MODULAR FORM CONGRUENCES AND SELMER GROUPS

William J. McGraw and Ken Ono

In celebration of Barry Mazur's 65th birthday.

1. Introduction and Statement of Results.

Motivated by Cremona and Mazur's notion of *visibility* of elements in Shafarevich-Tate groups [6, 27], there have been a number of recent works which test its compatibility with the Birch and Swinnerton-Dyer Conjecture and the Bloch-Kato Conjecture. These conjectures provide formulas for the orders of Shafarevich-Tate groups in terms of values of L-functions. For example, one may see recent work of Agashe, Dummigan, Stein and Watkins [1, 2, 10, 11]. In their examples, they find that the presence of visible elements agrees with the expected divisibility properties of the relevant L-values.

Here we aim to obtain further results in this direction. In our setting there are two routes which one may take when setting out to prove "congruences" between Selmer-type groups. One natural approach is to start with congruences for the associated Galois modules, compute cohomology, and then compare. Here we adopt the second natural approach, one which involves the theory of half-integral weight modular forms. We proceed by immediately passing to modular forms and then to L-functions (for integral weight modular forms), and then to Fourier coefficients of half-integral weight modular forms. We prove general theorems regarding congruences between spaces of such half-integral weight modular forms, and then work back to the Selmer groups. The general context in which we are working is in the p-adic interpolation of square-roots of central values of L-functions. Among others, we note related earlier works of Guerzhoy, Hida, Sofer, and Stevens [14, 18, 32, 33] on such questions.

We begin by briefly recalling the relevant objects. Suppose that $\mathcal{F}(z) = \sum_{n=1}^{\infty} A(n)q^n \in S_{2k}^{\text{new}}(\Gamma_0(N))$ is an even weight newform whose coefficients are algebraic integers in a number field K. If D is the fundamental discriminant of a quadratic field, then let $\mathcal{F}_D(z)$ denote the D-quadratic twist of $\mathcal{F}(z)$. Similarly, if $E/\mathbb{Q}$ is an elliptic curve, then let $E(D)$ denote its D-quadratic twist.

1991 *Mathematics Subject Classification.* Primary 11F33, 11F37, 11F67, 11G40.

Key words and phrases. Congruences, Selmer groups, modular forms.

The first author thanks the Number Theory Foundation for their generous support. The second author is grateful for the support of the Alfred P. Sloan, David and Lucile Packard, and H. I. Romnes Fellowships, and the support of the National Science Foundation.

By a classical theorem of Deligne [7], for each finite prime λ of K there is a two dimensional vector space V_λ over K_λ, and a continuous Galois representation

$$\rho_\lambda : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(V_\lambda)$$

with the property that for primes $p \nmid N\ell$ (where $\lambda \mid \ell$) we have

$$\mathrm{Tr}(\rho_\lambda(\mathrm{Frob}_p)) = A(p) \quad \text{and} \quad \det(\rho_\lambda(\mathrm{Frob}_p)) = p^{2k-1}.$$

By work of Scholl [29], the spaces V_λ are λ-adic realizations of a Grothendieck motive, say $M_{\mathcal{F}}$. If j is a positive integer, then let $M_{\mathcal{F}}^{(j)}$ denote the usual jth *Tate twist* of $M_{\mathcal{F}}$. Furthermore, if D is a fundamental discriminant, then let $M_{\mathcal{F}}^{(j,D)}$ denote the motive

$$M_{\mathcal{F}}^{(j,D)} := M_{\mathcal{F}}^{(j)} \otimes_{\mathbb{Q}} \mathcal{D}, \tag{1.1}$$

where $\mathcal{D}$ denotes the motive associated to the usual Kronecker character for $\mathbb{Q}(\sqrt{D})$. Let $S\left(M_{\mathcal{F}}^{(j,D)}\right)$ $\left(\text{resp. } Ш\left(M_{\mathcal{F}}^{(j,D)}\right)\right)$ denote the associated Selmer group (resp. Shafarevich-Tate group). By the Bloch-Kato Conjecture, if $L(\mathcal{F}_D, k) \neq 0$, then $\#Ш\left(M_{\mathcal{F}}^{(k,D)}\right)$ is predicted by the formula [4]

$$L(\mathcal{F}_D, k) = \frac{\left(\prod_p c_p(\chi_D, k)\right) \Omega(\mathcal{F}_D, k) \cdot \#Ш\left(M_{\mathcal{F}}^{(k,D)}\right)}{\#\Gamma_{\mathbb{Q}}(\mathcal{F}_D, k)^2}. \tag{1.2}$$

Here the $c_p(\chi_D, k)$ are the Tamagawa numbers for $M_{\mathcal{F}}^{(k,D)}$, $\Omega(\mathcal{F}_D, k)$ is its Deligne period [8], and $\Gamma_{\mathbb{Q}}(\mathcal{F}_D, k)$ denotes the set of its global points. Note that this is in general an equality of fractional ideals. For convenience, we define the *algebraic part* of $L(\mathcal{F}_D, k)$ by

$$L^{\mathrm{alg}}(\mathcal{F}_D, k) = \frac{L(\mathcal{F}_D, k)}{\Omega(\mathcal{F}_D, k)}. \tag{1.3}$$

Note that the exact definition of the quantities in (1.2) and (1.3) depends on the choices of lattices in the realizations of the motive $M_{\mathcal{F}}^{(k)}$ (for example, see [4, 8, 10, 29]). For our purposes, we may suppress these technical considerations since the p-parts of the Shafarevich-Tate group are independent of these choices and the quotients of the relevant Deligne periods in Theorem 1 are always p-units.

Throughout we adopt the following notation. If p is an odd prime and D is a fundamental discriminant coprime to p, then let $D(p)$ denote the fundamental discriminant

$$D(p) := (-1)^{(p-1)/2} Dp. \tag{1.4}$$

We shall refer to a prime p as a *congruence prime for a newform* $f(z) \in S_{2k}^{\mathrm{new}}(\Gamma_0(M))$ if there is another newform $f_1(z) \in S_{2k}^{\mathrm{new}}(\Gamma_0(M))$ for which

$$f(z) \equiv f_1(z) \pmod{\mathfrak{p}},$$

for some prime ideal $\mathfrak{p}$ above p in the ring of algebraic integers of a suitably large number field.

Using this notation, we describe a natural strategy for visualizing elements in Selmer groups of motives of higher weight modular forms. Suppose that $E/\mathbb{Q}$ is an elliptic curve, and that $f(z)$ is the weight 2 newform associated to E in the usual way. Suppose that p is a prime of bad reduction that is not a congruence prime for $f(z)$. Then there may be a newform of weight $p+1$, say $\mathcal{F}(z)$, and a prime ideal $\mathfrak{p}$ above p in a suitable number field for which

$$f(z) \equiv \mathcal{F}(z) \pmod{\mathfrak{p}}$$

and

$$L^{\text{alg}}(f_D, 1) \equiv L^{\text{alg}}(\mathcal{F}_{D(p)}, (p+1)/2) \pmod{\mathfrak{p}}, \tag{1.5}$$

for certain fundamental discriminants D. If $E(D)$ has positive rank over $\mathbb{Q}$, then the p-part of the Selmer group of $E(D)$ is non-trivial, and one then hopes to visualize elements of order p in $S\left(M_{\mathcal{F}}^{(k,D(p))}\right)$ and the $\mathfrak{p}$-divisibility of $L^{\text{alg}}(\mathcal{F}_{D(p)}, (p+1)/2)$.

