}{2}} \quad \text{on} \quad S^{\text{new}}_{k+\frac{1}{2}}(4Np). \tag{2.11}$$

Finally, we recall the trace map

$$\text{Tr}^{4Np}_{4N} \ : \ S_{k+\frac{1}{2}}(4Np) \to S_{k+\frac{1}{2}}(4N),$$

whose definition can be found on pages 66-67 of [19]. We have

$$\text{Tr}^{4Np}_{4N}(f) = f + \left(\frac{-4}{p}\right)^{-k-\frac{1}{2}} p^{-\frac{k}{2}+\frac{3}{4}} f|W(p)^{4Np}_{k+\frac{1}{2}} U(p). \tag{2.12}$$

We will require some special modular forms. First we recall that the normalized Eisenstein series $E_{p-1} \in M_{p-1}(1)$ satisfies

$$E_{p-1} \equiv 1 \pmod{p}.$$

We recall the fact (see for example Section 3 of [34]) that there is a modular form $E \in M_{p-1}(p)$ with rational p-integral coefficients and with the properties $E \equiv 1 \pmod{p}$ and

$$E|_{p-1} \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix} = p^{\frac{p+1}{2}} E', \tag{2.13}$$

where $E' \in M_{p-1}(p)$ has p-integral rational coefficients.

We will also require the form

$$E_1(z) := \frac{\eta^p(z)}{\eta(pz)} \in M_{\frac{p-1}{2}}\left(p, \left(\frac{\bullet}{p}\right)\right). \tag{2.14}$$

Here, $\eta(z) = q^{1/24} \prod_{n=1}^{\infty}(1 - q^n)$ is the usual Dedekind eta function. Then E_1 has integer coefficients and $E_1 \equiv 1 \pmod{p}$. Moreover, it can be checked (using the transformation laws for the eta function) that

$$E_1|_{\frac{p-1}{2}} \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix} = p^{\frac{p+1}{4}} i^{\frac{p-1}{4}} E_1', \tag{2.15}$$

where $E_1' \in M_{\frac{p-1}{2}}\left(p, \left(\frac{\bullet}{p}\right)\right)$ has integer coefficients.

Finally, we recall Kohnen's refinement [18] of the Shimura lifting for forms of level four. For each non-negative integer k and each fundamental discriminant D with $(-1)^k D > 0$, we have a map

$$\mathrm{Sh}_{D,k} : S_{k+\frac{1}{2}}(4) \to S_{2k}(1)$$

defined in the following way. If $F(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{k+\frac{1}{2}}(4)$, then

$$\mathrm{Sh}_{D,k}(F) = \sum_{n=1}^{\infty} \left(\sum_{d|n} \left(\frac{D}{d}\right) d^{k-1} a\left(\frac{n^2}{d^2}|D|\right) \right) q^n. \tag{2.16}$$

3. Results on half-integral weight forms

In this section, we take up the issue of congruences between forms of half-integral weight. Dummigan's study [11] of congruences of modular forms and Selmer groups rests on an example of such a congruence. In particular, if $f \in S_{1+\frac{1}{2}}(44)$ and $F \in S_{6+\frac{1}{2}}(4)$ are the unique newforms (normalized suitably) in the respective spaces, then Dummigan proves that

$$f \equiv F|U(11) \pmod{11}. \tag{3.1}$$

It follows (since all spaces in question are one-dimensional) that the mod 11 congruence between the newforms $g = \eta^2(z)\eta^2(11z) \in S_2(11)$ and $G = \eta^{24}(z) \in S_{12}(1)$ "descends" through the Shimura correspondence to the congruence (3.1). McGraw and Ono [28] generalize (3.1) in the following way: given a Kohnen newform $f \in S_{k+\frac{1}{2}}^{\mathrm{new}}(4Np)$, they prove the existence of an integer κ and a form $F \in S_{\kappa+\frac{1}{2}}(4N)$ such that $f \equiv F|U(p) \pmod{p}$. Here the weight κ is typically quite large; it grows like p^k with k. Using these congruences, and an unstated assumption about the uniqueness of half-integral weight modular forms with a given set of mod p eigenvalues (see the argument in the proof of Theorem 2) they generalize Dummigan's example of congruences which descend through the Shimura correspondence.

A special case of our results is a generalization of a natural reinterpretation of (3.1). Note that the form F above is an eigenform of $U(11^2) \pmod{11}$ (which is the same as the Hecke operator T_{11^2} (mod 11)), with eigenvalue 1 (mod 11). It follows that (3.1) is equivalent to the congruence

$$f|U(11) \equiv F \pmod{11}. \tag{3.2}$$

With $k = 1$, this congruence is predicted by the second part of Corollary 3.2 below. In general, if $f \in S^{\text{new}}_{k+\frac{1}{2}}(4Np)$ is a newform, then we consider pairs of congruences for the newforms f and $g = f|U(p)$ (after renormalization). We show that at least one of these forms can be found modulo p at relatively low weight (by way of contrast, the weights we obtain are bounded by $kp + \frac{1}{2}$).

To state these results, we introduce some notation. Suppose that N is odd and square-free, that $p \geq 5$ is a prime with $p \nmid N$, and that K is an algebraic number field containing i and $p^{\frac{1}{4}}$. Let v be a place of K over p, and let $\mathcal{O}_v$ be the local ring consisting of those elements of K which are integral at K. Let π be a uniformizer for $\mathcal{O}_v$, and let v_p be an extension of the standard p-adic valuation on $\mathbb{Q}$ to K. We will consider forms

$$f \in S^{\text{new}}_{k+\frac{1}{2}}(4Np) \cap S^{\epsilon,p}_{k+\frac{1}{2}}(4Np) \cap \mathcal{O}_v[[q]] \tag{3.3}$$

for some choice of $\epsilon \in \{\pm 1\}$. Every newform $f \in S^{\text{new}}_{k+\frac{1}{2}}(4Np)$ is an eigenform for all of the Hecke operators (including those whose index divides the level). In particular, every such f is an eigenform of $U(p^2)$, and so by (2.11) and the remark following Theorem 1.2 we see that (3.3) holds for suitable K.

