LIFTING CONGRUENCES TO WEIGHT 3/2

NEIL DUMMIGAN AND SRILAKSHMI KRISHNAMOORTHY

Abstract. Given a congruence of Hecke eigenvalues between newforms of weight 2, we prove, under certain conditions, a congruence between corresponding weight-3/2 forms.

1. Introduction

Let $f = \sum_{n=0}^{\infty} a_n(f)q^n$ and $g = \sum_{n=1}^{\infty} a_n(g)q^n$ be normalised newforms of weight 2 for $\Gamma_0(N)$, where $N$ is square-free. For each prime $p | N$, let $w_p(f)$ and $w_p(g)$ be the eigenvalues of the Atkin-Lehner involution $W_p$ acting on $f$ and $g$, respectively. Write $N = DM$, where $w_p(f) = w_p(g) = -1$ for primes $p | D$ and $w_p(f) = w_p(g) = 1$ for primes $p | M$. We suppose that the number of primes dividing $D$ is odd. (In particular, the signs in the functional equations of $L(f,s)$ and $L(g,s)$ are both $+1$.)

Let $B$ be the quaternion algebra over $\mathbb{Q}$ ramified at $\infty$ and at the primes dividing $D$, with canonical anti-involution $x \mapsto \overline{x}$, $\text{tr}(x) := x + \overline{x}$ and $\text{Nm}(x) := x\overline{x}$. Let $\hat{R}$ be a fixed Eichler order of level $N$ in a maximal order of $B$. Let $\phi_f, \phi_g$ (determined up to non-zero scalars) be $(\mathbb{C}\text{-valued})$ functions on the finite set $B^\times(Q) \backslash B^\times(\mathbb{A}_{f}) / \hat{R}$ corresponding to $f$ and $g$ via the Jacquet-Langlands correspondence, where $\mathbb{A}_f$ is the “finite” part of the adele ring of $Q$ and $\hat{R} = R \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}$. Let $\{y_i\}_{i=1}^h$ be a set of representatives in $B^\times(\mathbb{A}_f)$ of $B^\times(Q) \backslash B^\times(\mathbb{A}_f) / \hat{R}$, $R_i := B^\times(Q) \cap (y_i\hat{R}y_i^{-1})$ and $w_i := |R_i^\times|$. Let $L_i := \{x \in \mathbb{Z} + 2R_i : \text{tr}(x) = 0\}$, and $\theta_i := \sum_{x \in L_i} q^{\text{Nm}(x)}$, where $q = e^{2\pi i z}$, for $z$ in the complex upper half-plane. For $\phi = \phi_f$ or $\phi_g$, let

$$W(\phi) := \sum_{i=1}^h \phi(y_i)\theta_i.$$ 

This is Waldspurger’s theta-lift [Wa1], and the Shimura correspondence [Sh] takes $W(\phi_f)$ and $W(\phi_g)$, which are cusp forms of weight 3/2 for $\Gamma_0(4N)$, to $f$ and $g$, respectively (if $W(\phi_f)$ and $W(\phi_g)$ are non-zero). In the case that $N$ is odd (and square-free), $W(\phi_f)$ and $W(\phi_g)$ are, if non-zero, the unique (up to scaling) elements of Kohnen’s space $S^+_{3/2}(\Gamma_0(4N))$ mapping to $f$ and $g$ under the Shimura correspondence [K]. Still in the case that $N$ is odd, $W(\phi_f) \neq 0$ if and only if $L(f,1) \neq 0$, by a theorem of Böcherer and Schulze-Pillot [BS1, Corollary, p.379], proved by Gross in the case that $N$ is prime [G1, §13].

Böcherer and Schulze-Pillot’s version of Waldspurger’s Theorem [Wa2],[BS2, Theorem 3.2] is that for any fundamental discriminant $-d < 0$,

$$\sqrt{d} \left( \prod_{p | d, \text{prime}} \left( 1 + \left( \frac{-d}{p} \right) w_p(f) \right) \right) L(f,1)L(f,\chi_{-d},1) = \frac{4\pi^2 \langle f, f \rangle}{\langle \phi_f, \phi_f \rangle} (a(W(\phi_f),d))^2,$$

Date: November 8th, 2016.
and similarly for $g$, where $W(\phi_f) = \sum_{n=1}^{\infty} a(W(\phi_f), n)q^n$, $\langle f, f \rangle$ is the Petersson norm and $\langle \phi_f, \phi_f \rangle = \sum_{i=1}^{h} w_i|\phi_f(y_i)|^2$. (They scale $\phi_f$ in such a way that $\langle \phi_f, \phi_f \rangle = 1$, so it does not appear in their formula.)