Examples of this strategy can be worked out explicitly. For example, Dummigan [10] analyzes the classical mod 11 congruence ($q = e^{2\pi iz}$ throughout)

$$\Delta(z) \equiv f(z) = q - 2q^2 - q^3 + \dots \pmod{11}, \tag{1.6}$$

where $\Delta(z)$ is the unique normalized weight 12 cusp form on $SL_2(\mathbb{Z})$, and $f(z)$ is the unique normalized form in $S_2(\Gamma_0(11))$ which is associated to the elliptic curve $E = X_0(11)$. He shows how (1.6) naturally provides relations between the 11-parts of the corresponding Selmer groups. He then confirms the expected congruences between the relevant L-values by employing work of Kohnen and Zagier [24, 25] on Shimura's correspondence [31]. These works show that the relevant L-values are essentially the squares of the coefficients of the Kohnen newforms

$$g(z) = q^3 - q^4 - q^{11} - q^{12} + q^{15} + \dots \in S_{3/2}^{\text{new}}(\Gamma_0(44)),$$
$$G(z) = q - 56q^4 + 120q^5 - 240q^8 + \dots \in S_{13/2}^{\text{new}}(\Gamma_0(4)).$$

The conjectured L-value congruences follow from the fact that

$$g(z) \equiv -G(z) \mid U(11) \pmod{11}, \tag{1.7}$$

where $U(d)$ denotes the Atkin U-operator

$$\left(\sum_{n=0}^{\infty} c(n)q^n\right) \mid U(d) = \sum_{n=0}^{\infty} c(dn)q^n. \tag{1.8}$$

One naturally wonders how general these beautiful observations are; after all, the heuristics motivating these calculations suggest that such relations should be quite common. Indeed, works by Koblitz, Mazur and Vatsal [21, 26, 35] and others already consider questions

related to congruences between critical values of congruent L-functions. In this direction, Dummigan generalizes his mod 11 example using works of Hida [16] and Stevens [33] on Λ-adic modular forms of integral and half-integral weight. He shows that if E is an elliptic curve with prime conductor $p \equiv 3 \pmod 4$ for which $p \nmid \mathrm{ord}_p(j(E))$ and $L(E_{-p}, 1) \neq 0$, then there are Hecke eigenforms of large weights which play the roles of $\Delta(z)$ and $G(z)$ as above.

Here we concentrate on proving general theorems regarding congruences like (1.7). We obtain such general p-adic results from Kohnen's theory of half-integral weight modular forms [23, 24]. As a consequence, we obtain some further results on visibility. As a special case, combining our observations with Dummigan's computations [Th. 8.1, 10] leads to the following theorem.

Theorem 1. *Suppose that p is not a congruence prime for any newform in $S_{p+1}(\Gamma_0(1))$, and suppose that $E/\mathbb{Q}$ is an elliptic curve with prime conductor p with the property that $p \nmid \mathrm{ord}_p(j(E))$. Let $f(z) \in S_2^{\mathrm{new}}(\Gamma_0(p))$ be its associated newform. If K is a suitably large number field with integer ring O_K, and $\mathfrak{p}$ is a prime ideal in O_K above p, then there is a newform $\mathcal{F}(z) \in S_{p+1}(\Gamma_0(1))$ which satisfies:*

(1) *We have that $f(z) \equiv \mathcal{F}(z) \pmod{\mathfrak{p}}$.*
(2) *If $w_p \in \{\pm 1\}$ is the eigenvalue of $f(z)$ with respect to the Atkin-Lehner involution $W(p)$ and D is a negative fundamental discriminant D with $\left(\frac{D}{p}\right) = w_p$, then the sign of the functional equation of $L(\mathcal{F}_{D(p)}, s)$ is $+1$.*
(3) *There is a negative fundamental discriminant, say D_0, with the property that*

$$\mathbb{L}^{\mathrm{alg}}(\mathcal{F}_{D(p)}, (p+1)/2) := \frac{L^{\mathrm{alg}}(\mathcal{F}_{D(p)}, (p+1)/2)}{L^{\mathrm{alg}}(\mathcal{F}_{D_0(p)}, (p+1)/2)}$$

and

$$\mathbb{L}^{\mathrm{alg}}(f_D, 1) := \frac{L^{\mathrm{alg}}(f_D, 1)}{L^{\mathrm{alg}}(f_{D_0}, 1)}$$

are both $\mathfrak{p}$-integral for every negative fundamental discriminant D with $\left(\frac{D}{p}\right) = w_p$. Moreover, for such D we have that

$$\mathbb{L}^{\mathrm{alg}}(\mathcal{F}_{D(p)}, (p+1)/2) \equiv 0 \pmod{\mathfrak{p}} \quad \text{if and only if} \quad \mathbb{L}^{\mathrm{alg}}(f_D, 1) \equiv 0 \pmod{\mathfrak{p}}.$$

(4) *If D is a negative fundamental discriminant for which $\left(\frac{D}{p}\right) = w_p$ and $E(D)$ has rank ≥ 2 over $\mathbb{Q}$, then*

$$\mathbb{L}^{\mathrm{alg}}(\mathcal{F}_{D(p)}, (p+1)/2) \equiv 0 \pmod{\mathfrak{p}} \qquad \text{and} \qquad S\left(M_{\mathcal{F}}^{((p+1)/2, D(p))}\right)[p] \neq \{0\}.$$

Moreover, the number of such D with $-X < D < 0$ is $\gg_E \frac{X^{1/7}}{(\log X)^2}$.

Remarks. 1) Let K_1 (resp. K_2) be the number field obtained by adjoining all the Fourier coefficients of the newforms (resp. Kohnen newforms) in $S_2^{\text{new}}(\Gamma_0(p))$ and $S_{p+1}^{\text{new}}(\Gamma_0(1))$ (resp. $S_{\frac{3}{2}}^{\text{new}}(\Gamma_0(4p))$ and $S_{\frac{(p+2)}{2}}^{\text{new}}(\Gamma_0(4))$) to $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$. Any number field containing $K = K_1K_2$ is sufficiently large for Theorem 1.

2) W. Stein has informed us that the only prime $p < 10^4$ that is a congruence prime for any newform in $S_{p+1}(\Gamma_0(1))$ is $p = 389$. However the conclusion of Theorem 1 is still true for the isogeny class of elliptic curves with conductor 389. This follows since the proof of Theorem 1 only requires that there is at most one newform $\mathcal{F}(z) \in S_{p+1}(\Gamma_0(1))$ for which $\mathcal{F}(z) \equiv f(z) \pmod{\mathfrak{p}}$. We point out that there is always at least one newform $\mathcal{F}(z) \in S_{p+1}(\Gamma_0(1))$ which satisfies Theorem 1 (1).

3) By the proof of [Th. 1, 20], it follows that there are $\gg_E \sqrt{X}/\log X$ many choices for the D_0 in Theorem 1 (3) with $-X < D_0 < 0$. Similarly, the proof also implies that

$$\#\left\{-X < D < 0 \ : \ \left(\frac{D}{p}\right) = w_p \quad \text{and} \quad \mathbb{L}^{\text{alg}}(\mathcal{F}_{D(p)}, (p+1)/2) \not\equiv 0 \pmod{\mathfrak{p}}\right\} \gg_E \frac{\sqrt{X}}{\log X}.$$

4) Theorem 1 concerns elliptic curves $E/\mathbb{Q}$ with prime conductor p. The mod p Galois representation of such curves are well known to be irreducible.

It is natural to ask how often the elements in these Selmer groups are elements of Shafarevich-Tate groups. In this direction, we state a widely believed conjecture [5].