We assume that $v_p(f) = 0$, and we define

$$a := v_p(f|U(p)) \quad \text{and} \quad A := \lceil a \rceil. \tag{3.4}$$

Choose $e \geq 1$ such that

$$v_p(\pi^e) = v_p(p) = 1. \tag{3.5}$$

Then $ae \in \mathbb{Z}$, and we define

$$g = \frac{f|U(p)}{\pi^{ae}}. \tag{3.6}$$

For the remainder of this section we fix the notation

$$\chi := \left(\frac{\bullet}{p}\right). \tag{3.7}$$

Since $U(p)$ maps $S^{\text{new}}_{k+\frac{1}{2}}(4Np)$ isomorphically to $S^{\text{new}}_{k+\frac{1}{2}}(4Np, \chi)$ (see the Lemma on page 66 of [18]), we have

$$g \in S^{\text{new}}_{k+\frac{1}{2}}(4Np, \chi) \cap \mathcal{O}_v[[q]]. \tag{3.8}$$

Since $U(p)$ commutes with all of the relevant Hecke operators, we see that g is a Kohnen newform whenever f is a Kohnen newform.

Proposition 3.1. *Suppose that f, g, $\mathcal{O}_v$, and A are as defined in* (3.3), (3.4), *and* (3.6). *Then the following are true.*

(1) *There exists $F \in S_{k+(k-A)(p-1)+\frac{1}{2}}(4N) \cap \mathcal{O}_v[[q]]$ such that $v_p(F - f) > 0$.*

(2) *There exists $G \in S_{k+A(p-1)+\frac{p-1}{2}+\frac{1}{2}}(4N) \cap \mathcal{O}_v[[q]]$ such that $v_p(G - g) > 0$.*

Remark. We attempt to motivate the spirit of this result. If $f \in S^{\text{new}}_{k+\frac{1}{2}}(4Np)$ is a newform, then there is an integral weight newform $\mathcal{F} \in S^{\text{new}}_{2k}(Np)$ with the same Hecke eigenvalues. Using the trace map (see, for example, Theorem 4.1 of [5]) one can construct a form $\mathcal{G} \in S_{k(p+1)}(N)$ with $\mathcal{G} \equiv \mathcal{F} \pmod{p}$. Since $\mathcal{G}$ is an eigenform modulo p, it follows from a result of Deligne and Serre (Lemme 6.11 of [10]) that there is an eigenform $G' \in S_{k(p+1)}(N)$ with the same eigenvalues modulo p (to be precise, modulo some prime over p). This eigenform lifts through the Shimura correspondence to a form in $S_{k\left(\frac{p+1}{2}\right)+\frac{1}{2}}(4N)$ with the same Hecke eigenvalues.

The most natural explanation for this phenomenon would be the existence of a form $g \in S_{k\left(\frac{p+1}{2}\right)+\frac{1}{2}}(4N)$ such that $f \equiv g \pmod{p}$. However, examples (see below) show that such a form need not exist. Proposition 3.1 shows that if f itself is not congruent to a form of low weight and level $4N$, then it must be the case that $g = \pi^{-ae} f | U(p)$ is congruent to such a form. This result provides a concrete realization of the system of $\pmod{p}$ eigenvalues attached to the form G' at low weight, through a congruence for one of the two newforms f or g.

Example. We consider the case $k = 2$, $p = 13$ and $N = 1$. There is a newform

$$\mathcal{F}(z) = q - 5q^2 - 7q^3 + 17q^4 - 7q^5 + 35q^6 + \cdots \in S_4(13).$$

The Kohnen newform associated to $\mathcal{F}(z)$ is

$$f(z) = q^5 - q^8 - q^{13} - 3q^{20} + 3q^{21} + q^{24} - q^{28} + \cdots \in S_{2+\frac{1}{2}}(52).$$

Since the coefficient of q^{13} is coprime to 13, we see that $A = 0$. The form

$$\begin{aligned}\mathcal{G}(z) &= \Delta(z)E_4(z)E_6(z)^2 - 6\Delta(z)^2E_4(z)\\ &= q - 798q^2 - 1476q^3 + 67639888q^4 + 3213736350q^5 + 38635573752q^6 - \cdots\end{aligned}$$

lies in $S_{28}(1)$, and $\mathcal{F}(z) \equiv \mathcal{G}(z) \pmod{13}$. The Kohnen newform $g(z) \in S_{14+\frac{1}{2}}(4)$ given by

$$\begin{aligned}g(z) = q &+ (-12332 + 108\sqrt{18209})q^4 + (123360 - 1080\sqrt{18209})q^5\\ &+ (1126824 - 10152\sqrt{18209})q^8 + (-2237463 + 20736\sqrt{18209})q^9 + \cdots\end{aligned}$$

has the same Hecke eigenvalues as $f(z)$ when reduced modulo one of the prime ideals $\mathfrak{p}$ above 13 in $\mathbb{Z}\left[\frac{1+\sqrt{18209}}{2}\right]$. However, the Fourier expansion

$$g(z) \equiv q + 6q^4 + 3q^9 + 10q^{12} + 7q^{13} + q^{16} + \cdots \pmod{\mathfrak{p}}$$

is different. Indeed, there is no form $g(z) \in S_{14+\frac{1}{2}}(4)$ congruent to $f(z)$ mod $\mathfrak{p}$.

On the other hand, since $A = 0$, Proposition 3.1 implies that there is a form

$$F(z) = q^5 + 12q^8 - 104q^9 - 33800q^{12} + 134757q^{13} - 2650752q^{16} + \cdots \in S_{26+\frac{1}{2}}(4)$$

with $F(z) \equiv f(z) \pmod{13}$, and a form

$$G(z) = q + 88q^4 - 336q^5 + 3696q^8 - 5535q^9 + 6048q^{12} + \cdots \in S_{8+\frac{1}{2}}(4)$$

with $G(z) \equiv f(z)|U(13) \pmod{13}$. A simple check shows that the weights $26 + \frac{1}{2}$ and $8 + \frac{1}{2}$ are optimal for $f(z)$ mod 13 and $f(z)|U(p)$ mod 13 at level 4.

Remark. We use the computer algebra package MAGMA ([6] version 2.15-11) for computations. To compute Kohnen newforms, we use built-in routines in MAGMA to compute a basis for the full half-integer weight space of cusp forms. We then manually intersect with the Kohnen plus space, and repeatedly diagonalize each Hecke operator on this space, extending the base field as necessary. To check that a form is an eigenform, we identify a collection of Shimura lifts whose kernel has trivial intersection, and check that the image of our form under each Shimura lift is proportional to the same integer weight eigenform.

Before proceeding with the proof of Proposition 3.1, we give two corollaries. We note that, since $f|U(p^2) = -\epsilon p^{k-1} f$, we always have $A \leq k-1$. Using this fact together with the Eisenstein series E from (2.13), we have the following result.

