Pure and Applied Mathematics Quarterly
Volume 5, Number 1
(*Special Issue: In honor of
Jean-Pierre Serre, Part 2 of 2*)
1—, 2009

Critical Values of Symmetric Power L-functions

Neil Dummigan, Mark Watkins

Abstract: We consider the critical values of symmetric power L-functions attached to elliptic curves over $\mathbb{Q}$. We show how to calculate a canonical Deligne period, and in several numerical examples, especially for sixth and tenth powers, we examine the factorisation of the rational number apparently obtained when one divides the critical value by the canonical period. This seems to provide some support for the Bloch-Kato conjecture, when we compare it with calculations and bounds for Tamagawa factors and global torsion terms. For large odd powers (5th-9th), we see several examples fitting well with the squareness of the order of the Shafarevich-Tate group.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve. For any prime ℓ, let $T_\ell(E) := \varprojlim E[\ell^m]$ be the ℓ-adic Tate module of E, and let $V_\ell := (T_\ell(E) \otimes \mathbb{Q}_\ell)(-1)$ (the Tate twist as a representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$). (This V_ℓ is isomorphic to the first ℓ-adic étale cohomology of $E/\overline{\mathbb{Q}}$.) For any fixed $n \geq 1$, let $V'_\ell = \mathrm{Sym}^n(V_\ell)$. For any prime p, let D_p be a decomposition subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with inertia subgroup I_p. If $\ell \neq p$, let $P_p(T) = \det(1 - \mathrm{Frob}_p^{-1}\, T | V_\ell'^{I_p})$, where Frob_p is an arithmetic Frobenius element topologically generating $D_p/I_p \simeq \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. This polynomial is known to have integer coefficients and to be independent of the choice of $\ell \neq p$. Define

$$L(\mathrm{Sym}^n E, s) := \prod_p (P_p(p^{-s}))^{-1}.$$

Received July 4, 2006.
1991 Mathematics Subject Classification. 11G40.
Keywords. Elliptic curves, Bloch-Kato conjecture, symmetric power L-function.

This is the L-function attached to (the ℓ-adic realisations of) the motive $\mathrm{Sym}^n h^1(E)$, following the recipe in §2.2 of [Se2]. In the case $n = 1$ it is just the usual elliptic curve L-function $L(E, s)$, with $P_p(T) = 1 - a_p T + pT^2$ at any prime p of good reduction, where $\#E(\mathbb{F}_p) = 1 - a_p + p$. If (for such a prime of good reduction) we write $1 - a_p T + pT^2 = (1 - \alpha T)(1 - \beta T)$, then for general n we have $P_p(T) = \prod_{i=0}^{n}(1 - \alpha^i \beta^{n-i} T)$. It follows from the fact that $|a_p| < 2\sqrt{p}$ that the Dirichlet series for $L(\mathrm{Sym}^n E, s)$ necessarily converges (pointwise) to a holomorphic function for $\Re(s) > 1 + (n/2)$.

There is a conductor N_n, defined as in §2.1 of [Se2], and following the recipe in §3.2 of [Se2] we obtain a gamma factor

$$\gamma(s) = \begin{cases} \prod_{i=0}^{l}(2\pi)^{-(s-i)}\Gamma(s-i) & \text{if } n = 2l+1; \\ \pi^{-(s-l+1)/2}\Gamma((s-l+1)/2)\prod_{i=0}^{l-1}(2\pi)^{-(s-i)}\Gamma(s-i) & \text{if } n = 2l,\ l \text{ odd}; \\ \pi^{-(s-l)/2}\Gamma((s-l)/2)\prod_{i=0}^{l-1}(2\pi)^{-(s-i)}\Gamma(s-i) & \text{if } n = 2l,\ l \text{ even}. \end{cases}$$

Letting $\Lambda(s) := N_n^{s/2}\gamma(s)L(\mathrm{Sym}^n E, s)$ then, as in C_9 of [Se2], we expect $\Lambda(\mathrm{Sym}^n E, s)$ to have a meromorphic continuation to the whole of $\mathbb{C}$, and to satisfy a functional equation

$$\Lambda(s) = \pm\Lambda(n + 1 - s).$$

In fact, one expects the sign to be $+$ when n is even. For $n \leq 9$ the meromorphic continuation and functional equation are known (see [KS]). For higher values of n (even $n = 18$ in two cases), the precise functional equation has been tested numerically for many E by Watkins, see §5 of [MW]. For this, it is important to know the correct Euler factors even at primes of bad reduction, i.e., to work out explicitly the polynomials $P_p(T)$ defined above. These are well-known for $n = 1$, and were determined by Coates and Schmidt [CS] for $n = 2$ (with corrections by Watkins [W]). For general n they have been determined by P. Martin. See the summary in §3 of [MW], where one may also find explicit formulae for the conductors N_n.

Recently R. Taylor and his collaborators have proved the meromorphic continuation and functional equation of $L(\mathrm{Sym}^n E, s)$ for all $n \geq 1$, for any E with at least one prime of multiplicative reduction, [CHT, HSBT, T]. In fact their result applies to elliptic curves over arbitrary totally real fields, and one deduces that it is enough for E to have at least one prime of potentially multiplicative reduction, i.e. for E not to have integral j-invariant. See Theorem 5.7 of [T].

For the L-function of a motive, not only is there conjectured a meromorphic continuation and functional equation, but the orders and leading terms at integer points have a conjectural interpretation. See [Fl1] for a concise summary, and [Fo], [FP] for more details. At so-called critical points, Deligne's conjecture expresses the value of the L-function as a certain period, up to an undetermined rational multiple (if the motive has rational coefficients). The motives $\mathrm{Sym}^n h^1(E)$ are especially well-suited to experimental tests of Deligne's conjecture because

(1) there exist critical points $j = l+1$ (if $n = 2l+1$) or $j = l, l+1$ (if $n = 2l$ with l odd);
(2) the a_p are easily computed for many p, allowing one to obtain the many coefficients of the Dirichlet series necessary to get good approximations to L-values (as described in §4.4 of [MW]);
(3) from the real and imaginary periods of E one easily obtains the Deligne periods for the critical points of $L(\mathrm{Sym}^n E, s)$.

When we calculate (approximations to) the critical values and divide them by (approximations to) the Deligne periods, we find numbers whose continued fraction expansions show them to be good approximations to simple rational numbers, thus supporting Deligne's conjecture. (In practice one often divides by an expected rational factor before looking at the continued fraction, to make the rationality easier to recognise. See Table 8 of [MW] for various examples with $5 \le n \le 11$.) However, we wish to go further and to test the Bloch-Kato conjecture, which provides a conjectural interpretation of the rational number (up to sign). Again, it is important for this that we have the correct Euler factors at primes of bad reduction, whereas if we were only interested in Deligne's conjecture, they could be discarded.

If E happens to have complex multiplication by the ring of integers of an imaginary quadratic field K, then $L(\mathrm{Sym}^n E, s) = \prod_{i=0}^{[n/2]} L(\psi^{n-2i}, s-i)$, for a certain Hecke character ψ over K (with ψ^0 as in [MW]). Hence, the meromorphic continuation and functional equation are due to Hecke [H]. Furthermore, the p-part of the Bloch-Kato conjecture for $L(\mathrm{Sym}^n E, l+1)$ is known for primes $p > l+2$ of good, ordinary reduction, thanks to Theorem 1 of [Gu]. We do not consider any CM elliptic curves in this paper.

For the case $n = 1$ (the first symmetric power), the Bloch-Kato conjecture is just the Birch–Swinnerton-Dyer conjecture. For $n = 2$ (the symmetric square),

the ℓ-part of the Bloch-Kato conjecture (for $\ell > 3$ of good reduction such that $E[\ell]$ is an irreducible representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$) follows from the main theorem of [DFG]. For $n \geq 5$ nothing seems to have been proved even about Deligne's conjecture. (The case $n = 3$ of Deligne's conjecture is covered by Theorem 6.2 of [GH] or, in the case that N is square-free, by Corollary 11.3 of [GK].) An important motivation for Deligne's article [De] was the numerical data in [Z] concerning symmetric power L-functions ($n = 3$ and $n = 4$) for the normalised cusp form of weight 12 and level 1. No new conjecture has arisen as a result of the numerical data examined in our paper, and there are compelling aesthetic reasons for believing the Bloch-Kato conjecture in any case. However, since there are not very many cases in which much has been proved about the Bloch-Kato conjecture, we hope that the support offered by this paper is of some value.

In §2 we state the conjectures of Deligne and Bloch-Kato in the cases at hand. In §3 we show how to obtain a canonical Deligne period. An interesting determinant involving binomial coefficients arises here. In §4 we show how to calculate various Tamagawa factors appearing in the Bloch-Kato conjecture. If $p > n + 1$ is a prime of multiplicative reduction then the p-part of the Tamagawa factor at p was essentially calculated in §7 of [Du1]. It turns out to be in excellent agreement with the numerical results of §§6 and 7. For any prime p of multiplicative (or potentially multiplicative if $p \neq 2$) reduction, we show how to calculate the ℓ-part of the Tamagawa factor at p, for any prime $\ell \neq p$. The equations are very complicated for $\ell \leq n$, but such small primes, especially $\ell = 2$ (which is so important in the precise determination of a canonical Deligne period in §3) are of particular interest for the numerical examples of §§6 and 7. In §5 (and intermittently in §§6 and 7) we consider how to calculate or bound global torsion terms in the Bloch-Kato conjecture, and find some quite nice applications of invariant theory, again especially for small ℓ. Since it is difficult to prove anything about the Shafarevich-Tate group (though we make some tentative constructions), or about the p-part of a Tamagawa factor at p for $p \leq n$, and since often we can only bound global torsion terms, our numerical tests are somewhat incomplete, but they seem to provide some support for the Bloch-Kato conjecture at small primes. It is really at large primes that the numerical evidence is most convincing. Firstly, as mentioned above, there is the agreement with the p-part of the Tamagawa factor at a prime $p > n + 1$ of multiplicative reduction. Secondly, for odd n, some of the large primes appearing to even powers (in agreement with the

order of the Shafarevich-Tate group being a square or twice a square) are quite striking (see §6).

1.1. **Acknowledgments.** We thank Andrew Stacey for his assistance with the proof of Lemma 3.1. The second author was partially supported by Engineering and Physical Sciences Research Council (EPSRC) grant GR/T00658/01 (United Kingdom) and was a visitor at the Centre de Recherches Mathématiques at the Université de Montréal for part of this work.

2. Deligne's conjecture and the Bloch-Kato conjecture

Let $E/\mathbb{Q}$ be an elliptic curve. Let $M = h^1(E)$ be the motive whose de Rham and Betti realisations are $H_{\mathrm{dR}}(M) = H^1_{\mathrm{dR}}(E/\mathbb{Q})$ (algebraic de Rham cohomology) and $H_B(M) = H^1(E(\mathbb{C}), \mathbb{Q})$ (singular cohomology), respectively. Since $M(1)$ is self-dual, the de Rham and Betti realisations of the Tate twist $M(1)$ are $H_{\mathrm{dR}}(M(1)) = H^1_{\mathrm{dR}}(E/\mathbb{Q})^*$ (the dual space) and $H_B(M(1)) = H^1(E(\mathbb{C}), \mathbb{Q})^* \simeq H_1(E(\mathbb{C}), \mathbb{Q})$, respectively.

For $H^1_{\mathrm{dR}}(E/\mathbb{Q})$ we choose a basis $\{\omega, \eta\}$, where ω is a Néron differential for E and the image of η in $H^1(E, O_E)$ is Serre dual to ω. Let e^+ and e^- be generators for $H_1(E(\mathbb{C}), \mathbb{Z})^{\pm}$ with respect to the natural action of complex conjugation. Then $\{e^+, e^-\}$ is a basis for $H_B(M(1))$. Let $c^{\pm} := \int_{e^{\pm}} \omega$ and $f^{\pm} := \int_{e^{\pm}} \eta$. Let $\{\omega^*, \eta^*\}$ be the basis for $H_{\mathrm{dR}}(M(1))$ dual to $\{\omega, \eta\}$. Then under the comparison isomorphism $H_B(M(1)) \otimes \mathbb{C} \simeq H_{\mathrm{dR}}(M(1)) \otimes \mathbb{C}$ we have

$$e^+ \mapsto c^+\omega^* + f^+\eta^*, \ e^- \mapsto c^-\omega^* + f^-\eta^*. \tag{1}$$

In the notation of §1.7 of [De], we have $F^+ = F^- = \langle \eta^* \rangle$, so ω^* may be viewed as a basis for $H_{\mathrm{dR}}(M(1))/F^{\pm}$, and the determinants (with respect to bases $\{e^{\pm}\}$ and $\{\omega^*\}$) of the induced isomorphisms

$$H_B(M(1))^{\pm} \otimes \mathbb{C} \simeq (H_{\mathrm{dR}}(M(1))/F^{\pm}) \otimes \mathbb{C}$$

are $c^{\pm}$. These are Deligne periods for the motive $M(1)$. Note that Deligne defined his periods up to non-zero rational multiples. The $c^{\pm}$ above are merely representatives. But throughout this paper, $c^{\pm}$ will mean the exact periods just defined (up to sign; note that different choices of integral bases will change the signs of $c^{\pm}$ and $f^{\pm}$ in pairs).