The main goal of this paper is to prove the following.

**Theorem 1.1.** Let $f, g, W(\phi_f), W(\phi_g)$, $N = DM$ be as above (with $N$ square-free but not necessarily odd). Suppose now that $D = q$ is prime. Let $\ell$ be a prime such that $\ell \mid 2M(q - 1)$. Suppose that, for some unramified divisor $\lambda \mid \ell$ in a sufficiently large number field,

$$a_p(f) \equiv a_p(g) \pmod{\lambda} \forall \text{ primes } p,$$

and that the residual Galois representation $\overline{\rho}_{f, \lambda} : \text{Gal}(\overline{Q}/Q) \to \text{GL}_2(\mathbb{F}_\lambda)$ is irreducible. Then (with a suitable choice of scaling, such that $\phi_f$ and $\phi_g$ are integral but not divisible by $\lambda$)

$$a(W(\phi_f), n) \equiv a(W(\phi_g), n) \pmod{\lambda} \forall n.$$

**Remarks.**

(1) Note that $a(W(\phi_f), d) = 0$ unless $\left( \frac{d}{p} \right) = w_p(f)$ for all primes $p \mid \gcd(N, W(d))$; in fact this is implied by the above formula. When $N$ is odd and square-free, for each subset $S$ of the set of primes dividing $N$, Baruch and Mao [BM, Theorem 10.1] provide a weight-3/2 form satisfying a similar relation, for discriminants such that $\left( \frac{d}{p} \right) = -w_p(f)$ precisely for $p \in S$, and of sign determined by the parity of $\#S$, the above being the case $S = \emptyset$. One might ask whether one can prove similar congruences for these forms in place of $W(\phi_f)$ and $W(\phi_g)$. In the case that $N$ is prime, one sees in [MRT] how to express the form for $S = \{N\}$ as a linear combination of generalised ternary theta series, with coefficients in the linear combination coming from values of $\phi$, so the same proof (based on a congruence between $\phi_f$ and $\phi_g$) should work. Moreover, the examples in [PT], with similar linear combinations of generalised ternary theta series in cases where $N$ is not even square-free, suggest that something much more general may be possible.

(2) Though $\phi_f$ and $\phi_g$ are not divisible by $\lambda$, we can still imagine that $W(\phi_f) = \sum_{i=1}^{h} \phi_f(y_i)\theta_i$ and $W(\phi_g) = \sum_{i=1}^{h} \phi_g(y_i)\theta_i$ could have all their Fourier coefficients divisible by $\lambda$, so the congruence could be just $0 \equiv 0 \pmod{\lambda}$ for all $n$. However, unless $W(\phi_f) = W(\phi_g) = 0$, this kind of mod $\ell$ linear independence of the $\theta_i$ seems unlikely, and one might guess that it never happens. This seems related to a conjecture of Kolyvagin, about non-divisibility of orders of Shafarevich-Tate groups of quadratic twists, discussed by Prasanna [P].

(3) The discussion in [P, §§5.2, 5.3] is also relevant to the subject of this paper. In particular, our congruence may be viewed as a square root of a congruence between algebraic parts of $L$-values. Such congruences may be proved in greater generality, as in [V, Theorem 0.2], but do not imply ours, since square roots are determined only up to sign. The idea for Theorem 1.1 came in fact from work of Quattrini [Q, §5], who proved something similar for congruences between cusp forms and Eisenstein series at prime level, using results of Mazur [M] and Emerton [Em] on the Eisenstein ideal. See Theorem 3.6, and the discussion following Proposition 3.3, in [Q].
Here we are looking at congruences between modular forms of the same weight (i.e. 2), and how to transfer them to half-integral weight. For work on the analogous question for congruences between forms of different weights, see [D] (which uses work of Stevens [Ste] to go beyond special cases), and [MO, Theorem 1.4] for a different approach by McGraw and Ono.