Conjecture Z. *If $\mathcal{F}(z) = \sum_{n=1}^{\infty} A(n)q^n \in S_{2k}^{\text{new}}(\Gamma_0(N))$ is a newform with $2k \geq 6$, then there are at most finitely many fundamental discriminants D for which*

$$\text{ord}_{s=k}(L(\mathcal{F}_D, s)) \equiv 0 \pmod 2 \quad \text{and} \quad L(\mathcal{F}_D, k) = 0.$$

Assuming Conjecture Z and conjectures $C_r(M)$ and $C_\lambda^i(M)$ of [§1, §6.5, 12] and the calculations [Lemmas 6.2-3, 10], the discriminants D in Theorem 1 (4), apart from finitely many exceptions, yield nontrivial elements in Ш$\left(M_{\mathcal{F}}^{((p+1)/2, D(p))}\right)[p]$ which are also predicted by the Bloch-Kato conjecture. In particular, we have

$$\#\left\{-X < D < 0 \ : \ \text{Ш}\left(M_{\mathcal{F}}^{((p+1)/2, D(p))}\right)[p] \neq \{0\}\right\} \gg_E \frac{X^{1/7}}{(\log X)^2}. \tag{1.9}$$

As mentioned above, these results follow from a general study of the p-adic properties of Kohnen's theory of half-integral weight modular forms (see §3 for notation and essential facts). For odd primes p and non-negative integers j, let $\kappa(p, j)$ denote the integer

$$\kappa(p, j) := \frac{p^j(p-1)}{2}. \tag{1.10}$$

If p, k and j satisfy some mild inequalities, then we obtain the following commutative diagram on modular forms modulo p^{j+1} when N is an odd square-free integer coprime to p:

$$\begin{array}{ccc} S_{2k}^{\text{new}}(\Gamma_0(Np)) & \xrightarrow{\qquad\equiv\qquad} & S^+_{2(k+\kappa(p,j))}(\Gamma_0(N)) \\ \uparrow & & \uparrow \\ S^{\text{new}}_{k+\frac{1}{2}}(\Gamma_0(4Np)) & \xrightarrow{\qquad\equiv'\qquad} & S^+_{k+\kappa(p,j)+\frac{1}{2}}(\Gamma_0(4N)) \end{array} \tag{1.11}$$

The vertical arrows denote the Shimura correspondence (i.e. Kohnen's isomorphism) modulo p^{j+1}. The two horizontal arrows denote the reduction of p-integral modular forms modulo p^{j+1}. However, the $\equiv'$ above the bottom arrow denotes a congruence with a form hit with the $U(p)$ operator. Notice that (1.7) is the case of this picture where $N = 1$, $p = 11$, $j = 0$ and $k = 1$.

Since there may be congruences between newforms of weight $2(k + \kappa(p, j))$, it is often difficult to tease arithmetic information out of (1.11). However, the next result provides a clear picture in some cases where this difficulty is not present.

Theorem 2. *Suppose that p is an odd prime and that Np is an odd square-free integer. Furthermore, suppose that $j \geq 0$ and $k \geq 1$ are integers for which $j \geq k - \frac{3}{2}$, and that*

$$f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{2k}^{\text{new}}(\Gamma_0(Np))$$

and

$$g(z) = \sum_{n=1}^{\infty} b(n)q^n \in S^{\text{new}}_{k+\frac{1}{2}}(\Gamma_0(4Np))$$

are newforms that are associated by Kohnen's isomorphism. Let K be the number field obtained by adjoining $\sqrt{(-1)^{(p-1)/2}p}$ and all the coefficients of all the newforms in all of the spaces $S_{2k}^{\text{new}}(\Gamma_0(N'))$ and $S^{\text{new}}_{k+\frac{1}{2}}(\Gamma_0(4N'))$ over all divisors N' of N. Let O_K denote its ring of algebraic integers, and suppose that $\mathfrak{p} \subset O_K$ is a prime ideal above p. If there is exactly one newform

$$\mathcal{F}(z) = \sum_{n=1}^{\infty} A(n)q^n \in S^{\text{new}}_{2(k+\kappa(p,j))}(\Gamma_0(N'))$$

for $N' \mid N$ with the property that

$$a(\ell) \equiv A(\ell) \pmod{\mathfrak{p}}$$

for every prime $\ell \nmid Np$, then $N' = N$ implies that there is a unique Kohnen newform $\mathcal{G}(z) = \sum_{n=1}^{\infty} B(n)q^n \in S^{\text{new}}_{k+\kappa(p,j)+\frac{1}{2}}(\Gamma_0(4N))$ for which

$$g(z) \equiv \mathcal{G}(z) \mid U(p) \pmod{\mathfrak{p}}.$$

Moreover, $\mathcal{F}(z)$ is the image of $\mathcal{G}(z)$ under Kohnen's isomorphism.

Theorem 2 is quite useful when combined with works by Kohnen and Zagier and Waldspurger (see [23, 24, 25, 36]) on Shimura's correspondence [31]. They provide useful formulae for the central critical values of quadratic twists of the L-functions of even weight newforms. These numbers are *essentially* the squares of suitable Fourier coefficients of half-integral weight eigenforms. As a consequence, we often obtain congruences between the algebraic parts of L-values associated to congruent modular forms.

We recall a well known formula due to Kohnen. Suppose that N is odd and square-free, and suppose further that

$$g(z) = \sum_{n=1}^{\infty} b(n)q^n \in S^{\text{new}}_{k+\frac{1}{2}}(\Gamma_0(4N))$$

is a Kohnen newform. By Kohnen's isomorphism, there is a unique newform, say $f(z) \in S^{\text{new}}_{2k}(\Gamma_0(N))$, associated to $g(z)$ under Shimura's correspondence. The coefficients of $g(z)$ determine the central critical values of many of the quadratic twists $L(f_D, s)$. To state these formulae, let $\nu(N)$ denote the number of distinct prime divisors of N, and let $\langle f, f\rangle$ (resp. $\langle g, g\rangle$) denote the Petersson inner product on $S_{2k}(\Gamma_0(N))$ (resp. $S_{k+\frac{1}{2}}(\Gamma_0(4N))$). If $\ell \mid N$ is prime, then let $w_\ell \in \{\pm 1\}$ be the eigenvalue of the Atkin-Lehner involution

$$f\ |_{2k} W(\ell) = w_\ell f.$$

If $(-1)^k D > 0$ and D has the additional property that $\left(\frac{D}{\ell}\right) = w_\ell$ for each prime $\ell \mid N$, then Kohnen proves [Cor. 1, 24] that

$$L(f_D, k) = \frac{\langle f, f\rangle \cdot \pi^k}{2^{\nu(N)}(k-1)!|D|^{k-\frac{1}{2}}\langle g, g\rangle} \cdot |b(|D|)|^2. \tag{1.12}$$

For all other fundamental discriminants D with $(-1)^k D > 0$, it turns out that $b(|D|) = 0$. For those D for which (1.12) holds, we define $L^{\text{alg}}_K(f_D, k)$, the *Kohnen algebraic part* of $L(f_D, k)$, by

$$L^{\text{alg}}_K(f_D, k) := |b(|D|)|^2. \tag{1.13}$$

Obviously, (1.13) depends on the normalization of $g(z)$. This discussion together with Theorem 2 immediately implies the following corollary.

Corollary 3. *Assume the hypotheses and notation from Theorem 2. Suppose that $\mathcal{F}(z)$ satisfies the uniqueness property in the statement of Theorem 2, and that $g(z)$ and $\mathcal{G}(z)$ have Fourier coefficients which are real numbers. If D is a fundamental discriminant with $(-1)^k D > 0$ with the additional property that $\left(\frac{D}{\ell}\right) = w_\ell$ for every prime $\ell \mid Np$, then*

$$L^{\text{alg}}_K(f_D, k) \equiv L^{\text{alg}}_K(\mathcal{F}_{D(p)}, k + \kappa(p, j)) \pmod{\mathfrak{p}}.$$

In §2 we prove certain p-adic facts regarding integral weight newforms, and in §3 we prove their analogs in Kohnen's theory of half-integral weight modular forms. In §4 we prove Theorems 1 and 2.

Acknowledgements

The authors thank Amod Agashe, Scott Ahlgren, Neil Dummigan, Winfried Kohnen, Barry Mazur, William Stein and the referee for their comments and suggestions and improvements which lead to the final form of this paper.