Corollary 3.2. *If f, g, and $\mathcal{O}_v$ are as in Proposition 3.1, then the following are true.*

(1) *There exists $F \in S_{kp+\frac{1}{2}}(4N) \cap \mathcal{O}_v[[q]]$ such that $v_p(F-f) > 0$.*

(2) *There exists $G \in S_{kp-\frac{p-1}{2}+\frac{1}{2}}(4N) \cap \mathcal{O}_v[[q]]$ such that $v_p(G-g) > 0$.*

In view of Proposition 3.1 and Theorem 6.1 below, it is clear that the twisted L-values of a newform $\mathcal{F}(z) \in S_{2k}^{\mathrm{new}}(Np)$ are interpolated modulo p by the squares of coefficients of half-integral weight forms of level $4N$. The corollary which follows makes this precise.

Corollary 3.3. *Suppose that N is a positive, odd, square-free integer and that $p \geq 5$ is a prime with $p \nmid N$. Suppose that $\mathcal{F}(z) \in S_{2k}^{\mathrm{new}}(Np)$ is a newform and that $f \in S_{k+\frac{1}{2}}^{\mathrm{new}}(4Np)$ is the newform (normalized as in the introduction) corresponding to $\mathcal{F}$ under the Shimura correspondence. Let χ be the quadratic character with conductor p. With the notations from* (3.3), (3.4), *and* (3.6), *write*

$$f(z) = \sum_{n=1}^{\infty} a(n) q^n \in \mathcal{O}_v[[q]]$$

and

$$g(z) = \frac{f|U(p)}{\pi^{ae}} = \sum_{n=1}^{\infty} b(n) q^n \in S_{k+\frac{1}{2}}^{\mathrm{new}}(4Np, \chi) \cap \mathcal{O}_v[[q]].$$

Moreover, let

$$F(z) = \sum_{n=1}^{\infty} A(n) q^n \in S_{k+(k-A)(p-1)+\frac{1}{2}}(4N)$$

and

$$G(z) = \sum_{n=1}^{\infty} B(n) q^n \in S_{k+A(p-1)+\frac{p-1}{2}+\frac{1}{2}}(4N)$$

be as in the conclusion of Proposition 3.1. Then for all fundamental discriminants D with $(-1)^k D > 0$ we have

$$A(|D|)^2 \equiv \prod_{p|N} \left(1 + \lambda_p \left(\tfrac{D}{p}\right)\right) \cdot \frac{|D|^{k-1/2} \langle f, f \rangle (k-1)!}{\langle \mathcal{F}, \mathcal{F} \rangle \pi^k} \cdot L(\mathcal{F}, D, k) \pmod{v},$$

and for all fundamental discriminants D with $(-1)^k \chi(-1) \cdot D > 0$ and $(D,p) = 1$ we have

$$B(|D|)^2 \equiv \prod_{p|N} \left(1 + \lambda_p \chi(p) \left(\tfrac{D}{p}\right)\right) \cdot \frac{|D|^{k-1/2} \langle g, g \rangle (k-1)!}{\langle \mathcal{F}, \mathcal{F} \rangle \pi^k} \cdot L\left(\mathcal{F} \otimes \chi\left(\tfrac{D}{\cdot}\right), k\right) \pmod{v}.$$

Proof of Corollary 3.3. This follows immediately by combining the results which are mentioned. □

Proof of Proposition 3.1. Let f, g, K, $\mathcal{O}_v$, A, π, and e be as defined in (3.3), (3.4), (3.6), and (3.5). Using (2.11) we find that

$$v_p(g|U(p)) = v_p\left(\frac{f|U(p^2)}{\pi^{ae}}\right) = k-1-a. \tag{3.9}$$

Now write

$$a = A - s/e, \qquad 0 \le s/e < 1 \tag{3.10}$$

and define

$$f' := \pi^s f. \tag{3.11}$$

Let $E \in M_{p-1}(p)$ be as in (2.13). Then we have

$$f' \cdot E(4z)^{k-A} \in S_{k+(k-A)(p-1)+\frac{1}{2}}(4Np),$$

and therefore

$$F' := \mathrm{Tr}^{4Np}_{4N}\left(f' \cdot E(4z)^{k-A}\right) \in S_{k+(k-A)(p-1)+\frac{1}{2}}(4N).$$

We claim that $F' \in K[[q]]$ and that

$$v_p(F' - f') \ge 1. \tag{3.12}$$

Setting $F := \pi^{-s}F'$ and using (3.11), the first statement of the proposition follows from (3.12).

To prove (3.12), we see from the definition (2.12) that it will suffice to show that

$$v_p\left(p^{-\frac{k}{2}-(k-A)\left(\frac{p-1}{2}\right)+\frac{3}{4}}(f' \cdot E(4z)^{k-A})|W(p)^{4Np}_{k+(k-A)(p-1)+\frac{1}{2}}|U(p)\right) \ge 1. \tag{3.13}$$

A calculation using (2.7), (2.1), and (2.2) gives

$$(f' \cdot E(4z)^{k-A})|W(p)^{4Np}_{k+(k-A)(p-1)+\frac{1}{2}} = f'|W(p)^{4Np}_{k+\frac{1}{2}} \cdot \left(E\big|_{p-1}\begin{pmatrix} p & 4a \\ Np & pb\end{pmatrix}|V(4)\right)^{k-A}. \tag{3.14}$$

By (2.10) we see that $f'|W(p)^{4Np}_{k+\frac{1}{2}}$ has coefficients in K, and by (2.12) we conclude that F' also has coefficients in K. Using (3.4) and (3.11) we find that

$$v_p\left(f'|W(p)^{4Np}_{k+\frac{1}{2}}\right) = -\tfrac{k}{2} + \tfrac{1}{4} + A,$$

and by (2.13) (using the fact that $\begin{pmatrix} p & 4a \\ Np & pb\end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ p & 0\end{pmatrix}$ are $\Gamma_0(p)$-equivalent) we see that the terms containing E in (3.14) contribute the power $p^{(k-A)\left(\frac{p+1}{2}\right)}$. From this we find that the quantity in (3.13) is at least equal to

$$-\tfrac{k}{2} - (k-A)\left(\tfrac{p-1}{2}\right) + \tfrac{3}{4} - \tfrac{k}{2} + \tfrac{1}{4} + A + (k-A)\left(\tfrac{p+1}{2}\right) = 1,$$

as desired. This establishes the first claim of the proposition.

