CONGRUENCES OF MODULAR FORMS AND SELMER GROUPS

NEIL DUMMIGAN

ABSTRACT. We show that the congruence modulo 11 between the normalized cusp form Δ of weight 12 and the normalized cusp form of weight 2 and level 11 'descends' to a congruence between forms of weights 13/2 and 3/2. Combining Waldspurger's theorem with the Bloch-Kato conjecture we predict the existence of elements of order 11 in Selmer groups for certain quadratic twists of Δ. These are then constructed using rational points on twists of the elliptic curve $X_0(11)$, assuming the Birch and Swinnerton-Dyer conjecture on the rank. Everything generalizes to forms of weights $2 + 10s$ in an 11-adic family, to congruences modulo higher powers of 11, and to other elliptic curves over $\mathbb{Q}$ of prime conductor $p \equiv 3 \pmod 4$ such that $L(E_{-p}, 1) \neq 0$ and $p \nmid \mathrm{ord}_p(j(E))$.

1. INTRODUCTION

The Tamagawa-number conjecture of Bloch and Kato [BK] is a very general conjecture on the special values (at integer points) of the L-functions arising from arithmetic geometry. Examples of such L-functions are those attached to modular forms. The connection with arithmetic geometry is through modular curves, and gives rise to the Galois representations famously associated with modular forms. In an earlier paper [Du1] we considered some numerical observations in the light of the conjecture, in the special case of modular forms of level one and weight k, comparing special values at different points in the critical range $1 \leq s \leq k - 1$. Looking at ratios of critical values avoided the difficulty of determining a canonical period, by making it cancel. In the present paper we look only at the central critical point $s = k/2$, but consider ratios of the values at that point of various quadratic twists of the L-function attached to the modular form.

The particular example on which we concentrate is the discriminant function

$$\Delta(z) = \eta(z)^{24} = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n,$$

where $q = e^{2\pi i z}$ and $\eta(z) = q^{1/24} \prod (1 - q^n)$ is Dedekind's eta function. Δ is the unique normalized cusp form of weight 12 and level one. Let E be the elliptic curve with minimal Weierstrass equation $y^2 + y = x^3 - x^2 - 10x - 20$. This is in fact the modular curve $X_0(11)$, so E is trivially 'modular'. The associated modular form,

the unique normalized cusp form of weight 2 on $\Gamma_0(11)$, is

$$F(z) = \eta(z)^2 \eta(11z)^2 = q \prod (1-q^n)^2 \prod (1-q^{11n})^2.$$

It is evident from the infinite products that the q-expansions of Δ and F are congruent modulo 11. It is this congruence which acts as a lever for us to pry some information out of the motives attached to quadratic twists of Δ.

A question raised by Hida is whether congruences between integer weight newforms descend to congruences between half-integral weight Hecke eigenforms which correspond to them under the Shimura map [Shim], [K1], [K2]. Maeda [Mae] produced an example with congruences modulo 433, using newforms of weight $k = 8$ and level $N = 52$. Further examples involving congruences between cusp forms and Eisenstein series were considered in [Kob] and [G1]. In our case, we can associate with F and Δ explicit Hecke eigenforms g and h, of weights $3/2$ and $13/2$, on $\Gamma_0(44)$ and $\Gamma_0(4)$ respectively. The forms F and Δ have different weights, and we find that the congruence modulo 11 between F and Δ descends to a congruence modulo 11 between the Fourier coefficients not quite of g and h, but of g and $h|T_{11}$. Put another way, if $g = \sum a_n q^n$ and $h = \sum b_n q^n$ then $a_n \equiv b_{11n} \pmod{11}$ for all n. We prove the congruence using a theorem of Sturm [Stu], which shows in our case that it suffices to check the congruence for $n \leq 156$. (Sturm's theorem applies to an appropriate pair of forms of integral weight.) A corollary is Theorem 10 of [BDO], that $11 \mid b_{11n}$ whenever n is a quadratic non-residue modulo 11. Their proof also uses Sturm's theorem, but necessitates checking the divisibility for $n \leq 95832$.

Let d, positive and coprime to 11, be such that $-d$ is the discriminant of a quadratic field. Let E_{-d} be the quadratic twist of E associated to the quadratic character $\left(\frac{-d}{n}\right)$. According to a theorem of Waldspurger [Wa], the central critical value $L(E_{-d}, 1)$ is (more or less) proportional to the square of the dth Fourier coefficient of g. If we restrict now to d which are quadratic residues modulo 11, the sign in the functional equation of $L(E_{-d}, s)$ is positive, so $L(E_{-d}, s)$ vanishes to even order at $s = 1$. If the dth Fourier coefficient of g is zero then $L(E_{-d}, s)$ vanishes to order at least two at $s = 1$. According to the Birch and Swinnerton-Dyer conjecture, the group of rational points $E_{-d}(\mathbb{Q})$ then has rank at least 2.

Waldspurger's theorem implies that the square of b_{11d} is more or less proportional to the central critical value of the twisted L-function, $L(\Delta, \chi_{11d}, 6)$. In those cases where $a_d = 0$, the aforementioned congruence implies that $11 \mid b_{11d}$. Take two different d and d' as above, both quadratic residues modulo 11. Suppose that $a_d = 0$ but that $a_{d'} \neq 0 \pmod{11}$. Then the ratio

$$\sqrt{d'/d} L(\Delta, \chi_{11d}, 6)/L(\Delta, \chi_{11d'}, 6)$$

is a rational number divisible by 11. If it is non-zero, then the Bloch-Kato conjecture, applied to these critical values, predicts that some Shafarevich-Tate group for Δ_{11d} has order divisible by 11, even by 11^2. (We already mentioned the cancellation of periods. Similarly, although we do not know the local fudge factors c_p appearing in the Bloch-Kato formula, we can show that their 11-parts do not change from one twist to another.)

Now, to provide some evidence for the Bloch-Kato conjecture, all we need to do is to produce an element of order 11 in the appropriate Selmer group for the motive attached to Δ_{11d}. Recall that since $a_d = 0$, $L(E_{-d}, s)$ vanishes to order at least two at $s = 1$. The Birch and Swinnerton-Dyer conjecture would then imply that

$E_{-d}(\mathbb{Q})$ has rank at least two. Assuming this is true (it can be checked in particular cases), we get two independent elements of order 11 in a Selmer group for E_{-d}. The congruence of F and Δ implies that the mod 11 Galois representations attached to E and Δ are isomorphic. This allows us to transfer these elements of order 11 to some Galois cohomology group attached to Δ_{11d}. To show that they are in the Selmer group, as required, we would have to show that they satisfy the necessary local conditions at every prime p. For $p \neq 11$ this is quite straightforward. For $p = 11$ we might be tempted to try to apply the theory of Fontaine and Lafaille, as in [Du2]. However, this does not apply when $p < k$, and here $p = 11$ while $k = 12$. Fortunately, it is a matter of simple linear algebra to show that some non-zero linear combination of the two classes must satisfy the local condition at 11, so we do get an element of order 11 in the Selmer group, as required. Note that the inequality $p < k$ is no accident, since for two modular forms (of trivial character) to be congruent modulo p, the difference of their weights must be divisible by $p - 1$ [SwD].

