Constructing elements in Shafarevich–Tate groups of modular motives

Neil Dummigan   William Stein   Mark Watkins

Abstract

We study Shafarevich–Tate groups of motives attached to modular forms on $\Gamma_0(N)$ of weight > 2. We deduce a criterion for the existence of nontrivial elements of these Shafarevich–Tate groups, and give 16 examples in which a strong form of the Beilinson–Bloch conjecture would imply the existence of such elements. We also use modular symbols and observations about Tamagawa numbers to compute nontrivial conjectural lower bounds on the orders of the Shafarevich–Tate groups of modular motives of low level and weight ≤ 12. Our methods build upon the idea of visibility due to Cremona and Mazur, but in the context of motives rather than abelian varieties.

1 Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ and $L(E,s)$ the associated L-function. The conjecture of Birch and Swinnerton-Dyer [BS-D] predicts that the order of vanishing of $L(E,s)$ at $s=1$ is the rank of the group $E(\mathbb{Q})$ of rational points, and also gives an interpretation of the leading term in the Taylor expansion in terms of various quantities, including the order of the Shafarevich–Tate group of E.

Cremona and Mazur [CM1] look, among all strong Weil elliptic curves over $\mathbb{Q}$ of conductor $N \leq 5500$, at those with nontrivial Shafarevich–Tate group (according to the Birch and Swinnerton-Dyer conjecture). Suppose that the Shafarevich–Tate group has predicted elements of prime order p. In most cases they find another elliptic curve, often of the same conductor, whose p-torsion is Galois-isomorphic to that of the first one, and which has positive rank. The rational points on the second elliptic curve produce classes in the common $H^1(\mathbb{Q}, E[p])$. They show [CM2] that these lie in the Shafarevich–Tate group of the first curve, so rational points on one curve explain elements of the Shafarevich–Tate group of the other curve.

The Bloch–Kato conjecture [BK] is the generalisation to arbitrary motives of the leading term part of the Birch and Swinnerton-Dyer conjecture. The Beilinson–Bloch conjecture [B, Be] generalises the part about the order of vanishing at the central point, identifying it with the rank of a certain Chow group.

This paper is a partial generalisation of [CM1] and [AS] from abelian varieties over $\mathbb{Q}$ associated to modular forms of weight 2 to the motives attached to modular forms of higher weight. It also does for congruences between modular forms of equal weight what [Du2] did for congruences between modular forms of different weights.

We consider the situation where two newforms f and g, both of even weight $k > 2$ and level N, are congruent modulo a maximal ideal $\mathfrak{q}$ of odd residue characteristic, and $L(g, k/2) = 0$ but $L(f, k/2) \neq 0$. It turns out that this forces $L(g, s)$ to vanish to order ≥ 2 at $s = k/2$. In Section 7, we give sixteen such examples (all with $k = 4$ and $k = 6$), and in each example, we find that $\mathfrak{q}$ divides the numerator of the algebraic number $L(f, k/2)/\mathrm{vol}_\infty$, where vol_∞ is a certain canonical period.

In fact, we show how this divisibility may be deduced from the vanishing of $L(g, k/2)$ using recent work of Vatsal [V]. The point is, the congruence between f and g leads to a congruence between suitable "algebraic parts" of the special values $L(f, k/2)$ and $L(g, k/2)$. In slightly more detail, a multiplicity one result of Faltings and Jordan shows that the congruence of Fourier expansions leads to a congruence of certain associated cohomology classes. These are then identified with the modular symbols which give rise to the algebraic parts of special values. If $L(g, k/2)$ vanishes then the congruence implies that $L(f, k/2)/\mathrm{vol}_\infty$ must be divisible by $\mathfrak{q}$.

The Bloch–Kato conjecture sometimes then implies that the Shafarevich–Tate group Ш attached to f has nonzero $\mathfrak{q}$-torsion. Under certain hypotheses and assumptions, the most substantial of which is the Beilinson–Bloch conjecture relating the vanishing of $L(g, k/2)$ to the existence of algebraic cycles, we are able to construct some of the predicted elements of Ш using the Galois-theoretic interpretation of the congruence to transfer elements from a Selmer group for g to a Selmer group for f. One might say that algebraic cycles for one motive explain elements of Ш for the other, or that we use the congruence to link the Beilinson–Bloch conjecture for one motive with the Bloch–Kato conjecture for the other.

We also compute data which, assuming the Bloch–Kato conjecture, provides lower bounds for the orders of numerous Shafarevich–Tate groups (see Section 7.3). We thank the referee for many constructive comments.

2 Motives and Galois representations

This section and the next provide definitions of some of the quantities appearing later in the Bloch–Kato conjecture. Let $f = \sum a_n q^n$ be a newform of weight $k \geq 2$ for $\Gamma_0(N)$, with coefficients in an algebraic number field E, which is necessarily totally real. Let λ be any finite prime of E, and let ℓ denote its residue characteristic. A theorem of Deligne [De1] implies the existence of a two-dimensional vector space V_λ over E_λ, and a continuous representation

$$\rho_\lambda\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{Aut}(V_\lambda),$$

such that

1. ρ_λ is unramified at p for all primes p not dividing ℓN, and
2. if Frob_p is an arithmetic Frobenius element at such a p then the characteristic polynomial of $\operatorname{Frob}_p^{-1}$ acting on V_λ is $x^2 - a_p x + p^{k-1}$.

Following Scholl [Sc], we can construct V_λ as the λ-adic realisation of a Grothendieck motive M_f. There are also Betti and de Rham realisations V_B and V_{dR}, both 2-dimensional E-vector spaces. For details of the construction see [Sc]. The de Rham realisation has a Hodge filtration $V_{\mathrm{dR}} = F^0 \supset F^1 = \cdots = F^{k-1} \supset F^k = \{0\}$. The Betti realisation V_B comes from singular cohomology, while V_λ comes from étale ℓ-adic cohomology. For each prime λ, there is a natural isomorphism $V_B \otimes E_\lambda \simeq V_\lambda$. We may choose a $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable O_λ-module T_λ inside each V_λ. Define $A_\lambda = V_\lambda/T_\lambda$. Let $A[\lambda]$ denote the λ-torsion in A_λ. There is the Tate twist $V_\lambda(j)$ (for any integer j), which amounts to multiplying the action of Frob_p by p^j.

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

$$H^1_f(\mathbb{Q}_p, V_\lambda(j)) = \ker\Big(H^1(D_p, V_\lambda(j)) \to H^1(I_p, V_\lambda(j))\Big).$$

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 $p = \ell$, let

$$H^1_f(\mathbb{Q}_\ell, V_\lambda(j)) = \ker\Big(H^1(D_\ell, V_\lambda(j)) \to H^1(D_\ell, V_\lambda(j) \otimes_{\mathbb{Q}_\ell} B_{\mathrm{cris}})\Big)$$

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

There is a natural exact sequence

$$0 \to T_\lambda(j) \to V_\lambda(j) \xrightarrow{\pi} A_\lambda(j) \to 0.$$

Let $H^1_f(\mathbb{Q}_p, A_\lambda(j)) = \pi_* H^1_f(\mathbb{Q}_p, V_\lambda(j))$. We then define the λ-Selmer group $H^1_f(\mathbb{Q}, A_\lambda(j))$ as the subgroup of elements of $H^1(\mathbb{Q}, A_\lambda(j))$ whose local restrictions lie in $H^1_f(\mathbb{Q}_p, A_\lambda(j))$ for all primes p. Note that the condition at $p = \infty$ is superfluous unless $\ell = 2$. Define the Shafarevich–Tate group

$$Ш(j) = \bigoplus_\lambda H^1_f(\mathbb{Q}, A_\lambda(j))/\pi_* H^1_f(\mathbb{Q}, V_\lambda(j)).$$

Define an ideal $\#Ш(j)$ of O_E, in which the exponent of any prime ideal λ is the length of the λ-component of $Ш(j)$. We shall only concern ourselves with the case $j = k/2$, and write Ш for $Ш(k/2)$. It depends on the choice of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable O_λ-module T_λ inside each V_λ. But if $A[\lambda]$ is irreducible then T_λ is unique up to scaling and the λ-part of Ш is independent of choices.

In the case $k = 2$ the motive comes from a (self-dual) isogeny class of abelian varieties over $\mathbb{Q}$, with endomorphism algebra containing E. We can choose an abelian variety B in the isogeny class whose endomorphism ring contains the full ring of integers O_E. If one takes all the $T_\lambda(1)$ to be λ-adic Tate modules, then what we have defined above coincides with the usual Shafarevich–Tate group of B (here we assume finiteness of the latter, or just take the quotient by its maximal divisible subgroup). To see this one uses [BK], 3.11 for $\ell = p$. For $\ell \neq p$, $H^1_f(\mathbb{Q}_p, V_\ell) = 0$. Considering the formal group, we can represent every class in $B(\mathbb{Q}_p)/\ell B(\mathbb{Q}_p)$ by an ℓ-power torsion point in $B(\mathbb{Q}_p)$, so that it maps to zero in $H^1(\mathbb{Q}_p, A_\ell)$.

Define the group of global torsion points

$$\Gamma_{\mathbb{Q}} = \bigoplus_\lambda H^0(\mathbb{Q}, A_\lambda(k/2)).$$

This is analogous to the group of rational torsion points on an elliptic curve. Define an ideal $\#\Gamma_{\mathbb{Q}}$ of O_E, in which the exponent of any prime ideal λ is the length of the λ-component of $\Gamma_{\mathbb{Q}}$.

3 Canonical periods

From now on, we assume for convenience that $N \geq 3$. We need to choose convenient O_E-lattices T_B and T_{dR} in the Betti and de Rham realisations V_B and V_{dR} of M_f. We do this in such a way that T_B and $T_{\mathrm{dR}} \otimes_{O_E} O_E[1/Nk!]$ agree respectively with the O_E-lattice $\mathfrak{M}_{f,B}$ and the $O_E[1/Nk!]$-lattice $\mathfrak{M}_{f,\mathrm{dR}}$ defined in [DFG1] using cohomology, with nonconstant coefficients, of modular curves. (See especially [DFG1], Sections 2.2 and 5.4, and the paragraph preceding Lemma 2.3.)