We also define, for each $n \geq 1$, periods $c^{\pm}(\mathrm{Sym}^n(M(1))) = c^{\pm}((\mathrm{Sym}^n M)(n))$ for the motives whose realisations are symmetric powers of those of $M(1)$. These periods are the determinants of isomorphisms

$$(\mathrm{Sym}^n H_B(M(1)))^{\pm} \otimes \mathbb{C} \simeq (\mathrm{Sym}^n H_{\mathrm{dR}}(M(1))/F^{\pm}) \otimes \mathbb{C}$$

with respect to rational bases, where $F^{\pm}$ are chosen far enough along the Hodge filtration for the dimensions of the two sides to match. (Call these dimensions $d^{\pm}$.) Again, the periods are defined only up to non-zero rational multiples. However, there are natural choices of bases on the left and right that lead to canonical representatives (up to sign). These are the periods appearing in Conjecture 2.3 and Proposition 3.3. In Lemma 3.1 we use a different basis on the left, and get a different representative, whose relation to the natural one is worked out in Lemma 3.2.

Let $\delta = \delta(M(1)) := c^+ f^- - c^- f^+$. It is convenient for us to use this notation, but in fact (up to sign)

$$\delta = \begin{cases} 2\pi i & \text{if } E(\mathbb{R}) \text{ is not connected, so } H_1(E(\mathbb{C}), \mathbb{Z}) = \langle e^+, e^- \rangle_{\mathbb{Z}}; \\ 4\pi i & \text{if } E(\mathbb{R}) \text{ is connected, so } [H_1(E(\mathbb{C}), \mathbb{Z}) : \langle e^+, e^- \rangle_{\mathbb{Z}}] = 2. \end{cases}$$

This follows from our choice of η, and is connected with Legendre's period relation, see A1.3.4 and A1.3.13 of [K]. The following is our case of Proposition 7.7 of [De] (note that if Δ is the minimal discriminant, then $E(\mathbb{R})$ is connected precisely when $\Delta < 0$).

Proposition 2.1 (Deligne)**.**

(1) *If $n = 2l + 1$ then $d^{\pm} = l + 1$ and (up to a non-zero rational multiple)*

$$c^{\pm}(\mathrm{Sym}^n M(n)) = (c^{\pm})^{(l+1)(l+2)/2} (c^{\mp})^{l(l+1)/2} \delta^{l(l+1)/2}.$$

(2) *If $n = 2l$ then $d^+ = l+1$, $d^- = l$ and (up to a non-zero rational multiple)*

$$c^+(\mathrm{Sym}^n M(n)) = (c^+ c^-)^{l(l+1)/2} \delta^{l(l+1)/2};$$

$$c^-(\mathrm{Sym}^n M(n)) = (c^+ c^-)^{l(l+1)/2} \delta^{l(l-1)/2}.$$

The statements about $d^{\pm}$ are trivial. Deligne proves those about $c^{\pm}(\mathrm{Sym}^n M(n))$ by an indirect method of "dimensional analysis". For any integer j, we define $c^{\pm}(\mathrm{Sym}^n M(j)) = (2\pi i)^{(j-n)d^{\pm(-1)^{j-n}}} c^{\pm(-1)^{j-n}}(\mathrm{Sym}^n M(n))$.

An integer j is said to be critical for $\mathrm{Sym}^n M$ if and only if $F^0 H_{\mathrm{dR}}(\mathrm{Sym}^n M(j)) = F^+(H_{\mathrm{dR}}(\mathrm{Sym}^n M(j)))$, i.e., if and only if we have the equality $F^j H_{\mathrm{dR}}(\mathrm{Sym}^n M) = F^{(-1)^{j-n}}(H_{\mathrm{dR}}(\mathrm{Sym}^n M(n)))$. Thus we get that j is critical for $\mathrm{Sym}^n M$ if and only if $\dim(H_{\mathrm{dR}}(\mathrm{Sym}^n M)/F^j) = d^{(-1)^{j-n}}$. If $n = 2l+1$ then $j = l+1$ (the central point of symmetry for the conjectured functional equation of $L(\mathrm{Sym}^n E, s)$) is the unique critical point. If $n = 2l$ with l odd then $j = l, l+1$ (the "near-central" points, paired by the conjectured functional equation) are the unique critical points. If $n = 2l$ with l even then there are no critical points. In the special case of the motive $\mathrm{Sym}^n M(j)$, Deligne's conjecture says the following:

Conjecture 2.2 (Deligne)**.** *If j is critical for $\mathrm{Sym}^n M$ then $L(\mathrm{Sym}^n E, j)$ is a rational multiple of $c^+(\mathrm{Sym}^n M(j))$.*

Below we shall state (a special case of) the Bloch-Kato conjecture, which removes the ambiguity about the rational multiple. First we need to define some of the terms that will appear in the conjecture. For each prime ℓ there is an ℓ-adic realisation $H_\ell(M)$ of the motive M. This is a 2-dimensional $\mathbb{Q}_\ell$-vector space with a continuous linear action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Its symmetric powers are the ℓ-adic realisations of the $\mathrm{Sym}^n M$, and to get the ℓ-adic realisations of the $\mathrm{Sym}^n M(j)$ we just take the appropriate Tate twists. Choose the $\mathbb{Z}$-lattice $T = H_1(E(\mathbb{C}), \mathbb{Z})$ in $H_B(M(1))$. Then $T_\ell := T \otimes \mathbb{Z}_\ell$ is naturally identified with a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant $\mathbb{Z}_\ell$-lattice in $H_\ell(M(1))$, and is the ℓ-adic Tate module of E.

For fixed n, define $T'_\ell(j) := (\mathrm{Sym}^n T_\ell)(j-n)$, $V'_\ell(j) := T'_\ell(j) \otimes \mathbb{Q}_\ell$ and $A'_\ell(j) := V'_\ell(j)/T'_\ell(j)$. Following [BK] (Section 3), for $p \neq \ell$ (including $p = \infty$) let

$$H^1_f(\mathbb{Q}_p, V'_\ell(j)) = \ker\big(H^1(D_p, V'_\ell(j)) \to H^1(I_p, V'_\ell(j))\big).$$

Here 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

$$H^1_f(\mathbb{Q}_l, V'_\ell(j)) = \ker\big(H^1(D_\ell, V'_\ell(j)) \to H^1(D_\ell, V'_\ell(j) \otimes B_{\mathrm{cris}})\big)$$

(see Section 1 of [BK] for the definition of Fontaine's ring B_{cris}). Let $H^1_f(\mathbb{Q}, V'_\ell(j))$ be the subspace of those elements of $H^1(\mathbb{Q}, V'_\ell(j))$ that, for all primes p, have local restriction lying in $H^1_f(\mathbb{Q}_p, V'_\ell(j))$. There is a natural exact sequence

$$0 \longrightarrow T'_\ell(j) \longrightarrow V'_\ell(j) \xrightarrow{\pi} A'_\ell(j) \longrightarrow 0.$$

Let $H^1_f(\mathbb{Q}_p, A'_\ell(j)) = \pi_* H^1_f(\mathbb{Q}_p, V'_\ell(j))$. Define the ℓ-Selmer group $H^1_f(\mathbb{Q}, A'_\ell(j))$ to be the subgroup of elements of $H^1(\mathbb{Q}, A'_\ell(j))$ whose local restrictions lie in $H^1_f(\mathbb{Q}_p, A'_\ell(j))$ for all primes p. Note that the condition at $p = \infty$ is superfluous unless $\ell = 2$. Define the Shafarevich-Tate group

$$Ш(j) = \bigoplus_\ell \frac{H^1_f(\mathbb{Q}, A'_\ell(j))}{\pi_* H^1_f(\mathbb{Q}, V'_\ell(j))}.$$

Beware that we are using the same notation for different values of n. Since almost always for us $j = l + 1$, we shall use "Ш" as alternative notation for $Ш(l + 1)$.

For a finite prime p, let $H^1_f(\mathbb{Q}_p, T'_\ell(j))$ be the inverse image of $H^1_f(\mathbb{Q}_p, V'_\ell(j))$ under the natural map. Suppose now that $p \neq \ell$. If $H^0(\mathbb{Q}_p, V'_\ell(j))$ is trivial (i.e., unless $n = 2l$ and $j = l$) then, by inflation-restriction, we find that $H^1_f(\mathbb{Q}_p, V'_\ell(j)) \simeq (V'_\ell(j)^{I_p})/(1 - \mathrm{Frob}_p)(V'_\ell(j)^{I_p})$ is trivial, so $H^1_f(\mathbb{Q}_p, T'_\ell(j))$ is the torsion part of $H^1(\mathbb{Q}_p, T'_\ell(j))$. Again using the triviality of $H^0(\mathbb{Q}_p, V'_\ell(j))$, we identify $H^1_f(\mathbb{Q}_p, T'_\ell(j))$ with $H^0(\mathbb{Q}_p, A'_\ell(j))$. This has a subgroup that is given by $(V'_\ell(j)^{I_p}/T'_\ell(j)^{I_p})^{\mathrm{Frob}_p = \mathrm{id}}$, whose order is the ℓ-part of $P_p(p^{-j})$, where $P_p(p^{-s}) = \det(1 - \mathrm{Frob}_p^{-1} p^{-s} | V_\ell'^{I_p})$ is the Euler factor at p in $L(\mathrm{Sym}^n E, s)$ (strictly speaking, its reciprocal). When p is a prime of good reduction, so that $V'_\ell(j)^{I_p} = V'_\ell(j)$ maps surjectively to $A'_\ell(j)$, the subgroup is the whole of $H^0(\mathbb{Q}_p, A'_\ell(j))$, but in general we define the ℓ-part of the Tamagawa factor $c_p(j)$ to be the index of the subgroup. It is also possible to define a p-part of $c_p(j)$ (which needn't be an integer) using a measure of $H^1_f(\mathbb{Q}_p, T'_p(j))$ arising from the Bloch-Kato exponential map (and the choice of basis for $H_{\mathrm{dR}}(\mathrm{Sym}^n M(j))/F^0$ specified below). The Tamagawa factor $c_\infty(j)$ is defined below, when we calculate it. Since almost always for us $j = l + 1$, we shall use "c_p" as alternative notation for $c_p(l + 1)$.

Having chosen T we get a $\mathbb{Z}$-lattice $\mathrm{Sym}^n T$ in $H_B(\mathrm{Sym}^n M(n))$. Let $(\mathrm{Sym}^n T)^\pm$ be the subgroups on which complex conjugation acts as ± 1. Any $\mathbb{Z}$-basis for $(\mathrm{Sym}^n T)^\pm$ is a $\mathbb{Q}$-basis for $(H_B(\mathrm{Sym}^n M(n)))^\pm$. Using this in conjunction with the basis $\{\omega^{*n}, \omega^{*n-1}\eta^*, \ldots, \omega^{*n-d^\pm+1}\eta^{*d^\pm-1}\}$ for $H_{\mathrm{dR}}(\mathrm{Sym}^n M(n))/F^\pm$ gives a natural choice for the Deligne period $c^\pm(\mathrm{Sym}^n M(n))$, used in the conjecture below.

Conjecture 2.3 (Bloch-Kato)**.**

(1) *Suppose that* $n = 2l+1$*, and that* $L(\mathrm{Sym}^n E, l+1) \neq 0$*. Then (up to sign)*

$$\frac{L(\mathrm{Sym}^n E, l+1)}{c^+(\mathrm{Sym}^n M(l+1))} = \frac{\left(\prod_{p\leq\infty} c_p\right) \#Ш}{(\#H^0(\mathbb{Q}, A'(l+1)))^2} \ .$$

(2) *Suppose that* $n = 2l$ *with* l *odd. Then*

$$\frac{L(\mathrm{Sym}^n E, l+1)}{c^+(\mathrm{Sym}^n M(l+1))} = \frac{\left(\prod_{p\leq\infty} c_p\right) \#Ш}{\#H^0(\mathbb{Q}, A'(l))\#H^0(\mathbb{Q}, A'(l+1))} \ .$$

Notice that in the first case $c^+(\mathrm{Sym}^n M(l+1)) = c^{(-1)^l}(\mathrm{Sym}^n M(n))/(2\pi i)^{l(l+1)}$, while in the second case (since l is odd) it is $c^+(\mathrm{Sym}^n M(n))/(2\pi i)^{l^2-1}$. Our first task is to find, for this choice of Deligne period, the undetermined rational multipliers in Proposition 2.1. We shall find that they are certain powers of 2.