We could have got away with assuming the congruence only for all but finitely many $p$. The Hecke eigenvalue $a_p(f)$, for a prime $p 
mid N\ell$, is the trace of $\rho_{f,\lambda}(\text{Frob}_{p^{-1}})$, where $\rho_{f,\lambda} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(K_\lambda)$ is the $\lambda$-adic Galois representation attached to $f$ and $\text{Frob}_p \in \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q})$ lifts the automorphism $x \mapsto x^p$ in $\text{Gal}(\mathbb{F}_p/\mathbb{F}_q)$. Since the $\text{Frob}_{p^{-1}}$ topologically generate $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the congruence for almost all $p$ implies an isomorphism of residual representations $\overline{\rho}_{f,\lambda}$ and $\overline{\rho}_{g,\lambda}$, hence the congruence at least for all $p \nmid N\ell$. For $p \mid N$, $a_p(f)$ can again be recovered from $\rho_{f,\lambda}$, this time as the scalar by which $\text{Frob}_{p^{-1}}$ acts on the unramified quotient of the restriction to $\text{Gal}(\overline{\mathbb{Q}}_p/Q_p)$, by a theorem of Deligne and Langlands [L]. For $p = \ell$ this also applies in the ordinary case, by a theorem of Deligne [Ed, Theorem 2.5], and in the supersingular case $a_{\ell}(f) \equiv a_{\ell}(g) \equiv 0 \pmod{\lambda}$. Since $\overline{\rho}_{f,\lambda} \simeq \overline{\rho}_{g,\lambda}$, it follows that $a_p(f) \equiv a_p(g) \pmod{\lambda}$ even for $p \mid N\ell$. Since $w_p = -a_p$ for $p \mid N$ and $\ell$ is odd, we find that if we didn't impose the condition that $w_p(f) = w_p(g)$ for all $p \mid N$, it would follow anyway. But note that we have actually imposed a stronger condition, not just that $w_p(f)$ and $w_p(g)$ are equal, but that they equal $-1$ for $p = q$ and $+1$ for $p \mid M$. (In the kind of generalisation envisaged in Remark (1), presumably this condition would be removed.)

The formula for $W(\phi)$ used by Böcherer and Schulze-Pillot has coefficient of $\theta_i$ equal to $\phi(y_i)/w_i$ rather than just $\phi(y_i)$, and their $\langle \phi, \phi \rangle$ has $w_i$ in the denominator (as in [G2, (6.2)]) rather than in the numerator. This is because our $\phi(y_i)$ is the same as their $\phi(y_i)/w_i$. Their $\phi$ is an eigenvector for standard Hecke operators $T_p$ defined using right translation by double cosets (as in [G2, (6.6)]), which are represented by Brandt matrices, and are self-adjoint for their inner product. The Hecke operators we use below are represented by the transposes of Brandt matrices (as in [G2, Proposition 4.4]), and are self-adjoint for the inner product we use here (see the final remark). This accounts for the adjustment in the eigenvectors.

2. Modular curves and the Jacquet-Langlands correspondence

In this section we work in greater generality than in the statement of Theorem 1.1. First we briefly collect some facts explained in greater detail in [R]. Let $N$ be any positive integer of the form $N = qM$, not necessarily square-free, but with $q$ prime and $(q, M) = 1$. Since $q \mid N$ but $q \nmid M$, the prime $q$ is of bad reduction for the modular curve $X_0(N)$, but good reduction for $X_0(M)$. There exists a regular model over $\mathbb{Z}_q$ of the modular curve $X_0(N)$, whose special fibre (referred to here as $X_0(N)/\mathbb{F}_q$) is two copies of the nonsingular curve $X_0(M)/\mathbb{F}_q$, crossing at points representing supersingular elliptic curves with cyclic subgroups of order $M$ (“enhanced” supersingular elliptic curves in the language of Ribet). For $\Gamma_0(N)$-level structure, each point of $X_0(N)/\mathbb{F}_q$ must also come with a cyclic subgroup scheme.
of order $q$. On one copy of $X_0(M)/\mathbb{F}_q$ this is $\ker F$, on the other it is $\ker V$ ($F$ and $V$ being the Frobenius isogeny and its dual), and at supersingular points $\ker F$ and $\ker V$ coincide. This finite set of supersingular points is naturally in bijection with $B^\times(\mathbb{Q}) \backslash B^\times(\mathbb{A}_f) / \hat{R}$, where $B$ is the quaternion algebra over $\mathbb{Q}$ ramified at $q$ and $\infty$ and $\hat{R}$ is an Eichler order of level $N$. If, as above, $(y_i)_{i=1}^n$ is a set of representatives in $B^\times(\mathbb{A}_f)$ of $B^\times(\mathbb{Q}) \backslash B^\times(\mathbb{A}_f) / \hat{R}$, then the bijection is such that $y_i$ corresponds to an enhanced supersingular elliptic curve with endomorphism ring $R_i$ (i.e. endomorphisms of the curve preserving the given cyclic subgroup of order $M$).