For any finite prime λ of O_E, define the O_λ module T_λ inside V_λ to be the image of $T_B \otimes O_\lambda$ under the natural isomorphism $V_B \otimes E_\lambda \simeq V_\lambda$. Then the O_λ-module T_λ is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable.

Let $M(N)$ be the modular curve over $\mathbb{Z}[1/N]$ parametrising generalised elliptic curves with full level-N structure. Let $\mathfrak{E}$ be the universal generalised elliptic curve over $M(N)$. Let $\mathfrak{E}^{k-2}$ be the $(k-2)$-fold fibre product of $\mathfrak{E}$ over $M(N)$. (The motive M_f is constructed using a projector on the cohomology of a desingularisation of $\mathfrak{E}^{k-2}$). We realise $M(N)(\mathbb{C})$ as the disjoint union of $\varphi(N)$ copies of the quotient $\Gamma(N)\backslash\mathfrak{H}^*$ (where $\mathfrak{H}^*$ is the completed upper half plane), and let τ be a variable on $\mathfrak{H}$, so that the fibre $\mathfrak{E}_\tau$ is isomorphic to the elliptic curve with period lattice generated by 1 and τ. Let $z_i \in \mathbb{C}/\langle 1, \tau\rangle$ be a variable on the ith copy of $\mathfrak{E}_\tau$ in the fibre product. Then $2\pi i f(\tau)\, d\tau \wedge dz_1 \wedge \cdots \wedge dz_{k-2}$ is a well-defined differential form on (a desingularisation of) $\mathfrak{E}^{k-2}$ and naturally represents a generating element of $F^{k-1}T_{\mathrm{dR}}$. (At least, we can make our choices locally at primes dividing $Nk!$ so that this is the case.) We shall call this element $e(f)$.

Under the de Rham isomorphism between $V_{\mathrm{dR}} \otimes \mathbb{C}$ and $V_B \otimes \mathbb{C}$, $e(f)$ maps to some element ω_f. There is a natural action of complex conjugation on V_B, breaking it up into one-dimensional E-vector spaces V_B^+ and V_B^-. Let ω_f^+ and ω_f^- be the projections of ω_f to $V_B^+ \otimes \mathbb{C}$ and $V_B^- \otimes \mathbb{C}$ respectively. Let $T_B^\pm$ be the intersections of $V_B^\pm$ with T_B. These are rank one O_E-modules, but not necessarily free, since the class number of O_E may be greater than one. Choose nonzero elements $\delta_f^\pm$ of $T_B^\pm$ and let $\mathfrak{a}^\pm$ be the ideals $[T_B^\pm : O_E\delta_f^\pm]$. Define complex numbers $\Omega_f^\pm$ by $\omega_f^\pm = \Omega_f^\pm \delta_f^\pm$.

4 The Bloch–Kato conjecture

In this section we extract from the Bloch–Kato conjecture for $L(f, k/2)$ a prediction about the order of the Shafarevich–Tate group, by analysing the other terms in the formula.

Let $L(f, s)$ be the L-function attached to f. For $\Re(s) > \frac{k+1}{2}$ it is defined by the Dirichlet series with Euler product $\sum_{n=1}^\infty a_n n^{-s} = \prod_p (P_p(p^{-s}))^{-1}$, but there is an analytic continuation given by an integral, as described in the next section. Suppose that $L(f, k/2) \neq 0$. The Bloch–Kato conjecture for the motive $M_f(k/2)$ predicts the following equality of fractional ideals of E:

$$\frac{L(f, k/2)}{\mathrm{vol}_\infty} = \left(\prod_p c_p(k/2)\right) \frac{\#\text{Ш}}{\mathfrak{a}^\pm (\#\Gamma_\mathbb{Q})^2}.$$

Here, **and from this point onwards,** $\pm$ represents the parity of $(k/2) - 1$. The quantity vol_∞ is equal to $(2\pi i)^{k/2}$ multiplied by the determinant of the isomorphism $V_B^\pm \otimes \mathbb{C} \simeq (V_{\mathrm{dR}}/F^{k/2}) \otimes \mathbb{C}$, calculated with respect to the lattices

$O_E\delta_f^{\pm}$ and the image of T_{dR}. For $l \neq p$, $\mathrm{ord}_\lambda(c_p(j))$ is defined to be

$$\begin{aligned}&\mathrm{length}\, H^1_f(\mathbb{Q}_p, T_\lambda(j))_{\mathrm{tors}} - \mathrm{ord}_\lambda(P_p(p^{-j}))\\ &\qquad = \mathrm{length}\left(H^0(\mathbb{Q}_p, A_\lambda(j))/H^0\left(\mathbb{Q}_p, V_\lambda(j)^{I_p}/T_\lambda(j)^{I_p}\right)\right).\end{aligned}$$

We omit the definition of $\mathrm{ord}_\lambda(c_p(j))$ for $\lambda \mid p$, which requires one to assume Fontaine's de Rham conjecture ([Fo1], Appendix A6), and depends on the choices of T_{dR} and T_B, locally at λ. (We shall mainly be concerned with the q-part of the Bloch–Kato conjecture, where q is a prime of good reduction. For such primes, the de Rham conjecture follows from Faltings [Fa], Theorem 5.6.)

Strictly speaking, the conjecture in [BK] is only given for $E = \mathbb{Q}$. We have taken here the obvious generalisation of a slight rearrangement of [BK], (5.15.1). The Bloch–Kato conjecture has been reformulated and generalised by Fontaine and Perrin-Riou, who work with general E, though that is not really the point of their work. [Fo2], Section 11 sketches how to deduce the original conjecture from theirs, in the case $E = \mathbb{Q}$.

Lemma 4.1 $\mathrm{vol}_\infty/\mathfrak{a}^{\pm} = c(2\pi i)^{k/2}\mathfrak{a}^{\pm}\Omega_{\pm}$, *with* $c \in E$ *and* $\mathrm{ord}_\lambda(c) = 0$ *for* $\lambda \nmid Nk!$.

Proof We note that vol_∞ is equal to $(2\pi i)^{k/2}$ times the determinant of the period map from $F^{k/2}V_{\mathrm{dR}} \otimes \mathbb{C}$ to $V_B^{\pm} \otimes \mathbb{C}$, with respect to lattices dual to those we used above in the definition of vol_∞ (cf. [De2], last paragraph of 1.7). Here we are using natural pairings. Meanwhile, $\Omega_{\pm}$ is the determinant of the same map with respect to the lattices $F^{k/2}T_{\mathrm{dR}}$ and $O_E\delta_f^{\pm}$. Recall that the index of $O_E\delta_f^{\pm}$ in $T_B^{\pm}$ is the ideal $\mathfrak{a}^{\pm}$. Then the proof is completed by noting that, locally away from primes dividing $Nk!$, the index of T_{dR} in its dual is equal to the index of T_B in its dual, both being equal to the ideal denoted η in [DFG2]. □

Remark 4.2 Note that the "quantities" $\mathfrak{a}^{\pm}\Omega_{\pm}$ and $\mathrm{vol}_\infty/\mathfrak{a}^{\pm}$ are independent of the choice of $\delta_f^{\pm}$.

Lemma 4.3 *Let* $p \nmid N$ *be a prime and* j *an integer. Then the fractional ideal* $c_p(j)$ *is supported at most on divisors of* p.

Proof As on [Fl2], p. 30, for odd $l \neq p$, $\mathrm{ord}_\lambda(c_p(j))$ is the length of the finite O_λ-module $H^0(\mathbb{Q}_p, H^1(I_p, T_\lambda(j))_{\mathrm{tors}})$, where I_p is an inertia group at p. But $T_\lambda(j)$ is a trivial I_p-module, so $H^1(I_p, T_\lambda(j))$ is torsion free. □

Lemma 4.4 *Let $q \nmid N$ be a prime satisfying $q > k$. Suppose that $A[\mathfrak{q}]$ is an irreducible representation of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*, where $\mathfrak{q} \mid q$. Let $p \mid N$ be a prime, and if $p^2 \mid N$ suppose that $p \not\equiv \pm 1 \pmod{q}$. Suppose also that f is not congruent modulo $\mathfrak{q}$ (for Fourier coefficients of index coprime to Nq) to any newform of weight k, trivial character, and level dividing N/p. Then* $\mathrm{ord}_{\mathfrak{q}}(c_p(j)) = 0$ *for all integers j.*

Proof There is a natural injective map from $V_{\mathfrak{q}}(j)^{I_p}/T_{\mathfrak{q}}(j)^{I_p}$ to $H^0(I_p, A_{\mathfrak{q}}(j))$ (i.e., $A_{\mathfrak{q}}(j)^{I_p}$). Consideration of $\mathfrak{q}$-torsion shows that

$$\dim_{O_E/\mathfrak{q}} H^0(I_p, A[\mathfrak{q}](j)) \geq \dim_{E_{\mathfrak{q}}} H^0(I_p, V_{\mathfrak{q}}(j)).$$

To prove the lemma it suffices to show that

$$\dim_{O_E/\mathfrak{q}} H^0(I_p, A[\mathfrak{q}](j)) = \dim_{E_{\mathfrak{q}}} H^0(I_p, V_{\mathfrak{q}}(j)),$$

since this ensures that $H^0(I_p, A_{\mathfrak{q}}(j)) = V_{\mathfrak{q}}(j)^{I_p}/T_{\mathfrak{q}}(j)^{I_p}$, and therefore that $H^0(\mathbb{Q}_p, A_{\mathfrak{q}}(j)) = H^0(\mathbb{Q}_p, V_{\mathfrak{q}}(j)^{I_p}/T_{\mathfrak{q}}(j)^{I_p})$.

Suppose that Condition (b) of [L], Proposition 2.3 is not satisfied. Then there exists a character $\chi\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to O_{\mathfrak{q}}^{\times}$ of q-power order such that the p-part of the conductor of $V_{\mathfrak{q}} \otimes \chi$ is strictly smaller than that of $V_{\mathfrak{q}}$. Let f_χ denote the *newform*, of level dividing N/p, associated with $V_{\mathfrak{q}} \otimes \chi$. The character of f_χ has conductor at worst p. Since χ has conductor p and q-power order, $p \equiv 1 \pmod{q}$, so by hypothesis $p^2 \nmid N$. Hence f_χ has level coprime to p and must have trivial character. Then the existence of f_χ contradicts our hypotheses.