We turn to the second claim. Recall the definition (2.14) of the form $E_1 \in M_{\frac{p-1}{2}}\left(p, \left(\frac{\bullet}{p}\right)\right)$. Using the definition (3.6) of the form g, and taking care with the computation of the characters and the plus-space condition, we find that

$$g \cdot E_1(4z) \cdot E(4z)^A \in S_{k+A(p-1)+\frac{p-1}{2}+\frac{1}{2}}(4Np),$$

and therefore that

$$G := \mathrm{Tr}_{4N}^{4Np}\left(g \cdot E_1(4z) \cdot E(4z)^A\right) \in S_{k+A(p-1)+\frac{p-1}{2}+\frac{1}{2}}(4N).$$

As above, we have $G \in K[[q]]$. Using (2.12), it will be enough to show that

$$v_p\left(p^{-\frac{k}{2}-A\left(\frac{p-1}{2}\right)-\frac{p-1}{4}+\frac{3}{4}}\left[(g \cdot E_1(4z) \cdot E(4z)^A)|W(p)^{4Np}_{k+A(p-1)+\frac{p-1}{2}+\frac{1}{2}}\right]|U(p)\right) > 0. \tag{3.15}$$

Using (2.13) and (2.15), and arguing as above, we find that the terms containing E_1 and E contribute the powers $p^{\frac{p+1}{4}}$ and $p^{A\left(\frac{p+1}{2}\right)}$ respectively. Using (2.9) and (3.6), we have

$$g|W(p)^{4Np}_{k+\frac{1}{2}} = \pi^{-ae} f|U(p)W(p)^{4Np}_{k+\frac{1}{2}} = \pi^{-ae} p^{\frac{k}{2}-\frac{1}{4}} \cdot \epsilon f.$$

Combining all of the contributions and recalling that $a = A - s/e$ with $0 \leq s/e < 1$, we find that the quantity in (3.15) is at least

$$-\tfrac{k}{2} - A\left(\tfrac{p-1}{2}\right) - \tfrac{p-1}{4} + \tfrac{3}{4} + \tfrac{p+1}{4} + A\left(\tfrac{p+1}{2}\right) - A + \tfrac{s}{e} + \tfrac{k}{2} - \tfrac{1}{4} \geq 1 + \tfrac{s}{e} > 0.$$

The proposition follows. □

4. Proof of Theorem 1.1

We begin with a proposition which follows from our work in the last section, together with the results of [4].

Proposition 4.1. *Suppose that $\epsilon \in \{\pm 1\}$, that p is an odd prime, that K is a number field which is Galois over $\mathbb{Q}$, and that v is a place of K above p. Suppose that $p > \frac{2k-1}{3}$, and that $f \in S^{\epsilon,p}_{k+\frac{1}{2}}(4p) \cap S^{new}_{k+\frac{1}{2}}(4p) \cap \mathcal{O}_v[[q]]$ satisfies*

$$f(z) \equiv \sum_{i=1}^{r}\sum_{n=1}^{\infty} a(t_i n^2) q^{t_i n^2} \not\equiv 0 \pmod{v}. \tag{4.1}$$

Then $\Theta(f) \not\equiv 0 \pmod{v}$.

Proof. Suppose that f has the form (4.1) and that $\Theta(f) \equiv 0 \pmod{v}$. By Corollary 3.2, there exists a form $F \in S_{kp+\frac{1}{2}}(4)$ with $F \equiv f \pmod{v}$. Proposition 5.1 of [4] implies that F (and hence f) has the form

$$f \equiv \sum a(n^2)q^{n^2} + \sum a(pn^2)q^{pn^2} \pmod{v}.$$

Since $\Theta(f) \equiv 0 \pmod{v}$, it follows that

$$f \equiv \sum a(p^2n^2)q^{p^2n^2} + \sum a(pn^2)q^{pn^2} \pmod{v}. \tag{4.2}$$

If $k = 1$, then $F \in S_{p+\frac{1}{2}}(4)$ and the first $p-1$ Fourier coefficients are all zero modulo v. Since $p - 1 > \frac{p+\frac{1}{2}}{12} \cdot [\Gamma_0(1) : \Gamma_0(4)]$, a theorem of Sturm [40] implies that $f \equiv F \equiv 0 \pmod{v}$, which provides the desired contradiction.

We may therefore assume that $k \geq 2$. By (2.11), we have

$$f|U(p^2) = -p^{k-1}\epsilon f \equiv 0 \pmod{p^{k-1}}.$$

Therefore (4.2) becomes

$$F \equiv f \equiv \sum_{p \nmid n} a(pn^2)q^{pn^2} \pmod{v}. \tag{4.3}$$

By Lemma 4.2 of [4] (see in particular equation (4.1)) there exists a form $g \in S_{\lambda_1+\frac{1}{2}}(4)$ such that

$$g \equiv F|U(p) \equiv \sum_{p\nmid n} a(pn^2)q^{n^2} \pmod{v}, \tag{4.4}$$

where for some $\alpha \geq 0$ we have

$$\lambda_1 + 1 = \frac{2\left[kp - \alpha(p-1)\right] + p + 1}{2p}. \tag{4.5}$$

Since $\lambda_1 \in \mathbb{Z}$, we have $\alpha \equiv \frac{p-1}{2} \pmod{p}$. It follows that $\alpha \geq \frac{p-1}{2}$; since also $p > \frac{2k-1}{3}$, we find from (4.5) that $\lambda_1 \leq p$. It follows from Proposition 5.4 of [4] that $g \equiv 0 \pmod{v}$, from which $f \equiv 0 \pmod{v}$, against the hypotheses. □

We are now in a position to prove Theorem 1.1.

Proof of Theorem 1.1. Let f and K be as in the statement of the theorem, and suppose that $p > \frac{2k-1}{3}$. We may suppose without loss of generality that K is Galois over $\mathbb{Q}$. By Proposition 3.1, there is an $F \in S_{pk+\frac{1}{2}}(4)$ with $F \equiv f \pmod{v}$. By Proposition 5.1 of [4], we may conclude that

$$f \equiv F \equiv \sum a(n^2)q^{n^2} + \sum a(pn^2)q^{pn^2} \pmod{v}.$$

If k is odd, then Theorem 5.3 of [4] implies that $\Theta(f) \equiv 0 \pmod{v}$, while Proposition 4.1 implies that $\Theta(f) \not\equiv 0 \pmod{v}$. Therefore k must be even. In this case, part 1 of Theorem 2.2 of [3] implies that either

$$f \equiv \sum a(n^2)q^{n^2} \pmod{v}$$

or

$$f \equiv \sum a(pn^2)q^{pn^2} \pmod{v}.$$

In the second case we have $\Theta(f) \equiv 0 \pmod{v}$, which contradicts Proposition 4.1. We must therefore be in the first case. Since $k \geq 2$ we have $f|U(p^2) \equiv 0 \pmod{p}$; it follows that

$$f \equiv F \equiv \sum_{p\nmid n} a(n^2)q^{n^2} \pmod{v}. \tag{4.6}$$

To prove that

$$f \equiv a(1)\sum_{n=1}^{\infty} n^k q^{n^2}$$

we appeal to part 2 of Theorem 2.2 of [3], setting $m_0 = n_1 = 1$. From this result together with (4.6) we conclude that

$$\sum_{n \text{ odd}} a(n^2)q^{n^2} \equiv a(1)\sum_{n \text{ odd}} n^k q^{n^2} \pmod{v}.$$