The Jacobian $J_0(N)/\mathbb{Q}_q$ of $X_0(N)/\mathbb{Q}_q$ has a Néron model, a certain group scheme over $\mathbb{Z}_p$. The connected component of the identity in its special fibre has an abelian variety quotient $(J_0(M)/\mathbb{F}_q)^2$, the projection maps to the two factors corresponding to pullback of divisor classes via the two inclusions of $X_0(M)/\mathbb{F}_q$ in $X_0(N)/\mathbb{F}_q$.

The kernel of the projection to $(J_0(M)/\mathbb{F}_q)^2$ is the toric part $T$, which is connected with the intersection points of the two copies of $X_0(M)$. To be precise, the character group $X := \text{Hom}(T, G_m)$ is naturally identified with the set of divisors of degree zero (i.e. $\mathbb{Z}$-valued functions summing to 0) on this finite set, hence on $B^\times(\mathbb{Q}) \backslash B^\times(\mathbb{A}_f) / \hat{R}$.

Let $\mathbb{T}$ be the $\mathbb{Z}$-algebra generated by the linear operators $T_p$ (for primes $p \nmid N$) and $U_p$ (for primes $p \mid N$) on the $q$-new subspace $S_2(\Gamma_0(N))^{q,\text{new}}$ (the orthogonal complement of the subspace of those old forms coming from $S_2(\Gamma_0(M))$). Let $f$ be a Hecke eigenform in $S_2(\Gamma_0(N))^{q,\text{new}}$, and let $K$ be a number field sufficiently large to accommodate all the Hecke eigenvalues $a_p(f)$. The homomorphism $\phi_f : \mathbb{T} \rightarrow K$ such that $T_p \mapsto a_p(f)$ and $U_p \mapsto a_p(f)$ has kernel $\mathfrak{p}_f$, say. Let $\lambda$ be a prime ideal of $O_K$, dividing a rational prime $\ell$. The homomorphism $\overline{\phi}_f : \mathbb{T} \rightarrow F_{\lambda} := O_K/\lambda$ such that $\overline{\phi}_f(t) = \overline{\phi}_f(t)$ for all $t \in \mathbb{T}$, has a kernel $\mathfrak{m}$ which is a maximal ideal of $\mathbb{T}$, containing $\mathfrak{p}_f$, with $k_m := \mathbb{T}/\mathfrak{m} \subseteq F_\lambda$.

The abelian variety quotient $(J_0(M)/\mathbb{F}_q)^2$ is connected with $q$-old forms, while the toric part $T$ is connected with $q$-new forms. In fact, by [R, Theorem 3.10], $\mathbb{T}$ may be viewed as a ring of endomorphisms of $T$, hence of $X$. We may find an eigenvector $\phi_f$ in $X \otimes \mathbb{K}$ (a $K$-valued function on $B^\times(\mathbb{Q}) \backslash B^\times(\mathbb{A}_f) / \hat{R}$, on which $T$ acts through $\mathbb{T}/\mathfrak{p}_f$. We may extend coefficients to $\mathbb{Q}_p$, and scale $\phi_f$ to lie in $X \otimes O_\lambda$ but not in $\lambda(X \otimes O_\lambda)$. This association $f \mapsto \phi_f$ gives a geometrical realisation of the Jacquet-Langlands correspondence.

3. A CONGRUENCE BETWEEN $\phi_f$ AND $\phi_g$

Again, in this section we work in greater generality than in the statement of Theorem 1.1.

Lemma 3.1. Let $N = qM$ with $q$ prime and $(q, M) = 1$. Let $f, g \in S_2(\Gamma_0(N))^{q,\text{new}}$ be Hecke eigenforms. Let $K$ be a number field sufficiently large to accommodate all the Hecke eigenvalues $a_p(f)$ and $a_p(g)$, and $\lambda \mid \ell$ a prime divisor in $O_K$ such that $a_p(f) \equiv a_p(g) \pmod{\lambda}$ for all primes $p$. Let $\phi_f$ be as in the previous section, and define $\phi_g$ similarly. If $\mathfrak{p}_{f,\lambda}$ is irreducible and $\ell \nmid 2M(q-1)$ then, with suitable choice of scaling, we have $\phi_f \equiv \phi_g \pmod{\lambda}$.