Suppose now that

$$\dim_{O_E/\mathfrak{q}} H^0(I_p, A[\mathfrak{q}](j)) > \dim_{E_{\mathfrak{q}}} H^0(I_p, V_{\mathfrak{q}}(j)),$$

(if not, there is nothing to prove). If Condition (a) of [L], Proposition 2.3 were not satisfied then [L], Proposition 2.2 would imply the existence of an impossible twist, as in the previous paragraph. (Here we are also using [L], Proposition 1.1.)

Since Condition (c) is clearly also satisfied, we are in a situation covered by one of the three cases in [L], Proposition 2.3. Since $p \not\equiv -1 \pmod{q}$ if $p^2 \mid N$, Case 3 is excluded, so $A[\mathfrak{q}](j)$ is unramified at p and $\mathrm{ord}_p(N) = 1$. (Here we are using Carayol's result that N is the prime-to-q part of the conductor of $V_{\mathfrak{q}}$ [Ca1].) But then [JL], Theorem 1 (which uses the condition $q > k$) implies the existence of a newform of weight k, trivial character and level dividing N/p, congruent to g modulo $\mathfrak{q}$, for Fourier coefficients of index coprime to Nq. This contradicts our hypotheses. □

Remark 4.5 For an example of what can be done when f is congruent to a form of lower level, see the first example in Section 7.4 below.

Lemma 4.6 *If $\mathfrak{q} \mid q$ is a prime of E such that $q \nmid Nk!$, then* $\mathrm{ord}_{\mathfrak{q}}(c_q) = 0$.

Proof It follows from [DFG1], Lemma 5.7 (whose proof relies on an application, at the end of Section 2.2, of the results of [Fa]) that $T_{\mathfrak{q}}$ is the $O_{\mathfrak{q}}[\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)]$-module associated to the filtered module $T_{\mathrm{dR}} \otimes O_{\mathfrak{q}}$ by the functor they call $\mathbb{V}$. (This property is part of the definition of an S-integral premotivic structure given in [DFG1], Section 1.2.) Given this, the lemma follows from [BK], Theorem 4.1(iii). (That $\mathbb{V}$ is the same as the functor used in [BK], Theorem 4.1 follows from [Fa], first paragraph of 2(h).) □

Lemma 4.7 *If* $A[\lambda]$ *is an irreducible representation of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*, then*

$$\mathrm{ord}_\lambda(\#\Gamma_{\mathbb{Q}}) = 0.$$

Proof This follows trivially from the definition. □

Putting together the above lemmas we arrive at the following:

Proposition 4.8 *Let* $q \nmid N$ *be a prime satisfying* $q > k$ *and suppose that* $A[\mathfrak{q}]$ *is an irreducible representation of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*, where* $\mathfrak{q} \mid q$*. Assume the same hypotheses as in Lemma 4.4 for all* $p \mid N$*. Choose* T_{dR} *and* T_B *which locally at* $\mathfrak{q}$ *are as in the previous section. If* $L(f, k/2)\mathfrak{a}^{\pm}/\mathrm{vol}_\infty \neq 0$ *then the Bloch–Kato conjecture predicts that*

$$\mathrm{ord}_{\mathfrak{q}}(\#\text{Ш}) = \mathrm{ord}_{\mathfrak{q}}(L(f, k/2)\mathfrak{a}^{\pm}/\mathrm{vol}_\infty).$$

5 Congruences of special values

Let $f = \sum a_n q^n$ and $g = \sum b_n q^n$ be newforms of equal weight $k \geq 2$ for $\Gamma_0(N)$. Let E be a number field large enough to contain all the coefficients a_n and b_n. Suppose that $\mathfrak{q} \mid q$ is a prime of E such that $f \equiv g \pmod{\mathfrak{q}}$, i.e. $a_n \equiv b_n \pmod{\mathfrak{q}}$ for all n. Assume that $A[\mathfrak{q}]$ is an irreducible representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and that $q \nmid N\varphi(N)k!$. Choose $\delta_f^{\pm} \in T_B^{\pm}$ in such a way that $\mathrm{ord}_{\mathfrak{q}}(\mathfrak{a}^{\pm}) = 0$, i.e., $\delta_f^{\pm}$ generates $T_B^{\pm}$ locally at $\mathfrak{q}$. Make two further assumptions:

$$L(f, k/2) \neq 0 \qquad \text{and} \qquad L(g, k/2) = 0.$$

Proposition 5.1 *With assumptions as above,* $\mathrm{ord}_{\mathfrak{q}}(L(f, k/2)/\mathrm{vol}_\infty) > 0$.

Proof This is based on some of the ideas used in [V], Section 1. Note the apparent typographical error in [V], Theorem 1.13 which should presumably refer to "Condition 2". Since $\mathrm{ord}_{\mathfrak{q}}(\mathfrak{a}^{\pm}) = 0$, we just need to show that $\mathrm{ord}_{\mathfrak{q}}\big(L(f, k/2)/((2\pi i)^{k/2}\Omega_{\pm})\big) > 0$, where $\pm 1 = (-1)^{(k/2)-1}$. It is well known, and easy to prove, that

$$\int_0^\infty f(iy)y^{s-1}dy = (2\pi)^{-s}\Gamma(s)L(f, s).$$

Hence, if for $0 \leq j \leq k-2$ we define the jth period

$$r_j(f) = \int_0^{i\infty} f(z) z^j \, dz,$$

where the integral is taken along the positive imaginary axis, then

$$r_j(f) = j!(-2\pi i)^{-(j+1)} L_f(j+1).$$

Thus we are reduced to showing that $\mathrm{ord}_{\mathfrak{q}}(r_{(k/2)-1}(f)/\Omega_{\pm}) > 0$.

Let $\mathcal{D}_0$ be the group of divisors of degree zero supported on $\mathbb{P}^1(\mathbb{Q})$. For a $\mathbb{Z}$-algebra R and integer $r \geq 0$, let $P_r(R)$ be the additive group of homogeneous polynomials of degree r in $R[X,Y]$. Both these groups have a natural action of $\Gamma_1(N)$. Let $S_{\Gamma_1(N)}(k,R) := \mathrm{Hom}_{\Gamma_1(N)}(\mathcal{D}_0, P_{k-2}(R))$ be the R-module of weight k modular symbols for $\Gamma_1(N)$.

Via the isomorphism (8) of [V], Section 1.5 combined with the argument of [V], 1.7, the cohomology class $\omega_f^{\pm}$ corresponds to a modular symbol $\Phi_f^{\pm} \in S_{\Gamma_1(N)}(k,\mathbb{C})$, and $\delta_f^{\pm}$ corresponds to an element $\Delta_f^{\pm} \in S_{\Gamma_1(N)}(k, O_{E,\mathfrak{q}})$. We are now dealing with cohomology over $X_1(N)$ rather than $M(N)$, which is why we insist that $q \nmid \varphi(N)$. It follows from the last line of [St], Section 4.2 that, up to some small factorials which do not matter locally at $\mathfrak{q}$,

$$\Phi_f^{\pm}([\infty]-[0]) = \sum_{\substack{j=0,\\ j \equiv (k/2)-1 \pmod 2}}^{k-2} r_f(j) X^j Y^{k-2-j}.$$

Since $\omega_f^{\pm} = \Omega_f^{\pm}\delta_f^{\pm}$, we see that

$$\Delta_f^{\pm}([\infty]-[0]) = \sum_{\substack{j=0,\\ j \equiv (k/2)-1 \pmod 2}}^{k-2} (r_f(j)/\Omega_f^{\pm}) X^j Y^{k-2-j}.$$

The coefficient of $X^{(k/2)-1}Y^{(k/2)-1}$ is what we would like to show is divisible by $\mathfrak{q}$. Similarly

$$\Phi_g^{\pm}([\infty]-[0]) = \sum_{\substack{j=0,\\ j \equiv (k/2)-1 \pmod 2}}^{k-2} r_g(j) X^j Y^{k-2-j}.$$

The coefficient of $X^{(k/2)-1}Y^{(k/2)-1}$ in this is 0, since $L(g,k/2)=0$. Therefore it would suffice to show that, for some $\mu \in O_E$, the element $\Delta_f^{\pm} - \mu\Delta_g^{\pm}$ is divisible by $\mathfrak{q}$ in $S_{\Gamma_1(N)}(k, O_{E,\mathfrak{q}})$. It suffices to show that, for some $\mu \in O_E$, the element $\delta_f^{\pm} - \mu\delta_g^{\pm}$ is divisible by $\mathfrak{q}$, considered as an element of $\mathfrak{q}$-adic cohomology of $X_1(N)$ with nonconstant coefficients. This would be the case if $\delta_f^{\pm}$ and $\delta_g^{\pm}$ generate the same one-dimensional subspace upon reduction modulo $\mathfrak{q}$. But this is a consequence of [FJ], Theorem 2.1(1) (for which we need the irreducibility of $A[\mathfrak{q}]$). $\square$

Remark 5.2 The signs in the functional equations of $L(f,s)$ and $L(g,s)$ are equal. They are determined by the eigenvalue of the Atkin–Lehner involution W_N, which is determined by a_N and b_N modulo $\mathfrak{q}$, because a_N and b_N are each $N^{k/2-1}$ times this sign and $\mathfrak{q}$ has residue characteristic coprime to $2N$. The common sign in the functional equation is $(-1)^{k/2}w_N$, where w_N is the common eigenvalue of W_N acting on f and g.

This is analogous to [CM1], remark at the end of Section 3, which shows that if $\mathfrak{q}$ has odd residue characteristic and $L(f,k/2) \neq 0$ but $L(g,k/2) = 0$ then $L(g,s)$ must vanish to order at least two at $s = k/2$. Note that Maeda's conjecture implies that there are no examples of g of level one with positive sign in their functional equation such that $L(g,k/2) = 0$ (see [CF]).