Note that if $\theta_0(z) = 1 + 2\sum_{n=1}^{\infty} q^{n^2} \in \mathfrak{G}_{\frac{1}{2}}(4)$, then by Lemma 4.1 of [4], there is a form

$$F_1(z) \equiv \tfrac{1}{2}\Theta^{\frac{k}{2}}(\theta_0(z)) \cdot E_{p-1}(4z)^{\frac{k}{2}} \equiv \sum_{n=1}^{\infty} n^k q^{n^2} \pmod{v}$$

with $F_1(z) \in S_{kp+\frac{1}{2}}(4)$. We have

$$a(1)F_1(z) - F(z) \equiv \sum b(4n^2)q^{4n^2} \pmod{v}.$$

Taking the $D = 1$ Shimura lift (see (2.16)) shows that there is an integer weight form

$$F_2(z) = \mathrm{Sh}_{1,kp}(a(1)F_1(z) - F(z)) \equiv \sum c(2n)q^{2n} \pmod{v}$$

with $F_2(z) \in S_{2kp}(1)$. Theorem 3.1 of [4] now implies that $F_2(z) \equiv 0 \pmod{v}$. Working through (2.16), we find that $a(1)F_1(z) - F(z) \equiv 0 \pmod{v}$. Thus,

$$f(z) \equiv F(z) \equiv a(1)F_1(z) \equiv a(1)\sum_{n=1}^{\infty} n^k q^{n^2} \pmod{v},$$

as desired. □

Corollaries 1.3 and 1.4 follow from the main theorem.

Proof of Corollary 1.3. Let $f = \sum a(n)q^n \in S^{\mathrm{new}}_{k+\frac{1}{2}}(4p)$ be the newform corresponding to $\mathcal{F}$, normalized as in the introduction, and assume that conditions (1)-(3) are satisfied. By Theorem 1.1 we find that there are infinitely many positive square-free t such that $a(tn_t^2) \not\equiv 0 \pmod{v}$ for some n_t. Using the plus-space condition we see that $tn_t^2 \equiv 0, 3 \pmod{4}$ for each such t. Therefore for each such t there is a fundamental discriminant $D_t < 0$ such that $tn_t^2 = |D_t|n_t'^2$. Using equation (11) of [20] we see that $a(|D_t|) \not\equiv 0 \pmod{v}$. The corollary then follows from (1.5). □

Proof of Corollary 1.4. Let $f = \sum a(n)q^n \in S^{\mathrm{new}}_{k+\frac{1}{2}}(4p)$ be the newform corresponding to $\mathcal{F}$, normalized as in the introduction, and assume that conditions (1)-(3) are satisfied. If there are infinitely many positive square-free t such that $a(tn_t^2) \not\equiv 0 \pmod{v}$ for some n_t, then arguing as in the odd case we find that there are infinitely many positive D such that $L^{\mathrm{alg}}(\mathcal{F}, D, k) \not\equiv 0 \pmod{v}$.

If there are only finitely many such t, then Theorem 1.1 implies that $D = 1$ is the only positive fundamental discriminant for which $a(D) \not\equiv 0 \pmod{v}$. Then (1.5) shows that we have $L^{\mathrm{alg}}(\mathcal{F}, D, k) \equiv 0 \pmod{v}$ for all positive fundamental discriminants $D \neq 1$. □

5. Proofs of results on elliptic curves

Suppose that $E/\mathbb{Q}$ is an elliptic curve of prime conductor p; this implies that $p \geq 11$. By Wiles' work on the modularity of semistable elliptic curves, there exists a newform $\mathcal{F} \in S_2(p)$ with $L(\mathcal{F}, s) = L(E, s)$. We let $\lambda_p \in \{\pm 1\}$ be the eigenvalue of $\mathcal{F}$ under the Atkin-Lehner involution W_p. There exists a newform $f \in S^{\mathrm{new}}_{3/2}(4p)$ which corresponds to $\mathcal{F}$ via the Shimura correspondence. By the remark following Theorem 1.2, the form

$$f(z) = \sum_{n=1}^{\infty} a(n)q^n$$

can be taken to have rational integer Fourier coefficients.

Combining (1.5) with the Birch and Swinnerton-Dyer Conjecture, we obtain, for each $D < 0$ with $L(E_D, 1) \neq 0$ (from which necessarily $\left(\frac{D}{p}\right) \neq -\lambda_p$) the formula

$$\#Ш(E_D) = \frac{1}{\left(1 + \lambda_p \left(\frac{D}{p}\right)\right)} \cdot \frac{(\#E_D(\mathbb{Q})_{\text{tors}})^2}{\Omega(E_D) \prod_q c_q(E_D)} \cdot \frac{\langle \mathcal{F}, \mathcal{F} \rangle \pi}{\langle f, f \rangle \sqrt{-D}} a(-D)^2.$$

Using the fact that

$$\Omega(E_D) = \frac{\Omega(E_{-4})}{\sqrt{-D_0}},$$

where

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

we conclude that if $D < 0$ and $L(E_D, 1) \neq 0$, then

$$\#Ш(E_D) = C \cdot \frac{1}{\left(1 + \lambda_p \left(\frac{D}{p}\right)\right)} \cdot \frac{(\#E_D(\mathbb{Q})_{\text{tors}})^2}{\prod_q c_q(E_D)} \cdot \frac{\sqrt{-D_0}}{\sqrt{-D}} \cdot a(-D)^2, \tag{5.1}$$

where C is a positive rational number that does not depend on D. Mazur's classification [27] of the torsion subgroups for elliptic curves over $\mathbb{Q}$ implies that p does not divide the order of the torsion subgroup. If $\mathcal{F}(z) = \sum A(n)q^n$, then $A(p) = -\lambda_p$. It follows that the pth Fourier coefficient of $\mathcal{F} \otimes \chi_D$ equals -1 or 0. This in turn implies that E_D has non-split multiplicative reduction or additive reduction at p and additive reduction at primes $q \mid D$. From Corollary 15.2.1 of Appendix C of [38], we see that all Tamagawa numbers c_q divide 3 or 4, and hence that they are coprime to p. It follows that for every $D < 0$ with $a(-D) \neq 0$ (which is the same as $L(E_D, 1) \neq 0$), we have

$$\text{ord}_p(\#Ш(E_D)) = \text{ord}_p(C) + 2\text{ord}_p(a(-D)). \tag{5.2}$$

The first result now follows easily.