In the rare event that $L(\Delta, \chi_{11d}, 6) = 0$, the Beilinson-Bloch generalization [B] of the Birch and Swinnerton-Dyer conjecture predicts the existence of a rational element of infinite order in the Chow group CH_0^6 of the motive attached to Δ_{11d}. Assuming injectivity of the 11-adic Abel-Jacobi map, this would predict an element of order 11 in a Selmer group, which would again be given by the construction outlined above.

Let us reflect a little on what has occurred. The mod 11 congruence between F and Δ, when lifted to g and h, directly links the vanishing of $L(E_{-d}, 1)$ with the divisibility by 11 of $\sqrt{d'/d}L(\Delta, \chi_{11d}, 6)/L(\Delta, \chi_{11d'}, 6)$. Conjecturally, the former is associated with rational points on E_{-d}, while the latter is associated with elements of order 11 in a Selmer group for Δ_{11d}. The same mod 11 congruence, when interpreted in terms of Galois representations, provides the link between the rational points and the Selmer group.

The use of rational points on an elliptic curve to produce elements in a Selmer group, which are then transferred to a Selmer group for another motive using a congruence of Galois representations, is somewhat analogous to Mazur's construction [CM], of 'visible' likely elements in Shafarevich-Tate groups of elliptic curves. The construction used in [Du2] and [Du3] may be viewed in the same light. It is shown in [GP], by analytic methods, that $a_d = 0$ is only possible if 5 divides the class number of $\mathbb{Q}(\sqrt{-d})$. We can also construct elements of order 5 in these class groups by starting from the assumed rational points on E_{-d}, getting from them elements of 5-Selmer groups, then using the fact that $E[5] \simeq \mathbb{Z}/5\mathbb{Z} \oplus \mu_5$ as a Galois module. The details are left to the reader.

So far we have been dealing with the case where d is a quadratic residue modulo 11, where the order of vanishing of $L(E_{-d}, s)$ at $s = 1$ is even. Balog, Darmon and Ono [BDO] concentrated on the case where d is a quadratic non-residue modulo 11, and the order of vanishing is odd. They expressed the hope that their result $(11 \mid b_{11d})$ could be explained in terms of the Bloch-Kato conjecture. Unfortunately, even if we calculated the canonical period, our ignorance of the 11-part of the fudge factor c_{11} would prevent us from doing this at present.

Most of this paper serves merely as an introduction and illustrative example for some general results stated in the last section. First, Δ can be replaced by any normalized Hecke eigenform of weight $2 + 10s$ in the Hida 11-adic family containing

F. When 11^{t-1} divides s, we find that 11^{2t} divides ratios of L-values, and we can construct the predicted elements of order 11^t in Selmer groups. Then, more generally, $E = X_0(11)$ can be replaced by any elliptic curve E, of prime conductor $p \equiv 3 \pmod 4$, such that $L(E_{-p}, 1) \neq 0$ and $p \nmid \mathrm{ord}_p(j(E))$. Stevens's Λ-adic Shintani lifting [Ste] is very useful for proving the congruences of half-integer weight forms, and could have been used in Section 3, instead of Sturm's theorem.

I thank the referee for numerous helpful suggestions for improving the exposition, and J. Cremona for the computations referred to in Section 7.

2. The Shimura correspondence

Let N be a positive integer. As usual, let $\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : N | c \right\}$. Let k be an even positive integer. A modular form of weight $(k+1)/2$ and character χ for $\Gamma_0(4N)$ is a holomorphic function g on the completed upper half plane, satisfying

$$g(\gamma z) = \chi(d) j(\gamma, z)^{k+1} g(z)$$

for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4N)$, where

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

$\epsilon_d = 1$ or i according as $d \equiv 1$ or $3 \pmod 4$ and $-\pi/2 < \arg(cz + d)^{1/2} \le \pi/2$. It has a q-expansion $\sum_{n=0}^{\infty} a_n q^n$, where $q = e^{2\pi i z}$. Following Shimura, $\left(\frac{0}{\pm 1} \right)$ is defined to be 1. Hence $g = 0$ unless $\chi(-1) = 1$. Note that the square of a modular form of half-integral weight is not necessarily a modular form of integral weight, but its fourth power is.

Shimura [Shim] defined a correspondence which associates to a Hecke eigenform $g = \sum a_n q^n$ of weight $(k+1)/2$, character χ and level $4N$ a Hecke eigenform f of weight k, character χ^2 and level dividing $4N$. For primes l not dividing $4N$, the eigenvalue of the Hecke operator T_l acting on f is the same as the eigenvalue of T_{l^2} acting on g. Given a square-free d, all the coefficients a_{dt^2} are determined by a_d and the coefficients of f. For a fixed square-free d, knowledge of all the a_{dt^2} determines the coefficients of f.

Let $S^+_{(k+1)/2}(\Gamma_0(4N))$ be the space of cusp forms (with trivial character) such that $a_n = 0$ unless $(-1)^{k/2} n \equiv 0$ or $1 \pmod 4$. This space is preserved by Hecke operators T_{l^2} for primes l not dividing $4N$. Kohnen [K1], [K2] proved that a slightly modified version of the Shimura correspondence induces an isomorphism between $S^+_{(k+1)/2}(\Gamma_0(4N))$ and $S_k(\Gamma_0(N))$. In the introduction we specified cusp forms $F \in S_2(\Gamma_0(11))$ and $\Delta \in S_{12}(\Gamma_0(1))$. Under Kohnen's isomorphism they correspond to forms $g = \sum a_n q^n \in S^+_{3/2}(\Gamma_0(44))$ and $h = \sum b_n q^n \in S^+_{13/2}(\Gamma_0(4))$ respectively. Both are determined only up to scalar multiples.

Shintani [Shin] devised a way of starting with a form of even integer weight k and going back to a form of weight $(k+1)/2$ which maps to it under the Shimura correspondence. But in the present case, since $S^+_{13/2}(\Gamma_0(4))$ and $S^+_{3/2}(\Gamma_0(44))$ are one-dimensional, all we need to do is to produce non-zero elements of these spaces. The main example in [KZ] provides the formula

$$h(z) = (60/2\pi i)(2G_4(4z)\theta'(z) - G_4'(4z)\theta(z)),$$

where $G_4(z) = \frac{1}{240} + \sum_{n=1}^{\infty} \sigma_3(n)q^n$ $(\sigma_3(n) = \sum_{d|n,d>0} d^3)$ and $\theta(z) = 1 + 2\sum_{n=1}^{\infty} q^{n^2}$. This formula is very suitable for the purpose of computing the Fourier coefficients b_n. Example 3.5 of [Shin] gives a useful formula for the Fourier coefficients a_n of g: $a_n = c_{4n}$ where

$$\sum c_n q^n = \theta(11z)\eta(2z)\eta(22z).$$

3. THE PROOF OF THE CONGRUENCE

Theorem 3.1. *Let* $g = \sum a_n q^n \in S_{3/2}^+(\Gamma_0(44))$ *and* $h = \sum b_n q^n \in S_{13/2}^+(\Gamma_0(4))$ *be the forms described above. Then* $a_n \equiv b_{11n} \pmod{11}$ *for all* n.