6 Constructing elements of the Shafarevich–Tate group

Let f, g and $\mathfrak{q}$ be as in the first paragraph of the previous section. In the previous section we showed how the congruence between f and g relates the vanishing of $L(g,k/2)$ to the divisibility by $\mathfrak{q}$ of an "algebraic part" of $L(f,k/2)$. Conjecturally the former is associated with the existence of certain algebraic cycles (for M_g) while the latter is associated with the existence of certain elements of the Shafarevich–Tate group (for M_f, as we saw in §4). In this section we show how the congruence, interpreted in terms of Galois representations, provides a direct link between algebraic cycles and the Shafarevich–Tate group.

For f we have defined V_λ, T_λ and A_λ. Let V'_λ, T'_λ and A'_λ be the corresponding objects for g. Since a_p is the trace of Frob_p^{-1} on V_λ, it follows from the Chebotarev Density Theorem that $A[\mathfrak{q}]$ and $A'[\mathfrak{q}]$, if irreducible, are isomorphic as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules.

Recall that $L(g,k/2) = 0$ and $L(f,k/2) \neq 0$. Since the sign in the functional equation for $L(g,s)$ is positive (this follows from $L(f,k/2) \neq 0$, see Remark 5.2), the order of vanishing of $L(g,s)$ at $s = k/2$ is at least 2. According to the Beilinson–Bloch conjecture [B, Be], the order of vanishing of $L(g,s)$ at $s = k/2$ is the rank of the group $\mathrm{CH}_0^{k/2}(M_g)(\mathbb{Q})$ of $\mathbb{Q}$-rational rational equivalence classes of null-homologous, algebraic cycles of codimension $k/2$ on the motive M_g. (This generalises the part of the Birch–Swinnerton-Dyer conjecture which says that for an elliptic curve $E/\mathbb{Q}$, the order of vanishing of $L(E,s)$ at $s=1$ is equal to the rank of the Mordell-Weil group $E(\mathbb{Q})$.)

Via the $\mathfrak{q}$-adic Abel–Jacobi map, $\mathrm{CH}_0^{k/2}(M_g)(\mathbb{Q})$ maps to $H^1(\mathbb{Q}, V_\mathfrak{q}'(k/2))$, and its image is contained in the subspace $H^1_f(\mathbb{Q}, V_\mathfrak{q}'(k/2))$, by [Ne], 3.1 and 3.2. If, as expected, the $\mathfrak{q}$-adic Abel–Jacobi map is injective, we get (assuming also the Beilinson–Bloch conjecture) a subspace of $H^1_f(\mathbb{Q}, V_\mathfrak{q}'(k/2))$ of dimension equal to the order of vanishing of $L(g,s)$ at $s=k/2$. In fact, one could simply conjecture that the dimension of $H^1_f(\mathbb{Q}, V_\mathfrak{q}'(k/2))$ is equal to the order of vanishing of $L(g,s)$ at $s=k/2$. This would follow from the "conjectures" $C_r(M)$ and $C^i_\lambda(M)$ of [Fo2], Sections 1 and 6.5. We shall call it the "strong" Beilinson–Bloch conjecture.

Similarly, if $L(f,k/2) \neq 0$ then we expect that $H^1_f(\mathbb{Q}, V_\mathfrak{q}(k/2)) = 0$, so that $H^1_f(\mathbb{Q}, A_\mathfrak{q}(k/2))$ coincides with the $\mathfrak{q}$-part of Ш.

Theorem 6.1 *Let $q \nmid N$ be a prime satisfying $q > k$. Let r be the dimension of $H^1_f(\mathbb{Q}, V_\mathfrak{q}'(k/2))$. Suppose that $A[\mathfrak{q}]$ is an irreducible representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and that for no prime $p \mid N$ is f congruent modulo $\mathfrak{q}$ (for Fourier coefficients of index coprime to Nq) to a newform of weight k, trivial character and level dividing N/p. Suppose that, for all primes $p \mid N$, $p \not\equiv -w_p \pmod{q}$, with $p \not\equiv \pm 1 \pmod{q}$ if $p^2 \mid N$. (Here w_p is the common eigenvalue of the Atkin–Lehner involution W_p acting on f and g.) Then the $\mathfrak{q}$-torsion subgroup of $H^1_f(\mathbb{Q}, A_\mathfrak{q}(k/2))$ has $\mathbb{F}_\mathfrak{q}$-rank at least r.*

Proof The theorem is trivially true if $r=0$, so we assume that $r > 0$. It follows easily from our hypothesis that the rank of the free part of $H^1_f(\mathbb{Q}, T_\mathfrak{q}'(k/2))$ is r. The natural map from $H^1_f(\mathbb{Q}, T_\mathfrak{q}'(k/2))/\mathfrak{q}H^1_f(\mathbb{Q}, T_\mathfrak{q}'(k/2))$ to $H^1(\mathbb{Q}, A'[\mathfrak{q}](k/2))$ is injective. Take a nonzero class c in the image, which has $\mathbb{F}_\mathfrak{q}$-rank r. Choose $d \in H^1_f(\mathbb{Q}, T_\mathfrak{q}'(k/2))$ mapping to c. Consider the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-cohomology of the short exact sequence

$$0 \to A[\mathfrak{q}](k/2) \to A_\mathfrak{q}(k/2) \xrightarrow{\pi} A_\mathfrak{q}(k/2) \to 0,$$

where π is multiplication by a uniformising element of $O_\mathfrak{q}$. By irreducibility, $H^0(\mathbb{Q}, A[\mathfrak{q}](k/2))$ is trivial. Hence $H^0(\mathbb{Q}, A_\mathfrak{q}(k/2))$ is trivial, so that $H^1(\mathbb{Q}, A[\mathfrak{q}](k/2))$ injects into $H^1(\mathbb{Q}, A_\mathfrak{q}(k/2))$, and we get a nonzero $\mathfrak{q}$-torsion class $\gamma \in H^1(\mathbb{Q}, A_\mathfrak{q}(k/2))$.

Our aim is to show that $\mathrm{res}_p(\gamma) \in H^1_f(\mathbb{Q}_p, A_\mathfrak{q}(k/2))$, for all (finite) primes p. We consider separately the cases $p \nmid qN$, $p \mid N$ and $p = q$.

Case 1, $p \nmid qN$:

Consider the I_p-cohomology of the short exact sequence

$$0 \to A'[\mathfrak{q}](k/2) \to A_\mathfrak{q}'(k/2) \xrightarrow{\pi} A_\mathfrak{q}'(k/2) \to 0$$

(the analogue for g of the above).

Since in this case $A'_{\mathfrak{q}}(k/2)$ is unramified at p, $H^0(I_p, A'_{\mathfrak{q}}(k/2)) = A'_{\mathfrak{q}}(k/2)$, which is $\mathfrak{q}$-divisible. Therefore $H^1(I_p, A'[\mathfrak{q}](k/2))$ (which, remember, is the same as $H^1(I_p, A[\mathfrak{q}](k/2)))$ injects into $H^1(I_p, A'_{\mathfrak{q}}(k/2))$. It follows from the fact that $d \in H^1_f(\mathbb{Q}, T'_{\mathfrak{q}}(k/2))$ that the image in $H^1(I_p, A'_{\mathfrak{q}}(k/2))$ of the restriction of c is zero, hence that the restriction of c to $H^1(I_p, A'[\mathfrak{q}](k/2)) \simeq H^1(I_p, A[\mathfrak{q}](k/2))$ is zero. Hence the restriction of γ to $H^1(I_p, A_{\mathfrak{q}}(k/2))$ is also zero. By [Fl1], line 3 of p. 125, $H^1_f(\mathbb{Q}_p, A_{\mathfrak{q}}(k/2))$ is equal to (not just contained in) the kernel of the map from $H^1(\mathbb{Q}_p, A_{\mathfrak{q}}(k/2))$ to $H^1(I_p, A_{\mathfrak{q}}(k/2))$, so we have shown that $\mathrm{res}_p(\gamma) \in H^1_f(\mathbb{Q}_p, A_{\mathfrak{q}}(k/2))$.

Case 2, $p \mid N$**:**

We first show that $H^0(I_p, A'_{\mathfrak{q}}(k/2))$ is $\mathfrak{q}$-divisible. It suffices to show that

$$\dim H^0(I_p, A'[\mathfrak{q}](k/2)) = \dim H^0(I_p, V'_{\mathfrak{q}}(k/2)),$$

since then the natural map from $H^0(I_p, V'_{\mathfrak{q}}(k/2))$ to $H^0(I_p, A'_{\mathfrak{q}}(k/2))$ is surjective; this may be done as in the proof of Lemma 4.4. It follows as above that the image of $c \in H^1(\mathbb{Q}, A[\mathfrak{q}](k/2))$ in $H^1(I_p, A[\mathfrak{q}](k/2))$ is zero. Then $\mathrm{res}_p(c)$ comes from $H^1(D_p/I_p, H^0(I_p, A[\mathfrak{q}](k/2)))$, by inflation-restriction. The order of this group is the same as the order of the group $H^0(\mathbb{Q}_p, A[\mathfrak{q}](k/2))$ (this is [W], Lemma 1), which we claim is trivial. By the work of Carayol [Ca1], the level N is the conductor of $V_{\mathfrak{q}}(k/2)$, so $p \mid N$ implies that $V_{\mathfrak{q}}(k/2)$ is ramified at p, hence $\dim H^0(I_p, V_{\mathfrak{q}}(k/2)) = 0$ or 1. As above, we see that $\dim H^0(I_p, V_{\mathfrak{q}}(k/2)) = \dim H^0(I_p, A[\mathfrak{q}](k/2))$, so we need only consider the case where this common dimension is 1. The (motivic) Euler factor at p for M_f is $(1 - \alpha p^{-s})^{-1}$, where Frob_p^{-1} acts as multiplication by α on the one-dimensional space $H^0(I_p, V_{\mathfrak{q}})$. It follows from [Ca1], Theoréme A that this is the same as the Euler factor at p of $L(f, s)$. By [AL], Theorems 3(ii) and 5, it then follows that $p^2 \nmid N$ and $\alpha = -w_p p^{(k/2)-1}$, where $w_p = \pm 1$ is such that $W_p f = w_p f$. We twist by $k/2$, so that Frob_p^{-1} acts on $H^0(I_p, V_{\mathfrak{q}}(k/2))$ (hence also on $H^0(I_p, A[\mathfrak{q}](k/2)))$ as $-w_p p^{-1}$. Since $p \not\equiv -w_p \pmod{q}$, we see that $H^0(\mathbb{Q}_p, A[\mathfrak{q}](k/2))$ is trivial. Hence $\mathrm{res}_p(c) = 0$ so $\mathrm{res}_p(\gamma) = 0$ and certainly lies in $H^1_f(\mathbb{Q}_p, A_{\mathfrak{q}}(k/2))$.