Proof of Theorem 1.5. If there is a single $D < 0$ with $a(-D) \not\equiv 0 \pmod{p}$ for which $Ш(E_D)[p] = 0$, then the constant C in (5.2) has $\text{ord}_p(C) = 0$. Corollary 1.3 implies that there are infinitely many $D < 0$ with $\text{ord}_p(a(-D)) = 0$. Theorem 1.5 follows from (5.2). □

The second result is more involved.

Proof of Theorem 1.6. In light of Theorem 1.5 it suffices to demonstrate the existence of a single D^* satisfying the three conditions of Theorem 1.5. Applying Sturm's theorem (see [40]) to the form $f(z)$, we find that for each curve E of conductor p, there there is a discriminant $D^* = D^*(E)$ such that $D^* < 0$, $a(-D^*) \not\equiv 0 \pmod{p}$, and

$$0 < -D^* \leq \frac{(p+1)}{8} < p. \tag{5.3}$$

The Birch and Swinnerton-Dyer conjecture gives

$$\frac{\#Ш(E_{D^*}) \prod_q c_q(E_{D^*})}{\#(E_{D^*}(\mathbb{Q})_{\text{tors}})^2} = \frac{L(E, D^*, 1)}{\Omega(E_{D^*})}.$$

Since $\prod_q c_q(E_{D^*}) \geq 1$ and $\#(E_{D^*}(\mathbb{Q})_{\text{tors}})^2 \leq 256$, we have

$$\#Ш(E_{D^*}) \ll \frac{L(E, D^*, 1)}{\Omega(E_{D^*})}.$$

(Note: Here and in what follows, the constants implied by the notation $\ll$ do not depend on the prime p, and the inequalities are valid for curves of sufficiently large conductor p.)

We have $\Omega(E_{D^*}) = \frac{\Omega(E_{-4})}{\sqrt{-D_0^*}}$, and so

$$\#Ш(E_{D^*}) \ll \frac{L(E, D^*, 1)|D^*|^{1/2}}{\Omega(E_{-4})}. \tag{5.4}$$

We require the convexity bound for degree 2 L-functions (see [14], p. 100-101, or [13], Theorem F.4.1.9 for an explicit version for elliptic curves), which implies that for a degree 2 L-function $L(f, s)$ of conductor N, we have $|L(f, 1)| \ll N^{1/4+\epsilon}$. The conductor of $L(E, D, 1)$ is pD^2. So from (5.4) and the convexity bound, we obtain

$$\#Ш(E_{D^*}) \ll \frac{p^{1/4+\epsilon}|D^*|^{1+\epsilon}}{\Omega(E_{-4})} \ll \frac{p^{5/4+\epsilon}}{\Omega(E_{-4})}. \tag{5.5}$$

To finish, we must determine a lower bound for $\Omega(E_{-4})$. In [26], it is shown that for any elliptic curve A written in the form

$$A \; : \; y^2 = x^3 + ax + b,$$

we have

$$\Omega(A) \gg \frac{1}{\max\{|a|^{1/4}, |b|^{1/6}\}}.$$

In this case, the discriminant is given by

$$\Delta(A) = -16(4a^3 + 27b^2) = \frac{1}{27}((-12a)^3 - (216b)^2).$$

Assuming the weak version (1.6) of Hall's conjecture, we have $|\Delta(A)| \gg \max\{a^{1/3+\delta}, b^{2/9+\delta}\}$, and so

$$\Omega(A) \gg |\Delta(A)|^{-3/4+\delta}.$$

The minimal model for the curve E_{-4} may not have the form $y^2 = x^3 + ax + b$, but there is a model E' which does have this form. It follows that there is a positive integer v (which divides 6) for which

$$\Delta(E') = v^{12}\Delta(E_{-4}) \quad \text{and} \quad \Omega(E') = \frac{1}{v}\Omega(E_{-4}). \tag{5.6}$$

Applying these relations, together with the fact that $|\Delta(E_{-4})| \ll |\Delta_{\min}(E)|$, we get

$$\#Ш(E_{D^*}) \ll p^{5/4+\epsilon}|\Delta_{\min}(E)|^{3/4-\delta}.$$

Under the assumption (no longer required) that E is modular, Serre ([35] Proposition 8) showed that for $p > 37$, either $|\Delta_{\min}(E)| = p$, or $|\Delta_{\min}(E)| = p^2$ and E has a rational two-torsion point. In the first case, it follows that for some $\delta' > 0$ we have

$$\#Ш(E_{D^*}) \ll p^{2-\delta'}.$$

Therefore for all sufficiently large p we have

$$\#Ш(E_{D^*}) < p^2. \tag{5.7}$$

In the second case, E is one of two curves considered by Neumann and Setzer (see [29], [30], [36]). It follows that $p = u^2 + 64$, where u is an integer which we take to be congruent to $3 \pmod 4$. We have

$$E \ : \ y^2 + xy = x^3 - \frac{u+1}{4}x^2 + 4x - u,$$

and $|\Delta_{\min}(E)| = p^2$. A (not necessarily minimal) model of E_{-4} is given by

$$E' \ : \ y^2 = x^3 - (-27u^2 + 5184) + (-54u^3 - 31104u),$$

from which we obtain $|\Omega(E')| \gg p^{-1/4}$. Then from (5.6), we obtain

$$\#\text{Ш}(E_{D*}) \ll \frac{p^{5/4+\epsilon}}{\Omega(E_{-4})} \ll p^{3/2+\epsilon}.$$

In either case, we conclude that for all sufficiently large p, there exists a discriminant $D^* = D^*(E, p)$ such that $D^* < 0$, $a(-D^*) \neq 0$, and such that (5.7) holds. The Cassels pairing implies that if $\text{Ш}(E_{D^*})$ is finite, its order is a perfect square, and so if $\#\text{Ш}(E_{D^*}) < p^2$, its order is coprime to p. This proves that $\text{Ш}(E_{D^*})[p] = 0$, which concludes the proof. □

6. Remarks on formulas for L-values

We begin with a brief explanation of the formula in Theorem 1.2. To see that this formula holds, we follow the argument on page 243 of [20], keeping in mind the correct orientation of the geodesics C_Q which is described in Section 1 of [21]. We see that the sum $\sum_{t|N} 1$ in [20] can be replaced by the more general quantity $\sum_{t|N} \lambda_t \left(\frac{D}{t}\right)$ (where λ_t denotes the eigenvalue of $\mathcal{F}$ under the Atkin-Lehner involution W_t^N). Using multiplicativity, this sum is seen to be equal to the product which appears as a normalizing factor in (1.2).