Proof. We need to show that the coefficients of g and $h|T_{11}$ are congruent modulo 11. (Note that although h has level 4, we consider it at level 44, so that 11 divides the level and the Hecke operator T_{11} exists. Also, though h has trivial character, $h|T_{11}$ has character $(\frac{11}{\cdot})$.) It is equivalent to show the same thing for the coefficients of g^2 and $(h|T_{11})^2$, since $a_3 = 2$ while $b_{33} = -8968320 \equiv 2 \pmod{11}$, so $g \equiv -h|T_{11} \pmod{11}$ is impossible. Going one step further, it suffices to prove the congruence for g^4 and $(h|T_{11})^4$, which are modular forms of weights 6 and 26 respectively.

For even $r > 2$ let $E_r = 1 - \frac{2r}{B_r}\sum_{n=1}^{\infty} \sigma_{r-1}(n)q^n$ be the normalized Eisenstein series of weight r. A well known consequence of the Clausen-Von Staudt theorem is that for an odd prime number $p > 3$ the q-expansion of E_{p-1} is congruent to 1 mod p. Letting $p = 11$, multiplying g^4 by E_{10}^2 will not make any difference to its Fourier coefficients modulo 11. Now the forms $g^4 E_{10}^2$ and $(h|T_{11})^4$ have the same weight $k = 26$, and are both forms on $\Gamma_0(M)$ with $M = 44$. This allows us to apply the theorem of Sturm [Stu] which guarantees that the congruence holds for all n as long as it holds for all $n \leq \frac{kM}{12}\prod_{p|M}(1 + \frac{1}{p})$. In our case the bound is only 156, so the condition is easily checked using the computer algebra system Maple.
∎

4. WALDSPURGER'S THEOREM

The Shimura correspondence tells us relations among the Fourier coefficients a_{dt^2} of an eigenform g of half-integral weight, for a fixed square-free d, in terms of the coefficients of the Shimura lift f. It does not say anything about the relation between the a_d for different square-free values of d (or $d/4$). Waldspurger [Wa] proved a theorem to the effect that the ratios of the squares of these coefficients are more or less the ratios of the central critical values of the L-functions associated to f with quadratic twists. We state a refined version in a special case which covers what we need. This is Corollary 1 to Theorem 3 in [K3].

Theorem 4.1. *Suppose that* N *is an odd, square-free positive integer and* k *is a positive even integer. Temporarily abandoning earlier names, let* $g = \sum b_n q^n \in S_{(k+1)/2}^+(\Gamma_0(4N))$ *correspond to* $f = \sum c_n q^n \in S_k(\Gamma_0(N))$ *under Kohnen's isomorphism, where* f *is a newform. Let* d *be a positive integer such that* $D := (-1)^{k/2}d$ *is the discriminant of a quadratic field. Let* $L(f, \chi_D, s)$ *be the analytic continuation of* $\sum_{n=1}^{\infty} \chi_D(n)c_n n^{-s}$, *where* $\chi_D(n) = (\frac{D}{n})$. *Let* $\langle f, f \rangle$ *be the Petersson norm and let* $\nu(N)$ *be the number of distinct prime divisors of* N. *Suppose that for every prime* $l \mid N$, $(\frac{D}{l}) = w_l$, *the eigenvalue for* f *with respect to the Atkin-Lehner involution*

W_l. *Then*

$$\frac{b_d^2}{\langle g, g \rangle} = 2^{\nu(N)} \frac{(\frac{k}{2} - 1)!}{\pi^{k/2}} d^{(k-1)/2} \frac{L(f, \chi_D, k/2)}{\langle f, f \rangle}.$$

Corollary 4.2. *For two different d' and d as above, supposing the conditions about $(\frac{D}{l})$ and $(\frac{D'}{l})$ are satisfied, and that $L(f, \chi_D, k/2) \neq 0$,*

$$L(f, \chi_{D'}, k/2)/L(f, \chi_D, k/2) = (d/d')^{(k-2)/2} \sqrt{d/d'} b_{d'}^2 / b_d^2.$$

In the example with Δ of weight $k = 12$ and h of weight $(k+1)/2 = 13/2$, $N = 1$ so there are no conditions to check. In the example with F of weight $k = 2$ and g of weight $(k+1)/2 = 3/2$, $N = 11$ and $w_{11} = -1$ so we require $(\frac{-d}{11}) = -1$, which is equivalent to $(\frac{d}{11}) = 1$. Actually, we shall only be using the above corollary in the example where $k = 12$.

5. MOTIVES AND GALOIS REPRESENTATIONS

Let $f = \sum e_n q^n$ be a newform of weight k for $\Gamma_0(N)$ (and let's say trivial character and rational coefficients, since that is all we need). A special case of a theorem of Deligne [De1] implies the existence, for each prime l, of a continuous representation

$$\rho_l : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(V_l)$$

(V_l is a two-dimensional vector space over $\mathbb{Q}_l$), such that

(1) ρ_l is unramified at p for all primes p not dividing lN;
(2) if Frob_p is an arithmetic Frobenius element at such a p then the characteristic polynomial of Frob_p^{-1} acting on V_l is $x^2 - e_p x + p^{k-1}$.

Following Scholl [Sc], V_l may be constructed as the l-adic realisation of a Grothendieck motive M. There are also Betti and de Rham realisations V_B and V_{dR}, both 2-dimensional $\mathbb{Q}$-vector spaces. For details of the construction see [Sc]. The de Rham realisation has a Hodge filtration $V_{\mathrm{dR}} = F^0 \supset F^1 = \ldots = F^{k-1} \supset F^k = \{0\}$. The Betti realisation V_B comes from singular cohomology, while V_l comes from étale l-adic cohomology. There are natural isomorphisms $V_B \otimes \mathbb{Q}_l \simeq V_l$. Using a basis for singular cohomology with $\mathbb{Z}$-coefficients, we get $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable $\mathbb{Z}_l$-modules T_l inside each V_l. Define $A_l = V_l/T_l$. There are two kinds of twist we shall have to consider. There is the Tate twist $V_l(j)$ (for an integer j), which amounts to multiplying the action of Frob_p by p^j. Then, for D the discriminant of a quadratic field, there is the quadratic twist $V_l(\chi_D)$, which is the tensor product of V_l with a one-dimensional space on which $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts via the quadratic character χ_D.

Following [BK] (Section 3), for $p \neq l$ (including $p = \infty$) let

$$H_f^1(\mathbb{Q}_p, V_l(\chi_D, j)) = \ker(H^1(D_p, V_l(\chi_D, j)) \to H^1(I_p, V_l(\chi_D, j))).$$

The subscript f stands for "finite part". D_p is a decomposition subgroup at a prime above p, I_p is the inertia subgroup, and the cohomology is for continuous cocycles and coboundaries. For $p = l$ let

$$H_f^1(\mathbb{Q}_l, V_l(\chi_D, j)) = \ker(H^1(D_l, V_l(\chi_D, j)) \to H^1(D_l, V_l(\chi_D, j) \otimes B_{\mathrm{cris}}))$$

(see Section 1 of [BK] for definitions of Fontaine's rings B_{cris} and B_{dR}). Let $H_f^1(\mathbb{Q}, V_l(\chi_D, j))$ be the subspace of elements of $H^1(\mathbb{Q}, V_l(\chi_D, j))$ whose local restrictions lie in $H_f^1(\mathbb{Q}_p, V_l(\chi_D, j))$ for all primes p.