Case 3, $p = q$**:**

Since $q \nmid N$ is a prime of good reduction for the motive M_g, $V'_{\mathfrak{q}}$ is a crystalline representation of $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$, which means that $D_{\mathrm{cris}}(V'_{\mathfrak{q}})$ and $V'_{\mathfrak{q}}$ have the same dimension, where $D_{\mathrm{cris}}(V'_{\mathfrak{q}}) := H^0(\mathbb{Q}_q, V'_{\mathfrak{q}} \otimes_{\mathbb{Q}_q} B_{\mathrm{cris}})$. (This is a consequence of [Fa], Theorem 5.6.) As already noted in the proof of Lemma 4.6, $T_{\mathfrak{q}}$ is the $O_{\mathfrak{q}}[\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)]$-module associated to the filtered module $T_{\mathrm{dR}} \otimes O_{\mathfrak{q}}$.

Since also $q > k$, we may now prove, in the same manner as [Du1], Proposition 9.2, that $\mathrm{res}_q(\gamma) \in H^1_f(\mathbb{Q}_q, A_{\mathfrak{q}}(k/2))$. For the convenience of the reader, we give some details.

In [BK], Lemma 4.4, a cohomological functor $\{h^i\}_{i\geq 0}$ is constructed on the Fontaine–Lafaille category of filtered Dieudonné modules over $\mathbb{Z}_q$. $h^i(D) = 0$ for all $i \geq 2$ and all D, and $h^i(D) = \mathrm{Ext}^i(1_{FD}, D)$ for all i and D, where 1_{FD} is the "unit" filtered Dieudonné module.

Now let $D = T_{\mathrm{dR}} \otimes O_{\mathfrak{q}}$ and $D' = T'_{\mathrm{dR}} \otimes O_{\mathfrak{q}}$. By [BK], Lemma 4.5(c),

$$h^1(D) \simeq H^1_e(\mathbb{Q}_q, T_{\mathfrak{q}}),$$

where

$$H^1_e(\mathbb{Q}_q, T_{\mathfrak{q}}) = \ker(H^1(\mathbb{Q}_q, T_{\mathfrak{q}}) \to H^1(\mathbb{Q}_q, V_{\mathfrak{q}})/H^1_e(\mathbb{Q}_q, V_{\mathfrak{q}}))$$

and

$$H^1_e(\mathbb{Q}_q, V_{\mathfrak{q}}) = \ker(H^1(\mathbb{Q}_q, V_{\mathfrak{q}}) \to H^1(\mathbb{Q}_q, B^{f=1}_{\mathrm{cris}} \otimes_{\mathbb{Q}_q} V_{\mathfrak{q}})).$$

Likewise $h^1(D') \simeq H^1_e(\mathbb{Q}_q, T'_{\mathfrak{q}})$. When applying results of [BK] we view D, $T_{\mathfrak{q}}$ etc. simply as $\mathbb{Z}_q$-modules, forgetting the $O_{\mathfrak{q}}$-structure.

For an integer j, let $D(j)$ be D with the Hodge filtration shifted by j. Then

$$h^1(D(j)) \simeq H^1_e(\mathbb{Q}_q, T_{\mathfrak{q}}(j))$$

(provided that $k - p + 1 < j < p - 1$, so that $D(j)$ satisfies the hypotheses of [BK], Lemma 4.5). By [BK], Corollary 3.8.4,

$$H^1_f(\mathbb{Q}_q, V_{\mathfrak{q}}(j))/H^1_e(\mathbb{Q}_q, V_{\mathfrak{q}}(j)) \simeq (D(j) \otimes_{\mathbb{Z}_q} \mathbb{Q}_q)/(1 - f)(D(j) \otimes_{\mathbb{Z}_q} \mathbb{Q}_q),$$

where f is the Frobenius operator on crystalline cohomology. By Scholl [Sc], 1.2.4(ii), and the Weil conjectures, $H^1_e(\mathbb{Q}_q, V_{\mathfrak{q}}(j)) = H^1_f(\mathbb{Q}_q, V_{\mathfrak{q}}(j))$, since $j \neq (k-1)/2$. Similarly $H^1_e(\mathbb{Q}_q, V'_{\mathfrak{q}}(j)) = H^1_f(\mathbb{Q}_q, V'_{\mathfrak{q}}(j))$.

We have

$$h^1(D(k/2)) \simeq H^1_f(\mathbb{Q}_q, T_{\mathfrak{q}}(k/2)) \quad \text{and} \quad h^1(D'(k/2)) \simeq H^1_f(\mathbb{Q}_q, T'_{\mathfrak{q}}(k/2)).$$

The exact sequence in [BK], middle of p. 366, gives a commutative diagram

$$\begin{array}{ccccc}
h^1(D'(k/2)) & \xrightarrow{\pi} & h^1(D'(k/2)) & \longrightarrow & h^1(D'(k/2)/\mathfrak{q}D'(k/2)) \\
\downarrow & & \downarrow & & \downarrow \\
H^1(\mathbb{Q}_q, T'_{\mathfrak{q}}(k/2)) & \xrightarrow{\pi} & H^1(\mathbb{Q}_q, T'_{\mathfrak{q}}(k/2)) & \longrightarrow & H^1(\mathbb{Q}_q, A'[\mathfrak{q}](k/2)).
\end{array}$$

The vertical arrows are all inclusions, and we know the image of $h^1(D'(k/2))$ in $H^1(\mathbb{Q}_q, T'_{\mathfrak{q}}(k/2))$ is exactly $H^1_f(\mathbb{Q}_q, T'_{\mathfrak{q}}(k/2))$. The top right horizontal map is surjective since $h^2(D'(k/2)) = 0$.

The class $\mathrm{res}_q(c) \in H^1(\mathbb{Q}_q, A'[\mathfrak{q}](k/2))$ is in the image of $H^1_f(\mathbb{Q}_q, T'_{\mathfrak{q}}(k/2))$, by construction, and therefore is in the image of $h^1(D'(k/2)/\mathfrak{q}D'(k/2))$. By the fullness and exactness of the Fontaine–Lafaille functor [FL] (see [BK], Theorem 4.3), $D'(k/2)/\mathfrak{q}D'(k/2)$ is isomorphic to $D(k/2)/\mathfrak{q}D(k/2)$.

It follows that the class $\mathrm{res}_q(c) \in H^1(\mathbb{Q}_q, A[\mathfrak{q}](k/2))$ is in the image of $h^1(D(k/2)/\mathfrak{q}D(k/2))$ by the vertical map in the exact sequence analogous to the above. Since the map from $h^1(D(k/2))$ to $h^1(D(k/2)/\mathfrak{q}D(k/2))$ is surjective, $\mathrm{res}_q(c)$ lies in the image of $H^1_f(\mathbb{Q}_q, T_{\mathfrak{q}}(k/2))$. From this it follows that $\mathrm{res}_q(\gamma) \in H^1_f(\mathbb{Q}_q, A_{\mathfrak{q}}(k/2))$, as desired. □

[AS], Theorem 2.7 is concerned with verifying local conditions in the case $k = 2$, where f and g are associated with abelian varieties A and B. (Their theorem also applies to abelian varieties over number fields.) Our restriction outlawing congruences modulo $\mathfrak{q}$ with cusp forms of lower level is analogous to theirs forbidding q from dividing Tamagawa factors $c_{A,l}$ and $c_{B,l}$. (In the case where A is an elliptic curve with $\mathrm{ord}_l(j(A)) < 0$, consideration of a Tate parametrisation shows that if $q \mid c_{A,l}$, i.e., if $q \mid \mathrm{ord}_l(j(A))$, then it is possible that $A[q]$ is unramified at l.)

In this paper we have encountered two technical problems which we dealt with in quite similar ways:

1. dealing with the $\mathfrak{q}$-part of c_p for $p \mid N$;

2. proving local conditions at primes $p \mid N$, for an element of $\mathfrak{q}$-torsion.

If our only interest was in testing the Bloch–Kato conjecture at $\mathfrak{q}$, we could have made these problems cancel out, as in [DFG1], Lemma 8.11, by weakening the local conditions. However, we have chosen not to do so, since we are also interested in the Shafarevich–Tate group, and since the hypotheses we had to assume are not particularly strong. Note that, since $A[\mathfrak{q}]$ is irreducible, the $\mathfrak{q}$-part of Ш does not depend on the choice of $T_{\mathfrak{q}}$.

7 Examples and Experiments

This section contains tables and numerical examples illustrating the main themes of this paper. In Section 7.1, we explain Table 1, which contains 16 examples of pairs f, g such that the strong Beilinson–Bloch conjecture and Theorem 6.1 together imply the existence of nontrivial elements of the Shafarevich–Tate group of the motive attached to f. Section 7.2 outlines the higher-weight modular symbol computations used in making Table 1. Section 7.3 discusses Table 2, which summarizes the results of an extensive computation of conjectural orders of Shafarevich–Tate groups for modular motives of low level and weight. Section 7.4 gives specific examples in which various hypotheses fail.

Note that in §7 "modular symbol" has a different meaning from in §5, being related to homology rather than cohomology. For precise definitions see [SV].