2. p-adic properties of integer weight newforms.

We begin this section by recalling some preliminary facts about modular forms. For more general information, consult [22, 28]. Let k be a positive integer. The group

$$GL_2^+(\mathbb{R}) = \{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \text{ and } ad - bc > 0\}$$

acts on functions $f : \mathfrak{h} \to \mathbb{C}$ by the operator

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

where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Here, $\mathfrak{h} = \{x + iy \in \mathbb{C} \mid y > 0\}$. For a prime divisor p of N for which $\gcd(p, N/p) = 1$, define the operator $|_kW(p)$ on $M_k(\Gamma_0(N))$ by the matrix

$$W(p) = \begin{pmatrix} p & a \\ N & pb \end{pmatrix} \in M_2(\mathbb{Z}) \tag{2.2}$$

with determinant p. Since $W(p)$ is unique up to left multiplication by an element of $\Gamma_0(N)$, this indeed defines an action on $M_k(\Gamma_0(N))$. It turns out that $W(p)$ is an involution on $M_k(\Gamma_0(N))$, a so-called *Atkin-Lehner involution*. Notice that if $N = p$, then we may select the following representative for $W(p)$

$$W(p) = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}. \tag{2.3}$$

If d is a positive integer, then the V-operator $V(d)$ is defined by

$$\left(\sum_{n=0}^{\infty} c(n)q^n\right) \mid V(d) = \sum_{n=0}^{\infty} c(n)q^{dn}. \tag{2.4}$$

Our main result (i.e. Theorem 2.3) in this section depends on these operators, the U-operators defined in (1.8), the Atkin-Lehner theory of newforms, and the p-adic properties of certain Eisenstein series.

We now briefly recall some essential features of the Atkin-Lehner theory of newforms [3]. For a positive integer ℓ, let $\delta_\ell = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}$. Then we define the subspace

$$S_k^{\text{old}}(\Gamma_0(N)) := \oplus_{\ell M | N} \; S_k(\Gamma_0(M))|_k\delta_\ell,$$

where the sum runs over $\ell M \mid N$ with $M \neq N$. Define $S_k^{\text{new}}(\Gamma_0(N))$ to be the orthogonal complement of $S_k^{\text{old}}(\Gamma_0(N))$ with respect to the Petersson inner product. The Hecke operators are defined as usual on $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_k(\Gamma_0(N))$; for primes $\ell \nmid N$, $T(\ell)$ is given by

$$f(z)|_k T(\ell) = \sum_{n=1}^{\infty} c(n)q^n,$$

where

$$c(n) = a(\ell n) + \ell^{k-1} a\left(\frac{n}{\ell}\right).$$

A *newform* of level N is a normalized cusp form that is an eigenform of all the Hecke operators and all of the Atkin-Lehner involutions. It is well-known that the coefficients of a newform are algebraic integers in a fixed number field, and that $S_k^{\text{new}}(\Gamma_0(N))$ has a basis consisting of newforms.

If $k \geq 2$ is even, then let $E_k(z)$ denote the classical Eisenstein series

$$E_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n. \tag{2.5}$$

As usual, B_k denotes the kth Bernoulli number and $\sigma_r(n) := \sum_{d|n} d^r$. For $k \geq 4$, $E_k(z) \in M_k(\Gamma_0(1))$. If $p \geq 5$ is prime, then define the modular form $\mathcal{E}_p(z) \in M_{p-1}(\Gamma_0(p))$ by

$$\mathcal{E}_p(z) := E_{p-1}(z) - p^{\frac{p-1}{2}} \left(E_{p-1}|_{p-1} W(p)\right)(z). \tag{2.6}$$

Although $E_2(z) = 1 - 24\sum_{n=1}^{\infty} \sigma_1(n)q^n$ is not a modular form, it plays an important role here. In particular, if $p = 3$, then define $\mathcal{E}_3(z) \in M_2(\Gamma_0(3))$ [p. 817, 15] by

$$\mathcal{E}_3(z) := E_2(z) - 3E_2(3z). \tag{2.7}$$

Lemma 2.1. *If p is an odd prime, then we have*

$$\mathcal{E}_p(z) \equiv 1 \pmod{p}, \tag{2.8}$$

$$(\mathcal{E}_p|_{p-1} W(p))(z) \equiv 0 \pmod{p^{\kappa(p,0)+1}}. \tag{2.9}$$

Proof. By (2.3), we first note that, for $p \geq 5$,

$$\begin{aligned} E_{p-1}|_{p-1} W(p) &= E_{p-1}|_{p-1} \left(\begin{smallmatrix} 0 & -1 \\ p & 0 \end{smallmatrix}\right) \\ &= E_{p-1}|_{p-1} \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \\ &= p^{\frac{p-1}{2}} E_{p-1}|V(p). \end{aligned} \tag{2.10}$$

This is clear for $p = 3$ by definition. In particular $\mathcal{E}_p(z) \equiv E_{p-1}(z) \pmod{p}$, but $E_{p-1}(z) \equiv 1 \pmod{p}$ since the von Staudt-Clausen congruences imply that $B_{p-1}^{-1} \equiv 0 \pmod{p}$. This gives (2.8).

By (2.10), we have

$$\begin{aligned}\mathcal{E}_p|_{p-1}W(p) &= E_{p-1}|_{p-1}W(p) - p^{\frac{p-1}{2}}E_{p-1}\\ &= p^{\frac{p-1}{2}}(E_{p-1}|V(p) - E_{p-1}).\end{aligned}$$

This formula together with (2.5) and the von Staudt-Clausen congruences implies (2.9).

□

If M and N are relatively prime positive integers, we define the trace operator

$$\mathrm{Tr}_N^{MN} : M_k(\Gamma_0(MN)) \to M_k(\Gamma_0(N))$$

by

$$\mathrm{Tr}_N^{MN}(f) = \sum_{i=1}^{r} f|_k\gamma_i, \tag{2.11}$$

where $\{\gamma_1, \dots, \gamma_r\}$ is a complete set of coset representatives for $\Gamma_0(NM)\backslash\Gamma_0(N)$. Obviously, these trace operators have the property that they take cusp forms to cusp forms. The next lemma provides a closed formula for these operators.

Lemma 2.2. *Suppose that p is an odd prime and that $p \nmid N$. If $f \in M_k(\Gamma_0(Np))$, then*

$$\mathrm{Tr}_N^{Np}(f) = f + p^{1-k/2}f|_kW(p)U(p).$$

Proof. A complete set of representatives for $\Gamma_0(Np)\backslash\Gamma_0(N)$ is given by the matrices

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

However,

$$\begin{pmatrix}1 & 0\\ N & 1\end{pmatrix}\begin{pmatrix}1 & j\\ 0 & 1\end{pmatrix} = \begin{pmatrix}\frac{1}{p} & 0\\ 0 & \frac{1}{p}\end{pmatrix}\begin{pmatrix}p & a\\ Np & pb\end{pmatrix}\begin{pmatrix}1 & j-a\\ 0 & p\end{pmatrix},$$

where $\begin{pmatrix}p & a\\ Np & pb\end{pmatrix}$ is the matrix for $W(p)$. Since scalar matrices act trivially on $M_k(\Gamma_0(Np))$,

$$\mathrm{Tr}_N^{MN}(f) = f + \sum_{j=1}^{p-1} f|_kW(p)\begin{pmatrix}1 & j\\ 0 & p\end{pmatrix}.$$

A simple calculation shows that, for $g \in M_k(\Gamma_0(Np))$,

$$\sum_{j=0}^{p-1} g\left(\frac{z+j}{p}\right) = p(g|U(p))(z).$$

This proves the assertion.