3. The exact Deligne period

Lemma 3.1. *Consider the periods* $\tilde{c}^{\pm}(\mathrm{Sym}^n M(n))$ *calculated with respect to bases* $\{(e^+)^n, (e^+)^{n-2}(e^-)^2, \ldots\}$ *and* $\{(e^+)^{n-1}(e^-), (e^+)^{n-3}(e^-)^3, \ldots\}$ *for the Betti spaces* $(H_B(\mathrm{Sym}^n M(n)))^{\pm}$*, and* $\{\omega^{*n}, \omega^{*n-1}\eta^*, \ldots, \omega^{*n-d^{\pm}+1}\eta^{*d^{\pm}-1}\}$ *for the de Rham spaces* $H_{\mathrm{dR}}(\mathrm{Sym}^n M(n))/F^{\pm}$*.*

(1) *If* $n = 2l+1$ *then* $d^{\pm} = l+1$ *and*

$$\tilde{c}^{\pm}(\mathrm{Sym}^n M(n)) = (c^{\pm})^{(l+1)(l+2)/2}(c^{\mp})^{l(l+1)/2}(2\delta)^{l(l+1)/2}.$$

(2) *If* $n = 2l$ *then* $d^+ = l+1$*,* $d^- = l$ *and*

$$\tilde{c}^+(\mathrm{Sym}^n M(n)) = (c^+c^-)^{l(l+1)/2}(2\delta)^{l(l+1)/2};$$

$$\tilde{c}^-(\mathrm{Sym}^n M(n)) = (c^+c^-)^{l(l+1)/2}(2\delta)^{l(l-1)/2}.$$

Proof. First consider the example $\tilde{c}^+(\mathrm{Sym}^2 M(2))$. Recall that

$$e^+ \mapsto c^+\omega^* + f^+\eta^*, \ e^- \mapsto c^-\omega^* + f^-\eta^*,$$

so, modulo F^+,

$$(e^+)^2 \mapsto (c^+)^2(\omega^*)^2 + 2c^+f^+\omega^*\eta^*, \ (e^-)^2 \mapsto (c^-)^2(\omega^*)^2 + 2c^-f^-\omega^*\eta^*,$$

and

$$\tilde{c}^+(\mathrm{Sym}^2 M(2)) = \det\begin{bmatrix}(c^+)^2 & 2c^+f^+\\ (c^-)^2 & 2c^-f^-\end{bmatrix} = 2c^+c^-\delta.$$

By Proposition 2.1, we had to get a rational multiple of $c^+c^-\delta$. As in Deligne's proof of Proposition 2.1, this follows from the fact that η is determined only up to the addition of a multiple of ω. Moreover, if we change bases over $\mathbb{C}$, changing c^+, c^- and δ, we still get the same rational multiple of the new $c^+c^-\delta$. To discover which rational multiple, we adjust η by a multiple of ω to make $f^- = 0$, then rescale e^+ and e^- to make $c^+ = c^- = 1$, then rescale η to make $f^+ = 1$ (hence $\delta = -1$). Now, to discover which rational multiple we have (the sign doesn't matter), we set $c^+ = c^- = f^+ = 1$ and $f^- = 0$ in the above matrix, and take the determinant of the resulting $\begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix}$ to find ± 2.

In general we get a matrix containing certain binomial coefficients, and we must show that the absolute value of its determinant is the appropriate power of 2. For example, for $\tilde{c}^+(\mathrm{Sym}^8 M(8))$ the matrix we consider is

$$A = \begin{bmatrix} 1 & 8 & 28 & 56 & 70 \\ 1 & 6 & 15 & 20 & 15 \\ 1 & 4 & 6 & 4 & 1 \\ 1 & 2 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{which is column-equivalent to} \quad \begin{bmatrix} 1 & 8 & 24 & 32 & 16 \\ 1 & 6 & 12 & 8 & 0 \\ 1 & 4 & 4 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

For $\tilde{c}^-(\mathrm{Sym}^8 M(8))$ the matrix we consider is

$$B = \begin{bmatrix} 1 & 7 & 21 & 35 \\ 1 & 5 & 10 & 10 \\ 1 & 3 & 3 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix} \quad \text{which is column-equivalent to} \quad \begin{bmatrix} 1 & 6 & 12 & 8 \\ 1 & 4 & 4 & 0 \\ 1 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Clearly, if we can prove that column reduction will always produce this pattern of ascending powers of 2 on the diagonal, then for the absolute value of the determinant we will get the power of 2 specified by the lemma. In fact, it appears to be the case that in the j^{th} column (starting from $j = 0$) we have, going up from the diagonal, 2^j multiplied by part of the j^{th} diagonal of Pascal's triangle.

This is in fact a special case of Corollary 3.1 of [St]. For the convenience of the reader we explain the argument in our special case. (As pointed out by Stacey, presumably it can be derived also using the techniques of [Kr].)

The binomial coefficient $\binom{w}{j}$ is a polynomial of degree j in w, and can be expressed in the form $\binom{w}{j} = \frac{1}{j!}w^j + \sum_{0 \le k < j} a_k \binom{w}{k}$, for some rational numbers a_k.

Substituting $2w$ for w,

$$\binom{2w}{j} - \sum_{0\le k<j} a_k \binom{2w}{k} = \frac{1}{j!}2^j w^j = 2^j \left[\binom{w}{j} - \sum_{0\le k<j} a_k \binom{w}{k} \right].$$

This proves precisely the column equivalence we sought, for matrices such as A, involving even rows of Pascal's triangle. Matrices such as B, involving odd rows of Pascal's triangle, are easily obtained from the others by elementary column operations, using the fundamental recurrence relation for binomial coefficients. □

Recall that we have chosen the $\mathbb{Z}$-lattice $T = H_1(E(\mathbb{C}), \mathbb{Z})$ in $H_B(M(1))$, with $e^{\pm}$ generators for $T^{\pm}$.

Lemma 3.2.

(1) *If $\Delta > 0$ then bases for $(\mathrm{Sym}^n T)^{\pm}$ are given by $\{(e^+)^n, (e^+)^{n-2}(e^-)^2, \ldots\}$ and $\{(e^+)^{n-1}(e^-), (e^+)^{n-3}(e^-)^3, \ldots\}$.*

(2) *If $\Delta < 0$, let E^+ be the $\mathbb{Z}$-span of $\{(e^+)^n, (e^+)^{n-2}(e^-)^2, \ldots\}$, let E^- be the $\mathbb{Z}$-span of $\{(e^+)^{n-1}(e^-), (e^+)^{n-3}(e^-)^3, \ldots\}$, and let $E = E^+ \oplus E^-$. Let $2^{b^{\pm}}$ be the orders of $(\mathrm{Sym}^n T)^{\pm}/E^{\pm}$.*
   (a) *If $n = 2l+1$ then $b^+ = b^- = l(l+1)$.*
   (b) *If $n = 2l$ then $b^+ = l(l+1)$ and $b^- = l(l-1)$.*

Proof.

(1) If $\Delta > 0$ then T is spanned by $\{e^+, e^-\}$, so this is obvious.

(2) If $\Delta < 0$ then T is spanned by $\{e^+, (e^+ + e^-)/2\}$. An alternative $\mathbb{Z}$-basis for T is $\{v^+, v^-\}$, where $v^{\pm} := (e^+ \pm e^-)/2$. We should say right away that, despite the notation, complex conjugation switches v^+ and v^-. Observe that $e^{\pm} = v^+ \pm v^-$, so that, apart from the factor of $1/2$, there is a symmetrical relation between (e^+, e^-) and (v^+, v^-). Hence if we let 2^a be the index of E in $\mathrm{Sym}^n T$, then this is also the index of $\mathrm{Sym}^n T$ in $(1/2^n)E$, so $2a = n(n+1)$ and $a = n(n+1)/2$.

   A basis for $(\mathrm{Sym}^n T)^+$ is $\{(v^+)^n + (v^-)^n, (v^+)^{n-1}v^- + (v^-)^{n-1}v^+, \ldots\}$, while a basis for $(\mathrm{Sym}^n T)^-$ is $\{(v^+)^n - (v^-)^n, (v^+)^{n-1}v^- - (v^-)^{n-1}v^+, \ldots\}$. Expressing the associated basis for $(\mathrm{Sym}^n T)^+ \oplus (\mathrm{Sym}^n T)^-$ in terms of the basis $\{(v^+)^n, (v^-)^n, (v^+)^{n-1}v^-, (v^-)^{n-1}v^+, \ldots\}$ for $\mathrm{Sym}^n T$, we get a

matrix with l blocks of $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ along the diagonal (and a 1 in the bottom corner) if n is even, or $l+1$ blocks in n is odd. Hence the index of $(\mathrm{Sym}^n T)^+ \oplus (\mathrm{Sym}^n T)^-$ in $\mathrm{Sym}^n T$ is 2^l if n is even, 2^{l+1} if n is odd. It follows that $b^+ + b^- + l = a$ or $a-1$, so

$$b^+ + b^- = \begin{cases} 2l(l+1) & \text{if } n = 2l+1; \\ 2l^2 & \text{if } n = 2l. \end{cases}$$

Let σ be complex conjugation, and consider the following table showing how we can generate some elements of $(\mathrm{Sym}^n T)^{\pm}$.

v	$(1+\sigma)v$
$(e^+)^n$	$2(e^+)^n$
$(e^+)^{n-1}v^+$	$(e^+)^n$
$(e^+)^{n-2}(v^+)^2$	$(1/2)\big((e^+)^n + (e^+)^{n-2}(e^-)^2\big)$
$(e^+)^{n-3}(v^+)^3$	$(1/4)\big((e^+)^n + 3(e^+)^{n-2}(e^-)^2\big)$
$(e^+)^{n-4}(v^+)^4$	$(1/8)\big((e^+)^n + 6(e^+)^{n-2}(e^-)^2 + (e^+)^{n-4}(e^-)^4\big)$
$(e^+)^{n-5}(v^+)^5$	$(1/16)\big((e^+)^n + 10(e^+)^{n-2}(e^-)^2 + 5(e^+)^{n-4}(e^-)^4\big)$

v	$(1-\sigma)v$
$(e^+)^n$	0
$(e^+)^{n-1}v^+$	$(e^+)^{n-1}e^-$
$(e^+)^{n-2}(v^+)^2$	$(1/2)\big(2(e^+)^{n-1}e^-\big)$
$(e^+)^{n-3}(v^+)^3$	$(1/4)\big(3(e^+)^{n-1}e^- + (e^+)^{n-3}(e^-)^3\big)$
$(e^+)^{n-4}(v^+)^4$	$(1/8)\big(4(e^+)^{n-1}e^- + 4(e^+)^{n-3}(e^-)^3\big)$
$(e^+)^{n-5}(v^+)^5$	$(1/16)\big(5(e^+)^{n-1}e^- + 10(e^+)^{n-3}(e^-)^3 + (e^+)^{n-5}(e^-)^5\big)$

We then let $W^{\pm}$ be the subgroup of $(\mathrm{Sym}^n T)^{\pm}$ that is generated by the $(1 \pm \sigma)\big((e^+)^{n-j}(v^+)^j\big)$ for odd j (and also by $(v^+v^-)^{n/2}$ for W^+ if n is even). Let $2^{B^{\pm}}$ be the order of $(W^{\pm} \otimes \mathbb{Z}_2)/(E^{\pm} \otimes \mathbb{Z}_2)$. Necessarily $B^{\pm} \le b^{\pm}$. Looking at the pattern in the above tables, and considering the diagonal entries of the triangular matrix expressing our generators for $W^{\pm}$ in terms of the standard bases for $E^{\pm}$, it is easy to determine the $B^{\pm}$.

- If $n = 2l+1$ then $B^+ = B^- = 2(1 + 2 + \ldots + l) = l(l+1)$.
- If $n = 2l$ then $B^+ = l(l+1)$ and $B^- = 2(1 + 2 + \ldots + l - 1) = l(l-1)$.

In both cases, $B^+ + B^- = b^+ + b^-$. Since $B^+ \leq b^+$ and $B^- \leq b^-$, the lemma follows.

□

Below, $c^{\pm}(\mathrm{Sym}^n M(l+1))$ are the natural Deligne periods appearing in Conjecture 2.3. We gather together what we have found so far, combining Lemmas 3.1 and 3.2.

Proposition 3.3. *Suppose that* $n = 2l+1$.

(1) *If* $\Delta > 0$ *then*

$$c^+(\mathrm{Sym}^n M(l+1)) = 2^{l(l+1)/2}(c^{\pm})^{(l+1)(l+2)/2}(c^{\mp})^{l(l+1)/2}/(2\pi i)^{l(l+1)/2},$$

where $\pm = (-1)^l$.

