Math. Res. Lett. **16** (2009), *no.* 4, 683–701

CONGRUENCES FOR LEVEL FOUR CUSP FORMS

Scott Ahlgren, Dohoon Choi, and Jeremy Rouse

Abstract. In this paper, we study congruences for modular forms of half-integral weight on $\Gamma_0(4)$. Suppose that $\ell \geq 5$ is prime, that K is a number field, and that v is a prime of K above ℓ. Let $\mathcal{O}_v$ denote the ring of v-integral elements of K, and suppose that $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in \mathcal{O}_v[[q]]$ is a cusp form of weight $\lambda + 1/2$ on $\Gamma_0(4)$ in Kohnen's plus space. We prove that if the coefficients of f are supported on finitely many square classes modulo v and $\lambda + 1/2 < \ell(\ell + 1 + 1/2)$, then λ is even and

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

This result is a precise analogue of a characteristic zero theorem of Vignéras [22]. As an application, we study divisibility properties of the algebraic parts of the central critical values of modular L-functions.

1. Introduction

Recent works of Bruinier [5], Bruinier and Ono [6], Ono and Skinner [16] and Ahlgren and Boylan [1], [2] have considered the distribution of the coefficients of half-integral weight modular forms modulo primes and prime powers. There are many applications, for example to the study of divisibility properties of the algebraic parts of the central critical values of modular L-functions and orders of Tate-Shafarevich groups of elliptic curves, and to the study of congruences for combinatorial generating functions which can be expressed in terms of these forms.

Many of these results can be viewed as modulo ℓ versions of a characteristic zero theorem of Vignéras [22], which states that a half-integral weight modular form whose coefficients are supported on finitely many square classes of integers must in fact be a linear combination of single-variable theta series. To be precise, we have the following (a different proof of this result was given by Bruinier [4]).

Theorem 1.1 ([22], 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 $t_1, t_2, \ldots, t_m$ for which*

$$F(z) = \sum_{i=1}^{m} \sum_{n=0}^{\infty} a(t_i n^2) q^{t_i n^2}, \quad q = e^{2\pi i z}$$

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

2000 *Mathematics Subject Classification.* Primary 11F33; Secondary 11F80.

Let $\ell \geq 5$ be prime and let v be a place of $\overline{\mathbb{Q}}$ over ℓ; then we consider modular forms $f(z) \in S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi)$ for which we have a congruence of the form

$$f(z) \equiv \sum_{i=1}^{m} \sum_{n=1}^{\infty} a(t_i n^2) q^{t_i n^2} \not\equiv 0 \pmod{v}. \tag{1.1}$$

The results of [5], [6], and [16] imply that for a fixed f which is not a linear combination of theta series, there are only finitely many ℓ for which such a congruence can occur. Moreover, if there is such a congruence, then detailed information about the action of the Hecke algebra on the form f and the distribution of the coefficients of f in residue classes modulo v is obtained.

In [2], given the additional assumption that f is a Hecke eigenform modulo v, it is shown that such a form must be congruent to some iterated derivative of a single-variable theta series of weight $1/2$ or $3/2$; this yields a precise description of those coefficients of f outside of certain arithmetic progressions (in which information is lost due to the incomplete theory of newforms in the general case).

In this paper, we will obtain a precise analog of the theorem of Vignéras in the most basic setting; namely we will study forms $f(z)$ which lie in the Kohnen plus-space $S^+_{\lambda+\frac{1}{2}}(\Gamma_0(4))$. We prove, with a suitable assumption on the size of ℓ, that if such a form f satisfies (1.1), then it must be the case that f is congruent to the image of the single variable theta series

$$\theta_0(z) := \sum_{n \in \mathbb{Z}} q^{n^2} \tag{1.2}$$

under some number of iterations of the differential operator

$$\Theta\left(\sum a(n) q^n\right) := \sum n a(n) q^n. \tag{1.3}$$

Although this is the simplest case which one could consider, it will be seen that the methods which we require are still quite involved. Our main result is the following.

Theorem 1.2. *Suppose that $\ell \geq 5$ is prime, that K is a number field, and that v is a prime of K above ℓ. Let $\mathcal{O}_v$ denote the ring of v-integral elements of K. Suppose that $f(z) \in S^+_{\lambda+\frac{1}{2}}(\Gamma_0(4)) \cap \mathcal{O}_v[[q]]$ satisfies*

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

where each t_i is a square-free positive integer. If $\lambda + 1/2 < \ell(\ell + 1 + 1/2)$, then λ is even and

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

Example. If $\ell = 5$ and $\lambda = 6$, there is a form $g(z) \in S^+_{13/2}(\Gamma_0(4))$ given by

$$\begin{aligned} g(z) &= \theta_0 F(\theta_0^4 - 2F)(\theta_0^4 - 16F) \\ &= q - 56q^4 + 120q^5 - 240q^8 + 9q^9 + 1440q^{12} - 1320q^{13} + \cdots, \end{aligned}$$

where $F(z) := \sum_{n=0}^{\infty} \sigma_1(2n+1)q^n \in M_2(\Gamma_0(4))$. We have

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

Remark. The bound on the weight in Theorem 1.2 is sharp. In particular, for any prime $\ell \geq 5$ there is a form

$$f \equiv \frac{1}{2}\Theta(\theta_0)^\ell \equiv \sum_{n=1}^{\infty} n^2 q^{\ell n^2} \pmod \ell$$

of weight $\ell(\ell+1+1/2)$, in the plus-space, for which the conclusion of Theorem 1.2 is false.

The results of [14], [13], and [23] connect the coefficients of modular forms of half-integral weight to the central L-values of twists of integral weight forms. More precisely, suppose that $f \in S_{2k}(\Gamma_0(1))$ is a normalized Hecke eigenform, with $f(z) = \sum_{n=1}^{\infty} a(n)q^n$. Suppose that $g(z) = \sum_{n=1}^{\infty} c(n)q^n \in S^+_{k+1/2}(\Gamma_0(4))$ is a Hecke eigenform with the same Hecke eigenvalues as f. Theorem 1 of [14] states the following.

Theorem 1.3. *Suppose that f and g are as above, D is a fundamental discriminant with $(-1)^k D > 0$, and $L(f, D, s)$ is the twisted L-series*

$$L(f, D, s) = \sum_{n=1}^{\infty} \left(\tfrac{D}{n}\right) a(n) n^{-s}.$$

Then

$$\frac{c(|D|)^2}{\langle g, g\rangle} = \frac{(k-1)!}{\pi^k} |D|^{k-\frac{1}{2}} \frac{L(f, D, k)}{\langle f, f\rangle}.$$

Here, $\langle g, g\rangle$ and $\langle f, f\rangle$ are the normalized Petersson scalar products

$$\langle g, g\rangle = \frac{1}{6} \int_{\mathbb{H}/\Gamma_0(4)} |g(z)|^2 y^{k-3/2}\, dx\, dy$$

$$\langle f, f\rangle = \int_{\mathbb{H}/\Gamma_0(1)} |f(z)|^2 y^{2k-2}\, dx\, dy.$$

Note that $g(z)$ is only defined up to a scalar multiple. We will choose the scalar multiple so that $g(z)$ has Fourier coefficients which are algebraic integers, and relatively prime. With this notation, let

$$L^{\text{alg}}(f, D, k) = \frac{\langle g, g\rangle (k-1)! |D|^{k-1/2} L(f, D, k)}{\langle f, f\rangle \pi^k} = c(|D|)^2.$$

Next, we state some corollaries of Theorem 1.2 pertaining to central L-values.