□

Theorem 2.3. *Suppose that p is an odd prime and that*

$$f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{2k}^{\text{new}}(\Gamma_0(Np))$$

is an even integer weight newform. If N is coprime to p and j is a non-negative integer for which $M := \min(j+1, p^j - k + 1)$ is positive, then there is a cusp form

$$F(z) = \sum_{n=1}^{\infty} A(n)q^n \in S_{2(k+\kappa(p,j))}(\Gamma_0(N))$$

which satisfies the congruence

$$f(z) \equiv F(z) \pmod{p^M}.$$

Theorem 2.3 is a straightforward generalization of work of Serre in the $N = 1$ case [§3, 30].

Proof. For a power series $P(z) = \sum c(n)q^n$, we define

$$\nu_p(P) := \inf\{\text{ord}_p(c(n))\}, \tag{2.13}$$

where ord_p is the standard p-adic valuation. If L is a number field and O_L is its ring of integers, we take ord_p to mean $\text{ord}_{\mathfrak{p}}$ for any prime ideal $\mathfrak{p}$ above p suitably normalized so that $\text{ord}_p(p) = \text{ord}_{\mathfrak{p}}(p) = 1$.

Define the cusp form $f_j(z) \in S_{2(k+\kappa(p,j))}(\Gamma_0(Np))$ by

$$f_j(z) := f(z)\mathcal{E}_p(z)^{p^j}. \tag{2.14}$$

By Lemma 2.2, we have

$$\begin{aligned} \text{Tr}_N^{Np}(f_j) &= f_j + p^{1-k-\kappa(p,j)} f_j|_{2(k+\kappa(p,j))}\ W(p)U(p) \\ &= f_j + p^{1-k-\kappa(p,j)} \left((f|_{2k}\ W(p)) \left(\mathcal{E}_p|_{2\kappa(p,0)} W(p)\right)^{p^j} \right)\ |\ U(p). \end{aligned} \tag{2.15}$$

Since f is a newform, [Th.3, 3] implies that there an eigenvalue $w_p \in \{\pm 1\}$ of the Atkin-Lehner involution $W(p)$ for which

$$f|_{2k}W(p) = w_p f.$$

In particular it follows that $\nu_p\left(f|_{2k}W(p)\right) = 0$. Therefore by (2.9) it follows that

$$\nu_p\left(f|_{2k}W(p) \cdot \left(\mathcal{E}_p|_{2\kappa(p,0)}W(p)\right)^{p^j}\right) \geq p^j(\kappa(p,0)+1) = \kappa(p,j) + p^j.$$

Therefore by (2.15), we have

$$\nu_p\left(\text{Tr}_N^{Np}(f_j) - f_j\right) \geq p^j - k + 1.$$

Since $f_j \equiv f \pmod{p^{j+1}}$, this completes the proof.

□

3. p-adic properties of Kohnen newforms.

Here we obtain a result which is analogous to Theorem 2.3, but we need, first, to discuss the work of Kohnen on newforms of half-integral weight. For a general reference on half-integral weight modular forms, see [22]. Shimura [31] defines a correspondence between certain integral weight and half-integral weight modular forms. This correspondence commutes with the respective actions of the Hecke algebras. However, it is not, in general, an isomorphism. Kohnen [23] clarified this problem by defining suitable subspaces of cusp forms for which the Shimura correspondence is an isomorphism of Hecke modules.

Suppose that N is a positive odd square-free integer, and that k is a positive integer. Moreover, suppose that χ is a Dirichlet character modulo N and that $\varepsilon = \chi(-1)$. Kohnen [23] defines the space $S_k^+(\Gamma_0(4N), \chi)$ to be the space of cusp forms $g(z) = \sum_{n=1}^{\infty} b(n)q^n$ of weight $k + \frac{1}{2}$ and character $\left(\frac{4\varepsilon}{\cdot}\right)\chi$ on $\Gamma_0(4N)$ with the property that

$$b(n) = 0 \quad \text{whenever} \quad \varepsilon(-1)^k n \equiv 2, 3 \pmod 4. \tag{3.1}$$

In Kohnen's notation, this space is $S_k^+(N, \chi)$ (or simply $S_k(N, \chi)$). If χ is trivial, we suppress χ from the notation and refer to the space as $S_{k+\frac{1}{2}}^+(\Gamma_0(4N))$.

As in the integral weight case, $S_{k+\frac{1}{2}}^+(\Gamma_0(4N))$ decomposes into subspaces

$$S_{k+\frac{1}{2}}^+(\Gamma_0(4N)) = S_{k+\frac{1}{2}}^{\text{new}}(\Gamma_0(4N)) \oplus S_{k+\frac{1}{2}}^{\text{old}}(\Gamma_0(4N)). \tag{3.2}$$

As before, we can define Hecke operators on $S_{k+\frac{1}{2}}^+(\Gamma_0(4N))$. However, in this case, we have only the Hecke operators $T(n^2)$ for positive integers n. If $\ell \nmid 4N$ is prime, $T(\ell^2)$ acts on $g(z) = \sum b(n)q^n \in S_{k+\frac{1}{2}}^+(\Gamma_0(4N))$ by

$$g(z)|_k T(\ell^2) = \sum_{n=1}^{\infty} c(n)q^n,$$

where

$$c(n) = b(\ell^2 n) + \left(\frac{\varepsilon(-1)^k n}{\ell}\right)\ell^{k-1}b(n) + \ell^{2k-1}b\left(\frac{n}{\ell^2}\right).$$

As in the integer weight theory due to Atkin and Lehner, the spaces $S_{k+\frac{1}{2}}^{\text{new}}(\Gamma_0(4N))$ have bases of cusp forms which are eigenforms of the Atkin-Lehner involutions and the half-integral weight Hecke operators. By Kohnen's theory, there is a suitable linear combination of Shimura lifts under which the image of a half integral weight eigenform in $S_{k+\frac{1}{2}}^{\text{new}}(\Gamma_0(4N))$ is a newform in $S_{2k}^{\text{new}}(\Gamma_0(N))$. In fact, such a combination is an isomorphism between $S_{k+\frac{1}{2}}^{\text{new}}(\Gamma_0(4N))$ and $S_{2k}^{\text{new}}(\Gamma_0(N))$ as Hecke modules.

Unlike the integer weight case there is no canonical normalization of these eigenforms. For example, normalizing the first non-zero Fourier coefficient to be 1 may produce a form with non-integral coefficients. Nevertheless, by combining Kohnen's theory with a result of

Stevens [Prop. 2.3.1, 33], it follows that such a form can be normalized to have coefficients in O_K, the ring of algebraic integers in the number field K obtained by adjoining the coefficients of the integral weight newform that is its image under the Shimura correspondence. We refer to such forms as *Kohnen newforms*.