(2) *If* $\Delta < 0$ *then*

$$c^+(\mathrm{Sym}^n M(l+1)) = (c^{\pm})^{(l+1)(l+2)/2}(c^{\mp})^{l(l+1)/2}/(2\pi i)^{l(l+1)/2},$$

where $\pm = (-1)^l$.

Suppose that $n = 2l$ *with* l *odd.*

(1) *If* $\Delta > 0$ *then*

$$c^+(\mathrm{Sym}^n M(l+1)) = 2^{l(l+1)/2}(c^+c^-)^{l(l+1)/2}/(2\pi i)^{(l^2-l-2)/2}.$$

(2) *If* $\Delta < 0$ *then*

$$c^+(\mathrm{Sym}^n M(l+1)) = (c^+c^-)^{l(l+1)/2}/(2\pi i)^{(l^2-l-2)/2}.$$

Note that if we let $\Omega^+ = c^+$ and $i\Omega^- = c^-$ or $c^-/2$ according as $\Delta > 0$ or $\Delta < 0$ (respectively), so that $i\Omega^-$ is the imaginary part of "the" complex period, then in the case $n = 2l$ with l odd, we can write uniformly

$$c^+(\mathrm{Sym}^n M(l+1)) = 2^{l(l+1)/2}(\Omega^+\Omega^-)^{l(l+1)/2}/(2\pi)^{(l^2-l-2)/2}. \tag{2}$$

The Tamagawa factor $c_\infty(j)$ is, by definition, the order of the group

$$\frac{(H_B(\mathrm{Sym}^n M(n))/\mathrm{Sym}^n T)^{\pm}}{H_B(\mathrm{Sym}^n M(n))^{\pm}/(\mathrm{Sym}^n T)^{\pm}},$$

where $\pm = (-1)^{j-n}$. It is easy to prove the following.

Lemma 3.4. *Let* $\pm = (-1)^{j-n}$.

(1) *If* $\Delta > 0$ *then* $c_\infty(j) = 1$.
(2) *If* $\Delta < 0$ *then* $c_\infty(j) = 2^{d^\mp}$, *in fact the above group is generated by the image of* $((1/2)(\mathrm{Sym}^n T)^\mp)/(\mathrm{Sym}^n T)^\mp$.

Note that if $j = l + 1$, then $d^\mp = l + 1$ when $n = 2l + 1$, and $d^\mp = l$ when $n = 2l$ with l odd.

4. Tamagawa factors at primes of potentially multiplicative reduction

Recall the definition of $c_p(j)$, from the second paragraph before Conjecture 2.3. First suppose that p is a prime of good reduction for E, and consider the motive $\mathrm{Sym}^n M$. For a prime $\ell \neq p$, the ℓ-part of $c_p(j)$ is trivial. It is also trivial for $p = \ell$, as long as $p > n + 1$, as may be proved using Theorem 4.1(iii) of [BK]. See the proof of Lemma 1 of [Fl2].

Guess 4.1. *If* p *is* any *prime of good reduction, then* $c_p(j) = 1$ *for all* j.

Suppose now that E has multiplicative reduction at p. The following comes from calculations similar to those in §7 of [Du1], where Proposition 7.5 is the case $n = 6$.

Proposition 4.2. *Suppose that* $p > n + 1$ *is a prime of multiplicative reduction. Let* $d_p := \mathrm{ord}_p(\Delta)$. *If* $n = 2l$ *or* $2l + 1$ *then*

$$\mathrm{ord}_p(c_p) = \mathrm{ord}_p(d_p) - l(l + 1)/2.$$

Guess 4.3. *If* p *is* any *prime of multiplicative reduction, then*

$$\mathrm{ord}_p(c_p) = \mathrm{ord}_p(d_p) - l(l + 1)/2.$$

Next we consider the ℓ-part of $c_p(j)$, where p is a prime of multiplicative reduction and $\ell \neq p$. Suppose that E has *split* multiplicative reduction at p. If n is even then this is no loss of generality, since E may be replaced by an appropriate quadratic twist. We have an isomorphism $E(\overline{\mathbb{Q}}_p) \simeq \overline{\mathbb{Q}}_p^\times / q^{\mathbb{Z}}$ respecting the action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ on both sides, where q is the Tate parameter. We have $\mathrm{ord}_p(q) = d_p$, so if $\ell^a \mid\mid d_p$ then $q^{1/\ell^a} \in \mathbb{Q}_p^{\mathrm{unr}}$ whereas $q^{1/\ell^{a+1}} \notin \mathbb{Q}_p^{\mathrm{unr}}$. Let $\{x, y\}$ be a $\mathbb{Z}_\ell$-basis for the ℓ-adic Tate module $T_\ell = T_\ell(E)$, where, viewed in $\overline{\mathbb{Q}}_p^\times / q^{\mathbb{Z}}$, x

is the image of a compatible system of ℓ-power roots of unity, and y is the image of a compatible system of ℓ-power roots of q.

Recall that $T'_\ell(j) := (\mathrm{Sym}^n T_\ell)(j-n)$, $V'_\ell(j) := T'_\ell(j) \otimes \mathbb{Q}_\ell$ and $A'_\ell(j) := V'_\ell(j)/T'_\ell(j)$. We need to calculate $H^0(\mathbb{Q}_p, A'_\ell(j))$. Suppose that q is an ℓ^c-power in $\mathbb{Q}_p$, but not an ℓ^{c+1}-power. Necessarily $c \leq a$. We may choose x, a topological generator σ of the ℓ-part of the tame quotient of the inertia group I_p, and a Frobenius element Frob_p, in such a way that

$$\sigma(x) = x,\ \sigma(y) = \ell^a x + y;$$

$$\mathrm{Frob}_p(x) = px,\ \mathrm{Frob}_p(y) = \ell^c x + y.$$

(If the reduction is bad but potentially multiplicative, and $\ell = 2$, then the action of σ is multiplied by -1. If $\ell \neq 2$, it stays the same, but the 2-part of I_p also acts non-trivially, through a quotient of order 2. If the reduction is non-split multiplicative then the action of σ stays the same but the action of Frob_p is multiplied by -1.)

Consider $z = \sum_{i=0}^n a_i x^{n-i} y^i \in A'_\ell(j)$, with each $a_i \in \mathbb{Q}_\ell/\mathbb{Z}_\ell$. Then

$$\sigma(z) = \sum_{i=0}^{n} a_i x^{n-i} (\ell^a x + y)^i.$$

Taking into account the twist, in $A'_\ell(j)$,

$$\mathrm{Frob}_p(z) = \sum_{i=0}^{n} a_i p^{j-i} x^{n-i} (\ell^c x + y)^i.$$

The condition that z should be fixed by σ (hence by I_p) leads to a triangular set of equations in $\mathbb{Q}_\ell/\mathbb{Z}_\ell$. Considering the coefficient of $x^{n-i}y^i$, for $0 \leq i \leq n-1$, gives

$$\sum_{k=i+1}^{n} \ell^{a(k-i)} \binom{k}{i} a_k = 0. \tag{3}$$

(If n is odd and the reduction is bad but potentially multiplicative, there are two cases to consider. If $\ell = 2$, then each equation must have $2a_i$ added to the left hand side, and there is an extra equation $2a_n = 0$. If $\ell \neq 2$ then $z = 0$. If n is odd and the reduction is non-split then the equations are unchanged.)

If $\ell > n$ then none of the binomial coefficients is divisible by ℓ, and the equations reduce to $\ell^a a_i = 0$ for each $i \geq 1$, but if $\ell \leq n$ then it can be much more complicated (see the numerical examples later). The further condition that z

should be fixed by Frob_p (hence, overall, by $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$) leads similarly to the set of equations, for $0 \le i \le n-1$,

$$(p^{j-i}-1)a_i + \sum_{k=i+1}^{n} p^{j-k}\ell^{c(k-i)}\binom{k}{i}a_k = 0. \tag{4}$$

(If n is odd and the reduction is non-split then the coefficients $p^{j-i}-1$ are replaced by $p^{j-i}+1$.)

Proposition 4.4. *Suppose that p is a prime of split multiplicative reduction and $\ell \neq p$.*

$$\mathrm{ord}_\ell(c_p(j)) \ge \sum_{i=1}^{n} \min\{\mathrm{ord}_\ell(p^{j-i}-1), c\},$$

with equality if $c = a$ and $\ell > n$.

Proof. We need to count the number of ways of choosing the a_i so that the equations (3) and (4) are satisfied, to get the order of $H^0(\mathbb{Q}_p, A'_\ell(j))$. To get a lower bound we just look at those solutions such that $\ell^c a_i = 0$ for all $i \ge 1$. If $\kappa := \mathrm{ord}_\ell(p^j-1)$ then we must have $\ell^\kappa a_0 = 0$, i.e. ℓ^κ choices for a_0. This just accounts for the power of ℓ in the Euler factor at p, evaluated at $s = j$. It is the terms for $i \ge 1$ that actually contribute to the ℓ-part of $c_p(j)$, and if $\ell^c a_i = 0$ for all $i \ge 1$ then the equations (3) are automatically satisfied (because $c \le a$) and the equations (4) for $i \ge 1$ reduce to $(p^{j-i}-1)a_i = 0$. □

Note that the Euler factor is given by

$$P_p(p^{-s}) = \begin{cases} (1-p^{-s}) & \text{if } n \text{ is even or reduction is split multiplicative;} \\ (1+p^{-s}) & \text{if } n \text{ is odd and reduction is non-split multiplicative;} \\ 1 & \text{if } n \text{ is odd and reduction is additive, potentially multiplicative.} \end{cases}$$

We gather now some facts that will be directly applicable in §6.1.

Lemma 4.5. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, and fix $n \ge 1$.*

1. *Let $\ell > n+1$ be a prime. For any prime p of good reduction, the ℓ-part of c_p is trivial. For any prime $p \neq \ell$ of multiplicative reduction such that $\ell \nmid \mathrm{ord}_p(\Delta)$, the ℓ-part of c_p is trivial.*
2. *If n is odd and p is a prime of bad, but potentially multiplicative, reduction, and if $\ell \neq 2$, then the ℓ-part of c_p is trivial.*

(3) *Let ℓ be a prime such that $\ell > 3$. For any prime $p \neq \ell$ of bad, but potentially good, reduction, the ℓ-part of c_p is trivial.*

Proof.

(1) We need only consider $p \mid N$ (c.f. first paragraph of §4). In the equations (3) (which apply since $\ell \neq p$) we have $a = c = 0$ (since $\ell \nmid \mathrm{ord}_p(\Delta)$) and ℓ does not divide any of the binomial coefficients in the equations (since $\ell > n$). Hence $a_1 = a_2 = \ldots = a_n = 0$.
(2) It was noted above that in this case $z = 0$. In this case the Euler factor at p is trivial (because ${V_\ell}'^{I_p}$ is).
(3) This follows, as in the proof of Lemma 1 of [Fl2], from the fact (see §5.6(a) of [Se1]) that for any prime p of potentially good reduction, the image in $\mathrm{Aut}(E[\ell])$ of the inertia group I_p has order divisible at most by the primes 2 and 3.

□

5. Global torsion

The 2-adic cyclotomic character is trivial (mod 2), so the 2-torsion subgroups of both $H^0(\mathbb{Q}, A'(l))$ and $H^0(\mathbb{Q}, A'(l+1))$ are isomorphic to $H^0(\mathbb{Q}, \mathrm{Sym}^n E[2])$, and the order of this group is a lower bound for the 2-part of $\#H^0(\mathbb{Q}, A'(l))$ and also for the 2-part of $H^0(\mathbb{Q}, A'(l+1))$. Let G be the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(E[2])$. Then $H^0(\mathbb{Q}, \mathrm{Sym}^n E[2]) = (\mathrm{Sym}^n E[2])^G$.

Proposition 5.1.

(1) *If $\#E[2](\mathbb{Q}) = 4$ then G is trivial, and $\#H^0(\mathbb{Q}, \mathrm{Sym}^n E[2]) = 2^{n+1}$.*
(2) *If $\#E[2](\mathbb{Q}) = 2$ then $G \simeq \mathbb{Z}/2\mathbb{Z}$, and $\#H^0(\mathbb{Q}, \mathrm{Sym}^n E[2]) = 2^{[(n+1)/2]}$.*
(3) *If $\#E[2](\mathbb{Q}) = 1$ and Δ is not a square then we have $G = \mathrm{GL}_2(\mathbb{F}_2)$ and $\#H^0(\mathbb{Q}, \mathrm{Sym}^n E[2]) = 2^r$, where r is the number of solutions in non-negative integers a, b to $2a + 3b = n$. In fact, $r = [n/6] + 1$ unless we have $n \equiv 1 \pmod 6$, in which case $r = [n/6]$.*

(By Proposition 3 of [MO], if N is square-free then the case that $\#E[2] = 1$ and Δ is a square does not occur.) The first two parts are trivial. In the last, the assertion about G is discussed in §5.3(a) of [Se1], and the rest is a consequence of

the fact that the ring of invariants for the natural action of $\mathrm{GL}_2(\mathbb{F}_2)$ on $\mathbb{F}_2[x,y]$ is generated by x^2+xy+y^2 and xy^2+x^2y, of degrees 2 and 3, see §3.2, Example 4 of [Sm]. See the numerical examples below for what can be done in some cases for $\ell \neq 2$. An important fact, that we will use repeatedly in §§6 and 7, is that the determinant of the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[\ell]$ is the (mod ℓ) cyclotomic character.