There is a natural exact sequence

$$0 \longrightarrow T_l(\chi_D, j) \longrightarrow V_l(\chi_D, j) \xrightarrow{\pi} A_l(\chi_D, j) \longrightarrow 0.$$

Let $H^1_f(\mathbb{Q}_p, A_l(\chi_D, j)) = \pi_* H^1_f(\mathbb{Q}_p, V_l(\chi_D, j))$. Define the l-Selmer group $H^1_f(\mathbb{Q}, A_l(\chi_D, j))$ to be the subgroup of elements of $H^1(\mathbb{Q}, A_l(\chi_D, j))$ whose local restrictions lie in $H^1_f(\mathbb{Q}_p, A_l(\chi_D, j))$ for all primes p. Note that the condition at $p = \infty$ is superfluous unless $l = 2$. In future, p will always be a finite prime. Define the Shafarevich-Tate group

$$\mathrm{III}(\chi_D, j) = \oplus_l H^1_f(\mathbb{Q}, A_l(\chi_D, j))/\pi_* H^1_f(\mathbb{Q}, V_l(\chi_D, j)).$$

For $1 \le j \le k - 1$ define the set of global points

$$\Gamma_{\mathbb{Q}}(\chi_D, j) = \oplus_l H^0(\mathbb{Q}, A_l(\chi_D, j)).$$

This is analogous to the group of rational torsion points on an elliptic curve. To relate it to the Bloch-Kato definition, see their Lemma 5.10 (i) (in [BK]).

6. The Bloch-Kato conjecture

In this section we assume further that f has level $N = 1$. Let j be an integer such that $k/2 \le j \le k - 1$. (Certainly then $L(f, \chi_D, j)$ is a critical value in the sense of [De2].) If $j = k/2$ we suppose we are in the case that $L(f, \chi_D, k/2) \ne 0$. The Bloch-Kato conjecture for the motive $M(\chi_D, j)$ predicts that

$$L(f, \chi_D, j) = \frac{\left(\prod_p c_p(\chi_D, j)\right) \mathrm{vol}_\infty(\chi_D, j) \# \mathrm{III}(\chi_D, j)}{\# \Gamma_{\mathbb{Q}}(\chi_D, j) \# \Gamma_{\mathbb{Q}}(\chi_D, k - j)}.$$

The local factors $\mathrm{vol}_\infty(\chi_D, j)$ and $c_p(\chi_D, j)$ depend on the choice of a basis for V_{dR}, but their product does not. A careful treatment of real periods such as $\mathrm{vol}_\infty(\chi_D, j)$ is given in [De2]. Note that the definition of $\mathrm{vol}_\infty(j)$ given in Section 4 of [Du1] is mistaken, what is defined there actually being $1/\mathrm{vol}_\infty(j)$. The calculation of the periods of Artin motives in terms of generalized Gauss sums, in Section 6 of [De2], yields the following lemma.

Lemma 6.1. $\mathrm{vol}_\infty(\chi_D, j) = \mathrm{vol}_\infty(j)/\sqrt{D}$ if $D > 0$.

Define $H^1_f(\mathbb{Q}_p, T_l(\chi_D, j))$ to be the inverse image of $H^1_f(\mathbb{Q}_p, V_l(\chi_D, j))$ under the natural map from $H^1(\mathbb{Q}_p, T_l(\chi_D, j))$ to $H^1(\mathbb{Q}_p, V_l(\chi_D, j))$. The factor $c_p(\chi_D, j)$, which is 1 for all but finitely many p, is defined to be $\mathrm{vol}_p(\chi_D, j)$ divided by the Euler factor $(1 - \chi_D(p)a_p p^{-j} + p^{k-1-2j})$. Here, $\mathrm{vol}_p(\chi_D, j)$ is the product of the size of $\oplus_{l \ne p} H^1_f(\mathbb{Q}_p, T_l(\chi_D, j))$ and a certain measure of $H^1_f(\mathbb{Q}_p, T_p(\chi_D, j))$.

We need to look a bit more carefully at the definition of the p-part of $\mathrm{vol}_p(\chi_D, j)$. Let $D_{\mathrm{dR}}(V_p) = H^0(\mathbb{Q}_p, V_p \otimes B_{\mathrm{dR}})$. This $D_{\mathrm{dR}}(V_p)$ is a filtered $\mathbb{Q}_p$-vector space which, according to Fontaine's de Rham conjecture ([Fo], Appendix A6), should be naturally isomorphic to $V_{\mathrm{dR}} \otimes \mathbb{Q}_p$ with its Hodge filtration.

Since p is a prime of good reduction for the motive M, V_p is a crystalline representation of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, meaning $D_{\mathrm{cris}}(V_p)$ and V_p have the same dimension, where $D_{\mathrm{cris}}(V_p) := H^0(\mathbb{Q}_p, V_p \otimes B_{\mathrm{cris}})$. (This is a consequence of Theorem 5.6 of [Fa].) It follows from Theorem 4.1(ii) of [BK] that

$$D_{\mathrm{dR}}(V_p)/F^j D_{\mathrm{dR}}(V_p) \simeq H^1_f(\mathbb{Q}_p, V_p(j)),$$

via their exponential map. Now if we admit the de Rham conjecture, then a choice of basis for V_{dR} will give a measure on the right-hand side, with respect to which $|\mathrm{vol}_p(j)|_p^{-1}$ is defined to be the volume of $H^1_f(\mathbb{Q}_p, T_p(j))$.

Fortunately, since p is a prime of good reduction, the de Rham conjecture is a consequence of the crystalline conjecture, which follows from Theorem 5.6 of [Fa]. In Section 7 of [Du1], we had a condition that $p > k$, because we needed a comparison theorem with $\mathbb{Z}_p$ coefficients rather than just $\mathbb{Q}_p$ coefficients. That condition is not necessary here, which is good, given that $11 < 12$.

Lemma 6.2. *Let q be an odd prime and D a quadratic discriminant. For any prime $p \neq q$, we have $\mathrm{ord}_q(c_p(\chi_D, j)) = 0$. In other words, for any prime p, the rational number $c_p(\chi_D, j)$ is at worst the product of a power of p and a power of 2.*

Proof. As on p. 30 of [Fl1], for $p \neq q$,

$$|c_p(\chi_D, j)|_q^{-1} = \#H^0(\mathbb{Q}_p, H^1(I_p, T_q(\chi_D, j))_{\mathrm{tors}}),$$

where I_p is an inertia group at p. If p does not divide D then $T_q(\chi_D, j)$ is a trivial I_p-module, so $H^1(I_p, T_q(\chi_D, j))$ is torsion-free. In general, since $q \neq p$,

$$H^1(I_p, T_q(\chi_D, j)) \simeq T_q(\chi_D, j)/(1 - \tau)T_q(\chi_D, j),$$

where τ is a topological generator of the tame quotient of I_p. If $p \mid D$ then thanks to the quadratic twist ramified at p, τ acts as multiplication by -1 on $T_q(\chi_D, j)$, hence $H^1(I_p, T_q(\chi_D, j))$ is trivial (remember $q \neq 2$). ∎

Lemma 6.3. *Suppose that D and D' are two quadratic discriminants, both divisible by an odd prime q, with $\chi_{D/\epsilon q}(q) = \chi_{D'/\epsilon q}(q)$, where $\epsilon = \chi_{-4}(q)$. Then $c_q(\chi_D, j) = c_q(\chi_{D'}, j)$.*