7.1 Table 1: visible Ш

Table 1 lists sixteen pairs of newforms f and g (of equal weights and levels)

g	$\deg g$	f	$\deg f$	possible q
127k4A	1	**127k4C**	17	43
159k4B	1	**159k4E**	16	5, 23
365k4A	1	**365k4E**	18	29
369k4B	1	**369k4I**	9	13
453k4A	1	**453k4E**	23	17
465k4B	1	**465k4I**	7	11
477k4B	1	**477k4L**	12	73
567k4B	1	**567k4H**	8	23
581k4A	1	**581k4E**	34	19^2
657k4A	1	**657k4C**	7	5
657k4A	1	**657k4G**	12	5
681k4A	1	**681k4D**	30	59
684k4C	1	**684k4K**	4	7^2
95k6A	1	**95k6D**	9	31, 59
122k6A	1	**122k6D**	6	73
260k6A	1	**260k6E**	4	17

Table 1: Visible Ш

along with at least one prime q such that there is a prime $\mathfrak{q} \mid q$ with $f \equiv g \pmod{\mathfrak{q}}$. In each case, $\mathrm{ord}_{s=k/2} L(g, k/2) \geq 2$ while $L(f, k/2) \neq 0$. It uses the following notation: the first column contains a label whose structure is

[Level]k[Weight][GaloisOrbit]

This label determines a newform $g = \sum a_n q^n$ up to Galois conjugacy. For example, **127k4C** denotes a newform in the third Galois orbit of newforms in

$S_4(\Gamma_0(127))$. Galois orbits are ordered first by the degree of $\mathbb{Q}(\ldots, a_n, \ldots)$, then by the sequence of absolute values $|\mathrm{Tr}(a_p(g))|$ for p not dividing the level, with positive trace being first in the event that the two absolute values are equal, and the first Galois orbit is denoted **A**, the second **B**, and so on. The second column contains the degree of the field $\mathbb{Q}(\ldots, a_n, \ldots)$. The third and fourth columns contain f and its degree, respectively. The fifth column contains at least one prime q such that there is a prime $\mathfrak{q} \mid q$ with $f \equiv g \pmod{\mathfrak{q}}$, and such that the hypotheses of Theorem 6.1 are satisfied for f, g, and $\mathfrak{q}$.

For the two examples **581k4E** and **684k4K**, the square of a prime q appears in the q-column, which means that q^2 divides the order of the group $S_k(\Gamma_0(N), \mathbb{Z})/(W + W^{\perp})$ defined at the end of 7.3 below.

We describe the first line of Table 1 in more detail. The next section gives further details on how the computations were performed.

Using modular symbols, we find that there is a newform

$$g = q - q^2 - 8q^3 - 7q^4 - 15q^5 + 8q^6 - 25q^7 + \cdots \in S_4(\Gamma_0(127))$$

with $L(g, 2) = 0$. Because $W_{127}(g) = g$, the functional equation has sign $+1$, so $L'(g, 2) = 0$ as well. We also find a newform $f \in S_4(\Gamma_0(127))$ whose Fourier coefficients generate a number field K of degree 17, and by computing the image of the modular symbol $XY\{0, \infty\}$ under the period mapping, we find that $L(f, 2) \neq 0$. The newforms f and g are congruent modulo a prime $\mathfrak{q}$ of K of residue characteristic 43. The mod $\mathfrak{q}$ reductions of f and g are both equal to

$$\overline{f} = q + 42q^2 + 35q^3 + 36q^4 + 28q^5 + 8q^6 + 18q^7 + \cdots \in \mathbb{F}_{43}[[q]].$$

There is no form in the Eisenstein subspaces of $M_4(\Gamma_0(127))$ whose Fourier coefficients of index n, with $(n, 127) = 1$, are congruent modulo 43 to those of $\overline{f}$, so $\rho_{f,\mathfrak{q}} \approx \rho_{g,\mathfrak{q}}$ is irreducible. Since 127 is prime and $S_4(\mathrm{SL}_2(\mathbb{Z})) = 0$, $\overline{f}$ does not arise from a level 1 form of weight 4. Thus we have checked the hypotheses of Theorem 6.1, so if r is the dimension of $H^1_f(\mathbb{Q}, V'_{\mathfrak{q}}(k/2))$ then the $\mathfrak{q}$-torsion subgroup of $H^1_f(\mathbb{Q}, A_{\mathfrak{q}}(k/2))$ has $\mathbb{F}_{\mathfrak{q}}$-rank at least r.

Recall that since $\mathrm{ord}_{s=k/2} L(g, s) \geq 2$, we expect that $r \geq 2$. Then, since $L(f, k/2) \neq 0$, we expect that the $\mathfrak{q}$-torsion subgroup of $H^1_f(\mathbb{Q}, A_{\mathfrak{q}}(k/2))$ is equal to the $\mathfrak{q}$-torsion subgroup of Ш. Admitting these assumptions, we have constructed the $\mathfrak{q}$-torsion in Ш predicted by the Bloch–Kato conjecture.

For particular examples of elliptic curves one can often find and write down rational points predicted by the Birch and Swinnerton-Dyer conjecture. It would be nice if likewise one could explicitly produce algebraic cycles predicted by the Beilinson–Bloch conjecture in the above examples. Since $L'(g, k/2) = 0$, Heegner cycles have height zero (see [Z], Corollary 0.3.2), so ought to be trivial in $\mathrm{CH}_0^{k/2}(M_g) \otimes \mathbb{Q}$.

7.2 How the computation was performed

We give a brief summary of how the computation was performed. The algorithms we used were implemented by the second author, and most are a standard part of MAGMA (see [BCP]).

Let g, f, and q be some data from a line of Table 1 and let N denote the level of g. We verified the existence of a congruence modulo q, that $L(g, k/2) = L'(g, k/2) = 0$ and $L(f, k/2) \neq 0$, and that $\rho_{f,\mathfrak{q}} = \rho_{g,\mathfrak{q}}$ is irreducible and does not arise from any $S_k(\Gamma_0(N/p))$, as follows:

To prove there is a congruence, we showed that the corresponding *integral* spaces of modular symbols satisfy an appropriate congruence, which forces the existence of a congruence on the level of Fourier expansions. We showed that $\rho_{g,\mathfrak{q}}$ is irreducible by computing a set that contains all possible residue characteristics of congruences between g and any Eisenstein series of level dividing N, where by congruence, we mean a congruence for all Fourier coefficients of index n with $(n, N) = 1$. Similarly, we checked that g is not congruent to any form h of level N/p for any p that exactly divides N by listing a basis of such h and finding the possible congruences, where again we disregard the Fourier coefficients of index not coprime to N.

To verify that $L(g, k/2) = 0$, we computed the image of the modular symbol $\mathbf{e} = X^{\frac{k}{2}-1}Y^{\frac{k}{2}-1}\{0, \infty\}$ under a map with the same kernel as the period mapping, and found that the image was 0. The period mapping sends the modular symbol $\mathbf{e}$ to a nonzero multiple of $L(g, \frac{k}{2})$, so that $\mathbf{e}$ maps to 0 implies that $L(g, k/2) = 0$. In a similar way, we verified that $L(f, k/2) \neq 0$. Next, we checked that $W_N(g) = (-1)^{k/2}g$ which, because of the functional equation, implies that $L'(g, k/2) = 0$. Table 1 is of independent interest because it includes examples of modular forms of even weight > 2 with a zero at $k/2$ that is not forced by the functional equation. We found no such examples of weights ≥ 8.

7.3 Conjecturally nontrivial Ш

In this section we apply some of the results of Section 4 to compute lower bounds on conjectural orders of Shafarevich–Tate groups of many modular motives. The results of this section suggest that Ш of a modular motive is usually "not visible at level N", that is, not explained by congruences at level N (compare with the observations of [CM1] and [AS]). For example, when $k > 6$ we find many examples of conjecturally nontrivial Ш but no examples of nontrivial visible Ш.

For any newform f, let $L(M_f/\mathbb{Q}, s) = \prod_{i=1}^{d} L(f^{(i)}, s)$ where $f^{(i)}$ runs over the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates of f. Let T be the complex torus $\mathbb{C}^d/(2\pi i)^{k/2}\mathcal{L}$, where $\mathcal{L}$ is the lattice defined by integrating integral cuspidal modular symbols for $\Gamma_0(N)$ against the conjugates of f. Let $\Omega_{M_f/\mathbb{Q}}$ denote the volume of the $(-1)^{(k/2)-1}$ eigenspace $T^{\pm} = \{z \in T : \overline{z} = (-1)^{(k/2)-1}z\}$ for complex conjugation on T.

Lemma 7.1 *Suppose that $p \nmid Nk!$ is such that f is not congruent to any of its Galois conjugates modulo a prime dividing p. Then the p-parts of*

$$\frac{L(M_f/\mathbb{Q}, k/2)}{\Omega_{M_f/\mathbb{Q}}} \qquad \textit{and} \qquad \mathrm{Norm}\left(\frac{L(f,k/2)}{\mathrm{vol}_\infty}\mathfrak{a}^{\pm}\right)$$

are equal, where vol_∞ *is as in Section 4.*

Proof Let H be the $\mathbb{Z}$-module of all integral cuspidal modular symbols for $\Gamma_0(N)$. Let I be the image of H under projection into the submodule of $H \otimes \mathbb{Q}$ corresponding to f and its Galois conjugates. Note that I is not necessarily contained in H, but it is contained in $H \otimes \mathbb{Z}[\frac{1}{m}]$ where m is divisible by the residue characteristics of any primes of congruence between f and cuspforms of weight k for $\Gamma_0(N)$ which are not Galois conjugate to f.