For any prime $p \neq \ell$ of good reduction, the ℓ-part of the Euler factor at p, evaluated at $l+1$, is the order of $H^0(\mathbb{Q}_p, A'_\ell(l+1))$. Running a short PARI [P] program to evaluate the Euler factor, we may thus get an upper bound for $H^0(\mathbb{Q}, A'_\ell(l+1))$. This doesn't work for $j=l$ when $n=2l$, since the Euler factor vanishes and $H^0(\mathbb{Q}_p, A'_\ell(l))$ is infinite.

The following is directly applicable to §6.1.

Lemma 5.2. *Let $\ell > n$ be a prime such that the natural map from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\mathrm{Aut}(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$ is surjective. (For example, if N is square-free and $\ell \geq 11$, by Theorem 4 of* [Mz]*.) Then the ℓ-part of $H^0(\mathbb{Q}, A'(j))$ is trivial, for any j.*

Proof. Since $n < \ell$, there are no non-zero invariants in degree n for the natural action of $\mathrm{SL}_2(\mathbb{F}_\ell)$ on $\mathbb{F}_\ell[x,y]$. The determinant of the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[\ell]$ is the cyclotomic character, so this $\mathrm{SL}_2(\mathbb{F}_\ell)$ (as a subquotient of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$) acts trivially on $\mathbb{F}_\ell(1)$, and so we get that any non-zero element of $H^0(\mathbb{Q}, A'[\ell](j)) \simeq (\mathrm{Sym}^n(E[\ell]))(j-n)$ would give a non-zero invariant in degree n for $\mathrm{SL}_2(\mathbb{F}_\ell)$. □

6. Numerical examples–odd n

See §4.4 of [MW] for a description of the method by which all the L-value approximations used below were obtained. The method gives an approximation to the L-value, provided that the expected functional equation holds, but also gives a numerical check on that functional equation. (As already noted in the introduction, the functional equation follows from recent work of Taylor et.al., whenever E has a prime of potentially multiplicative reduction.) Some of the computations (for instance, the ninth symmetric power for 46A1 to 16 decimal digits) needed almost 2 billion terms in the L-series, but this still only takes a few hours.

6.1. **Squares of large primes, and the Shafarevich-Tate group.** Now looking at Conjecture 2.3, in the case $n = 2l+1$, and using Lemmas 4.5 and 5.2, we see that if $\ell \nmid N$ is sufficiently large, any factor of ℓ in $L(\mathrm{Sym}^n E, l+1)/c^+(\mathrm{Sym}^n M(l+1))$ should be accounted for by Ш. The Weil pairing $T_\ell(E) \times T_\ell(E) \to \mathbb{Z}_\ell(1)$ induces a perfect, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant pairing $T'_\ell(l+1) \times T'_\ell(l+1) \to \mathbb{Z}'_\ell(1)$. According to the main result of [Fl3], there is then a non-degenerate skew-symmetric pairing on Ш, so its order is a perfect square (or twice a perfect square). Hence these large primes should appear only in the numerators of the computed values of $L(\mathrm{Sym}^n E, l+1)/c^+(\mathrm{Sym}^n M(l+1))$, and always to an even power. This is amply demonstrated in the table below. When n is even (say $n = 2l$), Ш(l) and Ш$(l+1)$ are in duality with each other, hence have the same order, not necessarily a square. The tables give apparent values for the L-ratios: $L(\mathrm{Sym}^5 E, 3)(2\pi)^3/((\Omega^+)^6(\Omega^-)^3)$, $L(\mathrm{Sym}^7 E, 4)(2\pi)^6/((\Omega^-)^{10}(\Omega^+)^6)$ and $L(\mathrm{Sym}^9 E, 5)(2\pi)^{10}/((\Omega^+)^{15}(\Omega^-)^{10})$, for selected examples. One can check that in each case the ℓ in boldface does not divide any $d_p = \mathrm{ord}_p(\Delta)$ for $p \,||\, N$.

5th powers	
116A1	$2^{11}5^4\mathbf{43^2}/29^3$
123B1	$2^7 5 \cdot \mathbf{7^2}/(3^3 41^3)$
124B1	$2^6\mathbf{53^2}/31^3$
132B1	$2^{11}5^2\mathbf{7^2}/(3^3 11^3)$
185C1	$2^{14}5 \cdot \mathbf{19^2}/(5^3 37^3)$
7th powers	
61A1	$2^{11}3^3 5 \cdot 7^2\mathbf{13^2}/61^6$
63A1	$2^{17}\mathbf{13^2}/7^5$
83A1	$2^{13}3^2 5 \cdot 7^2\mathbf{43^2}/83^6$
89A1	$2^{17}3 \cdot 5^3 7^2\mathbf{19^2}/89^6$
91A1	$2^{16}3 \cdot 5 \cdot \mathbf{37^2}/(7^4 13^6)$

9th powers	
21A4	$2^{20}5 \cdot \mathbf{59^2}/(3^{10}7^{10})$
26B1	$2 \cdot 3^2 5 \cdot 7^3\mathbf{1933^2}/13^{10}$
30A1	$2^6\mathbf{37^2}/(3^5 5^5)$
33A2	$2^{24}5 \cdot \mathbf{107^2 167^2}/(3^{10}11^{10})$
34A1	$2^{13}3^5 5 \cdot 7^2\mathbf{53^2}/(17^{10})$
37B3	$2^{20}3^2 5 \cdot 7^2\mathbf{53^2}/(37^{10})$
38A3	$2 \cdot 3^{14}5 \cdot \mathbf{19^2}/19^{10}$
38B1	$2 \cdot 5^8\mathbf{109^2}/19^{10}$
42A1	$2^{15}5 \cdot \mathbf{223^2 241^2}/(3^{10}7^{10})$
45A1	$2^{16}7 \cdot \mathbf{13^2}/(3 \cdot 5^8)$
46A1	$2^4 3^{10} 5^3\mathbf{14071^2}/23^{10}$

Notice how well the denominators fit with Proposition 4.2; indeed, in our computations we can often predict these (and possibly powers-of-2 in the numerator) ahead of time, and then only need to recognise integers or rationals with small

denominator, which is significantly easier than using continued fractions on the Bloch-Kato quotient in general.

In the remaining examples of this and the next section, we shall concern ourselves with the ℓ-part of the Bloch-Kato conjecture, where ℓ is a small prime (i.e., less than n). Our choice of examples is motivated by a desire to exhibit various facets of what goes into the computations of the components in the Bloch-Kato conjecture. It might be possible to automate some of our fiddling with Tamagawa numbers, etc., but we have not investigated this too deeply; as noted in the introduction, construction of elements in the Shafarevich-Tate groups is at best conjectural. We label elliptic curves as in Cremona's tables [Cr].

6.2. **n = 9.**
Here we have $n = 2l + 1$, where $l = 4$, so $l + 1 = 5$ and $l(l + 1)/2 = 10$.

The equations (3) for $a_1, \dots, a_9$ have coefficient matrix

$$\begin{bmatrix}
\ell^a & \ell^{2a} & \ell^{3a} & \ell^{4a} & \ell^{5a} & \ell^{6a} & \ell^{7a} & \ell^{8a} & \ell^{9a} \\
0 & 2\ell^a & 3\ell^{2a} & 4\ell^{3a} & 5\ell^{4a} & 6\ell^{5a} & 7\ell^{6a} & 8\ell^{7a} & 9\ell^{8a} \\
0 & 0 & 3\ell^a & 6\ell^{2a} & 10\ell^{3a} & 15\ell^{4a} & 21\ell^{5a} & 28\ell^{6a} & 36\ell^{7a} \\
0 & 0 & 0 & 4\ell^a & 10\ell^{2a} & 20\ell^{3a} & 35\ell^{4a} & 56\ell^{5a} & 84\ell^{6a} \\
0 & 0 & 0 & 0 & 5\ell^a & 15\ell^{2a} & 35\ell^{3a} & 70\ell^{4a} & 126\ell^{5a} \\
0 & 0 & 0 & 0 & 0 & 6\ell^a & 21\ell^{2a} & 56\ell^{3a} & 126\ell^{4a} \\
0 & 0 & 0 & 0 & 0 & 0 & 7\ell^a & 28\ell^{2a} & 84\ell^{3a} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 8\ell^a & 36\ell^{2a} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9\ell^a
\end{bmatrix}.$$

The equations (4) for $a_1, \dots, a_9$ have coefficient matrix

$$\begin{bmatrix}
p^4\ell^c & p^3\ell^{2c} & p^2\ell^{3c} & p\ell^{4c} & \ell^{5c} & p^{-1}\ell^{6c} & p^{-2}\ell^{7c} & p^{-3}\ell^{8c} & p^{-4}\ell^{9c} \\
p^4-1 & 2p^3\ell^c & 3p^2\ell^{2c} & 4p\ell^{3c} & 5\ell^{4c} & 6p^{-1}\ell^{5c} & 7p^{-2}\ell^{6c} & 8p^{-3}\ell^{7c} & 9p^{-4}\ell^{8c} \\
0 & p^3-1 & 3p^2\ell^c & 6p\ell^{2c} & 10\ell^{3c} & 15p^{-1}\ell^{4c} & 21p^{-2}\ell^{5c} & 28p^{-3}\ell^{6c} & 36p^{-4}\ell^{7c} \\
0 & 0 & p^2-1 & 4p\ell^c & 10\ell^{2c} & 20p^{-1}\ell^{3c} & 35p^{-2}\ell^{4c} & 56p^{-3}\ell^{5c} & 84p^{-4}\ell^{6c} \\
0 & 0 & 0 & p-1 & 5\ell^c & 15p^{-1}\ell^{2c} & 35p^{-2}\ell^{3c} & 70p^{-3}\ell^{4c} & 126p^{-4}\ell^{5c} \\
0 & 0 & 0 & 0 & 0 & 6\ell^c p^{-1} & 21p^{-2}\ell^{2c} & 56p^{-3}\ell^{3c} & 126p^{-4}\ell^{4c} \\
0 & 0 & 0 & 0 & 0 & p^{-1}-1 & 7p^{-2}\ell^c & 28p^{-3}\ell^{2c} & 84p^{-4}\ell^{3c} \\
0 & 0 & 0 & 0 & 0 & 0 & p^{-2}-1 & 8p^{-3}\ell^c & 36p^{-4}\ell^{2c} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & p^{-3}-1 & 9p^{-4}\ell^c
\end{bmatrix},$$

and a term $(p^5 - 1)a_0$ should be added to the first equation.

(1) $E = 35A3 = [0,1,1,-1,0]$. We have $\Delta = -35 < 0$. One finds that apparently $L(\mathrm{Sym}^9 E, 5)(2\pi)^{10}/(\Omega^+)^{15}(\Omega^-)^{10} = \mathbf{2^{25}3^4}/(\mathbf{5^9 7^{10}})$. We shall compare this rational number with what Conjecture 2.3 says it should be:

$$\frac{L(\mathrm{Sym}^n E, l+1)}{c^+(\mathrm{Sym}^n M(l+1))} = \frac{\left(\prod_{p\leq\infty} c_p\right) \#Ш}{(\#H^0(\mathbb{Q}, A'(l+1)))^2} \ .$$

We work out as much as we can about the various terms on the right hand side, and use Proposition 3.3 to relate $L(\mathrm{Sym}^9 E, 5)(2\pi)^{10}/(\Omega^+)^{15}(\Omega^-)^{10}$ to the left hand side (they differ at most by a power of 2).

By Proposition 21 of [Se1], the natural homomorphism from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\mathrm{Aut}(E[7])$ is surjective. By §5.6, Example 5 of [Sm], the ring of invariants of $\mathrm{SL}_2(\mathbb{F}_7)$ on $\mathbb{F}_7[x,y]$ is generated by elements of degrees $\ell+1=8$ and $\ell^2-\ell=42$, hence $H^0(\mathbb{Q}, A'_7(5))$ is trivial. For the prime $p=5$ of non-split multiplicative reduction, $d_p = \mathrm{ord}_p(\Delta) = 1$, and, in the notation of §4, $a = c = 0$ for $\ell = 7$. Working back up the triangular set of equations (3) gives

$$a_8 = a_9 = 0,\ 7a_7 = 0,\ a_2 = a_3 = a_4 = a_5 = a_6 = 0,\ a_1 = -a_7,$$

but the equations (4) (with + signs because n is odd and the reduction is non-split) give also $a_7 = 0$. The coefficient of a_0 is (p^5+1), so the number of ways of choosing a_0 (for each solution $(a_1,\ldots,a_9)$) is the ℓ-part of the Euler factor (evaluated at 5), and does not contribute to c_5. Hence $\mathrm{ord}_7(c_5) = 0$. According to Guess 4.3, $\mathrm{ord}_7(c_7) = -10$, accounting perfectly for the power of 7.