Corollary 1.4. *Suppose that k is odd, that $\ell \geq 5$ is a prime with $k + 1/2 < \ell(\ell + 1 + 1/2)$, that $f \in S_{2k}(\Gamma_0(1))$ is a normalized Hecke eigenform, and that v is a prime of $\overline{\mathbb{Q}}$ above ℓ. Then there are infinitely many fundamental discriminants $D < 0$ so that*

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

Corollary 1.5. *Suppose that k is even, that $\ell \geq 5$ is a prime with $k+1/2 < \ell(\ell+1+1/2)$, that $f \in S_{2k}(\Gamma_0(1))$ is a normalized Hecke eigenform, and that v is a prime of $\overline{\mathbb{Q}}$ above ℓ. If there are only finitely many fundamental discriminants $D > 0$ so that*

$$L^{\mathrm{alg}}(f, D, k) \not\equiv 0 \pmod{v},$$

then

$$L^{\mathrm{alg}}(f, 1, k) \not\equiv 0 \pmod{v},$$

and

$$L^{\mathrm{alg}}(f, D, k) \equiv 0 \pmod{v} \text{ for } D > 1.$$

Remark. If $f(z) = \Delta(z) := q\prod_{n=1}^{\infty}(1-q^n)^{24}$ is the normalized Hecke eigenform of weight 12, then the corresponding form

$$g(z) = \theta_0 F(\theta_0^4 - 2F)(\theta_0^4 - 16F)$$

was given above. In this case, $L^{\mathrm{alg}}(f, 1, k) \equiv 1 \pmod 5$, but $L^{\mathrm{alg}}(f, D, k) \equiv 0 \pmod 5$ for all other fundamental discriminants $D > 0$.

2. Preliminaries

Suppose that λ is a non-negative integer, that N is a positive integer with $4|N$, and that χ is a Dirichlet character defined modulo N. Then we denote by $S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi)$ the usual complex vector space of cusp forms of weight $\lambda+\frac{1}{2}$ on $\Gamma_0(N)$ with character χ. For definitions and basic facts about the theory of modular forms of integer weight, see [9]. For facts about the theory of modular forms of half-integer weight, see [11], Chapter IV.

If k is an integer and N is a positive integer, then we denote by $M_k(\Gamma_1(N))$ the space of weight k modular forms on $\Gamma_1(N)$ and by $S_k(\Gamma_1(N))$ the subspace of cusp forms; we have the decomposition

$$M_k(\Gamma_1(N)) = \bigoplus_{\chi} M_k(\Gamma_0(N), \chi),$$

where the sum runs over all Dirichlet characters modulo N. Let χ_D denote the Kronecker character associated to the extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ (or the trivial character if $D = 1$). Then we have

$$M_k(\Gamma_1(4)) = \begin{cases} M_k(\Gamma_0(4)) & \text{if } k \text{ is even,} \\ M_k(\Gamma_0(4), \chi_{-1}) & \text{if } k \text{ is odd.} \end{cases} \tag{2.1}$$

In [12], Kohnen introduces the plus space $S^+_{\lambda+\frac{1}{2}}(\Gamma_0(4))$ of cusp forms $g(z)$ of weight $\lambda+\frac{1}{2}$ on $\Gamma_0(4)$ with a Fourier expansion of the form

$$g(z) = \sum_{(-1)^\lambda n \equiv 0,1 \pmod 4} b(n) q^n.$$

We recall Kohnen's refinement of the Shimura lifting (see [12], Theorem 1). For each non-negative integer λ and each fundamental discriminant D with $(-1)^\lambda D > 0$, we have a map

$$\mathrm{Sh}^+_{D,\lambda} : S^+_{\lambda+\frac{1}{2}}(\Gamma_0(4)) \to S_{2\lambda}(\Gamma_0(1))$$

defined in the following way. If $F(z) = \sum_{n=1}^{\infty} a(n)q^n \in S^+_{\lambda+\frac{1}{2}}(\Gamma_0(4))$, then

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

The Shimura correspondence commutes with the action of the Hecke operators. In particular, if p is an odd prime, then

$$\mathrm{Sh}^+_{D,\lambda}(F|T(p^2, \lambda + \tfrac{1}{2}, 1)) = \mathrm{Sh}^+_{D,\lambda}(F)|T(p, 2\lambda, 1),$$

where the Hecke operators are the usual operators of half-integral and integral weights, respectively.

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 $K = \mathbb{Q}$ (the version which we state here follows in exactly the same way).

Theorem 2.1. *Suppose that $\ell \geq 5$ is prime, that K is a number field, and that v is a prime of K above ℓ. Suppose that*

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

that $\ell \nmid N$, and that $p \nmid N\ell$ is prime. If there exists $\epsilon_p \in \{\pm 1\}$ such that

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

then we have

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

Finally, we recall some facts about the algebra of modular forms mod ℓ, where $\ell \geq 5$ is prime. Suppose that K is a number field and that v is a prime ideal of K above ℓ. Let $\mathcal{O}_v$ be the ring of v-integral elements of K, and set $\mathbb{F}_v := \mathcal{O}_v/v$. If $f = \sum a(n)q^n \in \mathcal{O}_v[[q]]$, then we define $\overline{f} := \sum \overline{a(n)} q^n \in \mathbb{F}_v[[q]]$, and we define

$$\overline{M_k(\Gamma_1(N))} := \{\overline{f} \ : \ f \in M_k(\Gamma_1(N)) \cap \mathcal{O}_v[[q]]\} \tag{2.2}$$

and

$$\overline{M(N)} = \bigoplus_{k=0}^{\infty} \overline{M_k(\Gamma_1(N))}$$

(we will require only the cases $N = 1$ and $N = 4$ here). If $\overline{f} \in \overline{M_k(\Gamma_1(N))}$ then we define

$$\omega(f) = \omega(\overline{f}) := \inf\{k' \ : \ \text{there exists } \overline{g} \in \overline{M_{k'}(\Gamma_1(N))} \text{ with } \overline{f} = \overline{g}\} \tag{2.3}$$

Recall the definition (1.3) of the theta operator; it is well-known that Θ maps modular forms mod ℓ to modular forms mod ℓ. With this notation we summarize some important properties of the filtration.

Proposition 2.2. *Suppose that $N = 1$ or $N = 4$, that $\ell \geq 5$ is prime, and that $\overline{f} \in \overline{M_k(\Gamma_1(N))}$. Then we have the following.*

(1) *If* $\overline{g} \in \overline{M_{k'}(\Gamma_1(N))}$ *has* $\overline{f} = \overline{g} \neq 0$, *then* $k \equiv k' \pmod{\ell - 1}$.
(2) $\omega(\Theta(f)) \equiv \omega(f) + 2 \pmod{\ell - 1}$.
(3) $\omega(\Theta(f)) \leq \omega(f) + \ell + 1$, *with equality if and only if* $\ell \nmid \omega(f)$.
(4) $\omega(f^i) = i\omega(f)$ *for all* $i \geq 1$.

Proof. In the case when $N = 1$ these facts follow from the work of Serre and Swinnerton-Dyer [20], [18] (a good account is in Chapter X of [15]). When $N = 4$, one can appeal to the general results of Gross [10] or one can argue directly using work of Tupan [21]. Recall the definition (1.2) of $\theta_0(z)$, and set $F := \sum_{n=0}^{\infty} \sigma_1(2n+1)q^{2n+1}$. Let $A(X, Y) \in \mathbb{Z}_{(\ell)}[X, Y]$ be the polynomial satisfying $A(\theta_0^4, F) = E_{p-1}(z)$. Then Theorem A of [21] implies that there is an isomorphism

$$\overline{\mathbb{F}}_v[X, Y]/(\overline{A}(X^2, Y) - 1) \to \bigoplus_{k=0}^{\infty} \overline{M_k(\Gamma_1(4))},$$

which is realized by mapping X to θ_0^2 and Y to F. Using this fact, one can argue exactly as in Sections 7 and 8 of Chapter X of [15] to obtain the desired results. □

3. Modular forms of integral weight

In this section we prove two results on modular forms of integral weight modulo ℓ. For any function $f(z)$ on $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ and any positive integer d we define the operators

$$f(z)\big|V_d := f(dz), \tag{3.1}$$

$$f(z)\big|U_d := \frac{1}{d}\sum_{j=0}^{d-1} f\left(\frac{z+j}{d}\right). \tag{3.2}$$

If f has a Fourier expansion $f(z) = \sum a(n)q^n$, then $f\big|U_d = \sum a(nd)q^n$.