Proof. For all primes l, $T_l(\chi_D, j)$ and $T_l(\chi_{D'}, j)$ are exactly the same as modules for $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$. Furthermore, the Euler factors $(1 - \chi_D(q)a_q q^{-j} + q^{k-1-2j})$ and $(1 - \chi_{D'}(q)a_q q^{-j} + q^{k-1-2j})$ are both equal to $1 + q^{k-1-2j}$. For primes $l \neq q$ we have $\mathrm{ord}_l(\mathrm{vol}_q(\chi_D, j)) = \#H^1_f(\mathbb{Q}_q, T_l(\chi_D, j))$, so it is a triviality that $\mathrm{ord}_l(\mathrm{vol}_q(\chi_D, j)) = \mathrm{ord}_l(\mathrm{vol}_q(\chi_{D'}, j))$. For $l = q$,

$$(V_{\mathrm{dR}}(\chi_D) \otimes \mathbb{Q}_q)/F^j \simeq H^1_f(\mathbb{Q}_q, V_q(\chi_D, j)),$$

and a choice of basis for V_{dR} determines the q-part of $c_q(\chi_D, j)$. If $\chi_{D/\epsilon q}(q) = \chi_{D'/\epsilon q}(q)$ then replacing D by D' introduces no essential change on either side, so $c_q(\chi_D, j) = c_q(\chi_{D'}, j)$. ∎

Remark 6.4. *We will use only the 'q-part' of the above lemma. In the main example, $q = 11$.*

Lemma 6.5. $\mathrm{ord}_l(\#\Gamma_{\mathbb{Q}}(\chi_D, j)) = 0$ *unless the coefficients of $f = \sum e_n q^n$ satisfy the congruence $e_p \equiv \chi_D(p)(p^j + p^{k-1-j}) \pmod{l}$ for all primes $p \neq l$.*

This follows from the interpretation of e_p as a trace of Frobenius. Note that in the case of interest to us, where $f = \Delta$, $j = k/2 = 6$ and $l = 11$, the congruence is not satisfied for any D. See [SwD].

Now let us concentrate on the case where $f = \Delta$ and $j = k/2 = 6$. Recall the forms F, $g = \sum a_n q^n$ and $h = \sum b_n q^n$ of weights $2, 3/2$ and $13/2$ respectively. Now $b_{33} = -8968320 \equiv 2 \pmod{11}$ so we can take $d' = 3$ and have 11 not dividing

$b_{11d'}$. When $a_d = 0$, the congruence $a_n \equiv b_{11n}$ (mod 11) implies that $11 \mid b_{11d}$. Combining the above lemmas with Theorem 4.1, we find the following.

Proposition 6.6. *Consider the case* $k = 12$, $f = \Delta$. *Suppose* d *is a positive integer such that* $11d$ *is the discriminant of a quadratic field,* d *is a quadratic residue modulo* 11, $a_d = 0$ *and* $L(\Delta, \chi_{11d}, 6) \neq 0$. *If the Bloch-Kato conjecture is true then* $11^2 \mid \#\mathrm{III}(\chi_{11d}, 6)$, *so* $H^1_f(\mathbb{Q}, A_{11}(\chi_{11d}, 6))$ *contains elements of order* 11.

Remark 6.7. *Via Flach's generalization of the Cassels-Tate pairing* [Fl2], *if* $11 \mid \#\mathrm{III}(\chi_{11d}, 6)$ *then* $11^2 \mid \#\mathrm{III}(\chi_{11d}, 6)$.

Even if $L(\Delta, \chi_{11d}, 6) = 0$, as explained in the introduction, we still expect that $H^1_f(\mathbb{Q}, A_{11}(\chi_{11d}, 6))$ contains an element of order 11. Using the computer algebra system Maple we checked that $L(\Delta, \chi_{11d}, 6) \neq 0$, for all relevant d with $1 \leq d \leq 10,000$. See [OS] for what can be proved about non-vanishing.

As noted in the next section, the sign in the functional equation of $L(\Delta, \chi_{11d}, s)$ is positive, so the order of vanishing at $s = 6$ is always even. Our task in the next section is to construct an element of order 11 in the Selmer group $H^1_f(\mathbb{Q}, A_{11}(\chi_{11d}, 6))$ (when $(\frac{d}{11}) = 1$ and $a_d = 0$).

7. Local conditions

Given a prime l, we have defined V_l, T_l and A_l for a modular form f of even weight k, and retained this notation for the special case $f = \Delta, k = 12$. For the modular form F of weight 2 and level 11 associated to the elliptic curve $E = X_0(11)$, we shall use the notation V'_l, T'_l and A'_l. The l-adic Tate module of E is then $T'_l(1)$. We use the notation $A'[l]$ for the l-torsion subgroup of A'_l.

Theorem 7.1. *Suppose that* $d > 0$ *and* $11d$ *is the discriminant of a quadratic field. Let* r *be the rank of the group of rational points* $E_{-d}(\mathbb{Q})$. *If* $r > 1$, *the* 11-*torsion subgroup of the Selmer group* $H^1_f(\mathbb{Q}, A_{11}(\chi_{11d}, 6))$ *has* $\mathbb{F}_{11}$-*rank at least* $r - 1$.

Proof. As $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules, $E_{-d}[11] \simeq A'(\chi_{-d}, 1)[11] \simeq A(\chi_{-d}, 1)[11]$, the second isomorphism being thanks to the congruence between Δ and F, and the irreducibility of these modules. The fifth power of the 11-cyclotomic character is congruent mod 11 to the quadratic character of conductor 11, so this in turn is isomorphic to $A(\chi_{11d}, 6)[11]$.

The injection from $E_{-d}(\mathbb{Q})/11E_{-d}(\mathbb{Q})$ to $H^1(\mathbb{Q}, E_{-d}[11])$ then gives us an $\mathbb{F}_{11}$-subspace of dimension r in $H^1(\mathbb{Q}, A(\chi_{11d}, 6)[11])$, which injects into $H^1(\mathbb{Q}, A_{11}(\chi_{11d}, 6))$ because, as already noted, $H^0(\mathbb{Q}, A_{11}(\chi_{11d}, 6))$ is trivial. Choose some element $c \in H^1(\mathbb{Q}, A(\chi_{11d}, 6)[11])$, coming from $E_{-d}(\mathbb{Q})/11E_{-d}(\mathbb{Q})$, mapping to (say) $\gamma \in H^1(\mathbb{Q}, A_{11}(\chi_{11d}, 6))$. First we show that $\mathrm{res}_p(\gamma) \in H^1_f(\mathbb{Q}_p, A_{11}(\chi_{11d}, 6))$, for all primes $p \neq 11$.