By Proposition 21 of [Se1], the natural homomorphism from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\mathrm{Aut}(E[5])$ is surjective. By §5.6, Example 5 of [Sm], the ring of invariants of $\mathrm{SL}_2(\mathbb{F}_5)$ on $\mathbb{F}_5[x,y]$ is generated by elements of degrees $\ell+1=6$ and $\ell^2-\ell=20$, hence $H^0(\mathbb{Q}, A'_5(5))$ is trivial. For the prime $p=7$ of split multiplicative reduction, $d_p = \mathrm{ord}_p(\Delta) = 1$, and $a = c = 0$ for $\ell = 5$. The equations (3) give

$$a_6 = a_7 = a_8 = a_9 = 0,\ 5a_5 = 0,\ a_2 = a_3 = a_4 = 0,\ a_1 = -a_5.$$

Since $5 \mid 0$ and $5 \mid (7^4-1)$, the equations (4) do not impose any further conditions on $a_1,\ldots,a_9$. Hence $\mathrm{ord}_5(c_7) = 1$. According to Guess 4.3, $\mathrm{ord}_5(c_5) = -10$, and $1-10 = -9$, accounting perfectly for the power of 5.

Note that E has a rational point of order 3. Let $\{x, y\}$ be an $\mathbb{F}_3$-basis for $E[3]$, with x a rational point of order 3 and y representing the $\mathbb{F}_3(1)$ composition factor. The image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(E[3])$ is contained in a Borel subgroup, but is not diagonal. It is generated by elements that are given by the maps $g : x \mapsto x,\ y \mapsto y + x$ and $h : x \mapsto x,\ y \mapsto -y$. Noting that $\mathrm{Sym}^9 E[3] \simeq A'[3](9)$, we then find independent elements $x^9(-4),\ x^3(y^3 - x^2y)^2(-4)$ in $H^0(\mathbb{Q}, A'[3](5))$, so that we get $\#H^0(\mathbb{Q}, A'_3(5)) \geq 3^2$. For the prime $p = 7$ of split multiplicative reduction, we have $d_p = \mathrm{ord}_p(\Delta) = 1$, and $a = c = 0$ for $\ell = 3$. The equations (3) give

$$9a_9 = 0,\ a_8 = 0,\ a_7 = -3a_9,\ 3a_6 = 0,\ a_5 = 3a_9,\ a_4 = a_6,$$

$$3a_3 = -3a_9,\ a_2 = a_6,\ a_1 = -(a_3 + a_9).$$

Since $7 \equiv 1 \pmod 3$ but $7^2 \not\equiv 1 \pmod 9$, the equations (4) impose the further condition $3a_3 = 0$ (hence $3a_9 = 0$), so $\mathrm{ord}_3(c_7) = 3$. For the prime $p = 5$ of non-split multiplicative reduction, $d_p = \mathrm{ord}_p(\Delta) = 1$, and $a = c = 0$ for $\ell = 3$. The equations (3) again give

$$9a_9 = 0,\ a_8 = 0,\ a_7 = -3a_9,\ 3a_6 = 0,\ a_5 = 3a_9,\ a_4 = a_6,$$

$$3a_3 = -3a_9,\ a_2 = a_6,\ a_1 = -(a_3 + a_9).$$

Labouring through the equations (4) (with + signs because n is odd and the reduction is non-split), we eventually arrive at the net result

$$a_1 = a_3 = a_5 = a_7 = a_8 = a_9 = 0,\ a_2 = a_4 = a_6,\ 3a_6 = 0,$$

so $\mathrm{ord}_3(c_5(5)) = 1$. There is still a factor of 3^4 to be accounted for by the 3-parts of $\#Ш$ and/or c_3, which we are unable to deal with.

Since $\#E[2](\mathbb{Q}) = 1$ and Δ is not a square, Proposition 5.1 implies that $\#H^0(\mathbb{Q}, A'_2(5)) \geq 2^2$. For the prime $p = 7$ of split multiplicative reduction, $d_p = \mathrm{ord}_p(\Delta) = 1$, and $a = c = 0$ for $\ell = 2$. The equations (3) give

$$a_9 = 0,\ 8a_8 = 0,\ a_7 = 4a_8,\ 2a_6 = 4a_8,\ a_5 = a_6 - 2a_8,\ 4a_4 = 4a_8,$$

$$a_3 = -(2a_4 + a_6),\ 2a_2 = 2(a_4 - a_8),\ a_1 = -a_2 + a_4 - a_6 - 3a_8.$$

Working (backwards) through equations (4) leads eventually to a net result

$$2a_2 = 2a_4 = 2a_6 = 2a_8 = 0,\ a_7 = 0,$$

$$a_3 = a_5 = a_6,\ a_1 = a_2 + a_4 + a_6 + a_8.$$

Hence $\mathrm{ord}_2(c_7) = 4$. For the prime $p = 5$ of non-split multiplicative reduction, $d_p = \mathrm{ord}_p(\Delta) = 1$, and $a = c = 0$ for $\ell = 2$. The equations (3) and (4) (with + signs) lead to exactly the same set of relations for $a_1, \ldots, a_9$ as in the case $p = 7$, with the result that $\mathrm{ord}_2(c_5) = 4$. We get 2^{10} from Proposition 3.3 (combined with $c^- = 2i\Omega^-$), while we get that $c_\infty = 2^5$ from Lemma 3.4. We have scraped together $2^{10+5+4+4-4} = 2^{19}$, a little short of the target.

7. Numerical examples—even n

7.1. $\mathbf{n = 6}, E$ **semi-stable.**

Here we have $n = 2l$, where $l = 3$, so that $l + 1 = 4$ and $l(l+1)/2 = 6$.

The equations (3) become

$$\begin{array}{cccccc|c}
\ell^a a_1 & +\ell^{2a} a_2 & +\ell^{3a} a_3 & +\ell^{4a} a_4 & +\ell^{5a} a_5 & +\ell^{6a} a_6 & = 0 \\
 & 2\ell^a a_2 & +3\ell^{2a} a_3 & +4\ell^{3a} a_4 & +5\ell^{4a} a_5 & +6\ell^{5a} a_6 & = 0 \\
 & & 3\ell^a a_3 & +6\ell^{2a} a_4 & +10\ell^{3a} a_5 & +15\ell^{4a} a_6 & = 0 \\
 & & & 4\ell^a a_4 & +10\ell^{2a} a_5 & +20\ell^{3a} a_6 & = 0 \\
 & & & & 5\ell^a a_5 & +15\ell^{2a} a_6 & = 0 \\
 & & & & & 6\ell^a a_6 & = 0
\end{array}$$

while the equations (4) become

$$\begin{array}{cccccccc|c}
(p^4-1)a_0 & +p^3\ell^c a_1 & +p^2\ell^{2c} a_2 & +p\ell^{3c} a_3 & +\ell^{4c} a_4 & +p^{-1}\ell^{5c} a_5 & +p^{-2}\ell^{6c} a_6 & = 0 \\
 & (p^3-1)a_1 & +2p^2\ell^c a_2 & +3p\ell^{2c} a_3 & +4\ell^{3c} a_4 & +5p^{-1}\ell^{4c} a_5 & +6p^{-2}\ell^{5c} a_6 & = 0 \\
 & & (p^2-1)a_2 & +3p\ell^c a_3 & +6\ell^{2c} a_4 & +10p^{-1}\ell^{3c} a_5 & +15p^{-2}\ell^{4c} a_6 & = 0 \\
 & & & (p-1)a_3 & +4\ell^c a_4 & +10p^{-1}\ell^{2c} a_5 & +20p^{-2}\ell^{3c} a_6 & = 0 \\
 & & & & & 5p^{-1}\ell^c a_5 & +15p^{-2}\ell^{2c} a_6 & = 0 \\
 & & & & & (p^{-1}-1)a_5 & +6p^{-2}\ell^c a_6 & = 0
\end{array}$$

(1) $E = 11A1 = [0, -1, 1, -10, -20]$. We have $\Delta = -11^5$. One finds that apparently $L(\mathrm{Sym}^6 E, 4)(2\pi)^2/(\Omega^+\Omega^-)^6 = \mathbf{2^4 5^7/11^6}$. According to Conjecture 2.3, we have that

$$\frac{L(\mathrm{Sym}^n E, l+1)}{c^+(\mathrm{Sym}^n M(l+1))} = \frac{\left(\prod_{p \le \infty} c_p\right) \#Ш}{\#H^0(\mathbb{Q}, A'(l))\#H^0(\mathbb{Q}, A'(l+1))}\ .$$

The 11^6 is accounted for by the 11-part of c_{11}, as in Proposition 4.2.

Now let us try to account for the power of 2 using Conjecture 2.3. We get 2^6 from (2) (just after Proposition 3.3), which says that

$$c^+(\mathrm{Sym}^n M(l+1)) = 2^{l(l+1)/2}(\Omega^+\Omega^-)^{l(l+1)/2}/(2\pi)^{(l^2-l-2)/2},$$

and $c_\infty = 2^3$ from Lemma 3.4. (Please note that when this example was used in §7.1 of [Du1], the period was out by a power of 2.) Both factors $\#H^0(\mathbb{Q}, A_2'(3))$ and $\#H^0(\mathbb{Q}, A_2'(4))$ are bounded below by 2^2, by Proposition 5.1, since $\#E[2](\mathbb{Q}) = 1$ and Δ is not a square.

For the prime $p = 11$ of multiplicative reduction, we have $d_p = 5$, and with $\ell = 2$ we have $a = c = 0$. Working backwards up the triangular set (3) of equations gives

$$2a_6 = 0,\ a_5 = a_6,\ 4a_4 = 0,\ a_3 = 2a_4 + a_6,\ 2a_2 = a_3 + a_5 = 2a_4,$$

$$a_1 = -(a_2 + a_3 + a_4 + a_5 + a_6) = a_6 + (a_2 - a_4).$$

There are 16 solutions $(a_1, \ldots, a_6)$ to these equations. Working backwards up the triangular set (4) of equations gives nothing new, until we reach the equation for a_0, but since the coefficient of a_0 is $(p^4 - 1)$, the number of ways of choosing a_0 (for each solution $(a_1, \ldots, a_6)$) is the 2-part of the Euler factor evaluated at 4, and does not contribute to $c_{11}(4)$. Hence $\mathrm{ord}_2(c_{11}) = 4$. We have now got a contribution of $2^{6+3+4-2-2}$, that is 2^9. We only wanted 2^4, but perhaps the global torsion factors are significantly bigger than our crude lower bounds. We get an upper bound of 2^5 for $\#H^0(\mathbb{Q}, A_2'(4))$, from $\#H^0(\mathbb{Q}_5, A_2'(4))$.

The power of 5 is difficult to deal with directly, requiring the construction of elements of Ш, so we do it by looking at a 5-isogenous curve instead.

(2) $E = 11A3 = [0, -1, 1, 0, 0]$. We have $\Delta = -11 < 0$. This curve is isogenous to $11A1$, and apparently $L(\mathrm{Sym}^6 E, 4)(2\pi)^2/(\Omega^+\Omega^-)^6 = \mathbf{2^4 5/11^6}$. The Bloch-Kato conjecture is invariant under "isogeny", i.e., different choices of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable T_ℓ' inside V_ℓ'. Here, $11A1$ and $11A3$ are 5-isogenous, and it is only at $\ell = 5$ that there is a difference. This is in keeping with the fact that, in the rational number apparently coming from the L-value, only the power of 5 has changed. In the example $11A1$, it would have been difficult to account for the power of 5. We can do

much better by exploiting the isogeny invariance and using $11A3$ instead. For $p = 11$ and $\ell = 5$ we have $a = c = 0$. The equations (3) give

$$a_6 = 0,\ 5a_5 = 0,\ a_4 = 0,\ a_3 = 0,\ a_2 = 0,\ a_1 + a_5 = 0,$$

and since $11 \equiv 1 \pmod 5$, the equations (4) do not impose any further conditions on $a_1, \ldots, a_6$, so $\mathrm{ord}_5(c_{11}) = 1$. Let $\{x, y\}$ be an $\mathbb{F}_5$-basis for $E[5]$, with x a rational point of order 5 and y representing the $\mathbb{F}_5(1)$ composition factor. The image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(E[5])$ is contained in a Borel subgroup, but is not diagonal. It contains elements $g : x \mapsto x,\ y \mapsto y+x$ and $h : x \mapsto x,\ y \mapsto \zeta y$, where ζ is some primitive fourth root of unity in $\mathbb{F}_5$. In $\mathrm{Sym}^6(E[5])$, the invariants of g are spanned by x^6 and $xy^5 - x^5y$, but, noting that h acts on $\mathbb{F}_5(1)$ by ζ and that $\mathrm{Sym}^6(E[5]) = A'[5](6)$, we find that there are no elements of $A'[5](3)$ or $A'[5](4)$ invariant under both g and h. Hence $H^0(\mathbb{Q}, A'_5(3))$ and $H^0(\mathbb{Q}, A'_5(4))$ are both trivial. So we have accounted perfectly for the power of 5 in the L-value, without having to assume the existence of any elements of order 5 in Ш.