Now we recall the explicit operators we require to prove the main result of this section (i.e. Theorem 3.3). If k is a positive integer, then, following Kohnen, define the group

$$\widetilde{GL_2}^+(\mathbb{R})_k = \left\{ (\gamma, \phi) \mid \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2^+(\mathbb{R}) \text{ and } |\phi(z)| = (\det \gamma)^{-\frac{k}{2}-\frac{1}{4}} |cz+d|^{k+\frac{1}{2}} \right\}. \tag{3.3}$$

The functions ϕ above are holomorphic functions on $\mathfrak{h}$. This group acts on functions $f : \mathfrak{h} \to \mathbb{C}$ by the operator

$$\left(f|_{k+\frac{1}{2}}(\gamma, \phi) \right)(z) = \phi(z)^{-1} f(\gamma z). \tag{3.4}$$

For a prime divisor p of N such that $\gcd(p, 4N/p) = 1$, there is an operator $W(p)_k$ given by

$$W(p)_k = \left(\begin{pmatrix} p & a \\ 4N & pb \end{pmatrix}, \left(\frac{-4}{p} \right)^{-(k+\frac{1}{2})} p^{-\frac{1}{2}(k+\frac{1}{2})} (4Nz + pb)^{k+\frac{1}{2}} \right), \tag{3.5}$$

with $a, b \in \mathbb{Z}$ and determinant p. We note that $W(p)_k$ is unique up to left multiplication by an element of $\Gamma_0(4N)$ and therefore as an action on $M_{k+\frac{1}{2}}(\Gamma_0(4N))$. The map

$$W(p)_k : S^+_{k+\frac{1}{2}}(\Gamma_0(4N)) \to S^+_{k+\frac{1}{2}}\left(\Gamma_0(4N), \left(\frac{\cdot}{p} \right) \right) \tag{3.6}$$

is an isomorphism and $W(p)_k^2$ acts as the identity [p. 39, 23]. We will suppress k in this notation as it will be clear in context. If $p \mid N$, then the operator $U(p)$ defined by (1.8) also maps [Prop. 1.5, 31]

$$U(p) : S^+_{k+\frac{1}{2}}(\Gamma_0(4N)) \to S^+_{k+\frac{1}{2}}\left(\Gamma_0(4N), \left(\frac{\cdot}{p} \right) \right). \tag{3.7}$$

Therefore, for every prime $p \mid N$ this defines a Hermitian involution $\mathfrak{w}_p$ on $S^+_{k+\frac{1}{2}}(\Gamma_0(4N))$ given by

$$\mathfrak{w}_p = p^{-\frac{k}{2}+\frac{1}{4}} U(p) W(p). \tag{3.8}$$

By Shimura's correspondence and Kohnen's isomorphism, the ± 1-eigenspaces of $\mathfrak{w}_p$ correspond to the ± 1-eigenspaces under the $W(p)$ operator on $S_{2k}^{\text{new}}(\Gamma_0(N))$ [Prop. 4, 23].

Suppose that k is a positive integer. If p is an odd prime, and χ_p denotes the Legendre symbol modulo p, then there is an Eisenstein series $E_{k,\chi_p}(z) \in M_k(\Gamma_0(p), \chi_p)$, whose Fourier expansion is given by

$$E_{k,\chi_p}(z) = 1 - \frac{2k}{B_{k,\chi_p}} \sum_{n=1}^{\infty} \sigma_{k-1}(n, \chi_p) q^n, \tag{3.9}$$

where B_{k,χ_p} is a generalized Bernoulli number and $\sigma_k(n,\chi_p) = \sum_{d|n}\chi_p(d)d^k$. It is well known that $E_{k,\chi_p}(z)$ is the weight k Eisenstein series which is 1 at infinity and vanishes at the cusp 0. The complementary Eisenstein series which vanishes at ∞ and is non-zero at 0 is (see [§5.1, 17])

$$\left(E_{k,\chi_p}|_k W(p)\right)(z) = -\chi_p(-1)p^{\frac{k}{2}-1}\mathfrak{g}(\chi_p)\frac{2k}{B_{k,\chi_p}}\sum_{n=1}^{\infty}\sigma'_{k-1}(n,\chi_p)q^n, \tag{3.10}$$

where $\mathfrak{g}(\chi_p) = \sum_{a \pmod p}\chi_p(a)e^{\frac{2\pi i a}{p}}$ is the Gauss sum and $\sigma'_k(n,\chi_p) = \sum_{d|n}\chi_p(d)\left(\frac{n}{d}\right)^k$. If p is an odd prime, then define $\tilde{\mathcal{E}}_p(z) \in M_{\kappa(p,0)}(\Gamma_0(p),\chi_p)$ by

$$\tilde{\mathcal{E}}_p(z) = E_{\frac{p-1}{2},\chi_p}(z). \tag{3.11}$$

Lemma 3.1. *If p is an odd prime, then we have*

$$\tilde{\mathcal{E}}_p(z) \equiv 1 \pmod p, \tag{3.12}$$

$$\left(\tilde{\mathcal{E}}_p|_{\frac{p-1}{2}}W(p)\right)(z) \equiv 0 \pmod{p^{(\kappa(p,0)+1)/2}}. \tag{3.13}$$

Proof. Property (3.12) follows from the von Staudt-Clausen congruences; in this case, the generalized Bernoulli number

$$\left(B_{\frac{p-1}{2},\left(\frac{\cdot}{p}\right)}\right)^{-1} \equiv 0 \pmod p. \tag{3.14}$$

This congruence, combined with (3.10), and the fact that [p. 75, 19]

$$\mathfrak{g}(\chi_p) = \sqrt{\left(\frac{-1}{p}\right)p}$$

gives (3.13).

□

In light of (3.13), we will write

$$\left(\tilde{\mathcal{E}}_p|_{\frac{p-1}{2}}W(p)\right)(z) = p^{(\kappa(p,0)+1)/2}\tilde{\mathcal{E}}'_p(z), \tag{3.15}$$

where $\tilde{\mathcal{E}}'_p(z)$ is clear from (3.10).

As in the last section, if M and N are relatively prime positive integers, we define the trace operator

$$\mathrm{Tr}_{4N}^{4MN} : M_{k+\frac{1}{2}}(\Gamma_0(4MN)) \to M_{k+\frac{1}{2}}(\Gamma_0(4N))$$

by

$$\mathrm{Tr}_{4N}^{4MN}(f) = \sum_{i=1}^{r} f|_{k+\frac{1}{2}}\gamma_i, \tag{3.16}$$

where $\{\gamma_1,\ldots,\gamma_r\}$ is a complete set of coset representatives for $\Gamma_0(4NM)\backslash\Gamma_0(4N)$. Clearly, the trace operator sends cusp forms to cusp forms. The following lemma shows that it preserves the +-space, while providing a closed formula for these traces. Its proof is analogous to the proof of Lemma 2.2, and so we omit it for brevity (note: this calculation may also be found on [p. 67, 23]).

Lemma 3.2. *If p is an odd prime and N is an odd square-free integer such that $p \nmid N$, then, for $f \in M_{k+\frac{1}{2}}(\Gamma_0(Np))$,*

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

Theorem 3.3. *Suppose that Np is an odd square-free integer, where p is an odd prime, and that*

$$g(z) = \sum_{n=1}^{\infty} b(n)q^n \in S_{k+\frac{1}{2}}^{\mathrm{new}}(\Gamma_0(4Np))$$

is a Kohnen newform. If j is a non-negative integer for which

$$M = \min\left(j - k + 2, \frac{p^j+3}{2} - k\right)$$

is positive, then there is a cusp form $G(z) = \sum_{n=1}^{\infty} B(n)q^n \in S_{k+\kappa(p,j)+\frac{1}{2}}^{+}(\Gamma_0(4N))$ with p-integral coefficients which satisfies the congruence

$$g(z) \equiv G(z) \mid U(p) \pmod{p^M}.$$

Proof. Mimicking the proof of Theorem 2.3, we let

$$g_j(z) = (g(z)|U(p)) \cdot \tilde{\mathcal{E}}_p(4z)^{p^j} \in S_{k+\kappa(p,j)+\frac{1}{2}}^{+}(\Gamma_0(4Np)). \tag{3.17}$$

In this case, we take the trace of $g_j|U(p) \in S_{k+\kappa(p,j)+\frac{1}{2}}^{+}(\Gamma_0(4Np))$. We have, by Lemma 3.2,

$$\begin{aligned} &\mathrm{Tr}_{4N}^{4Np}(g_j) \\ &\quad = g_j + \left(\frac{-4}{p}\right)^{-k-\kappa(p,j)-\frac{1}{2}} p^{-(k+\kappa(p,j))/2+\frac{3}{4}} g_j|_{k+\kappa(p,j)+\frac{1}{2}} W(p)U(p). \end{aligned} \tag{3.18}$$