Theorem 3.1. *Suppose that* K *is a number field and that* v *is a prime ideal of* K *above the rational prime* ℓ. *Suppose that* $f = \sum a(n)q^n \in S_{2k}(\Gamma_0(N)) \cap \mathcal{O}_v[[q]]$. *If* $t > 1$ *and*

$$f \equiv \sum_{n=1}^{\infty} a(tn)q^{tn} \pmod{v}$$

where $\gcd(t, \ell N) = 1$, *then* $f \equiv 0 \pmod{v}$.

Proof. We may assume without loss of generality that t is prime. We have the decomposition

$$S_{2k}(\Gamma_0(N)) = \bigoplus_{d|N} \bigoplus_{e|d} S_{2k}^{\mathrm{new}}(\Gamma_0(N/d))|V(e).$$

Each of the spaces $S_{2k}^{\mathrm{new}}(\Gamma_0(N/d))$ is spanned by newforms with coefficients which are algebraic integers, and the extension L of K generated by all of these coefficients is a finite extension. Letting ν_d denote the dimension of $S_{2k}^{\mathrm{new}}(\Gamma_0(N/d))$, we may write

$$f = \sum_{d|N} \sum_{i=1}^{\nu_d} \sum_{e|d} c_{d,i,e} f_{d,i}|V(e),$$

where the $f_{d,i}$ run over newforms in $S_{2k}^{\mathrm{new}}(\Gamma_0(N/d))$ and each $c_{d,i,e} \in L$. Let O_L denote the ring of integers of L and let $\mathfrak{l}$ be a prime ideal above v in O_L. Let $n =$

$\max(1, 1 - \min(\mathrm{ord}_{\mathfrak{l}}(c_{d,i,e})))$. For each form $f_{d,i}$, it follows from the work of Deligne that there is a Galois representation $\rho_{d,i} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(O_L/\mathfrak{l}^n)$, unramified outside of ℓN, such that if

$$f_{d,i} = \sum_{n=1}^{\infty} a_{d,i}(n) q^n,$$

then for all primes $p \nmid \ell N$, we have

$$\begin{aligned} \mathrm{Tr}(\rho_{d,i}(\mathrm{Frob}_p)) &\equiv a_{d,i}(p) \pmod{\mathfrak{l}^n}, \\ \mathrm{Det}(\rho_{d,i}(\mathrm{Frob}_p)) &\equiv p^{2k-1} \pmod{\mathfrak{l}^n}. \end{aligned}$$

To prove the theorem, suppose that m is a positive integer; we will show that $a(m) \equiv 0 \pmod{v}$. Write $m = t^a m_1$ where $t \nmid m_1$ (we may assume that $a \geq 1$). From the properties of the Hecke algebra it follows that there is a polynomial $P_a(x, y) \in \mathbb{Z}[x, y]$ such that for each prime $p \nmid N$ and each i, we have

$$a_{d,i}(p^a) = P_a(a_{d,i}(p), p^{2k-1}).$$

Then,

$$\begin{aligned} a(m) &= \sum_{d|N} \sum_{i=1}^{\nu_d} \sum_{e|\gcd(d,m_1)} c_{d,i,e} a_{d,i}(m_1/e) a_{d,i}(t^a) \\ &= \sum_{d|N} \sum_{i=1}^{\nu_d} \sum_{e|\gcd(d,m_1)} c_{d,i,e} a_{d,i}(m_1/e) P_a(a_{d,i}(t), t^{2k-1}). \end{aligned}$$

The compositum of the fixed fields of all of the $\rho_{d,i}$ is a finite extension. By the Chebotarev density theorem we conclude that there is a prime $p > N\ell t$ such that $\rho_{d,i}(p) = \rho_{d,i}(t)$ for all d and i; it follows that

$$\begin{aligned} a_{d,i}(p) &\equiv a_{d,i}(t) \pmod{\mathfrak{l}^n}, \\ p^{2k-1} &\equiv t^{2k-1} \pmod{\mathfrak{l}^n}. \end{aligned}$$

Then we have

$$\begin{aligned} a(p^a m_1) &\equiv \sum_{d|N} \sum_{i=1}^{\nu_d} \sum_{e|\gcd(d,m_1)} c_{d,i,e} a_{d,i}(m_1/e) P_a(a_{d,i}(p), p^{2k-1}) \\ &\equiv \sum_{d|N} \sum_{i=1}^{\nu_d} \sum_{e|\gcd(d,m_1)} c_{d,i,e} a_{d,i}(m_1/e) P_a(a_{d,i}(t), t^{2k-1}) \\ &\equiv a(m) \pmod{\mathfrak{l}}. \end{aligned}$$

Since $a(p^a m_1) \equiv 0 \pmod{v}$ by assumption, we conclude that $a(m) \equiv 0 \pmod{\mathfrak{l}}$. Since $a(m) \in \mathcal{O}_v$ we have $a(m) \equiv 0 \pmod{v}$, as desired. □

The next result is a mod ℓ analog of a well-known result in characteristic zero (see Lemma 16 of [3]).

Theorem 3.2. *Suppose that N is an odd integer and that $\ell \geq 5$ is a prime with $\ell \nmid N$. Suppose that K is a number field and that v is a prime ideal of K above ℓ. Suppose*

that $f(z) \in S_k(\Gamma_0(2N)) \cap \mathcal{O}_v[[q]]$ has the property that

$$f(z) \equiv \sum_{n=1}^{\infty} a(n) q^{4n} \pmod{v}$$

for some $a(n) \in \mathcal{O}_v$. Then $f \equiv 0 \pmod{v}$.

Before starting the proof, we recall that if M and Q are integers with $Q \mid M$, $\gcd(Q, M/Q) = 1$, then the Atkin-Lehner operator on $S_k(\Gamma_0(M))$ is given by any matrix

$$W_Q^M := \begin{pmatrix} Qx & y \\ Mz & Qw \end{pmatrix}, \quad \det(W_Q) = Q. \tag{3.3}$$

For convenience we record a short lemma.

Lemma 3.3. *Suppose that $\ell \geq 5$ is prime with $\ell \nmid N$, that K is a number field, and that v is a prime ideal of K above ℓ. Suppose that $F \in S_k(\Gamma_0(8N)) \cap \mathcal{O}_v[[q]]$ has $F \equiv 0 \pmod{v}$. Then the Fourier expansion of F at each cusp is congruent to zero modulo v in the ring $\mathcal{O}_v[\zeta_{8N}][[q^{1/8N}]]$ (where ζ_{8N} denotes a primitive $8N$th root of unity).*

Proof. This follows from the q-expansion principle (see, for example, Remark 12.3.5 of [8]), which implies that if $F \in S_k(\Gamma_0(8N)) \cap \mathcal{O}_v[[q]]$, then the q-expansion of F at each cusp has coefficients in $\mathcal{O}_v[\zeta_{8N}]$. Suppose that $F \equiv 0 \pmod{v}$. Then, letting λ be a uniformizer for $\mathcal{O}_v$, we have $F = \lambda F'$, where $F' \in \mathcal{O}_v[[q]]$. The desired result follows. □

For any positive integer d we define the matrices

$$w_d := \begin{pmatrix} 0 & -1 \\ d & 0 \end{pmatrix}, \tag{3.4}$$

$$A_d := \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}. \tag{3.5}$$

If $Q \mid 2N$ and $\gcd(Q, 2N/Q) = 1$ then we have $W_Q^{2N} = \gamma A_Q$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$; it follows from Lemma 3.3 that for $\ell \nmid 2N$ and for forms $f, g \in S_k(\Gamma_0(8N)) \cap \mathcal{O}_v[[q]]$ we have

$$f \equiv g \pmod{v} \implies f\big|_k W_Q^{2N} \equiv g\big|_k W_Q^{2N} \pmod{v}. \tag{3.6}$$

Similarly, since $w_d = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} A_d$ we have

$$f \equiv g \pmod{v} \implies f\big|_k w_d \equiv g\big|_k w_d \pmod{v}. \tag{3.7}$$

We are now in a position to prove Theorem 3.2.