Looking at $c \in H^1(\mathbb{Q}, A'(\chi_{-d}, 1)[11])$, it maps to some $\gamma' \in H^1_f(\mathbb{Q}, A'_{11}(\chi_{-d}, 1))$, so $\mathrm{res}_p(\gamma')$ in $H^1(I_p, A'_{11}(\chi_{-d}, 1))$ is zero. Now $A'_{11}(1)$ is unramified at $p \neq 11$, so $H^0(I_p, A'_{11}(\chi_{-d}, 1))$ is either the whole of $A'_{11}(\chi_{-d}, 1)$ (if $p \nmid d$) or zero (if $p \mid d$). Either way, it is 11-divisible, so $H^1(I_p, A'(\chi_{-d}, 1)[11])$ injects into $H^1(I_p, A'_{11}(\chi_{-d}, 1))$. Hence $\mathrm{res}_p(c)$ in $H^1(I_p, A'(\chi_{-d}, 1)[11]) = H^1(I_p, A(\chi_{11d}, 6)[11])$ is zero, and its image $\mathrm{res}_p(\gamma)$ in $H^1(I_p, A_{11}(\chi_{11d}, 6))$ is zero. If $p \nmid d$, so that $A_{11}(\chi_{11d}, 6)$ is unramified at p, then $H^1_f(\mathbb{Q}_p, A_{11}(\chi_{11d}, 6))$ is equal to (not just contained in) the kernel of the map from $H^1(\mathbb{Q}_p, A_{11}(\chi_{11d}, 6))$ to $H^1(I_p, A_{11}(\chi_{11d}, 6))$, by line 3 of p. 125 of [Fl2],

so we have shown that $\mathrm{res}_p(\gamma) \in H^1_f(\mathbb{Q}_p, A_{11}(\chi_{11d}, 6))$. If $p \mid d$, instead we deduce
from the inflation-restriction sequence, and from $H^0(I_p, A_{11}(\chi_{11d}, 6)) = \{0\}$ that
$\mathrm{res}_p(\gamma) = 0$ in $H^1(\mathbb{Q}_p, A_{11}(\chi_{11d}, 6))$, so again $\mathrm{res}_p(\gamma) \in H^1_f(\mathbb{Q}_p, A_{11}(\chi_{11d}, 6))$, as
required.

It remains to deal with the local condition at $p = 11$. The exponential map of
Bloch and Kato gives an isomorphism

$$V_{\mathrm{dR}}(\chi_{11d}) \otimes \mathbb{Q}_{11}/F^6 \simeq H^1_f(\mathbb{Q}_{11}, V_{11}(\chi_{11d}, 6)).$$

Meanwhile, Section 3 of [BK] tells us that $H^1_f(\mathbb{Q}_{11}, V_{11}(\chi_{11d}, 6))$ is its own anni-
hilator in $H^1(\mathbb{Q}_{11}, V_{11}(\chi_{11d}, 6))$ with respect to the Tate duality pairing. Hence
$H^1_f(\mathbb{Q}_{11}, V_{11}(\chi_{11d}, 6))$ has codimension one in $H^1(\mathbb{Q}_{11}, V_{11}(\chi_{11d}, 6))$. It follows that
our r-dimensional $\mathbb{F}_{11}$-subspace of the 11-torsion in $H^1(\mathbb{Q}, A_{11}(\chi_{11d}, 6))$ has at least
an $(r-1)$-dimensional subspace landing in $H^1_f((\mathbb{Q}_{11}, A_{11}(\chi_{11d}, 6))$.
∎

Remark 7.2. *To fully justify the last step we need to check that the natural map
from $H^1(\mathbb{Q}_{11}, V_{11}(\chi_{11d}, 6))$ to $H^1(\mathbb{Q}, A_{11}(\chi_{11d}, 6))$ is surjective. The cokernel in-
jects into $H^2(\mathbb{Q}_{11}, T_{11}(\chi_{11d}, 6))$, which is Tate-dual to $H^0(\mathbb{Q}_{11}, A_{11}(\chi_{11d}, 6))$, so it
suffices to show that $H^0(\mathbb{Q}_{11}, A[11](\chi_{11d}, 6))$, i.e. $H^0(\mathbb{Q}_{11}, A'[11](\chi_{-d}, 1))$, is trivial.
Consideration of a Tate parametrisation of E shows that even $H^0(I_{11}, A'[11](\chi_{-d}, 1))$
is trivial unless $11 \mid \mathrm{ord}_{11}(j(E))$, but in fact $\mathrm{ord}_{11}(j(E)) = -5$.*

For a newform f of weight k on $\Gamma_0(N)$, and D (coprime to N) the discrim-
inant of a quadratic field, the sign in the functional equation of $L(f, \chi_D, s)$ is
$(-1)^{k/2} w_N \chi_D(-N)$. For $L(\Delta, 11d, s)$ as above, the sign is always positive, since
$\chi_D(-1) = 1$ for the character associated to a real quadratic field. For our F of
weight 2 and level 11 we have $w_{11} = -1$, so the sign in the functional equation of
$L(F, s)$ is positive. When we twist by $-d$ as above, the sign becomes $\chi_{-d}(-11)$.
Hence when $(\frac{d}{11}) = 1$ the sign is positive and the L-function vanishes to even order
at $s = 1$. If also the coefficient $a_d = 0$ then Waldspurger's theorem implies that
$L(E_{-d}, s)$ vanishes at $s = 1$, and we now know it must do so to order at least
2. According to the Birch and Swinnerton-Dyer conjecture, in this case $r \geq 2$, so
the above theorem provides the required element of order 11 in the Selmer group
$H^1_f(\mathbb{Q}, A_{11}(\chi_{11d}, 6))$.

The squarefree $d < 550$ such that $d \equiv 3 \pmod 4, (\frac{d}{11}) = 1$ and $a_d = 0$ are
$d = 47, 103, 119, 159$ and 455. Cremona has checked, for all these values of d, that
the order of vanishing of $L(E_{-d}, s)$ at $s = 1$ is precisely two, and that $E_{-d}(\mathbb{Q})$
does have rank 2. Guerzhoy and Panchishkin [GP] found the simple rational points
$(-1, 1), (-3, 1)$ and $(1, 1)$, of infinite order on E_{-47}, E_{-103} and E_{-119} respectively,
with reference to Weierstrass equations $-dy^2 = 4x^3 - 4x^2 - 40x - 79$.

As noted in the introduction, since $11 < 12$ we are unable to apply the theory
of Fontaine and Lafaille to show that the 11-torsion in $H^1_f(\mathbb{Q}, A_{11}(\chi_{11d}, 6))$ and the
11-torsion in $H^1_f(\mathbb{Q}, A'_{11}(\chi_{-d}, 1))$ are isomorphic. This is actually a good thing,
since if $(\frac{d}{11}) = -1$, so that the order of vanishing of $L(E_{-d}, s)$ at $s = 1$ is odd, we
would expect the dimensions of these $\mathbb{F}_{11}$-vector spaces to differ in parity.

8. More general results

Let E be an elliptic curve of prime conductor p. Suppose that $p \nmid \mathrm{ord}_p(j(E))$.
Let f_2 be the normalized Hecke eigenform of weight 2 and level p attached to E.

Since E has multiplicative reduction at p, the form f_2 is ordinary at p. In other words, p does not divide the pth Fourier coefficient. Hence, according to [H], if $k > 2$ is an integer such that $k \equiv 2 \pmod{p^{t-1}(p-1)}$ then, if t is sufficiently large, there exists a normalized eigenform f_k, an oldform of weight k on $\Gamma_0(p)$, such that $f_k \equiv f_2 \pmod{p^t}$ as q-expansions. (In the example with $p = 11$, it happens that $t = 1$ is large enough.) There is a normalized newform F_k of level one such that $f_k(z) = F_k(z) - \beta F_k(pz)$, where β is the non-unit root of Frobenius.

Let $\epsilon = \pm 1$, $\nu = (-1)^{(p-1)/2}$ and let d be a positive integer such that ϵd is the discriminant of a quadratic field. The sign in the functional equation of $L(E_{\epsilon d}, s)$ is $-w_p \chi_{\epsilon d}(-p)$. We shall be interested in those d such that this sign is positive, so that if $L(E_{\epsilon d}, s)$ vanishes at $s = 1$, it does so to order at least two.