(3) $E = 15A1 = [1, 1, 1, -10, -10]$. We have $\Delta = 3^4 5^4 > 0$. One finds that apparently $L(\mathrm{Sym}^6 E, 4)(2\pi)^2/(\Omega^+\Omega^-)^6 = \mathbf{2^{22}}/(\mathbf{3^6 5^6})$. The 3^6 and 5^6 are accounted for by the p-part of $c_p(4)$, according to Guess 4.3. We must also check that $\mathrm{ord}_5(c_3)$ and $\mathrm{ord}_3(c_5)$ are both zero. The former may be done as in the example $19A1$ below. For the latter, with $\ell = 3$, $p = 5$ and $a = c = 0$, the equations (3) give

$$3a_6 = 0,\ a_5 = 0,\ a_4 = a_6,\ 3a_3 = 0,\ a_2 = a_4,\ a_1 = -a_3.$$

These equations have 9 solutions. But since $3 \nmid p - 1$, the equations (4) impose $a_3 = 0$ (and nothing else on $a_1, \ldots, a_6$, since $p^2 \equiv 1 \pmod 3$). Hence, in fact, $\mathrm{ord}_3(c_5) = 1$. But we can balance this against a factor of 3 in one of the global torsion terms in the denominator of Conjecture 2.3. An easy application of Proposition 21 of [Se1] shows that the natural map from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\mathrm{Aut}(E[3])$ is surjective. The ring of invariants for the natural action of $\mathrm{GL}_2(\mathbb{F}_3)$ on $\mathbb{F}_3[x, y]$ is generated by elements of degrees $\ell^2 - 1 = 8$ and $\ell^2 - \ell = 6$, see §5.6, Example 5 of [Sm]. Hence $\#H^0(\mathbb{Q}, A'[3](6)) = 3$. Since $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $\mathbb{F}_3(1)$ via square roots of unity, also $\#H^0(\mathbb{Q}, A'[3](4)) = 3$, so $\#H^0(\mathbb{Q}, A'_3(4)) \geq 3$. The Euler factor method gives an upper bound of 3^2 for $\#H^0(\mathbb{Q}, A'_3(4))$. The ring

of invariants for the natural action of $\mathrm{SL}_2(\mathbb{F}_3)$ on $\mathbb{F}_3[x,y]$ is generated by elements of degrees $\ell+1=4$ and $\ell^2-\ell=6$, so $H^0(\mathbb{Q},A_3'(3))$ is trivial.

We should just check that the global torsion terms for $\ell=5$ are trivial. By Proposition 21 of [Se1] the natural map from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\mathrm{Aut}(E[5])$ is surjective. The ring of invariants for the natural action of $\mathrm{SL}_2(\mathbb{F}_5)$ on $\mathbb{F}_5[x,y]$ is generated by elements of degrees $\ell+1=6$ and $\ell^2-\ell=20$, see §5.6, Example 5 of [Sm]. The invariants of degree 6 are spanned by xy^5-x^5y, on which $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts via the cyclotomic character (consider $\mathrm{diag}(\zeta,1)$). It follows that $(xy^5-x^5y)(-3)$ and $(xy^5-x^5y)(-2)$ are not fixed by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, so $H^0(\mathbb{Q},A_5'(3))$ and $H^0(\mathbb{Q},A_5'(4))$ are indeed trivial.

Now let us try to account for the large power of 2 using Conjecture 2.3. We get 2^6 from (2), and $c_\infty=1$ from Lemma 3.4. Both factors $\#H^0(\mathbb{Q},A_2'(3))$ and $\#H^0(\mathbb{Q},A_2'(4))$ are bounded below by 2^7, by Proposition 5.1, since $\#E[2](\mathbb{Q})=4$. Actually, $\#H^0(\mathbb{Q},A_2'(4))$ is bounded below by 2^8, as a consequence of E having a rational point of order 4. For the prime $p=3$ of multiplicative reduction, we have $d_p=4$, and with $\ell=2$ we have $a=c=2$, since $3^4j(E)\equiv 1 \pmod 3$, hence $q/3^4\equiv 1 \pmod 3$ and is a 4^{th} power in $\mathbb{Q}_3$. The equations (3) give

$$8a_6=4a_5=16a_4=4a_3=8a_2=4a_1=0.$$

The equations (4) impose the further conditions $2a_5=2a_3=2a_1=0$, so there are $2^{3+1+4+1+3+1}=2^{13}$ solutions for $(a_1,\dots,a_6)$. As before, the equation for a_0 may be ignored, and $\mathrm{ord}_2(c_3)=13$.

For the prime $p=5$ of multiplicative reduction, we have again $d_p=4$, and $a=c=2$ for $\ell=2$. Again the equations (3) give

$$8a_6=4a_5=16a_4=4a_3=8a_2=4a_1=0,$$

but this time the equations (4) give nothing further (the difference is that $5\equiv 1 \pmod 4$), so $\mathrm{ord}_2(c_5)=3+2+4+2+3+2=16$. We have accounted for $2^{6+0-8-7+13+16}=2^{20}$, not far off target.

(4) $E=26B1=[1,-1,1,-3,3]$. We have $\Delta=-2^7 13<0$. One finds that apparently $L(\mathrm{Sym}^6E,4)(2\pi)^2/(\Omega^+\Omega^-)^6=\mathbf{2\cdot 3\cdot 7^3 23/13^6}$. The 13^6 is accounted for by the 13-part of c_{13}, as in Proposition 4.2.

Compared to 15A1, this time the power of 2 is much smaller. Let us see if we can explain this. According to Guess 4.3, $\mathrm{ord}_2(c_2)=-6$. We get 2^6 from (2), and $c_\infty=2^3$ from Lemma 3.4. Both factors $\#H^0(\mathbb{Q},A_2'(3))$

and $\#H^0(\mathbb{Q}, A_2'(4))$ are bounded below by 2^2, by Proposition 5.1, since $\#E[2](\mathbb{Q}) = 1$ and Δ is not a square. For the prime $p = 13$ of multiplicative reduction we have $d_p = 1$ and $a = c = 0$ for $\ell = 2$. As for $11A1$ we get $\mathrm{ord}_2(c_{13}) = 4$. We have gathered $2^{-6+6+3+4-2-2} = 2^3$. An upper bound for $\#H^0(\mathbb{Q}, A_2'(4))$ is $\#H^0(\mathbb{Q}_3, A_2'(4)) = 2^5$.

Calculating somewhat as for $15A1$, one finds easily that $\mathrm{ord}_3(c_2) = 1$ and $\mathrm{ord}_3(c_{13}) = 2$. Just as for $15A1$, $\#H^0(\mathbb{Q}, A_3'(3))$ is trivial and $\#H^0(\mathbb{Q}, A_3'(4)) \geq 3$. An upper bound for $\#H^0(\mathbb{Q}, A_3'(4))$ is given by $\#H^0(\mathbb{Q}_5, A_3'(4)) = 3^2$. It would need to be attained for the power of 3 to be as expected (assuming Guess 4.1).

Using Proposition 4.4 we find that $\mathrm{ord}_7(c_2) = 2$ and $\mathrm{ord}_7(c_{13}) = 0$. Somewhat as in the analysis of global 5-torsion for $11A3$ (but now ζ is a primitive 6^{th}-root of unity and the space of invariants of g is spanned by x^6 alone), we find that $H^0(\mathbb{Q}, A_7'(4))$ and $H^0(\mathbb{Q}, A_7'(3))$ are both trivial. That leaves just one factor of 7 to be accounted for by Ш. For $L(\mathrm{Sym}^5 E, s)$, the local root number at 2 is $w_2^5 = (-1)^5 = -1$, while that at 13 is $w_{13}^5 = 1$. By the table in §5.3 of [De], the local root number at infinity is 1. Hence the sign in the functional equation is -1, and $L(\mathrm{Sym}^5 E, s)$ vanishes at the central point $s = 3$. The order of vanishing is conjecturally the dimension of $H_f^1(\mathbb{Q}, V_7''(3))$, where $V_7'' := \mathrm{Sym}^5 V_7$, etc. From this we would easily get a non-zero element of $H^1(\mathbb{Q}, A''[7](3))$, which maps to $H^1(\mathbb{Q}, A'[7](4))$ using the map induced by multiplication by a rational point of order 7, and using $E[7] \simeq A[7](1)$. The image of this element in $H^1(\mathbb{Q}, A_7'(4))$ is non-zero, since $H^0(\mathbb{Q}, A_7'(4))$ is trivial. The Bloch-Kato local condition at $p = 7$ can be proved as in Proposition 9.2 of [Du2], and those at $p \neq 7, 2, 13$ can be proved as in Proposition 9.1 of [Du1]. In fact, that at $p = 13$ can be proved the same way, since we need only the divisibility of ${A_7'}^{I_p}$, which follows from $7 \nmid d_{13}$ and $7 > 6$, bearing in mind the equations for inertia invariants in §4. Assuming also the condition at $p = 2$, and the expected finiteness of $H_f^1(\mathbb{Q}, A_7'(4))$, we would have the desired element of order 7 in Ш.

7.2. $\mathbf{n = 6}, E$ **not semi-stable.**

(1) $E = 52A2 = [0, 0, 0, -4, -3]$. We have $\Delta = 2^4 13 > 0$. One finds that apparently we have $L(\mathrm{Sym}^6 E, 4)(2\pi)^2/(\Omega^+\Omega^-)^6 = \mathbf{2^5 11 \cdot 61/13^6}$. The

prime $p = 2$ is one where E has bad, but potentially good reduction. As in (3) of Lemma 4.5, $\mathrm{ord}_\ell(c_2) = 0$ for any $\ell > 3$ (which also forces $\ell \neq p$). Even had p been greater than n, we would have no way of calculating $\mathrm{ord}_p(c_p)$. However, we can calculate $\mathrm{ord}_3(c_2)$.

Lemma 7.1. $\mathrm{ord}_3(c_2) = 0$.

Proof. According to Table 4 in §3.4 of [MW] (among other places), the image in $\mathrm{Aut}(T_3(E))$ of the inertia subgroup I_2 of $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$ is cyclic of order 3, and the image of $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$ is non-abelian. Let τ be a generator of the image in $\mathrm{Aut}(E[3])$ of I_2. Then τ has order 3. Let σ be the image in $\mathrm{Aut}(E[3])$ of a Frobenius element of $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$. Then $\sigma\tau\sigma^{-1} = \tau^{-1}$.

Since τ has order 3 and $\mathbb{F}_3^\times$ has order 2, τ cannot be a scalar transformation, so it effects a non-trivial permutation of the four elements $\{a, b, c, d\}$ of $\mathbb{P}^1(\mathbb{F}_3)$. This is necessarily a 3-cycle, (a, b, c) without loss of generality. Let x be a generator of the line a in $E[3]$, and let $y = \tau(x)$. From the fact that τ has order 3, one deduces easily that $\tau(y) = -(x+y)$.