We record a general formula for L-values which follows easily from Theorem 1.2. Suppose that N is odd and square-free and that $\mathcal{F} \in S_{2k}^{\text{new}}(N)$ is a normalized newform. Suppose that χ is a quadratic character with conductor $\mathfrak{f} \mid N$. Via Kohnen's theory, there is a unique (up to normalization) newform

$$g = \sum_{n=1}^{\infty} b(n)q^n \in S_{k+\frac{1}{2}}^{\text{new}}(4N, \chi)$$

associated to $\mathcal{F}$ via the Shimura correspondence. As above, we may assume that the coefficients lie in the field generated by the coefficients of $\mathcal{F}$. With this notation, we have the following extension of Theorem 1.2.

Theorem 6.1. *Let the notation be as in the last paragraph. Suppose that D is a fundamental discriminant with*

$$(-1)^k\chi(-1) \cdot D > 0 \qquad \textit{and} \qquad (D, \mathfrak{f}) = 1. \tag{6.1}$$

Then we have

$$b(|D|)^2 = \prod_{p|N} \left(1 + \lambda_p \chi(p) \left(\tfrac{D}{p}\right)\right) \cdot \frac{|D|^{k-1/2}\langle g, g\rangle (k-1)!}{\langle \mathcal{F}, \mathcal{F}\rangle \pi^k} \cdot L\left(\mathcal{F} \otimes \chi\left(\tfrac{D}{\cdot}\right), k\right). \tag{6.2}$$

Remark. This does not agree with the formula given by Theorem 4.2 of [23] applied to this case.

Example. We illustrate Theorem 1.2 with a numerical example. There is a newform

$$\mathcal{F}(z) = q - 2q^2 - 9q^3 - 28q^4 - 25q^5 + 18q^6 - 132q^7 + \cdots \in S_6^{\mathrm{new}}(15).$$

Let

$$f(z) = 2q^{11} - q^{15} - 2q^{20} - 4q^{24} + 4q^{35} + 6q^{39} + 4q^{44} - \cdots \in S_{7/2}^{\mathrm{new}}(60)$$

be the Kohnen newform which corresponds to it. We see that $\lambda_3 = \lambda_5 = 1$. Expressing f as a linear combination of Poincaré series, and using the well-known relation between the nth coefficient of a form and its inner product with a Poincaré series, we compute that

$$\langle f, f\rangle \approx 0.0000001926781582$$

(this is only accurate to about 7 significant digits). Computing the special value of the adjoint square L-function of $\mathcal{F}$ and using the relation between this value and the Petersson norm of $\mathcal{F}$, we find that $\langle \mathcal{F}, \mathcal{F}\rangle \approx 0.00001361809013$. We can then compute the following table of data involving fundamental discriminants $D < 0$ for which $\prod_{p|15}(1 + \lambda_p(\frac{D}{p})) \neq 0$.

D	$a(\lvert D\rvert)^2$	Right hand side of (1.2)
-11	4	4.000000207
-15	1	1.000000052
-20	4	4.000000207
-24	16	16.00000083
-35	16	16.00000083
-39	36	36.00000186
-51	4	4.000000207
-56	64	64.00000331
-59	36	36.00000186
-71	64	64.00000331
-84	144	144.0000074
-95	196	196.0000101
-104	64	64.00000331
-111	36	36.00000186
-116	1936	1936.000100
-119	144	144.0000074
-120	576	576.0000297

Proof of Theorem 6.1. Let

$$f = \sum_{n=1}^{\infty} a(n)q^n \in S_{k+\frac{1}{2}}^{\mathrm{new}}(4N)$$

be the form associated to $\mathcal{F}$ as in Theorem 1.2. By (2.5) and the following discussion, and noting that the truth of (6.2) is independent of the normalization of g, we may assume that

$$g = f|U(\mathfrak{f}).$$

For a fundamental discriminant D as in (6.1) we define the fundamental discriminant D^* by

$$D^* := \chi(-1)\cdot \mathfrak{f}D. \tag{6.3}$$

We have

$$b(|D|) = a(|D^*|) \quad \text{and} \quad (-1)^k D^* > 0.$$

Applying Theorem 1.2, we find that for all D as in (6.1) we have

$$b(|D|)^2 = \prod_{p|N} \left(1 + \lambda_p \left(\tfrac{D^*}{p}\right)\right) \cdot \frac{|D^*|^{k-1/2}\langle f, f\rangle (k-1)!}{\langle \mathcal{F}, \mathcal{F}\rangle \pi^k} \cdot L(\mathcal{F}, D^*, k). \tag{6.4}$$

Note that $\chi = \left(\frac{\chi(-1)\mathfrak{f}}{\cdot}\right)$; it follows that for each p, we have

$$\left(\tfrac{D^*}{p}\right) = \chi(p) \left(\tfrac{D}{p}\right). \tag{6.5}$$

We recall (see the discussion preceding Proposition 2 of [19]) that if ϕ is any quadratic character modulo Np, then $\left(\frac{-1}{p}\right)^{-\frac{k}{2}-\frac{1}{4}} W(p)_{k+\frac{1}{2}}^{4Np}$ is a unitary involution on the sum of the spaces $S_{k+\frac{1}{2}}(4Np, \phi)$ and $S_{k+\frac{1}{2}}\left(4Np, \phi\left(\frac{\cdot}{p}\right)\right)$. Also (see the proof of Proposition 3 of [19]), if $p \nmid \operatorname{cond}(\phi)$, then $p^{-k/2+1/4}U(p)W(p)_{k+\frac{1}{2}}^{4Np}$ is a Hermitian involution on $S_{k+\frac{1}{2}}(4Np, \phi)$.