Consider the motive attached to F_k, with its V_λ, T_λ and A_λ, for prime ideals λ in the ring of integers of the field generated by the coefficients of F_k. These coefficients are naturally regarded as elements of $\mathbb{Z}_p$, so there is a favoured split prime $\mathfrak{p}$ dividing p in the coefficient field.

Theorem 8.1. *Suppose that $d > 0$ is coprime to p, and that ϵd is the discriminant of a quadratic field. Let r be the rank of the group of rational points $E_{\epsilon d}(\mathbb{Q})$, and suppose that $r > 1$. Suppose that $k \equiv 2 \pmod{p^{t-1}(p-1)}$ (with t as above). If $k - 2$ is an odd multiple of $\phi(p^t)$, let $S = H^1_f(\mathbb{Q}, A_{\mathfrak{p}}(\chi_{\epsilon\nu pd}, k/2))$. Otherwise, let $S = H^1_f(\mathbb{Q}, A_{\mathfrak{p}}(\chi_{\epsilon d}, k/2))$. Then S has a subgroup isomorphic to $(\mathbb{Z}/p^t\mathbb{Z})^{r-1}$.*

This may be proved in essentially the same way as Theorem 7.1. Note that it follows from Hida's construction that $E[p^t](-1)$ and $A[p^t]$ are isomorphic as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules, not just that the traces of Frobenius (i.e. the Fourier coefficients modulo p^t) are equal (see Theorem II of [H]).

If $L(E_{\epsilon d}, s)$ vanishes to order at least two at $s = 1$, then the conjecture of Birch and Swinnerton-Dyer predicts that $r \geq 2$. If $r = 2$ then the above theorem provides a subgroup isomorphic to $\mathbb{Z}/p^t\mathbb{Z}$ in a suitable Selmer group. Assuming that the Selmer group equals the Shafarevich-Tate group, it follows from [Fl2] that its order is at least p^{2t}.

Now we just have to content ourselves that this is as predicted by the Bloch-Kato conjecture, applied to a ratio $\sqrt{d'/d}L(F_k, \chi_{\epsilon d}, k/2)/L(F_k, \chi_{\epsilon d'}, k/2)$ or $\sqrt{d'/d}L(F_k, \chi_{\epsilon\nu pd}, k/2)/L(F_k, \chi_{\epsilon\nu pd'}, k/2)$. First, the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[p]$ is irreducible, thanks to Theorem 4 of [Maz]. Hence factors such as $\Gamma_{\mathbb{Q}}(\chi_{\epsilon d}, k/2)$ make no contribution. Second, it may be shown just as in Section 6 that fudge factors such as $c_q(\chi_{\epsilon d}, k/2)$ make no contribution. (There is a minor complication in that we must consider their orders at all the primes dividing p.) What we need is then provided by the proposition below, except we must impose conditions $p \equiv 3 \pmod 4$, $\epsilon = -1$ and $L(E_{-p}, 1) \neq 0$. (If we allowed $\epsilon = 1$ then the relevant twisted L-functions attached to F_k would automatically vanish at $s = k/2$, thanks to the sign of the functional equation.)

Proposition 8.2. *Suppose that $p \equiv 3 \pmod 4$, with $E/\mathbb{Q}$ an elliptic curve of conductor p. Suppose that $L(E_{-p}, 1) \neq 0$. Let $d \equiv d' \pmod 8$ be positive, squarefree integers, coprime to p, with $d \equiv 3 \pmod 4$ and $-w_p\chi_{-d}(-p) = -w_p\chi_{-d'}(-p) = 1$. Suppose that $L(E_{-d}, 1) = 0$ but $L(E_{-d'}, 1) \neq 0$. Suppose that $k > 2$ is an integer with $k \equiv 2 \pmod{\phi(p^t)}$, and t sufficiently large. Let $s = (k-2)/\phi(p^t)$. If s is even, then the rational ratio*

$$\sqrt{d'/d}L(F_k, \chi_{-d}, k/2)/L(F_k, \chi_{-d'}, k/2)$$

(if defined) is divisible by $p^{2(t-u)}$. If s is odd, then

$$\sqrt{d'/d}L(F_k, \chi_{pd}, k/2)/L(F_k, \chi_{pd'}, k/2)$$

(if defined) is divisible by $p^{2(t-u)}$. Here, u is a non-negative integer which depends only on d', not on k.

Sketch of proof. Let χ be the trivial character if s is odd, the Legendre symbol $\left(\frac{\cdot}{p}\right)$ if s is even. Let $\theta_\chi(f_k) \in S_{(k+1)/2}(\Gamma_0(4p^m), \chi^*)$ be Shintani's lifting [Shin], where $m = (1 + (-1)^s)/2$ and $\chi^*(n) = \chi(n)\left(\frac{(-1)^{k/2}p}{n}\right)$. Note that if we allowed $p \equiv 1 \pmod 4$ then we would have $\chi^*(-1) = -1$, and necessarily $\theta_\chi(f_k) = 0$. Stevens [Ste] constructed a Λ-adic Shintani lifting, p-adically interpolating the Shintani liftings of the various f_k. Here we consider only a sufficiently small open neighbourhood of $k = 2$ in his $X(R)$. It follows from his Theorem 3.3 that, as q-expansions,

$$\Omega_{k,\chi}\theta_\chi(f_k)/\omega(f_k)|T_p^{1-m} \equiv \Omega_2\theta(f_2)/\omega(f_2) \pmod{p^t}.$$

Here, $\omega(f_k)$ and $\omega(f_2)$ are certain periods chosen so that the coefficients of $\theta_\chi(f_k)/\omega(f_k)$ and $\theta(f_2)/\omega(f_2)$ are algebraic numbers, integral at primes dividing p. The factors $\Omega_{k,\chi}$ and Ω_2 are elements of $\mathbb{Q}_p$.

For $\omega(f_2)$ we take $2\pi i$ times the canonical real period of the elliptic curve E. We choose E to be a strong Weil curve within its isogeny class. The rational coefficients of $\theta(f_2)/\omega(f_2)$ really are integral at p. This is because the coefficients of $\theta(f_2)$ are integer linear combinations of integrals of $f_2(\tau)\,d\tau$ over paths joining $\Gamma_0(p)$-equivalent cusps. (Manin's constant is coprime to p, in fact it is a power of 2, by Corollary 4.2 of [Maz], so $\frac{1}{2\pi i}f_2(\tau)\,d\tau$ is as good as the pullback of the canonical differential on E.)

The Ω_k in [Ste] are the same as those in [GS], where $\Omega_2 = 1$ for our choice of $\omega(f_2)$ (see [GS] between 0.8 and 0.9). Let $\theta(f_2)/\omega(f_2) = \sum a_n q^n$ and $\Omega_{k,\chi}\theta_\chi(f_k)/\omega(f_k) = \sum b_n q^n$. Then $a_n \equiv b_n \pmod{p^t}$ if s is even, while $a_n \equiv b_{pn} \pmod{p^t}$ if s is odd. It is important now to know that $\theta(f_2)$ is not identically zero. It is quite easy to check that the coefficient a_p is the product of a non-zero number and $L(E_{-p}, 1)$ (see Remark 3.1 following Example 3.5 of [Shin]). Since we are assuming that $L(E_{-p}, 1) \neq 0$, it follows that $a_p \neq 0$, hence that $\theta(f_2) \neq 0$. In fact, $\theta(f_2)$ is a non-zero element of $S_{3/2}^+(\Gamma_0(4p))$ corresponding to f_2 under Kohnen's isomorphism.