By Lemma 3.1, we have

$$\begin{aligned} g_j(z)|_{k+\kappa(p,j)+\frac{1}{2}} W(p)U(p) &= \left(\left(g(z)|_{k+\frac{1}{2}} U(p)W(p)\right)\left(\tilde{\mathcal{E}}_p^{p^j}(4z)|_{\kappa(p,j)} W(p)\right)\right)|U(p) \\ &= \left(p^{\frac{k}{2}-\frac{1}{4}}\left(g(z)|_{k+\frac{1}{2}} \mathfrak{w}_p\right) p^{(\kappa(p,j)+p^j)/2}\left(\tilde{\mathcal{E}}_p'(4z)^{p^j}\right)\right)|U(p) \\ &= w_p p^{\frac{k}{2}-\frac{1}{4}+\frac{\kappa(p,j)+p^j}{2}}\left(g(z)\tilde{\mathcal{E}}_p'(4z)\right)|U(p). \end{aligned}$$

where $w_p \in \{\pm 1\}$ is the eigenvalue of the Atkin-Lehner $\mathfrak{w}_p$ operator ([Th. 1, 23]). Moreover, by (3.10) $\tilde{\mathcal{E}}'_p(4z)$ has p-integral Fourier coefficients. Therefore, it turns out that

$$\begin{aligned}\nu_p\left(\mathrm{Tr}_{4N}^{4Np}(g_j) - g_j\right) &\geq \frac{k}{2} - \frac{1}{4} + \frac{\kappa(p,j) + p^j}{2} - \frac{(k + \kappa(p,j))}{2} + \frac{3}{4} \\ &\geq \frac{p^j + 1}{2}.\end{aligned}$$

By (3.12), $g_j(z) \equiv g(z)|U(p) \pmod{p^{j+1}}$; thus

$$\mathrm{Tr}_{4N}^{4Np}(g_j) \equiv g|U(p) \pmod{p^m},$$

where $m = \min\left(j+1, \frac{p^j+1}{2}\right)$. Since g is a newform [p. 64, 23],

$$g|U(p)U(p) = g|U(p^2) = -w_p p^{k-1} g. \tag{3.19}$$

Therefore,

$$-w_p p^{1-k} \mathrm{Tr}_{4N}^{4Np}(g_j)|U(p) \equiv g \pmod{p^M},$$

where

$$M = m - (k-1) = \min\left(j - k + 2, \frac{p^j + 3}{2} - k\right).$$

□

4. Proof of Theorems 1 and 2.

In this section we prove Theorems 1 and 2. We begin with the proof of Theorem 2 using Theorems 2.3 and 3.3.

Proof of Theorem 2. The hypotheses of Theorems 2.3 and 3.3 are satisfied when $j \geq k - \frac{3}{2}$, and so there are forms $F(z) \in S_{2(k+\kappa(p,j))}(\Gamma_0(N))$ and $G(z) \in S^+_{k+\kappa(p,j)+\frac{1}{2}}(\Gamma_0(4N))$ for which

$$\begin{aligned} f(z) &\equiv F(z) \pmod{p}, \\ g(z) &\equiv G(z) \mid U(p) \pmod{p}. \end{aligned}$$

By a famous lemma of Deligne and Serre [Lemma 6.11, 9], there is an eigenform in $O_K[[q]]$, say $\mathcal{F}(z)$ of weight $2(k+\kappa(p,j))$ (resp. $\mathcal{G}(z)$ of weight $k+\kappa(p,j)+\frac{1}{2}$), of the Hecke operators $T(\ell)$ (resp. $T(\ell^2)$) for primes $\ell \nmid Np$ with the same eigenvalues as $F(z)$ (resp. $G(z)$) modulo $\mathfrak{p}$.

If $\mathcal{F}(z) \in S^{\mathrm{new}}_{2(k+\kappa(p,j))}(\Gamma_0(4N))$ is a newform, then Kohnen's isomorphism implies that there is a normalization of the Kohnen newform $\mathcal{G}(z) \in S^{\mathrm{new}}_{k+\frac{1}{2}}(\Gamma_0(4N))$ corresponding to $\mathcal{F}(z)$ which satisfies the given congruence. Otherwise, there would be at least two newforms

of weight $2(k+\kappa(p,j))$ and level dividing N with the same Hecke eigenvalues modulo $\mathfrak{p}$ for the Hecke operators $T(\ell)$ for primes $\ell \nmid Np$.

□

We shall use Corollary 3 to prove Theorem 1. In addition, we shall require results giving a lower bound for the number of suitable quadratic twists of a fixed elliptic curve E with rank ≥ 2 over $\mathbb{Q}$. We also require the following result of Dummigan [Th. 8.1, 10] describing certain instances where elements of order p in the Selmer group of an elliptic curve can be used to produce elements in the Selmer group of a congruent motive.

Theorem. (Dummigan)
Let $E/\mathbb{Q}$ be an elliptic curve with prime conductor p for which $p \nmid \mathrm{ord}_p(j(E))$, and let $f(z) \in S_2(\Gamma_0(p))$ be its associated newform. Suppose there is an eigenform $\mathcal{F}(z) \in S_k(\Gamma_0(1))$ for which $k \equiv 2 \pmod{p-1}$, where $k-2$ is an odd multiple of $p-1$, with the property that

$$\mathcal{F}(z) \equiv f(z) \pmod{\mathfrak{p}}.$$

Here $\mathfrak{p}$ is a prime ideal above p in the number field obtained by adjoining the coefficients of the newforms in $S_2(\Gamma_0(p))$ and $S_k(\Gamma_0(1))$. If D is a negative fundamental discriminant for which the rank of $E(D)$ over $\mathbb{Q}$ is ≥ 2, then $S\left(M_{\mathcal{F}}^{(k/2,D(p))}\right)$ contains a subgroup isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Proof of Theorem 1. We are in the $N=1$, $k=1$ and $j=0$ case of Theorem 2. The hypothesis that p is not a congruence prime for the newforms in $S_{p+1}(\Gamma_0(1))$ together with the aforementioned lemma of Deligne and Serre [Lemma 6.11, 9] implies, for each prime ideal $\mathfrak{p}$ in O_K above p, that there is a unique newform $\mathcal{F}(z) \in S_{p+1}(\Gamma_0(1))$ for which

$$f(z) \equiv \mathcal{F}(z) \pmod{\mathfrak{p}}. \tag{4.1}$$

This proves claim (1).

If D' is a fundamental discriminant, then it is well known that the sign of the functional equation of $L(\mathcal{F}_{D'}, s)$ is $(-1)^{(p+1)/2}\chi_{D'}(-1) = (-1)^{(p+1)/2} \cdot \mathrm{sign}(D')$. If D is a negative fundamental discriminant coprime to p, then by (1.4) we have that $D(p)$ is positive if and only if $p \equiv 3 \pmod 4$. Therefore, it follows that the sign of the functional equation of $L(\mathcal{F}_{D(p)}, s)$ is $+1$ for every negative fundamental discriminant D. This is claim (2).