Proof of Theorem 3.2. Set

$$g := f\big|U_4, \quad h := f - f\big|U_4\big|V_4 \equiv 0 \pmod{v}.$$

By Lemma 17 of [3] we have $g \in S_k(\Gamma_0(2N))$ and $h \in S_k(\Gamma_0(8N))$. Moreover, we have

$$f = g\big|V_4 + h. \tag{3.8}$$

For any F and any d we have the identities

$$F\big|_k A_d = d^{k/2} F\big|V_d, \tag{3.9}$$

$$F\big|_k A_d w_{2N} = F\big|_k w_{2N} A_d^{-1}. \tag{3.10}$$

By (3.7)–(3.10) we conclude that

$$f\big|_k w_{2N} \equiv g\big|V_4\big|_k w_{2N} \equiv 2^{-k} g\big|_k w_{2N}\big|_k A_4^{-1} \pmod{v}.$$

From this and (3.9) it follows that

$$g\big|_k w_{2N} \equiv 4^k f\big|_k w_{2N}\big|V_4 \pmod{v}. \tag{3.11}$$

We define the usual trace map $\mathrm{Tr}_N^{2N} : S_k(\Gamma_0(2N)) \to S_k(\Gamma_0(N))$ by

$$\mathrm{Tr}_N^{2N}(F) := F + 2^{1-k/2} F\big|_k W_2^{2N}\big|U_2. \tag{3.12}$$

We have $g\big|_k W_N^{2N} \in S_k(\Gamma_0(2N))$, and therefore

$$A := \mathrm{Tr}_N^{2N}(g\big|_k W_N^{2N}) = g\big|_k W_N^{2N} + 2^{1-k/2} g\big|_k W_N^{2N} W_2^{2N}\big|U_2 \in S_k(\Gamma_0(N)).$$

Since $W_N^{2N} W_2^{2N}$ is $\Gamma_0(2N)$-equivalent to w_{2N} (see Lemma 9 of [3]) we see from (3.11) that

$$g\big|_k W_N^{2N} W_2^{2N}\big|U_2 \equiv 4^k f\big|_k w_{2N}|V_4|U_2 \equiv 4^k f\big|_k w_{2N}\big|V_2 \pmod{v}.$$

Therefore $A \in S_k(\Gamma_0(N))$ has the property that

$$A \equiv g\big|_k W_N^{2N} + 2^{3k/2+1} f\big|_k w_{2N}\big|V_2 \pmod{v}. \tag{3.13}$$

We now note that $f\big|U_2$, $f\big|U_2\big|_k W_2^{2N} \in S_k(\Gamma_0(2N))$, and we define

$$B := \mathrm{Tr}_N^{2N}(f\big|U_2\big|_k W_2^{2N}) \in S_k(\Gamma_0(N)).$$

We have

$$B = f\big|U_2\big|_k W_2^{2N} + 2^{1-k/2} f\big|U_4;$$

it follows after applying W_N^{2N} (which is the same as w_N for forms on $\Gamma_0(N)$) that

$$B\big|_k w_N = B\big|_k W_N^{2N} = f\big|U_2\big|_k w_{2N} + 2^{1-k/2} f\big|U_4\big|_k W_N^{2N}.$$

Since $f \equiv g\big|V_4 \pmod{v}$, it follows from (3.6) and (3.7) that

$$B\big|_k w_N \equiv g\big|V_2\big|_k w_{2N} + 2^{1-k/2} g\big|_k W_N^{2N} \pmod{v}.$$

Using $f\big|_k w_{2N} \equiv \big(g\big|V_2\big)\,\big|V_2\big|_k w_{2N} \pmod{v}$ and arguing as in (3.11) we find that

$$g\big|V_2\big|_k w_{2N} \equiv 2^k f\big|_k w_{2N}\big|V_2 \pmod{v},$$

so that finally we obtain

$$B\big|_k w_N \equiv 2^k f\big|_k w_{2N}\big|V_2 + 2^{1-k/2} g\big|_k W_N^{2N} \pmod{v}. \tag{3.14}$$

Combining (3.13) and (3.14) we find that

$$A - 2^{k/2-1} B\big|_k w_N \equiv 3 \cdot 2^{3k/2-1} f\big|_k w_{2N}\big|V_2 \pmod{v}. \tag{3.15}$$

Since the left side of (3.15) is a modular form of level N which is supported $\pmod{v}$ on even exponents, we conclude from Theorem 3.1 that $f\big|_k w_{2N} \equiv 0 \pmod{v}$. It follows from (3.6) that $f \equiv 0 \pmod{v}$, as desired. □

4. Modular forms of half-integral weight

In this section we record two short lemmas which are needed in the proof of the main theorem.

Lemma 4.1. *Suppose that $\ell \geq 5$ is prime, that K is a number field, that v is a prime ideal of K above ℓ, and that $f = \sum a(n)q^n \in S^+_{\lambda+\frac{1}{2}}(\Gamma_0(4)) \cap \mathcal{O}_v[[q]]$. Then there is a form $g(z) \in S^+_{\lambda+\ell+1+\frac{1}{2}}(\Gamma_0(4)) \cap \mathcal{O}_v[[q]]$ such that*

$$g(z) \equiv \Theta f(z) \pmod{v}.$$

Proof. If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, then we have (see page 68 of [17]) the transformation formula

$$E_2(\gamma z) = (cz+d)^2 E_2(z) + \frac{6c}{i\pi}(cz+d).$$

If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(4)$, then $4\gamma z = \gamma'(4z)$, where $\gamma' = \left(\begin{smallmatrix} a & 4b \\ c/4 & d \end{smallmatrix}\right)$. It follows that

$$E_2(4\gamma z) = (cz+d)^2 E_2(4z) + \frac{6c}{4i\pi}(cz+d).$$

Since f is a modular form of half-integral weight, we have

$$f(\gamma z) = \left(\frac{c}{d}\right)\epsilon_d^{-1}(cz+d)^{\lambda+\frac{1}{2}} f(z),$$

where $\left(\frac{c}{d}\right)$ denotes the usual Jacobi symbol when $d > 0$ and

$$\left(\frac{c}{d}\right) := \begin{cases} \left(\frac{c}{|d|}\right) & d < 0 \text{ and } c > 0, \\ -\left(\frac{c}{|d|}\right) & d < 0 \text{ and } c < 0, \end{cases}$$

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

We compute that

$$(\Theta f)(\gamma z) = \left(\frac{c}{d}\right)\epsilon_d^{-1}\left[(cz+d)^{\lambda+2+\frac{1}{2}} \cdot \Theta f(z) + \frac{(\lambda+\frac{1}{2})c}{2\pi i}(cz+d)^{\lambda+1+\frac{1}{2}} f(z)\right].$$

Setting $F(z) := \Theta f(z) - \frac{\lambda+\frac{1}{2}}{3} f(z) E_2(4z)$, a computation shows that for $\gamma \in \Gamma_0(4)$ we have

$$F(\gamma z) = \left(\frac{c}{d}\right)\epsilon_d^{-1}(cz+d)^{\lambda+2+\frac{1}{2}} F(z).$$

We then have

$$\Theta f(z) \equiv F(z)E_{\ell-1}(4z) + \frac{\lambda+\frac{1}{2}}{3} f(z) E_{\ell+1}(4z) \pmod{v},$$

where the form on the right side belongs to $S_{\lambda+\ell+1+\frac{1}{2}}(\Gamma_0(4))$. The lemma follows since the plus space condition clearly holds. □

Lemma 4.2. *Suppose that $\ell \geq 5$ is prime, that K is a number field which is Galois over $\mathbb{Q}$, and that v is a prime ideal of K above ℓ. Suppose that $g \in S^+_{\lambda+1/2}(\Gamma_0(4)) \cap \mathcal{O}_v[[q]]$ has the property that*

$$g \equiv \sum_{n=1}^{\infty} a(n) q^{\ell n} \pmod{v}.$$

Then there exists λ' with

(1) $\lambda' + \frac{1}{2} \leq \frac{1}{\ell}(\lambda + \frac{1}{2})$,
(2) $(-1)^{\lambda'} = (-1)^{\lambda} \left(\frac{-1}{\ell}\right)$,

and there exists a cusp form $f \in S^+_{\lambda'+\frac{1}{2}}(\Gamma_0(4)) \cap \mathcal{O}_v[[q]$ such that