Given the above, $L(E_{-d'}, 1) \neq 0$ implies that $a_{-d'} \neq 0$. Let $u = \text{ord}_p(a_{d'})$ and make sure t is large enough not only for f_k to exist, but for $t > u$. Since $a_d = 0$, the congruences imply that p^{t-u} divides $b_d/b_{d'}$, or $b_{pd}/b_{pd'}$ as appropriate.

Now the proposition follows directly from Corollaire 2 to Théorème 1 of [Wa], which, under our hypotheses, states that

$$(d/d')^{(k-1)/2}L(F_k, \chi_{-d}, k/2)/L(F_k, \chi_{-d'}, k/2) = b_d^2/b_{d'}^2$$

or

$$(d/d')^{(k-1)/2}L(F_k, \chi_{pd}, k/2)/L(F_k, \chi_{pd'}, k/2) = b_{pd}^2/b_{pd'}^2,$$

as appropriate, in both cases assuming that the L-value in the denominator is non-zero. ∎

Remark 8.3. *In the $p = 11$ case, we could choose d' so that $u = 0$. One might expect that this is typical. When $p = 11$ and $k = 12$, the character χ^* is non-trivial,*

so the form of weight 13/2 *appearing in the above proof is not the same one we were using earlier.*

Remark 8.4. *The sign in the functional equation of* $L(E_{-p}, s)$ *is always positive. (See the remark in Section 18 of Chapter I of* [MTT]*.)*

We should mention the work of Guerzhoy [G2], who considers certain p-adic families of cusp forms and generalizes the 'quadratic congruences' of [BDO]. His approach is via two-variable p-adic L-functions, and can be used to prove congruences of the type we have used. (This is true at least in certain special cases, but possibly more generally, see Remark 2 near the end of [G2].) If one is interested purely in special values rather than in half-integral weight modular forms, this approach has the merit that it allows one to by-pass Waldspurger's theorem. Also, it should work when $p \equiv 1 \pmod 4$ and $\epsilon = -1$.

REFERENCES

[BDO]   A. Balog, H. Darmon, K. Ono, Congruences for Fourier coefficients of half-integral weight modular forms and special values of L-functions. Analytic number theory, Vol. 1 (Allerton Park, IL, 1995), 105–128, Progr. Math., 138, Birkhäuser Boston, Boston, MA, 1996.

[B]   S. Bloch, Algebraic cycles and values of L-functions, *J. reine angew. Math.* **350** (1984), 94–108.

[BK]   S. Bloch, K. Kato, L-functions and Tamagawa numbers of motives, The Grothendieck Festschrift Volume I, 333–400, Progress in Mathematics, 86, Birkhäuser, Boston, 1990.

[CM]   J. E. Cremona, B. Mazur, Visualizing elements in the Shafarevich-Tate group, *Experiment. Math.* **9** (2000), 13–28.

[De1]   P. Deligne, Formes modulaires et représentations l-adiques. Sém. Bourbaki, éxp. 355, Lect. Notes Math. **179,** 139–172, Springer, 1969.

[De2]   P. Deligne, Valeurs de Fonctions L et Périodes d'Intégrales, *AMS Proc. Symp. Pure Math.,* Vol. 33 (1979), part 2, 313–346.

[Du1]   N. Dummigan, Period ratios of modular forms, *Math. Ann.* **318** (2000), 621–636.

[Du2]   N. Dummigan, Symmetric square L-functions and Shafarevich-Tate groups, *Experiment. Math.,* to appear.

[Du3]   N. Dummigan, A Hilbert modular motive and its symmetric square, submitted.

[Fa]   G. Faltings, Crystalline cohomology and p-adic Galois representations, *in* Algebraic analysis, geometry and number theory (J. Igusa, ed.), 25–80, Johns Hopkins University Press, Baltimore, 1989.

[Fl1]   M. Flach, On the degree of modular parametrisations, Séminaire de Théorie des Nombres, Paris 1991-92 (S. David, ed.), 23–36, Progress in mathematics, 116, Birkhäuser, Basel Boston Berlin, 1993.

[Fl2]   M. Flach, A generalisation of the Cassels-Tate pairing, *J. reine angew. Math.* **412** (1990), 113–127.

[Fo]   J.-M. Fontaine, Sur certains types de représentations p-adiques du groupe de Galois d'un corps local, construction d'un anneau de Barsotti-Tate, *Ann. Math.* **115** (1982), 529–577.

[G1]   P. Guerzhoy, On Ramanujan congruences between special values of Hecke and Dirichlet L-functions, *Acta Arith.* **81** (1997), 11–23.

[G2]   P. Guerzhoy, A note on quadratic congruences, *Manuscripta Math.* **94** (1997), 89–94.

[GP]   P.I. Guerzhoy, A.A. Panchishkin, A finiteness criterion for the number of rational points for twisted Weil elliptic curves, *J. Soviet Math.* **52** (1990), 3025–3035.

[GS]   R. Greenberg, G. Stevens, p-adic L-functions and p-adic periods of modular forms, *Invent. Math.* **111** (1993), 407–447.

[H]   H. Hida, Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms, *Invent. Math.* **85** (1986), 545–613.

[Kob]   N. Koblitz, p-adic congruences and modular forms of half integer weight, *Math. Ann.* **274** (1986), 199–220.

[K1]   W. Kohnen, Newforms of half-integral weight, *J. Reine Angew. Math.* **333** (1982), 32–72.

[K2]   W. Kohnen, A remark on the Shimura correspondence, *Glasgow Math J.* **30** (1988), 285–291.

[K3]   W. Kohnen, Fourier coefficients of modular forms of half-integral weight, *Math. Ann.* **271** (1985), 237–268.

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

[Mae]   Y. Maeda, A congruence between modular forms of half-integral weight, *Hokkaido Math. J.* **12** (1983), 64–73.

[Maz]   B. Mazur, Rational isogenies of prime degree, *Invent. Math.* **44** (1978), 129–62.

[MTT]   B. Mazur, J. Tate, J. Teitelbaum, On *p*-adic analogues of the conjectures of Birch and Swinnerton-Dyer, *Invent. Math.* **84** (1986), 1–48.

[OS]   K. Ono, C. M. Skinner, Non-vanishing of quadratic twists of modular *L*-functions, *Invent. Math.* **134** (1998), 651–660.

[Sc]   A. J. Scholl, Motives for modular forms, *Invent. Math.* **100** (1990), 419–430.

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

[Shin] T. Shintani, On construction of holomorphic cusp forms of half integral weight, *Nagoya Math. J.* **58** (1975), 83–126.

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

[Stu]   J. Sturm, On the congruence of modular forms, *Lect. Notes Math.* **1240,** Springer, 1984.

[SwD]   H. P. F. Swinnerton-Dyer, On *l*-adic representations and congruences for coefficients of modular forms,*Modular functions of one variable* III, Lect. Notes Math. **350,** Springer, 1973.

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

University of Sheffield, Department of Pure Mathematics, Hicks Building, Hounsfield Road, Sheffield, S3 7RH, U.K.

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