Proof. In the notation of the previous section, we can define $\theta_g$ just like $\theta_f$, and the congruence implies that we have a single maximal ideal $\mathfrak{m}$ for both $f$ and $g$. By [R, Theorem 6.4] (which uses the conditions that $\mathfrak{p}_{f,\lambda}$ is irreducible and that
\( \ell + 2N(q - 1) \), \( \text{dim}_{k_m}(X/mX) \leq 1 \). The proof of this theorem of Ribet uses his generalisation to non-prime level [R, Theorem 5.2(b)] of Mazur’s “multiplicity one” theorem that \( \text{dim}_{k_m}(J_0(N)[m]) = 2 \) [M, Proposition 14.2], and Mazur’s level-lowering argument for \( q \not\equiv 1 \pmod{\ell} \). We can relax the condition \( \ell + 2N(q - 1) \) to the stated \( \ell + 2M(q - 1) \) (i.e. allow \( \ell = q \) if \( q > 2 \)), using Wiles’s further generalisation of Mazur’s multiplicity one theorem [Wi, Theorem 2.1(ii)]. (Note that since \( q \mid N \), \( a_q(f) = \pm 1 \), in particular \( q \nmid a_q(f) \), so in the case \( \ell = q \) Wiles’s condition that \( m \) is ordinary, hence “\( D_{\ell}\)-distinguished” is satisfied.)

We can localise at \( m \) first, so \( \phi_f, \phi_g \in X_m \otimes O_\lambda \) and \( \text{dim}_{k_m}(X_m/mX_m) \leq 1 \). In fact, since we are looking only at a Hecke ring acting on \( q \)-new forms (what Ribet calls \( T_1 \)), we must have \( \text{dim}_{k_m}(X_m/mX_m) = 1 \). It follows from [R, Theorem 3.10], and its proof, that \( X_m \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \) is a free \( T_m \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \)-module of rank 1. Then an application of Nakayama’s Lemma shows that \( X_m \) is a free \( T_m \)-module of rank 1. Now \( T_m \) is a Gorenstein ring, as in [M, Corollary 15.2], so \( \text{dim}_{k_m}((T_m/\ell T_m)[m]) = 1 \) (by [T, Proposition 1.4(iii)]) and hence \( \text{dim}_{k_m}((X_m/\ell X_m)[m]) = 1 \). It follows by basic linear algebra that \((X_m \otimes_{\mathbb{Z}_\ell} \mathbb{O}_\lambda)/\ell(X_m \otimes_{\mathbb{Z}_\ell} \mathbb{O}_\lambda))\mathbb{O}_\lambda \) is a free \( (k_m \otimes_{\mathbb{F}_\lambda} \mathbb{F}_{\lambda}) \)-module of rank 1, using the assumption that \( K_\lambda/\mathbb{Q}_\ell \) is unramified.

Now \( (k_m \otimes_{\mathbb{F}_\lambda} \mathbb{F}_{\lambda}) \simeq \prod_{k_m \rightarrow \mathbb{F}_{\lambda}} \mathbb{F}_{\lambda} \), and it acts on both \( \phi_f \) and \( \phi_g \) through the single component corresponding to the map \( k_m \rightarrow \mathbb{F}_{\lambda} \) induced by \( \bar{f} \to \bar{g} \). Hence \( \phi_f \) and \( \phi_g \) reduce to the same 1-dimensional \( \mathbb{F}_{\lambda} \)-subspace of \( (X_m \otimes_{\mathbb{Z}_\ell} \mathbb{O}_\lambda)/\ell(X_m \otimes_{\mathbb{Z}_\ell} \mathbb{O}_\lambda) \), and by rescaling by a 1-adic unit, we may suppose that their reductions are the same, i.e. that \( \phi_f(y_i) \equiv \phi_g(y_i) \pmod{\lambda} \forall i \).

\[ \square \]

3.1. Proof of Theorem 1.1. This is now an immediate consequence of Lemma 3.1, of \( W(\phi) = \sum_{i=1}^b \phi(y_i)\theta_i \), and the integrality of the Fourier coefficients of the \( \theta_i \).

4. Two examples

Presumably one could obtain examples with smaller level by using \( \ell = 3 \) rather than our \( \ell = 5 \). Moreover we have looked, for simplicity, only at congruences between \( f \) and \( g \) which both have rational Hecke eigenvalues.