The lattice $\mathcal{L}$ defined before the lemma is obtained (up to divisors of $Nk!$) by pairing the cohomology modular symbols $\Phi^{\pm}_{f^{(i)}}$ (as in §5) with the homology modular symbols in H; equivalently, since the pairing factors through the map $H \to I$, the lattice $\mathcal{L}$ is obtained by pairing with the elements of I. For $1 \le i \le d$ let I_i be the O_E-module generated by the image of the projection of I into $I \otimes E$ corresponding to $f^{(i)}$. The finite index of $I \otimes O_E$ in $\bigoplus_{i=1}^{d} I_i$ is divisible only by primes of congruence between f and its Galois conjugates. Up to these primes, $\Omega_{M_f/\mathbb{Q}}/(2\pi i)^{((k/2)-1)d}$ is then a product of the d quantities obtained by pairing $\Phi^{\pm}_{f^{(i)}}$ with I_i, for $1 \le i \le d$. (These quantities inhabit a kind of tensor product of $\mathbb{C}^*$ over E^* with the group of fractional ideals of E.) Bearing in mind the last line of §3, we see that these quantities are the $\mathfrak{a}^{\pm}\Omega^{\pm}_{f^{(i)}}$, up to divisors of $Nk!$. Now we may apply Lemma 4.1. We then have a factorisation of the left hand side which shows it to be equal to the right hand side, to the extent claimed by the lemma. Note that $\frac{L(f,k/2)}{\mathrm{vol}_\infty}\mathfrak{a}^{\pm}$ has an interpretation in terms of integral modular symbols, as in §5, and just gets Galois conjugated when one replaces f by some $f^{(i)}$. $\square$

Remark 7.2 The newform $f = \mathbf{319k4C}$ is congruent to one of its Galois conjugates modulo 17 and 17 divides $L(M_f/\mathbb{Q}, k/2)/\Omega_{M_f/\mathbb{Q}}$, so the lemma and our computations say nothing about whether 17 divides $\mathrm{Norm}\left(\frac{L(f,k/2)}{\mathrm{vol}_\infty}\mathfrak{a}^{\pm}\right)$ or otherwise.

Let $\mathcal{S}$ be the set of newforms with level N and weight k satisfying either $k = 4$ and $N \le 321$, or $k = 6$ and $N \le 199$, or $k = 8$ and $N \le 149$, or $k = 10$ and $N \le 72$, or $k = 12$ and $N \le 49$. Given $f \in \mathcal{S}$, let B be defined as follows:

1. Let L_1 be the numerator of the rational number $L(M_f/\mathbb{Q}, k/2)/\Omega_{M_f/\mathbb{Q}}$. If $L_1 = 0$ let $B = 1$ and terminate.

2. Let L_2 be the part of L_1 that is coprime to $Nk!$.

3. Let L_3 be the part of L_2 that is coprime to $p \pm 1$ for every prime p such that $p^2 \mid N$.

4. Let L_4 be the part of L_3 coprime to the residue characteristic of any prime of congruence between f and a form of weight k, trivial character and lower level. (By congruence here, we mean a congruence for coefficients a_n with n coprime to the level of f.)

5. Let L_5 be the part of L_4 coprime to the residue characteristic of any prime of congruence between f and an Eisenstein series. (This eliminates residue characteristics of reducible representations.)

6. Let B be the part of L_5 coprime to the residue characteristic of any prime of congruence between f and any one of its Galois conjugates.

Proposition 4.8 and Lemma 7.1 imply that if $\mathrm{ord}_p(B) > 0$ then, according to the Bloch–Kato conjecture, $\mathrm{ord}_p(\#\text{Ш}) = \mathrm{ord}_p(B) > 0$.

We computed B for every newform in $\mathcal{S}$. There are many examples in which L_3 is large, but B is not, and this is because of Tamagawa factors. For example, **39k4C** has $L_3 = 19$, but $B = 1$ because of a 19-congruence with a form of level 13; in this case we must have $19 \mid c_3(2)$, where $c_3(2)$ is as in Section 4. See Section 7.4 for more details. Also note that in every example B is a perfect square, which, away from congruence primes, is as predicted by the existence of Flach's generalised Cassels–Tate pairing [Fl1]. (Note that if $A[\lambda]$ is irreducible then the lattice T_λ is at worst a scalar multiple of its dual, so the pairing shows that the order of the λ-part of Ш, if finite, is a square.) That our computed value of B should be a square is not *a priori* obvious.

For simplicity, we discard residue characteristics instead of primes of rings of integers, so our definition of B is overly conservative. For example, 5 occurs in row 2 of Table 1 but not in Table 2, because **159k4E** is Eisenstein at some prime above 5, but the prime of congruences of characteristic 5 between **159k4B** and **159k4E** is not Eisenstein.

The newforms for which $B > 1$ are given in Table 2 on pp. 112–115. The second column of the table records the degree of the field generated by the Fourier coefficients of f. The third contains B. Let W be the intersection of the span of all conjugates of f with $S_k(\Gamma_0(N), \mathbb{Z})$ and $W^\perp$ the Petersson orthogonal complement of W in $S_k(\Gamma_0(N), \mathbb{Z})$. The fourth column contains the odd prime divisors of $\#(S_k(\Gamma_0(N), \mathbb{Z})/(W + W^\perp))$, which are exactly the possible primes of congruence between f and nonconjugate cusp forms of the same weight and level. We place a $*$ next to the four entries of Table 2 that also occur in Table 1.

7.4 Examples in which hypotheses fail

We have some other examples where forms of different levels are congruent (for Fourier coefficients of index coprime to the levels). However, Remark 5.2 does not apply, so that one of the forms could have an odd functional equation, and the other could have an even functional equation. For instance, we have a 19-congruence between the newforms $g =$ **13k4A** and $f =$ **39k4C** of Fourier coefficients of index coprime to 39. Here $L(f, 2) \neq 0$, while $L(g, 2) = 0$ since $L(g, s)$ has *odd* functional equation. Here f fails the condition about not being congruent to a form of lower level, so in Lemma 4.4 it is possible that $\mathrm{ord}_{\mathfrak{q}}(c_3(2)) > 0$. In fact this does happen. Because $V'_{\mathfrak{q}}$ (attached to g of level 13) is unramified at $p = 3$, $H^0(I_p, A[\mathfrak{q}])$ (the same as $H^0(I_p, A'[\mathfrak{q}])$) is two-dimensional. As in (2) of the proof of Theorem 6.1, one of the eigenvalues of Frob_p^{-1} acting on this two-dimensional space is $\alpha = -w_p p^{(k/2)-1}$, where $W_p f = w_p f$. The other must be $\beta = -w_p p^{k/2}$, so that $\alpha\beta = p^{k-1}$. Twisting by $k/2$, we see that Frob_p^{-1} acts as $-w_p$ on the quotient of $H^0(I_p, A[\mathfrak{q}](k/2))$ by the image of $H^0(I_p, V_{\mathfrak{q}}(k/2))$. Hence $\mathrm{ord}_{\mathfrak{q}}(c_p(k/2)) > 0$ when $w_p = -1$, which is the case in our example here with $p = 3$. Likewise $H^0(\mathbb{Q}_p, A[\mathfrak{q}](k/2))$ is nontrivial when $w_p = -1$, so (2) of the proof of Theorem 6.1 does not work. This is just as well, since had it worked we would have expected $\mathrm{ord}_{\mathfrak{q}}(L(f, k/2)/\mathrm{vol}_\infty) \geq 3$, which computation shows not to be the case.

In the following example, the divisibility between the levels is the other way round. There is a 7-congruence between $g =$ **122k6A** and $f =$ **61k6B**, both L-functions have even functional equation, and $L(g, 3) = 0$. In the proof of Theorem 6.1, there is a problem with the local condition at $p = 2$. The map from $H^1(I_2, A'[\mathfrak{q}](3))$ to $H^1(I_2, A'_{\mathfrak{q}}(3))$ is not necessarily injective, but its kernel is at most one dimensional, so we still get the $\mathfrak{q}$-torsion subgroup of $H^1_f(\mathbb{Q}, A_{\mathfrak{q}}(2))$ having $\mathbb{F}_{\mathfrak{q}}$-rank at least 1 (assuming $r \geq 2$), and thus get elements of Ш for **61k6B** (assuming all along the strong Beilinson–Bloch conjecture). In particular, these elements of Ш are *invisible* at level 61. When the levels are different we are no longer able to apply [FJ], Theorem 2.1. However, we still have the congruences of integral modular symbols required to make the proof of Proposition 5.1 go through. Indeed, as noted above, the congruences of modular forms were found by producing congruences of modular symbols. Despite these congruences of modular symbols, Remark 5.2 does not apply, since there is no reason to suppose that $w_N = w_{N'}$, where N and N' are the distinct levels.

Finally, there are two examples where we have a form g with even functional equation such that $L(g, k/2) = 0$, and a congruent form f which has odd functional equation; these are a 23-congruence between $g =$ **453k4A** and $f =$ **151k4A**, and a 43-congruence between $g =$ **681k4A** and $f =$ **227k4A**. If $\mathrm{ord}_{s=2} L(f,s) = 1$, it ought to be the case that $\dim(H^1_f(\mathbb{Q}, V_\mathfrak{q}(2))) = 1$. If we assume this is so, and similarly that $r = \mathrm{ord}_{s=2}(L(g,s)) \geq 2$, then unfortunately the appropriate modification of Theorem 6.1 (with strong Beilinson–Bloch conjecture) does not necessarily provide us with nontrivial $\mathfrak{q}$-torsion in Ш. It only tells us that the $\mathfrak{q}$-torsion subgroup of $H^1_f(\mathbb{Q}, A_\mathfrak{q}(2))$ has $\mathbb{F}_\mathfrak{q}$-rank at least 1. It could all be in the image of $H^1_f(\mathbb{Q}, V_\mathfrak{q}(2))$. Ш appears in the conjectural formula for the first derivative of the complex L function, evaluated at $s = k/2$, but in combination with a regulator that we have no way of calculating.

Let $L_q(f,s)$ and $L_q(g,s)$ be the q-adic L functions associated with f and g by the construction of Mazur, Tate and Teitelbaum [MTT], each divided by a suitable canonical period. We may show that $\mathfrak{q} \mid L_q'(f, k/2)$, though it is not quite clear what to make of this. This divisibility may be proved as follows. The measures $d\mu_{f,\alpha}$ and (a q-adic unit times) $d\mu_{g,\alpha'}$ in [MTT] (again, suitably normalised) are congruent $\bmod\, \mathfrak{q}$, as a result of the congruence between the modular symbols out of which they are constructed. Integrating an appropriate function against these measures, we find that $L_q'(f,k/2)$ is congruent $\bmod\, \mathfrak{q}$ to $L_q'(g,k/2)$. It remains to observe that $L_q'(g,k/2) = 0$, since $L(g,k/2) = 0$ forces $L_q(g,k/2) = 0$, but we are in a case where the signs in the functional equations of $L(g,s)$ and $L_q(g,s)$ are the same, positive in this instance. (According to the proposition in [MTT], Section 18, the signs differ precisely when $L_q(g,s)$ has a "trivial zero" at $s = k/2$.)