Suppose that $h \in S_{k+\frac{1}{2}}(4Np, \phi)$ and that $p \nmid \operatorname{cond}(\phi)$. Combining the facts in the last paragraph (and recalling that the inner product is conjugate linear in the second entry) we see that

$$\langle h|U(p), h|U(p)\rangle = \left\langle h|U(p)W(p)_{k+\frac{1}{2}}^{4Np}, h|U(p)W(p)_{k+\frac{1}{2}}^{4Np}\right\rangle = p^{k-\frac{1}{2}}\langle h, h\rangle.$$

Arguing inductively using the last formula, we find that with f and $g = f|U(\mathfrak{f})$ as above, we have $\langle g, g\rangle = \mathfrak{f}^{k-\frac{1}{2}}\langle f, f\rangle$. Using this together with (6.5), the result follows from (6.4). □

References

[1] Scott Ahlgren and Matthew Boylan. Arithmetic properties of the partition function. *Invent. Math.*, 153(3):487–502, 2003.

[2] Scott Ahlgren and Matthew Boylan. Coefficients of half-integral weight modular forms modulo l^j. *Math. Ann.*, 331(1):219–239, 2005.

[3] Scott Ahlgren and Matthew Boylan. Central critical values of modular L-functions and coefficients of half-integral weight modular forms modulo l. *Amer. J. Math.*, 129(2):429–454, 2007.

[4] Scott Ahlgren, Dohoon Choi, and Jeremy Rouse. Congruences for level four cusp forms. *Math. Res. Lett.* To appear.

[5] Scott Ahlgren and Matthew Papanikolas. Higher Weierstrass points on $X_0(p)$. *Trans. Amer. Math. Soc.*, 355(4):1521–1535 (electronic), 2003.

[6] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[7] Jan H. Bruinier and Ken Ono. Coefficients of half-integral weight modular forms. *J. Number Theory*, 99(1):164–179, 2003.

[8] Jan Hendrik Bruinier. Nonvanishing modulo l of Fourier coefficients of half-integral weight modular forms. *Duke Math. J.*, 98(3):595–611, 1999.

[9] J. B. Conrey, D. W. Farmer, F. Mezzadri, and N. C. Snaith, editors. *Ranks of elliptic curves and random matrix theory*, volume 341 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2007.

[10] Pierre Deligne and Jean-Pierre Serre. Formes modulaires de poids 1. *Ann. Sci. École Norm. Sup. (4)*, 7:507–530 (1975), 1974.

[11] Neil Dummigan. Congruences of modular forms and Selmer groups. *Math. Res. Lett.*, 8(4):479–494, 2001.

[12] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[13] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2000. An introduction.

[14] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications.* American Mathematical Society, Providence, RI, 2004.

[15] Kevin James and Ken Ono. Selmer groups of quadratic twists of elliptic curves. *Math. Ann.*, 314(1):1–17, 1999.

[16] Ben Kane. Representations of integers by ternary quadratic forms. To appear.

[17] W. Kohnen and D. Zagier. Values of L-series of modular forms at the center of the critical strip. *Invent. Math.*, 64(2):175–198, 1981.

[18] Winfried Kohnen. Modular forms of half-integral weight on $\Gamma_0(4)$. *Math. Ann.*, 248(3):249–266, 1980.

[19] Winfried Kohnen. Newforms of half-integral weight. *J. Reine Angew. Math.*, 333:32–72, 1982.

[20] Winfried Kohnen. Fourier coefficients of modular forms of half-integral weight. *Math. Ann.*, 271(2):237–268, 1985.

[21] Winfried Kohnen. A remark on the Shimura correspondence. *Glasgow Math. J.*, 30(3):285–291, 1988.

[22] Winfried Kohnen and Ken Ono. Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication. *Invent. Math.*, 135(2):387–398, 1999.

[23] Hisashi Kojima and Yasushi Tokuno. On the Fourier coefficients of modular forms of half integral weight belonging to Kohnen's spaces and the critical values of zeta functions. *Tohoku Math. J. (2)*, 56(1):125–145, 2004.

[24] V. A. Kolyvagin. Finiteness of $E(\mathbf{Q})$ and $\mathrm{SH}(E, \mathbf{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(3):522–540, 670–671, 1988.

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

[26] Serge Lang. Conjectured Diophantine estimates on elliptic curves. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 155–171. Birkhäuser Boston, Boston, MA, 1983.

[27] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[28] William J. McGraw and Ken Ono. Modular form congruences and Selmer groups. *J. London Math. Soc. (2)*, 67(2):302–318, 2003.

[29] Olaf Neumann. Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten. I. *Math. Nachr.*, 49:107–123, 1971.

[30] Olaf Neumann. Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten. II. *Math. Nachr.*, 56:269–280, 1973.

[31] Ken Ono and Christopher Skinner. Fourier coefficients of half-integral weight modular forms modulo l. *Ann. of Math. (2)*, 147(2):453–470, 1998.

[32] Ken Ono and Christopher Skinner. Non-vanishing of quadratic twists of modular L-functions. *Invent. Math.*, 134(3):651–660, 1998.

[33] Ken Ono and K. Soundararajan. Ramanujan's ternary quadratic form. *Invent. Math.*, 130(3):415–454, 1997.

[34] Jean-Pierre Serre. Formes modulaires et fonctions zêta p-adiques. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972)*, pages 191–268. Lecture Notes in Math., Vol. 350. Springer, Berlin, 1973.

[35] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[36] Bennett Setzer. Elliptic curves of prime conductor. *J. London Math. Soc. (2)*, 10:367–378, 1975.

[37] Goro Shimura. On modular forms of half integral weight. *Ann. of Math. (2)*, 97:440–481, 1973.

[38] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[39] Glenn Stevens. Λ-adic modular forms of half-integral weight and a Λ-adic Shintani lifting. In *Arithmetic geometry (Tempe, AZ, 1993)*, volume 174 of *Contemp. Math.*, pages 129–151. Amer. Math. Soc., Providence, RI, 1994.

[40] Jacob Sturm. On the congruence of modular forms. In *Number theory (New York, 1984–1985)*, volume 1240 of *Lecture Notes in Math.*, pages 275–280. Springer, Berlin, 1987.

[41] M.-F. Vignéras. Facteurs gamma et équations fonctionnelles. In *Modular functions of one variable, VI (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 79–103. Lecture Notes in Math., Vol. 627. Springer, Berlin, 1977.

[42] J.-L. Waldspurger. Sur les coefficients de Fourier des formes modulaires de poids demi-entier. *J. Math. Pures Appl. (9)*, 60(4):375–484, 1981.

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