Let $g(z)$ and $\mathcal{G}(z)$ be the corresponding Kohnen newforms normalized so that there is a negative fundamental discriminant D_0 for which

$$0 \not\equiv b(|D_0|) \equiv B(|D_0(p)|) \pmod{\mathfrak{p}}.$$

Since the coefficients of $f(z)$ and $\mathcal{F}(z)$ are real, it follows that the coefficients of $g(z)$ and $\mathcal{G}(z)$ are real. Therefore, Corollary 3 allows us to conclude that if D is a negative fundamental discriminant with $\left(\frac{D}{p}\right) = w_p$, then

$$L_K^{\mathrm{alg}}(f_D, 1) \equiv L_K^{\mathrm{alg}}(\mathcal{F}_{D(p)}, (p+1)/2) \pmod{\mathfrak{p}}. \tag{4.2}$$

Therefore by (1.12) and (1.13), we find that if D is a negative fundamental discriminant with $\left(\frac{D}{p}\right) = w_p$, then

$$\begin{aligned}\frac{L(\mathcal{F}_{D(p)}, (p+1)/2) \cdot |D(p)|^{p/2}}{L(\mathcal{F}_{D_0(p)}, (p+1)/2) \cdot |D_0(p)|^{p/2}} &= \frac{L_K^{\mathrm{alg}}(\mathcal{F}_{D(p)}, (p+1)/2)}{L_K^{\mathrm{alg}}(\mathcal{F}_{D_0(p)}, (p+1)/2)} \\ &= \frac{B(|D(p)|)^2}{B(|D_0(p)|)^2} \equiv \frac{b(|D|)^2}{b(|D_0|)^2} \pmod{\mathfrak{p}} \\ &= \frac{L(f_D, 1)|D|^{1/2}}{L(f_{D_0}, 1)|D_0|^{1/2}}. \end{aligned} \tag{4.3}$$

A standard calculation (see [§6, 8], [10]) reveals that the quotients

$$\frac{\Omega(\mathcal{F}_{D(p)}, (p+1)/2)}{\Omega(\mathcal{F}_{D_0(p)}, (p+1)/2)} \quad \text{and} \quad \frac{\Omega(f_D, 1)}{\Omega(f_{D_0}, 1)}$$

are both coprime to $\mathfrak{p}$. Therefore the expression in (4.3) agrees with $\mathbb{L}^{\mathrm{alg}}(\mathcal{F}_{D(p)}, (p+1)/2) \pmod{\mathfrak{p}}$ up to a $\mathfrak{p}$-unit. Therefore we have

$$\mathbb{L}^{\mathrm{alg}}(\mathcal{F}_{D(p)}, (p+1)/2) \equiv 0 \pmod{\mathfrak{p}} \iff \mathbb{L}^{\mathrm{alg}}(f_D, 1) \equiv 0 \pmod{\mathfrak{p}}. \tag{4.4}$$

This proves (3).

Now suppose that D is a negative fundamental discriminant for which both $\left(\frac{D}{p}\right) = w_p$ and $E(D)$ has rank ≥ 2 over $\mathbb{Q}$. By Dummigan's Theorem, we have that

$$S\left(M_{\mathcal{F}}^{((p+1)/2, D(p))}\right)[p] \neq \{0\}.$$

Stewart and Top, generalizing a famous paper of Gouvêa and Mazur [13], [34] showed that the number of such $D \gg_E \frac{X^{1/7}}{(\log X)^2}$. Moreover for these D, Kolyvagin's famous theorem on the Birch and Swinnerton-Dyer Conjecture implies that $L(f_D, 1) = 0$, and so $b(|D|) = 0$. Therefore by (4.4), we have

$$\mathbb{L}^{\mathrm{alg}}(\mathcal{F}_{D(p)}, (p+1)/2) \equiv 0 \pmod{\mathfrak{p}}.$$

This proves (4).

□

References

1. A. Agashe and W. Stein, *Visible elements for the Birch and Swinnerton-Dyer Conjecture for rank 0 modular abelian varieties*, to appear, Math. Comp.
2. A. Agashe and W. Stein, *Visibility of Shafarevich-Tate groups of abelian varieties*, to appear, J. Number Th.

3. A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134-160.
4. S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, vol. 1, Prog. in Math., Birkhäuser, Boston (1990), 333-400.
5. J. B. Conrey, J. P. Keating, M. O. Rubinstein, N. C. Snaith, *On the frequency of vanishing of quadratic twists of modular L-functions*, preprint.
6. J. E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experiment. Math. **9** (2000), 13-28.
7. P. Deligne, *Formes modulaires et représentations* ℓ*-adiques*, Sém. Bourbaki, éxp. 355, Springer Lect. Notes Math. **179** (1969), 139-172.
8. P. Deligne, *Valeurs de fonctions L et périodes d'intégrales*, AMS Proc. Sympos. Pure Math. **33** (1979), 313-346.
9. P. Deligne and J.-P. Serre, *Formes modulaires de poids 1*, Ann. Sci. École Norm. Sup. **7** (1974), 507-530.
10. N. Dummigan, *Congruences of modular forms and Selmer groups*, Math. Res. Letters **8** (2001), 479-494.
11. N. Dummigan, W. Stein and M. Watkins, *Constructing elements in Shafarevich-Tate groups of modular motives*, preprint.
12. J.-M. Fontaine, *Valeurs spéciales des fonctions L des motifs*, Séminaire Bourbaki, Astérisque No. 751 **206** (1992), 205-249.
13. F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), 1-23.
14. P. Guerzhoy, *On a conjecture of Kohnen*, Math. Ann. **319** (2001), 65-73.
15. E. Hecke, *Mathematische Werke*, Vandenhoeck und Ruprecht, Göttingen, 1959.
16. H. Hida, *Galois representations into* $GL_2(\mathbb{Z}_p[[X]])$ *attached to ordinary cusp forms*, Invent. Math. **85** (1986), 545-613.
17. H. Hida, *Elementary theory of L-functions and Eisenstein series*, Cambridge Univ. Press, Cambridge, 1993.
18. H. Hida, *On* Λ*-adic forms of half integral weight for* $SL(2)(\mathbb{Q})$, Number Theory (Paris, 1992-1993), Lond Math. Soc. Lect. Note Ser., Cambridge Univ. Press **215** (1995), 139-166.
19. K. Ireland and M. Rosen, *A classical introduction to modern number theory, 2nd edition*, Springer-Verlag, New York 1990.
20. K. James and K. Ono, *Selmer groups of quadratic twists of elliptic curves*, Math. Ann. **314** (1999), 1-17.
21. N. Koblitz, *p-adic congruences and modular forms of half integer weight*, Math. Ann. **274** (1986), 199-220.
22. N. Koblitz, *Introduction to elliptic curves and modular forms*, Springer Verlag, New York, 1984.
23. W. Kohnen, *Newforms of half-integral weight*, J. Reine Angew. Math. **333** (1982), 32-72.
24. W. Kohnen, *Fourier coefficients of modular forms of half-integral weight*, Math. Ann. **271** (1985), 237-268.
25. W. Kohnen and D. Zagier, *Values of L-series of modular forms at the center of the critical strip*, Invent. Math. **64** (1981), 173-198.
26. B. Mazur, *On the arithmetic of special values of L-functions*, Invent. Math. **55** (1979), 207-240.
27. B. Mazur, *Visualizing elements of order three in the Shafarevich-Tate group*, Asian J. Math. **3** (1999), 221-232.
28. T. Miyake, *Modular forms*, Springer Verlag, New York, 1989.
29. A. J. Scholl, *Motives for modular forms*, Invent. Math. **100** (1990), 419-430.
30. J.-P. Serre, *Formes modulaires et fonctions zêta p-adiques*, Springer Lect. Notes in Math. **350** (1973), 191-268.
31. G. Shimura, *On modular forms of half-integral weight*, Ann. Math. **97** (1973), 440-481.
32. A. Sofer, *p-adic interpolation of square roots of central values of Hecke L-functions*, Duke Math. J. **83** (1996), 51-78.

33. G. Stevens, Λ-*adic modular forms of half-integral weight and a* Λ-*adic Shintani lifting*, Arith. Geometry (Tempe, Az. 1993) Contemp. Math., Amer. Math. Soc. **174** (1994), 129-151.
34. C. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. **8** (1995), 943-973.
35. V. Vatsal, *Canonical periods and congruence formulae*, Duke Math. J. **98** (1999), 397-419.
36. J.-L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures et Appl. **60** (1981), 375-484.

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: mcgraw@math.wisc.edu

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: ono@math.wisc.edu