We also found some examples for which the conditions of Theorem 6.1 were not met. For example, we have a 7-congruence between **639k4B** and **639k4H**, but $w_{71} = -1$, so that $71 \equiv -w_{71} \pmod 7$. There is a similar problem with a 7-congruence between **260k6A** and **260k6E** — here $w_{13} = 1$ so that $13 \equiv -w_{13} \pmod 7$. According to Propositions 5.1 and 4.8, Bloch–Kato still predicts that the $\mathfrak{q}$-part of Ш is nontrivial in these examples. Finally, there is a 5-congruence between **116k6A** and **116k6D**, but here the prime 5 is less than the weight 6 so Propositions 5.1 and 4.8 (and even Lemma 7.1) do not apply.

f	$\deg f$	B (bound for Ш)	all odd congruence primes
127k4C$*$	17	43^2	43, 127
159k4E$*$	8	23^2	3, 5, 11, 23, 53, 13605689
263k4B	39	41^2	263
269k4C	39	23^2	269
271k4B	39	29^2	271
281k4B	40	29^2	281
295k4C	16	7^2	3, 5, 11, 59, 101, 659, 70791023
299k4C	20	29^2	13, 23, 103, 20063, 21961
321k4C	16	13^2	3, 5, 107, 157, 12782373452377
95k6D$*$	9	$31^2 \cdot 59^2$	3, 5, 17, 19, 31, 59, 113, 26701
101k6B	24	17^2	101
103k6B	24	23^2	103
111k6C	9	11^2	3, 37, 2796169609
122k6D$*$	6	73^2	3, 5, 61, 73, 1303196179
153k6G	5	7^2	3, 17, 61, 227
157k6B	34	251^2	157
167k6B	40	41^2	167
172k6B	9	7^2	3, 11, 43, 787
173k6B	39	71^2	173
181k6B	40	107^2	181
191k6B	46	85091^2	191
193k6B	41	31^2	193
199k6B	46	200329^2	199

f	$\deg f$	B (bound for Ш)	all odd congruence primes
47k8B	16	19^2	47
59k8B	20	29^2	59
67k8B	20	29^2	67
71k8B	24	379^2	71
73k8B	22	197^2	73
74k8C	6	23^2	37, 127, 821, 8327168869
79k8B	25	307^2	79
83k8B	27	1019^2	83
87k8C	9	11^2	3, 5, 7, 29, 31, 59, 947, 22877, 3549902897
89k8B	29	44491^2	89
97k8B	29	$11^2 \cdot 277^2$	97
101k8B	33	$19^2 \cdot 11503^2$	101
103k8B	32	75367^2	103
107k8B	34	$17^2 \cdot 491^2$	107
109k8B	33	$23^2 \cdot 229^2$	109
111k8C	12	127^2	3, 7, 11, 13, 17, 23, 37, 6451, 18583, 51162187
113k8B	35	$67^2 \cdot 641^2$	113
115k8B	12	37^2	3, 5, 19, 23, 572437, 5168196102449
117k8I	8	19^2	3, 13, 181
118k8C	8	37^2	5, 13, 17, 59, 163, 3923085859759909
119k8C	16	1283^2	3, 7, 13, 17, 109, 883, 5324191, 91528147213
121k8F	6	71^2	3, 11, 17, 41
121k8G	12	13^2	3, 11
121k8H	12	19^2	5, 11
125k8D	16	179^2	5
127k8B	39	59^2	127

f	$\deg f$	B (bound for Ш)	all odd congruence primes
128k8F	4	11^2	1
131k8B	43	$241^2 \cdot 817838201^2$	131
134k8C	11	61^2	11, 17, 41, 67, 71, 421, 2356138931854759
137k8B	42	$71^2 \cdot 749093^2$	137
139k8B	43	$47^2 \cdot 89^2 \cdot 1021^2$	139
141k8C	14	13^2	3, 5, 7, 47, 4639, 43831013, 4047347102598757
142k8B	10	11^2	3, 53, 71, 56377, 1965431024315921873
143k8C	19	307^2	3, 11, 13, 89, 199, 409, 178397, 639259, 17440535 97287
143k8D	21	109^2	3, 7, 11, 13, 61, 79, 103, 173, 241, 769, 36583
145k8C	17	29587^2	5, 11, 29, 107, 251623, 393577, 518737, 9837145 699
146k8C	12	3691^2	11, 73, 269, 503, 1673540153, 11374452082219
148k8B	11	19^2	3, 37
149k8B	47	$11^4 \cdot 40996789^2$	149
43k10B	17	449^2	43
47k10B	20	2213^2	47
53k10B	21	673^2	53
55k10D	9	71^2	3, 5, 11, 251, 317, 61339, 19869191
59k10B	25	37^2	59
62k10E	7	23^2	3, 31, 101, 523, 617, 41192083
64k10K	2	19^2	3
67k10B	26	$191^2 \cdot 617^2$	67
68k10B	7	83^2	3, 7, 17, 8311
71k10B	30	1103^2	71

f	$\deg f$	B (bound for Ш)	all odd congruence primes
19k12B	9	67^2	5, 17, 19, 31, 571
31k12B	15	$67^2 \cdot 71^2$	31, 13488901
35k12C	6	17^2	5, 7, 23, 29, 107, 8609, 1307051
39k12C	6	73^2	3, 13, 1491079, 3719832979693
41k12B	20	54347^2	7, 41, 3271, 6277
43k12B	20	212969^2	43, 1669, 483167
47k12B	23	24469^2	17, 47, 59, 2789
49k12H	12	271^2	7

Table 2: Conjecturally nontrivial Ш (mostly invisible)

References

[AL] A. O. L. Atkin, J. Lehner, Hecke operators on $\Gamma_0(m)$, *Math. Ann.* **185** (1970) 135–160

[AS] A. Agashe, W. Stein, Visibility of Shafarevich–Tate groups of abelian varieties, preprint

[BS-D] B. J. Birch, H. P. F. Swinnerton-Dyer, Notes on elliptic curves. I and II, *J. reine angew. Math.* **212** (1963) 7–25 and **218** (1965) 79–108

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

[BCP] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997) no. 3-4, 235–265, Computational algebra and number theory (London, 1993)

[Be] A. Beilinson, Height pairing between algebraic cycles, *in* Current trends in arithmetical algebraic geometry (K. Ribet, ed.) *Contemp. Math.* **67** (1987) 1–24

[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

[Ca1] H. Carayol, Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert, *Ann. Sci. École Norm. Sup. (4)***19** (1986) 409–468

[Ca2] H. Carayol, Sur les représentations Galoisiennes modulo ℓ attachées aux formes modulaires, *Duke Math. J.* **59** (1989) 785–801

[CM1] J. E. Cremona, B. Mazur, Visualizing elements in the Shafarevich–Tate group, *Experiment. Math.* **9** (2000) 13–28

[CM2] J. E. Cremona, B. Mazur, Appendix to A. Agashe, W. Stein, Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of rank zero, preprint

[CF] B. Conrey, D. Farmer, On the non-vanishing of $L_f(s)$ at the center of the critical strip, preprint

[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

[DFG1] F. Diamond, M. Flach, L. Guo, Adjoint motives of modular forms and the Tamagawa number conjecture, preprint available from: http://www.andromeda.rutgers.edu/∼liguo/lgpapers.html

[DFG2] F. Diamond, M. Flach, L. Guo, The Bloch–Kato conjecture for adjoint motives of modular forms, *Math. Res. Lett.* **8** (2001) 437–442

[Du1] N. Dummigan, Symmetric square L-functions and Shafarevich–Tate groups, *Experiment. Math.* **10** (2001) 383–400

[Du2] N. Dummigan, Congruences of modular forms and Selmer groups, *Math. Res. Lett.* **8** (2001) 479–494

[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

[FJ] G. Faltings, B. Jordan, Crystalline cohomology and $\mathrm{GL}(2, \mathbb{Q})$, *Israel J. Math.* **90** (1995) 1–66

[Fl1] M. Flach, A generalisation of the Cassels-Tate pairing, *J. reine angew. Math.* **412** (1990) 113–127

[Fl2] 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

[Fo1] 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

[Fo2] J.-M. Fontaine, Valeurs spéciales des fonctions L des motifs, Sém. Bourbaki, 1991/92, Exp. No. 751 *Astérisque* **206** (1992) 205–249

[FL] J.-M. Fontaine, G. Lafaille, Construction de représentations p-adiques, *Ann. Sci. E.N.S.* **15** (1982) 547–608

[JL] B. W. Jordan, R. Livné, Conjecture "epsilon" for weight $k > 2$, *Bull. Amer. Math. Soc.* **21** (1989) 51–56

[L] R. Livné, On the conductors of mod ℓ Galois representations coming from modular forms, *J. Number Theory* **31** (1989) 133–141

[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

[Ne] J. Nekovár, p-adic Abel–Jacobi maps and p-adic heights. The arithmetic and geometry of algebraic cycles (Banff, AB, 1998) 367–379, CRM Proc. Lecture Notes, 24, Amer. Math. Soc., Providence, RI, 2000

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

[SV] W. A. Stein, H. A. Verrill, Cuspidal modular symbols are transportable, *L.M.S. Journal of Computational Mathematics* **4** (2001) 170–181

[St] 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

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

[W] L. C. Washington, Galois cohomology, *in* Modular Forms and Fermat's Last Theorem, (G. Cornell, J. H. Silverman, G. Stevens, eds.) 101–120, Springer-Verlag, New York, 1997

[Z] S. Zhang, Heights of Heegner cycles and derivatives of L-series, *Invent. Math.* **130** (1997) 99–152

Neil Dummigan,
University of Sheffield,
Department of Pure Mathematics,
Hicks Building,
Hounsfield Road,
Sheffield, S3 7RH, U.K.
e-mail: n.p.dummigan@shef.ac.uk

William Stein,
Harvard University,
Department of Mathematics,
One Oxford Street,
Cambridge, MA 02138, U.S.A.
e-mail: was@math.harvard.edu

Mark Watkins,
Penn State Mathematics Department,
University Park,
State College, PA 16802, U.S.A.
e-mail: watkins@math.psu.edu