**N = 170.** Let \( f \) and \( g \) be the newforms for \( \Gamma_0(170) \) attached to the isogeny classes of elliptic curves over \( \mathbb{Q} \) labelled 170b and 170e respectively, in Cremona’s data [C]. For both \( f \) and \( g \) the Atkin-Lehner eigenvalues are \( w_2 = w_5 = +1 \), \( w_{17} = -1 \). The modular degrees of the optimal curves in the isogeny classes 170b and 170e are 160 and 20, respectively. Both are divisible by 5, with the consequence that 5 is a congruence prime for \( f \) in \( S_2(\Gamma_0(170)) \), and likewise for \( g \). In fact \( f \) and \( g \) are congruent to each other mod 5.

\[
\begin{array}{c|cccccccccccc}
 p & 3 & 7 & 11 & 13 & 19 & 23 & 29 & 31 & 37 & 41 & 43 & 47 & 53 \\
 a_p(f) & -2 & 2 & 6 & 2 & -6 & -6 & 2 & 2 & -6 & -4 & 12 & 6 & -9 \\
 a_p(g) & 3 & -2 & -4 & -3 & 3 & -6 & 9 & -3 & -8 & -6 & 6 & -13 & -9 \\
\end{array}
\]

The Sturm bound [Stu] is \( \frac{2N}{\ell} \prod_{p \mid N} \left( 1 + \frac{1}{p} \right) = 54 \), so the entries in the table (together with the Atkin-Lehner eigenvalues) are sufficient to prove the congruence \( a_n(f) \equiv a_n(g) \) for all \( n \geq 1 \).

Using the computer package Magma, one can find matrices for Hecke operators acting on the Brandt module for \( D = 17 \), \( M = 10 \), for which \( h = 24 \). Knowing in
advance the Hecke eigenvalues, and computing the null spaces of appropriate matrices, one easily finds that we can take \([\phi_f(y_1), \ldots, \phi_f(y_{24})]\) and \([\phi_g(y_1), \ldots, \phi_g(y_{24})]\) (with the ordering as given by Magma) to be
\([-4, -4, -4, -4, 5, 5, 5, 5, 5, 2, 2, -1, -1, -1, -1, -1, -1, -1, -10, -10]\)
and
\([1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2, -1, -1, -1, -1, -1, -1, -1, 0, 0]\)
respectively, and we can observe directly a mod 5 congruence between \(\phi_f\) and \(\phi_g\).

Using the computer package Sage, and Hamieh’s function “shimura_lift_in_kohnen_subspace” \([H, §4]\), we found
\[W(\phi_f) = -4q^{20} + 16q^{24} - 24q^{31} + 16q^{39} + 20q^{40} + 8q^{56} - 8q^{71} - 40q^{79} + 4q^{80} + 16q^{95} - 16q^{96} + O(q^{100})\],
\[W(\phi_g) = -4q^{20} - 4q^{24} - 4q^{31} - 4q^{39} + 8q^{56} + 12q^{71} + 4q^{80} - 4q^{95} + 4q^{96} + O(q^{100})\],
in which the mod 5 congruence is evident. Unfortunately the condition \(\ell \nmid |2M|q - 1\) does not apply to this example.

\(\mathbf{N} = 174\). Let \(f\) and \(g\) be the newforms for \(\Gamma_0(174)\) attached to the isogeny classes of elliptic curves over \(\mathbb{Q}\) labelled 174a and 174d respectively, in Cremona’s data \([C]\). For both \(f\) and \(g\) the Atkin-Lehner eigenvalues are \(w_2 = w_{29} = +1\), \(w_3 = -1\). The modular degrees of the optimal curves in the isogeny classes 174a and 174d are 1540 and 10, respectively. Both are divisible by 5, with the consequence that 5 is a congruence prime for \(f\) in \(S_2(\Gamma_0(174))\), and likewise for \(g\). In fact \(f\) and \(g\) are congruent to each other mod 5.

| \(p\) | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 31 | 37 | 41 | 43 | 47 | 53 | 59 |
|-----|---|---|----|----|----|----|----|----|----|----|----|----|----|----|
| \(a_p(f)\) | -3 | 5 | 6 | -4 | 3 | -1 | 0 | -4 | -1 | -9 | -7 | -3 | -6 | 3 |
| \(a_p(g)\) | 2 | 0 | -4 | 6 | -2 | 4 | 0 | -4 | -6 | 6 | -12 | -8 | -6 | 8 |

The Sturm bound \([Stu]\) is \(\frac{4N}{12\prod p|N} (1 + \frac{1}{p}) = 60\), so the entries in the table (together with the Atkin-Lehner eigenvalues) are sufficient to prove the congruence \(a_n(f) \equiv a_n(g)\) for all \(n \geq 1\).