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

Proof. Let g be as in the hypotheses, and recall the definition (1.2) of $\theta_0(z)$. Set

$$h := \theta_0^{\ell} g \in S_{\lambda+\frac{\ell+1}{2}}(\Gamma_1(4)).$$

Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be a Frobenius automorphism for the prime v; then for $a \in \mathcal{O}_v$ we have $a^\sigma \in \mathcal{O}_v$ and

$$a^\sigma \equiv a^\ell \pmod{v}.$$

Since σ preserves the space $S_{\lambda+\frac{\ell+1}{2}}(\Gamma_1(4)) \cap \mathcal{O}_v[[q]]$, and U_ℓ acts as $T(\ell, \lambda+(\ell+1)/2, 1)$ modulo v, we find that $\overline{h^\sigma}$, $\overline{h\big|U_\ell} \in \overline{S_{\lambda+\frac{\ell+1}{2}}(\Gamma_1(4))}$ satisfy

$$\overline{h^\sigma} = (\overline{h\big|U_\ell})^\ell.$$

From Proposition 2.2, there is some $\alpha \geq 0$ so that

$$\omega(\overline{h\big|U_\ell}) = \frac{1}{\ell}\omega(\overline{h^\sigma}) = \frac{2[\lambda - \alpha(\ell-1)] + \ell + 1}{2\ell}. \tag{4.1}$$

Denoting the right side of (4.1) by $\lambda' + 1$, we conclude that there exists $H \in S_{\lambda'+1}(\Gamma_1(4))$ such that $\overline{H} = \overline{h\big|U_\ell}$.

The algebra of modular forms on $\Gamma_1(4)$ is generated by θ_0 and F, where $F = \sum_{n=0}^{\infty} \sigma_1(2n+1)q^n$ (see Proposition 4 on pg. 184 of [11]). The cusp forms are those forms divisible by $\theta_0 F(\theta_0^4 - 16F)$; it follows that every integer weight cusp form on $\Gamma_1(4)$ is a multiple of $\theta_0^2 F(\theta_0^4 - 16F)$. Set $f := H/\theta_0 \in S_{\lambda'+\frac{1}{2}}(4)$. Then $\overline{f} = \overline{g\big|U_\ell}$, as desired.

The first assertion about λ' follows immediately from (4.1). Multiplying (4.1) by ℓ gives the congruence

$$\lambda' \equiv \lambda + \frac{\ell - 1}{2} \pmod{2},$$

from which the second assertion follows. The plus space condition is checked using this assertion, since $(-1)^\lambda \ell \equiv (-1)^{\lambda'} \pmod 4$. □

5. Proof of main theorem

The proof of Theorem 1.2 proceeds in a number of steps. We begin with the following consequence of the results of the third section.

Proposition 5.1. *Suppose that $\ell \geq 5$ is prime, that K is a number field, and that v is a prime ideal of K above ℓ. Suppose that λ is a non-negative integer and that $f(z) \in S^+_{\lambda+\frac{1}{2}}(\Gamma_0(4)) \cap \mathcal{O}_v[[q]]$. Further, suppose that*

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

where each t_i is a square-free positive integer. Then

$$f(z) \equiv \sum_{n=1}^{\infty} a(n^2) q^{n^2} + \sum_{n=1}^{\infty} a(\ell n^2) q^{\ell n^2} \pmod{v}. \tag{5.1}$$

Proof. For each $i \in \{1, \dots, t\}$, we may assume that there exists an index n_i for which $a(t_i n_i^2) \not\equiv 0 \pmod{v}$. Following the argument of Lemma 4.1 of [1], we can find odd primes $p_1, \dots, p_s$, each relatively prime to $n_i t_i \ell$, and a modular form

$$G_i(z) \in S_{\lambda+\frac{1}{2}}(\Gamma_0(4p_1^2 \cdots p_s^2)) \cap \mathcal{O}_v[[q]]$$

with

$$G_i(z) \equiv \sum_{\gcd(n, \prod p_i)=1} a(t_i n^2) q^{t_i n^2} \not\equiv 0 \pmod{v}. \tag{5.2}$$

Thus, we have

$$G_i(z)^4 \equiv \sum_{n=1}^{\infty} b(t_i n) q^{t_i n} \pmod{v} \tag{5.3}$$

and

$$G_i(z)^4 \in S_{4\lambda+2}(\Gamma_0(4p_1^2 \cdots p_s^2)) \cap \mathcal{O}_v[[q]].$$

Theorem 3.1 implies that

$$t_i = 1,\ \ell,\ 2,\ \text{or } 2\ell.$$

It remains to rule out the last two possibilities. If $t_i = 2\ell$, then we find from the plus-space condition that the form G_i has the property that

$$G_i \equiv \sum a(8\ell n^2) q^{8\ell n^2} \pmod{v}.$$

Next, we use the fact (see Lemma 7 of [3]) that if $F \in S_k(\Gamma_0(M))$ and $p^2 | M$, then $F\big|U_p \in S_k(\Gamma_0(M/p))$. Setting $N = p_1^2 \cdots p_s^2$, we conclude that $G_i^4\big|U_2 \equiv \sum b(8\ell n) q^{4\ell n} \pmod{v}$ is a form of level $2N$, and so is identically zero modulo v by Theorem 3.2. It follows that $G_i \equiv 0 \pmod{v}$. If $t_i = 2$, then the proof is the same. □

After this result we are reduced to the consideration of forms f as in (5.1). The situation splits depending on the parity of λ as indicated by the next two results.

Theorem 5.2. *Suppose that $\ell \geq 5$ is prime, that K is a number field, and that v is a prime ideal of K above ℓ. Suppose that $f(z) \in S^+_{\lambda+\frac{1}{2}}(\Gamma_0(4)) \cap \mathcal{O}_v[[q]]$ has the form*

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

If λ is even, and

$$\ell > \sqrt{\lambda/2},$$

then

$$\sum_{\ell \nmid n} a(n^2)q^{n^2} \equiv a(1) \sum_{\ell \nmid n} n^{\bar{\lambda}} q^{n^2} \pmod{v},$$

where

$$\bar{\lambda} := \begin{cases} \lambda \bmod (\ell-1) & \text{if } \ell - 1 \nmid \lambda \\ \ell - 1 & \text{if } \ell - 1 \mid \lambda. \end{cases}$$

Proof of Theorem 5.2. Let f be as in the hypotheses, and recall the definition (1.2) of $\theta_0(z)$. From Lemma 4.1, there is a modular form $g(z) \in S^+_{(\ell+1)\frac{\bar{\lambda}+2}{2}+\frac{1}{2}}(\Gamma_0(4))$ such that

$$g(z) = \sum_{n=1}^{\infty} c(n)q^n \equiv \tfrac{1}{2}a(1)\Theta^{\frac{\bar{\lambda}+2}{2}}\theta_0(z) \equiv a(1)\sum_{n=1}^{\infty} n^{\bar{\lambda}+2}q^{n^2} \pmod{v}. \tag{5.4}$$

Again by Lemma 4.1 there is a modular form $h(z) \in S^+_{\lambda+\ell+1+\frac{1}{2}}(\Gamma_0(4))$ such that

$$h(z) = \sum_{n=1}^{\infty} b(n)q^n \equiv \Theta f(z) \equiv \sum_{n=1}^{\infty} a(n^2)n^2 q^{n^2} \pmod{v}. \tag{5.5}$$

It suffices to prove that $g \equiv h \pmod{v}$.