Using Magma, one can find matrices for Hecke operators acting on the Brandt module for \(D = 3, M = 58\), for which \(h = 16\). We find \([\phi_f(y_1), \ldots, \phi_f(y_{16})]\) and \([\phi_g(y_1), \ldots, \phi_g(y_{16})]\) to be
\([2, 2, -5, -5, -5, -5, 10, 10, 10, 10, -2, -2, -2, -8, -8]\)
and
\([2, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, -2, -2, -2, 2, 2]\)
respectively, and we can observe directly the mod 5 congruence between \(\phi_f\) and \(\phi_g\) proved on the way to Theorem 1.1.

Using the computer package Sage, and Hamieh’s function “shimura_lift_in_kohnen_subspace” \([H, §4]\), we found (with appropriate scaling)
\[W(\phi_f) = 2q^4 - 10q^7 - 2q^{16} - 8q^{24} + 10q^{28} + 2q^{36} + 20q^{52} - 10q^{63} + 2q^{64} - 12q^{87} - 4q^{88} + 8q^{96} + O(q^{100})\],
\[W(\phi_g) = 2q^4 - 2q^{16} + 2q^{24} + 2q^{36} + 2q^{64} - 2q^{87} - 4q^{88} - 2q^{96} + O(q^{100})\],
in which the mod 5 congruence is evident. The condition \( \ell \nmid 2M(q - 1) \) does apply to this example, and \( \mathbf{p}_{f, \ell} \) is irreducible, since we do not have \( a_p(f) \equiv 1 + p \pmod{\ell} \) for all \( p \nmid \ell N \).

Remark. The norm we used comes from a bilinear pairing \( \langle , \rangle : X \times X \to \mathbb{Z} \) such that \( \langle y_i, y_j \rangle = w_i \delta_{ij} \). The Hecke operators \( T_p \) for \( p \nmid N \) are self-adjoint for \( \langle , \rangle \), since if \( E_i \) is the supersingular elliptic curve associated to the class represented by \( y_i \), then \( \langle T_p y_i, y_j \rangle \) is the number of cyclic \( p \)-isogenies from \( E_i \) to \( E_j \), while \( \langle y_i, T_p y_j \rangle \) is the number of cyclic \( p \)-isogenies from \( E_j \) to \( E_i \), and the dual isogeny shows that these two numbers are the same. See the discussion preceding [R, Proposition 3.7], and note that the factor \( w_j = \# \text{Aut}(E_j) \) intervenes between counting isogenies and just counting their kernels.

We have \( \phi_f - \phi_g = \lambda \phi \) for some \( \phi \in X \otimes O_\lambda \). Hence \( \phi = \frac{1}{\lambda} (\phi_f - \phi_g) \). Now \( \phi_f \) and \( \phi_g \) are simultaneous eigenvectors for all the \( T_p \) with \( p \nmid N \), and are orthogonal to each other, so we must have \( \frac{1}{\lambda} = \frac{\langle \phi_f, \phi_g \rangle}{\langle \phi_f, \phi_f \rangle} \). Consequently, \( \lambda \mid \langle \phi_f, \phi_f \rangle \), and similarly \( \lambda \mid \langle \phi_g, \phi_g \rangle \). We can see this directly in the above examples, where \( \lambda = \ell = 5 \).

In the first one, the GramMatrix command in Magma shows that all \( w_i = 2 \), so \( \langle \phi_f, \phi_f \rangle = 960 \) and \( \langle \phi_g, \phi_g \rangle = 40 \). In the second example, \( w_1 = w_2 = 4 \) while \( w_3 = 2 \) for all \( 3 \leq i \leq 16 \), so \( \langle \phi_f, \phi_f \rangle = 1320 \) and \( \langle \phi_g, \phi_g \rangle = 80 \).

Acknowledgments. We are grateful to A. Hamieh for supplying the code for her Sage function “shimura_lift_in_kohnen_subspace”, as used in [H, §4]. The second named author would like to thank Sheffield University for the great hospitality. She was supported by a DST-INSPIRE grant.