Theorem 2.1 implies that for each odd prime p with $p \not\equiv 0, 1 \pmod{\ell}$, we have

$$h\big|T(p^2, \lambda+\ell+1+\tfrac{1}{2}, 1) \equiv (p^{\bar{\lambda}+2} + p^{\bar{\lambda}+1})h \pmod{v}. \tag{5.6}$$

For every such prime, and for every natural number n, we find from the definition of the Hecke operators that

$$b(n^2p^2) + \left(\tfrac{n^2}{p}\right)p^{\bar{\lambda}+1}b(n^2) + p^{2\bar{\lambda}+3}b(n^2/p^2) \equiv (p^{\bar{\lambda}+2} + p^{\bar{\lambda}+1})b(n^2) \pmod{v}. \tag{5.7}$$

Suppose that n is an odd integer which is divisible only by primes $p \not\equiv 0, 1 \pmod{\ell}$. If $p^a \,||\, n$, then writing $n = p^a n_0$, an induction argument using (5.7) shows that

$$b(p^{2a}n_0^2) \equiv p^{a(\bar{\lambda}+2)}b(n_0^2) \pmod{v}.$$

It follows that we have

$$b(n^2) \equiv n^{\bar{\lambda}+2}a(1) \equiv c(n^2) \pmod{v}. \tag{5.8}$$

Now let

$$k := \max\{\lambda+\ell+1,\ (\ell+1)(\bar{\lambda}+2)/2\}. \tag{5.9}$$

Since λ is even, we see that the two quantities in (5.9) are congruent modulo $\ell - 1$. Therefore, multiplying one of h or g by a power of $E_{\ell-1}(4z)$ if necessary, we may assume that each of the forms h, g lies in the space $S^+_{k+\frac{1}{2}}(\Gamma_0(4))$.

Recalling that the operator $U(4)$ preserves each space $S_{\lambda+\frac{1}{2}}(\Gamma_0(4))$, we define the forms

$$G(z) := g(z) - g(z)\big|U(4)\big|V(4), \qquad H(z) := h(z) - h(z)\big|U(4)\big|V(4). \tag{5.10}$$

Each of these lies in the space $S_{k+\frac{1}{2}}(\Gamma_0(16))$. From (5.4) and (5.5) we have

$$G(z) - H(z) \equiv \sum_{n \text{ odd}} (c(n^2) - b(n^2))q^{n^2}. \tag{5.11}$$

Using (5.4) and (5.8) together with the fact that $b(n) \equiv c(n) \equiv 0 \pmod{v}$ when $\ell \mid n$, we conclude that the form $G - H$ vanishes to order at least $(2\ell+1)^2$ modulo v at infinity. It is straightforward to check that if $\ell > \sqrt{\lambda/2}$, then

$$(2\ell+1)^2 > \tfrac{k+1/2}{12}[\Gamma_0(1) : \Gamma_0(16)].$$

By a theorem of Sturm [19] we conclude that $G - H$ is identically zero modulo v.

Recalling (5.11), it remains to prove that the forms g and h agree at even exponents. To see this define $F(z) := g(z) - h(z) \equiv \sum d(4n^2)q^{4n^2} \pmod{v}$. Then the Shimura lift $\mathrm{Sh}^+_{1,k} F(z) \in S_{2k}(\Gamma_0(1))$ satisfies $\mathrm{Sh}^+_{1,k} F(z) \equiv \sum A(2n)q^{2n} \pmod{v}$ for some numbers $A(2n)$. By Theorem 3.1, we conclude that $\mathrm{Sh}^+_{1,k} F(z) \equiv 0 \pmod{v}$. From the definition of the Shimura lift, we conclude that $F(z) \equiv 0 \pmod{v}$. □

In the next result, we use the theory of Galois representations to treat the case when λ is odd.

Theorem 5.3. *Suppose that $\ell \geq 5$ is prime, that K is a number field, and that v is a prime ideal of K above ℓ. Suppose that $f(z) \in S^+_{\lambda+\frac{1}{2}}(\Gamma_0(4)) \cap \mathcal{O}_v[[q]]$ has the form*

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

If λ is odd, then $\Theta(f) \equiv 0 \pmod{v}$.

Proof. Suppose to the contrary that $\Theta(f) \not\equiv 0 \pmod{v}$. Then there exists a form $g \in S^+_{\lambda+\ell+1+1/2}(\Gamma_0(4)) \cap \mathcal{O}_v[[q]]$ such that

$$\overline{\Theta(f)} = \sum_{n=1}^{\infty} \overline{n^2 a(n^2)} q^{n^2} = \overline{g} \neq 0.$$

Define $G(z) := \mathrm{Sh}^+_{-4,\lambda+\ell+1}(g) \in S_{2\lambda+2\ell+2}(\Gamma_0(1))$. Since λ is odd, $a(n^2) = 0$ unless n is even. From the definition of $\mathrm{Sh}^+_{-4,\lambda+\ell+1}$, it follows that $G \not\equiv 0 \pmod{v}$.

From Theorem 2.1, we have

$$g|T(p^2, \lambda+\ell+1+\tfrac{1}{2}, 1) \equiv \left(\tfrac{-1}{p}\right)\left(p^{\lambda+2} + p^{\lambda+1}\right) g \pmod{v},$$

for all odd primes $p \not\equiv 0, 1 \pmod{\ell}$. Since $\mathrm{Sh}^+_{-4,\lambda+\ell+1}$ commutes with the action of the Hecke operators, it follows that

$$G|T(p, 2\lambda+2\ell+2, 1) \equiv \left(\tfrac{-1}{p}\right)\left(p^{\lambda+2} + p^{\lambda+1}\right) G \pmod{v} \tag{5.12}$$

for the same set of primes p.

The Deligne-Serre lifting lemma (see Lemme 6.11 of [7]) implies that there is a number field $L \supset K$, a prime ideal β above v with valuation ring $\mathcal{O}_\beta$ and a nonzero form $\tilde{G}$ with coefficients in $\mathcal{O}_\beta$ so that

$$\tilde{G}|T(p, 2\lambda + 2\ell + 2, 1) = b(p)\tilde{G}$$

for all odd primes $p \not\equiv 0, 1 \pmod{\ell}$, where

$$b(p) \equiv \left(\tfrac{-1}{p}\right)\left(p^{\lambda+2} + p^{\lambda+1}\right) \pmod{\beta}. \tag{5.13}$$

Note that $b(p) \equiv 0 \pmod{\beta}$ implies that $p \equiv -1 \pmod{\ell}$. Now, write

$$\tilde{G} = \sum_{i=1}^{\dim S_{2\lambda+2l+2}} c_i G_i,$$

where the $G_i \in S_{2\lambda+2\ell+2}(\Gamma_0(1))$ are normalized Hecke eigenforms. Letting $\lambda_i(p)$ denote the pth coefficient of g_i, we have

$$\tilde{G}|T(p, 2\lambda + 2l + 2, 1) = \sum_{i=1}^{\dim S_{2\lambda+2l+2}} c_i\lambda_i(p)G_i = b(p)\tilde{G} = \sum_{i=1}^{\dim S_{2\lambda+2l+2}} c_i b(p)G_i.$$

Since the G_i are linearly independent, it follows that $b(p) = \lambda_i(p)$ for all i with $c_i \neq 0$ (note that there is at least one such c_i).

Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\beta)$ be the mod β Galois representation associated to one of the eigenforms G_i with $c_i \neq 0$. Then, ρ is unramified outside ℓ, and for $p \neq \ell$ prime, we have $\mathrm{Det}\,\rho(\mathrm{Frob}_p) \equiv p^{2\lambda+3} \pmod{\beta}$. Also, if p is an odd prime with $p \not\equiv 0, 1 \pmod{\ell}$, we have

$$\mathrm{Tr}\,\rho(\mathrm{Frob}_p) \equiv \left(\tfrac{-1}{p}\right)\left(p^{\lambda+2} + p^{\lambda+1}\right) \pmod{\beta}.$$

At this point, we argue as in [1]. We will show that ρ is reducible.

Suppose that ρ is not reducible. Then Lemmas 4.3 and 4.4 of [1] show that $\ell \nmid |\mathrm{im}(\rho)|$; it follows that the image of ρ in $\mathrm{PGL}_2(\mathbb{F}_\beta)$ is dihedral, or the image is isomorphic to A_4, S_4 or A_5.

If the projective image is dihedral, then $\left(\frac{p}{l}\right) = -1$ implies that $b(p) \equiv 0 \pmod{\beta}$, which is impossible, since $b(p) \equiv 0 \pmod{\beta}$ only when $p \equiv -1 \pmod{\ell}$.

Suppose that the projective image is A_4, S_4 or A_5. Setting $x = b(p)^2/p^{2\lambda+3}$, we have $x \equiv 4, 0, 1, 2 \pmod{\beta}$, or $x^2 - 3x + 1 \equiv 0 \pmod{\beta}$, depending on whether the image of $\rho(\mathrm{Frob}_p)$ in $\mathrm{PGL}_2(\mathbb{F}_\beta)$ has order 1, 2, 3, 4, or 5, respectively. However, (5.13) implies that

$$x \equiv p + 2 + p^{-1} \pmod{\beta}$$

for odd p with $p \not\equiv 0, 1 \pmod{\ell}$. There are $\frac{\ell-1}{2}$ elements of $\mathbb{F}_\ell$ of the form $p + 2 + p^{-1}$ where $p \not\equiv 0, 1 \pmod{\ell}$. Since $p + 2 + p^{-1}$ takes on at most six values, it follows that $\ell \leq 13$. Explicit computations show that $\ell = 7, 11$ and 13 are impossible. Suppose therefore that $\ell = 5$. Let $\tilde{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_\beta)$. For $p \equiv 2, 3 \pmod{5}$ we have $x \equiv 2 \pmod{\beta}$. This, together with the Chebotarev density theorem, implies that the order of at least half of the elements of the projective image is 4. This is a contradiction, since none of A_4, S_4 or A_5 has this property.

We conclude in every case that ρ is reducible; since ρ is unramified outside ℓ, it follows that for some a, b we have

$$\rho = \begin{bmatrix} \chi^a & * \\ 0 & \chi^b \end{bmatrix},$$

where χ is the mod ℓ cyclotomic character. Therefore

$$\operatorname{Tr}\rho(\mathrm{Frob}_p) \equiv \chi^a(\mathrm{Frob}_p) + \chi^b(\mathrm{Frob}_p) \equiv p^a + p^b \pmod{\beta}$$

for all primes $p \neq \ell$. Notice that $\operatorname{Tr}\rho(\mathrm{Frob}_p)$ only depends on p mod ℓ. Now, choose primes q and r such that $q \not\equiv 0, 1, -1 \pmod{\ell}$, $q \equiv 3 \pmod 4$, and $r \equiv q \pmod{\ell}$, $r \equiv 1 \pmod 4$. Then $\operatorname{Tr}\rho(\mathrm{Frob}_q) = \operatorname{Tr}\rho(\mathrm{Frob}_r)$, and (5.12) yields the contradiction

$$\left(\tfrac{-1}{q}\right)(q^{\lambda+2} + q^{\lambda+1}) \equiv \left(\tfrac{-1}{r}\right)(r^{\lambda+2} + r^{\lambda+1}).$$

Therefore we must have $\Theta(f) \equiv 0 \pmod v$, as desired. □

Before proving the main theorem we require one more result.

Proposition 5.4. *Suppose that $\ell \geq 5$ is prime, that K is a number field which is Galois over $\mathbb{Q}$, and that v is a prime ideal of K above ℓ. Suppose that $r \leq \ell$ and that $g \in S^+_{r+\frac{1}{2}}(\Gamma_0(4)) \cap \mathcal{O}_v[[q]]$ satisfies*

$$g \equiv \sum_{n=1}^{\infty} a(n^2) q^{n^2} + \sum_{n=1}^{\infty} a(\ell n^2) q^{\ell n^2} \pmod v.$$

Then $g \equiv 0 \pmod v$.

Proof. Suppose first that r is odd. Then Theorem 5.3 implies that $\Theta(g) \equiv 0 \pmod v$. Therefore g vanishes modulo v to order $\geq \ell$. However, the Sturm bound on the space $S^+_{r+\frac{1}{2}}(\Gamma_0(4))$ is $\frac{r+1/2}{12} \cdot 6 < \ell$ since $r \leq \ell$. Therefore $g \equiv 0 \pmod v$ in this case.

Suppose then that r is even. Applying Theorem 5.2 to g, we conclude that

$$\Theta^{\ell-1}(g) \equiv c \sum_{\ell \nmid n}^{\infty} n^r q^{n^2} \pmod v,$$

where $c := a(1)$, and hence that $a(n^2) \equiv cn^r \pmod v$ provided that $\ell \nmid n$. We will prove that $c \equiv 0 \pmod{\ell}$.

Let

$$G := \mathrm{Sh}^+_{1,r}(g) = \sum_{n=1}^{\infty} \sum_{d \mid n} d^{r-1} a((n/d)^2) q^n \in S_{2r}(\Gamma_0(1)).$$

It follows that if $\ell \nmid n$, then the nth coefficient of G is congruent to

$$c \sum_{d \mid n} d^{r-1}(n/d)^r = c \sum_{d \mid n} (n/d)^{r-1} d^r = cn^{r-1}\sigma_1(n).$$

This is the same as the nth coefficient of

$$-\overline{\tfrac{c}{24}\Theta^{r-1}(E_{\ell+1})} \in \overline{S_{r(\ell+1)}(\Gamma_0(1))}.$$

Note that $w(E_{\ell+1}) = \ell + 1 \equiv 1 \pmod{\ell}$. Hence, applying the Θ-operator $r-1$ times, we get

$$w(\overline{\Theta^{r-1}E_{\ell+1}}) = r(\ell+1).$$

Also note that $GE_{\ell-1}^r \in S_{r(\ell+1)}(\Gamma_0(1))$. Now define

$$\overline{H} := \overline{GE_{\ell-1}^r + \tfrac{c}{24}\Theta^{r-1}E_{\ell+1}} \in \overline{S_{r(\ell+1)}(\Gamma_0(1))}.$$

Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be a Frobenius element for the prime v. Since $\overline{H}$ has the form $\sum \overline{a(n)}q^{\ell n}$, we have $\overline{H}^\sigma = (\overline{H\big|U_\ell})^\ell$, which implies that

$$w(\overline{H}) = w(\overline{H^\sigma}) = \ell w(\overline{H\big|U_\ell}).$$

However, $\ell \nmid r(\ell+1)$ and hence $w(\overline{H}) < r(\ell+1)$. It follows that $w(\overline{H}) \le r(\ell+1)-(\ell-1)$ and thus,

$$\overline{H - GE_{\ell-1}^{r-1}} = \overline{\tfrac{c}{24}\Theta^{r-1}E_{\ell+1}}$$

has filtration at most $r(\ell+1)-(\ell-1)$. This is a contradiction unless $c \equiv 0 \pmod{v}$. This implies that $\Theta(g) \equiv 0 \pmod{v}$, which implies that $g \equiv 0 \pmod{v}$ as in the case when r is odd. □

We are now in a position to prove the main theorem.

Proof of Theorem 1.2. Assume that $f \in S^+_{\lambda+1/2}(\Gamma_0(4))$, where $\lambda+1/2 < \ell(\ell+1+1/2)$, satisfies the hypotheses of Theorem 1.2. We may suppose without loss of generality that the field K is a Galois extension of $\mathbb{Q}$. By Proposition 5.1, we have

$$f \equiv \sum_{n=1}^{\infty} a(n^2)q^{n^2} + \sum_{n=1}^{\infty} a(\ell n^2)q^{\ell n^2} \pmod{v}. \tag{5.14}$$

Suppose first that λ is even. From Theorem 5.2, we have

$$\Theta^{\ell-1}(f) \equiv \sum_{\ell\nmid n} a(n^2)q^{n^2} \equiv a(1)\sum_{\ell\nmid n} n^{\bar\lambda}q^{n^2} \pmod{v}.$$

Lemma 4.1 implies that

$$\overline{\Theta^{\ell-1}(f)} = \overline{\frac{a(1)}{2}\Theta^{\bar\lambda/2}(\theta_0)} \in \overline{S^+_{(\bar\lambda/2)(\ell+1)+\frac12}(\Gamma_0(4))}.$$

Since $\bar\lambda \le \ell-1$, we have

$$(\bar\lambda/2)(\ell+1)+\tfrac12 \le \tfrac{\ell^2-1}{2}+\tfrac12.$$

Since $\overline{\lambda}$ is even, it follows that $\frac{\bar\lambda}{2}(\ell+1)$ is even. We conclude that $\overline{f-\Theta^{\ell-1}f} \in \overline{S^+_{\lambda'+\frac12}(\Gamma_0(4))}$ where $\lambda'+1/2 < \ell(\ell+1+1/2)$ and λ' is even.