References

[BM] E. M. Baruch, Z. Mao, Central value of automorphic \( L \)-functions, Geom. Funct. Anal. 17 (2007), 333–384.
[BS1] S. Böcherer, R. Schulze-Pillot, On a theorem of Waldspurger and on Eisenstein series of Klingen type, Math. Ann. 288 (1990), 361-388.
[BS2] S. Böcherer, R. Schulze-Pillot, Vector valued theta series and Waldspurger’s theorem, Abh. Math. Sem. Univ. Hamburg 64 (1994), 211-233.
[C] J. Cremona, Elliptic curve data, http://homepages.warwick.ac.uk/staff/J.E.Cremona/ftp/data/INDEX.html.
[D] N. Dumigan, Congruences of modular forms and Selmer groups, Math. Res. Lett. 8 (2001), 479-494.
[Ed] B. Edixhoven, Serre’s Conjecture, in Modular Forms and Fermat’s Last Theorem, (G. Cornell, J. H. Silverman, G. Stevens, eds.), 209–242, Springer-Verlag, New York, 1997.
[Em] M. Emerton, Supersingular elliptic curves, theta series and weight two modular forms, J. Amer. Math. Soc. 15 (2002), 671-714.
[G1] B. Gross, Heights and the special values of \( L \)-series, in Number theory (Montreal, Que., 1985), 115-187, CMS Conf. Proc., 7, Amer. Math. Soc., Providence, RI, 1987.
[G2] B. Gross, Algebraic modular forms, Israel J. Math. 113 (1999), 61–93.
[H] A. Hamieh, Ternary quadratic forms and half-integral weight modular forms, LMS J. Comput. Math. 15 (2012), 418–435.
[K] W. Kohnen, Newforms of half-integral weight, J. Reine Angew. Math. 333 (1982), 32-72.
[L] R. P. Langlands, Modular forms and \( \ell \)-adic representations, in Modular Functions of One Variable II, Lect. Notes Math. 349, 361–500, Springer-Verlag, 1973.
[M] B. Mazur, Modular curves and the Eisenstein ideal, Publ. Math. IHES 47 (1977), 33–186.
[MRT] Z. Mao, F. Rodriguez-Villegas, G. Tornarà, Computation of central value of quadratic twists of modular \( L \)-function, 273–288 in Ranks of elliptic curves and random matrix theory, London Math. Soc. Lecture Note Ser. 341, Cambridge Univ. Press, Cambridge, 2007.
[MO] W. J. McGraw, K. Ono, Modular form congruences and Selmer groups, J. London Math. Soc. (2) 67 (2003), 302-318.
A. Pacetti, G. Tornaría, Computing central values of twisted $L$-series: the case of composite levels, *Experiment. Math.* **17** (2008), 459–471.

K. Prasanna, On $p$-adic properties of central $L$-values of quadratic twists of an elliptic curve, *Canad. J. Math* **62** (2010), 400–414.

P. L. Quattrini, The effect of torsion on the distribution of $\text{III}$ among the quadratic twists of an elliptic curve, *J. Number Theory* **131** (2011), 195–211.

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

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

G. Stevens, $\Lambda$-adic modular forms of half-integral weight and a $\Lambda$-adic Shintani lifting, *Contemp. Math.* **174** (1994), 129-151.

J. Sturm, On the congruence of modular forms, in *Number theory (New York 1984–1985)*, 275–280, Lect. Notes Math. **1240**, Springer-Verlag, 1987.

J. Tilouine, Hecke algebras and the Gorenstein property, in Modular Forms and Fermat’s Last Theorem, (G. Cornell, J. H. Silverman, G. Stevens, eds.), 327–342, Springer-Verlag, New York, 1997.

V. Vatsal, Canonical periods and congruence formulae, *Duke Math. J.* **98** (1999), 397-419.

J.-L. Waldspurger, Correspondances de Shimura et quaternions, *Forum Math.* **3** (1991), 219-307.

J.-L. Waldspurger, Sur les coefficients de fourier des formes modulaires de poids demi-entier, *J. Math. Pures Appl.* **60** (1981), 375-484.

A. Wiles, Modular elliptic curves and Fermat’s Last Theorem, *Ann. Math.* **141** (1995), 443–551.

**University of Sheffield, School of Mathematics and Statistics, Hicks Building, Hounsfield Road, Sheffield, S3 7RH, U.K.**

*E-mail address: n.p.dummigan@shef.ac.uk*

**IIT Madras, Chennai, India.**

*E-mail address: srilakshmi@iitm.ac.in*