We have

$$f - \Theta^{\ell-1}f \equiv \sum_{n=1}^{\infty} a(\ell n^2)q^{\ell n^2} + \sum_{n=1}^{\infty} a(\ell^2 n^2)q^{\ell^2 n^2} \pmod{v}. \tag{5.15}$$

It follows by Lemma 4.2 that there exists a form $g \in S^+_{r+\frac12}(\Gamma_0(4)) \cap \mathcal{O}_v[[q]]$ for some r with $r \le \ell$ such that

$$g \equiv \left(f - \Theta^{\ell-1}f\right)\big|U_\ell \pmod{v}.$$

By (5.15) we see that

$$g \equiv \sum_{n=1}^{\infty} a(\ell n^2)q^{n^2} + \sum_{n=1}^{\infty} a(\ell^2 n^2)q^{\ell n^2} \pmod{v}. \tag{5.16}$$

Applying Proposition 5.4, we conclude that $g \equiv 0 \pmod{v}$, so that $f \equiv \Theta^{\ell-1} f \pmod{v}$. This proves the theorem in the case when λ is even.

Suppose finally that λ is odd. In this case we wish to prove that $f \equiv 0 \pmod{v}$. Using (5.14) and Theorem 5.3 we conclude that

$$\Theta(f) \equiv 0 \pmod{v}.$$

It follows by Lemma 4.2 that there exists a form $g \in S^+_{r+\frac{1}{2}}(\Gamma_0(4)) \cap \mathcal{O}_v[[q]]$ for some r with $r \leq \ell$ such that

$$g \equiv f\big|U_\ell \equiv \sum_{n=1}^{\infty} a(\ell n^2) q^{n^2} + \sum_{n=1}^{\infty} a(\ell^2 n^2) q^{\ell n^2} \pmod{v}.$$

Then Proposition 5.4 implies that $g \equiv 0 \pmod{v}$. Since $g^\ell \equiv f^\sigma \pmod{v}$, this implies that $f^\sigma \equiv f \equiv 0 \pmod{v}$, which finishes the proof of the theorem.

□

From our main theorem, we obtain the proof of Corollaries 1.4 and 1.5.

Proof of Corollary 1.4 and 1.5. Let $g(z) = \sum_{n=1}^{\infty} c(n) q^n \in S^+_{k+1/2}(\Gamma_0(4))$ be a half-integral weight Hecke eigenform with the same eigenvalues as f, normalized to have Fourier coefficients which are relatively prime algebraic integers. Such a g exists from Theorem 1 of [12], which states that $S^+_{k+1/2}(\Gamma_0(4))$ and $S_{2k}(\Gamma_0(1))$ are isomorphic as Hecke modules. We have $g \not\equiv 0 \pmod{v}$. When $(-1)^k D > 0$, Theorem 1.3 implies that $c(|D|) \equiv 0 \pmod{v}$ if and only if $L^{\text{alg}}(f, D, k) \equiv 0 \pmod{v}$.

If k is odd, then the assumptions of Corollary 1.4 together with Theorem 1.2 imply that $\overline{g}$ is not supported on finitely many square classes modulo v. A straightforward argument using the plus-space condition and the fact that g is a Hecke eigenform implies that $c(|D|) \not\equiv 0 \pmod{v}$ for infinitely many fundamental discriminants D.

If k is even, the assumption that there are only finitely many D so that $L^{\text{alg}}(f, D, k) \equiv 0 \pmod{v}$ implies as above that $\overline{g}$ is supported on finitely many square classes modulo v. Then Theorem 1.2 implies that

$$g(z) \equiv a(1) \sum_{n=1}^{\infty} n^\lambda q^{n^2} \pmod{v}$$

with $a(1) \not\equiv 0 \pmod{v}$. Therefore $L^{\text{alg}}(f, 1, k) \not\equiv 0 \pmod{v}$ and $L^{\text{alg}}(f, D, k) \equiv 0 \pmod{v}$ for $D > 1$, as desired. □

References

[1] S. Ahlgren and M. Boylan, *Coefficients of half-integral weight modular forms modulo l^j*, Math. Ann. **331** (2005), no. 1, 219–239.

[2] ———, *Central critical values of modular L-functions and coefficients of half-integral weight modular forms modulo l*, Amer. J. Math. **129** (2007), no. 2, 429–454.

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

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

[5] ———, *Nonvanishing modulo l of Fourier coefficients of half-integral weight modular forms*, Duke Math. J. **98** (1999), no. 3, 595–611.

[6] J. H. Bruinier and K. Ono, *Coefficients of half-integral weight modular forms*, J. Number Theory **99** (2003), no. 1, 164–179.

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

[8] F. Diamond and J. Im, *Modular forms and modular curves*, in Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), Vol. 17 of *CMS Conf. Proc.*, 39–133, Amer. Math. Soc., Providence, RI (1995).

[9] F. Diamond and J. Shurman, A first course in modular forms, Vol. 228 of *Graduate Texts in Mathematics*, Springer-Verlag, New York (2005), ISBN 0-387-23229-X.

[10] B. H. Gross, *A tameness criterion for Galois representations associated to modular forms (mod p)*, Duke Math. J. **61** (1990), no. 2, 445–517.

[11] N. Koblitz, Introduction to elliptic curves and modular forms, Vol. 97 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, second edition (1993), ISBN 0-387-97966-2.

[12] W. Kohnen, *Modular forms of half-integral weight on* $\Gamma_0(4)$, Math. Ann. **248** (1980), no. 3, 249–266.

[13] ———, *Fourier coefficients of modular forms of half-integral weight*, Math. Ann. **271** (1985), no. 2, 237–268.

[14] W. Kohnen and D. Zagier, *Values of L-series of modular forms at the center of the critical strip*, Invent. Math. **64** (1981), no. 2, 175–198.

[15] S. Lang, Introduction to modular forms, Vol. 222 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*, Springer-Verlag, Berlin (1995), ISBN 3-540-07833-9. With appendixes by D. Zagier and Walter Feit, Corrected reprint of the 1976 original.

[16] K. Ono and C. Skinner, *Fourier coefficients of half-integral weight modular forms modulo l*, Ann. of Math. (2) **147** (1998), no. 2, 453–470.

[17] B. Schoeneberg, Elliptic modular functions: an introduction, Springer-Verlag, New York (1974). Translated from the German by J. R. Smart and E. A. Schwandt, Die Grundlehren der mathematischen Wissenschaften, Band 203.

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

[19] J. Sturm, *On the congruence of modular forms*, in Number theory (New York, 1984–1985), Vol. 1240 of *Lecture Notes in Math.*, 275–280, Springer, Berlin (1987).

[20] H. P. F. Swinnerton-Dyer, *On l-adic representations and congruences for coefficients of modular forms. II*, in Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), 63–90. Lecture Notes in Math., Vol. 601, Springer, Berlin (1977).

[21] A. Tupan, *Congruences for* $\Gamma_1(4)$*-modular forms of half-integral weight*, Ramanujan J. **11** (2006), no. 2, 165–173.

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

[23] J.-L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures Appl. (9) **60** (1981), no. 4, 375–484.

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

School of Liberal Arts and Sciences, Korea Aerospace University, 200-1, Hwajeon-dong, Goyang, Gyeonggi 412-791, Korea
E-mail address: choija@postech.ac.kr

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