Let $z = \sum_{i=0}^n a_i x^{n-i} y^i \in A'[3](6)$, where for us $n = 6$. Then $\tau(z) = \sum_{i=0}^n (-1)^i a_i y^{n-i}(x+y)^i$. The element $z(-2) \in A'[3](4)$ is fixed by τ if and only if, for all i such that $0 \leq i \leq n$,

$$a_i = \sum_{k \geq n-i} (-1)^k a_k \binom{k}{n-i}.$$

Working through this set of equations for $n = 6$ (and also remembering that $3a_i = 0$), one finds that a_4, a_5 and a_6 are independent, but

$$a_0 = a_6,\ a_1 = -a_5,\ a_2 = a_4 + a_5,\ a_3 = -a_4 + a_5 + a_6.$$

Hence $(A'[3](4))^{I_2}$ (of course, the twist is invisible to I_2) is 3-dimensional over $\mathbb{F}_3$. Since $V_3'(4)^{I_2}$ is also 3-dimensional (over $\mathbb{Q}_3$: this is easily checked by diagonalising τ over an extension field), we find that the natural map from $V_3'(4)^{I_2}/T_3'(4)^{I_2}$ to $A_3'(4)^{I_2}$ is surjective, hence $\mathrm{ord}_3(c_2) = 0$. □

As with $26B1$, we have $\mathrm{ord}_3(c_{13}) = 2$. The curve E is not 3-isogenous to another curve, so the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(E[3])$ is not contained in a Borel subgroup. But it has a cyclic subgroup of order 3 (the image of I_2), so it must be the whole of $\mathrm{Aut}(E[3])$, using Proposition 15 of [Se1]. Then, as with $26B1$, $\#H^0(\mathbb{Q}, A_3'(3))$ is trivial and $\#H^0(\mathbb{Q}, A_3'(4)) \geq 3$. An upper bound for $\#H^0(\mathbb{Q}, A_3'(4))$ is $\#H^0(\mathbb{Q}_5, A_3'(4)) = 3^2$. It would

need to be attained for the power of 3 to be as expected (assuming Guess 4.1).

Since $\#E[2](\mathbb{Q}) = 2$, from Proposition 5.1 we get 2^3 as a lower bound for both $H^0(\mathbb{Q}, A_2(3))$ and $H^0(\mathbb{Q}, A_2(4))$. As with $26B1$, we have that $\mathrm{ord}_2(c_{13}) = 4$. Since $\Delta > 0$, we get $c_\infty = 1$. From (2) we get 2^6. Since $6 + 4 + 0 - 3 - 3 = 4$, the powers of 2 seem to be balancing pretty well without much help from the 2-parts of Ш or c_2.

(2) $E = 184C1 = [0, 0, 0, 5, 6]$. We have $\Delta = -2^{10}23 < 0$. One finds that apparently $L(\mathrm{Sym}^6 E, 4)(2\pi)^2/(\Omega^+\Omega^-)^6 = \mathbf{2^{10}3 \cdot 11 \cdot 317/23^6}$. We will focus on the power of 3 here. The prime $p = 2$ is one where E has bad, but potentially good reduction. Since $\mathrm{ord}_2(N) = 3$, we find from Table 4 in §3.4 of [MW] that the image in $\mathrm{Aut}(T_3(E))$ of the inertia subgroup I_2 of $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$ is isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$. This arises in the natural way from the action on $E[3]$. Since the invariants of $\mathrm{SL}_2(\mathbb{F}_3)$ acting on $\mathbb{F}_3[x, y]$ are generated by an element in degree 4 and an element in degree 6, $\dim_{\mathbb{F}_3}((A'[3](4))^{I_2}) = 1$. By Table 1 in §3.1 of [MW] (or by a direct character calculation), we also have $\dim_{\mathbb{Q}_3}((V_3'(4))^{I_2}) = 1$. Hence the natural map from $(V_3'(4))^{I_2}$ to $(A_3'(4))^{I_2}$ is surjective. Put another way, $(A_3'(4))^{I_2}$ is divisible. Consequently $\mathrm{ord}_3(c_2) = 0$. Calculating as for $15A1$, we find that $\mathrm{ord}_3(c_{23}) = 1$. As with $52A2$, $\#H^0(\mathbb{Q}, A_3'(3))$ is trivial and $\#H^0(\mathbb{Q}, A_3'(4)) \geq 3$. An upper bound for $\#H^0(\mathbb{Q}, A_3'(4))$ is $\#H^0(\mathbb{Q}_5, A_3'(4)) = 3^4$. Anyway, assuming Guess 4.1, we need an element of order 3 in Ш. A tentative construction follows.

Let A_3'' etc. be for $\mathrm{Sym}^2 h^1(E)$. The minimal degree of a non-zero morphism from $X_0(184)$ to E is known to be 12. Since this is divisible by 3, it follows from Theorem 3.7 of [DFG] that there is an element of order 3 in $H^1_f(\mathbb{Q}, A_3''(1))$. We need to check several things to justify this application of their theorem (the case $\Sigma = \emptyset$). Firstly $(A_3''(1))^{I_2} = 0$, and using $3 \nmid \mathrm{ord}_{23}(\Delta)$ we find that $(A_3''(1))^{I_{23}}$ is also divisible. It follows that the local conditions defining the Selmer group in Theorem 3.7 of [DFG] are the usual Bloch-Kato local conditions that we have been using. (See the discussion preceding Lemma 2.1 of [DFG], and the proof of Theorem 3 of [Fl3].) The condition $\ell \nmid Nk!$ holds, where here $\ell = 3$ and $k = 2$. The natural homomorphism from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\mathrm{Aut}(E[3])$

is surjective (the image of I_2 already fills up $\mathrm{SL}_2(\mathbb{F}_3)$) so the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[3]$ is absolutely irreducible. In fact it remains so upon restriction to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{-3}))$. Any line in $E[3]\otimes_{\mathbb{F}_3}\overline{\mathbb{F}}_3$ invariant under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{-3}))$ cannot be invariant under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (by absolute irreducibility), so its image under $\mathrm{Gal}(\mathbb{Q}(\sqrt{-3})/\mathbb{Q})$ would be another line invariant under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{-3}))$. Using generators of these two lines as a basis for $E[3]\otimes_{\mathbb{F}_3}\overline{\mathbb{F}}_3$, the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{-3}))$ would lie in a diagonal subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_3)$, contrary to the fact that it contains an element of order 3 (because $\mathrm{SL}_2(\mathbb{F}_3)$ does). The local conductor at 2 of the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[3]$ must be 2^3 (rather than less), since $E[3]$ is wildly ramified at 2. Hence $T_3(E)$ is minimally ramified at 2 (unlike $52A2$ above, which appears to be congruent (mod 3) to $26B$, away from $p=2$). Lastly, using $3\nmid \mathrm{ord}_{23}(\Delta)$, we see $T_3(E)$ is also minimally ramified at 23.

Now that we have obtained an element of order 3 in $H^1_f(\mathbb{Q},A_3''(1))$, we let $c\in H^1(\mathbb{Q},A''[3](1))$ be an element mapping to it. Using the divisibility of $(A_3''(1))^{I_p}$, for all $p\neq 3$ the local condition implies that the restriction of c to I_p is trivial. Because we are working with vector spaces over $\mathbb{F}_3$, there is a Galois-equivariant cubing map from $\mathrm{Sym}^2(E[3])$ to $\mathrm{Sym}^6(E[3])$, hence $\phi: A''[3](1)\to A'[3](5)\simeq A'[3](3)$. As a representation of $GL_2(\mathbb{F}_3)$, $\mathrm{Sym}^6(\mathbb{F}_3^2)$ has composition factors $\mathrm{Sym}^2(\mathbb{F}_3^2)$, its dual, and the trivial representation. Hence $H^0(\mathbb{Q},A'[3](3)/\phi(A''[3](1)))$ is trivial. (Because of the odd twist, the $\mathrm{SL}_2(\mathbb{F}_3)$-invariants are not $\mathrm{GL}_2(\mathbb{F}_3)$-invariant.) It follows that $H^1(\mathbb{Q},A''[3](1))$ injects into $H^1(\mathbb{Q},A'[3](3))$, so $\phi_*(c)\neq 0$. Let d be the image of $\phi_*(c)$ in $H^1(\mathbb{Q},A_3'(3))$. Then $d\neq 0$, since $H^0(\mathbb{Q},A_3'(3))$ is trivial. Clearly, for all primes $p\neq 3$ the restriction of d to I_p is trivial, hence (using the divisibility of $(A_3'(3))^{I_p}$), the restriction of d to $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ lies in $H^1_f(\mathbb{Q}_p,A_3'(3))$, for all primes $p\neq 3$. We might hope that the same holds for $p=3$, but are unable to prove it using integral p-adic Hodge theory, because 3 is less than the length of the Hodge filtration of the de Rham realisation of $\mathrm{Sym}^6(h^1(E))$. If this wish were granted (and if, as expected, $H^1_f(\mathbb{Q},A_3'(3))$ is finite), then d would give an element of order 3 in Ш(3), and by [Fl3] we would get the existence of an element of order 3 in Ш(4), as desired.

The example $184D1 = [0,0,0,-55,-157]$, for which apparently we have that $L(\mathrm{Sym}^6 E,4)(2\pi)^2/(\Omega^+\Omega^-)^6 = \mathbf{2^7 3^3 5 \cdot 1451/23^6}$, may be dealt with similarly.

7.3. $\mathbf{n = 10.}$

Here we have $n = 2l$, where $l = 5$ so $l+1 = 6$ and $l(l+1)/2 = 15$.

The equations (3) for $a_1, \ldots, a_{10}$ have coefficient matrix

$$\begin{bmatrix}
\ell^a & \ell^{2a} & \ell^{3a} & \ell^{4a} & \ell^{5a} & \ell^{6a} & \ell^{7a} & \ell^{8a} & \ell^{9a} & \ell^{10a} \\
0 & 2\ell^a & 3\ell^{2a} & 4\ell^{3a} & 5\ell^{4a} & 6\ell^{5a} & 7\ell^{6a} & 8\ell^{7a} & 9\ell^{8a} & 10\ell^{9a} \\
0 & 0 & 3\ell^a & 6\ell^{2a} & 10\ell^{3a} & 15\ell^{4a} & 21\ell^{5a} & 28\ell^{6a} & 36\ell^{7a} & 45\ell^{8a} \\
0 & 0 & 0 & 4\ell^a & 10\ell^{2a} & 20\ell^{3a} & 35\ell^{4a} & 56\ell^{5a} & 84\ell^{6a} & 120\ell^{7a} \\
0 & 0 & 0 & 0 & 5\ell^a & 15\ell^{2a} & 35\ell^{3a} & 70\ell^{4a} & 126\ell^{5a} & 210\ell^{6a} \\
0 & 0 & 0 & 0 & 0 & 6\ell^a & 21\ell^{2a} & 56\ell^{3a} & 126\ell^{4a} & 252\ell^{5a} \\
0 & 0 & 0 & 0 & 0 & 0 & 7\ell^a & 28\ell^{2a} & 84\ell^{3a} & 210\ell^{4a} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 8\ell^a & 36\ell^{2a} & 120\ell^{3a} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9\ell^a & 45\ell^{2a} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 10\ell^a
\end{bmatrix}.$$

The equations (4) for $a_1, \ldots, a_{10}$ have coefficient matrix

$$\begin{bmatrix}
p^5\ell^c & p^4\ell^{2c} & p^3\ell^{3c} & p^2\ell^{4c} & p\ell^{5c} & \ell^{6c} & p^{-1}\ell^{7c} & p^{-2}\ell^{8c} & p^{-3}\ell^{9c} & p^{-4}\ell^{10c} \\
p^5-1 & 2p^4\ell^c & 3p^3\ell^{2c} & 4p^2\ell^{3c} & 5p\ell^{4c} & 6\ell^{5c} & 7p^{-1}\ell^{6c} & 8p^{-2}\ell^{7c} & 9p^{-3}\ell^{8c} & 10p^{-4}\ell^{9c} \\
0 & p^4-1 & 3p^3\ell^c & 6p^2\ell^{2c} & 10p\ell^{3c} & 15\ell^{4c} & 21p^{-1}\ell^{5c} & 28p^{-2}\ell^{6c} & 36p^{-3}\ell^{7c} & 45p^{-4}\ell^{8c} \\
0 & 0 & p^3-1 & 4p^2\ell^c & 10p\ell^{2c} & 20\ell^{3c} & 35p^{-1}\ell^{4c} & 56p^{-2}\ell^{5c} & 84p^{-3}\ell^{6c} & 120p^{-4}\ell^{7c} \\
0 & 0 & 0 & p^2-1 & 5p\ell^c & 15\ell^{2c} & 35p^{-1}\ell^{3c} & 70p^{-2}\ell^{4c} & 126p^{-3}\ell^{5c} & 210p^{-4}\ell^{6c} \\
0 & 0 & 0 & 0 & p-1 & 6\ell^c & 21p^{-1}\ell^{2c} & 56p^{-2}\ell^{3c} & 126p^{-3}\ell^{4c} & 252p^{-4}\ell^{5c} \\
0 & 0 & 0 & 0 & 0 & 0 & 7p^{-1}\ell^c & 28p^{-2}\ell^{2c} & 84p^{-3}\ell^{3c} & 210p^{-4}\ell^{4c} \\
0 & 0 & 0 & 0 & 0 & 0 & p^{-1}-1 & 8p^{-2}\ell^c & 36p^{-3}\ell^{2c} & 120p^{-4}\ell^{3c} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & p^{-2}-1 & 9p^{-3}\ell^c & 45p^{-4}\ell^{2c} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p^{-3}-1 & 10p^{-4}\ell^c
\end{bmatrix},$$

and a term $(p^6-1)a_0$ should be added to the first equation.

(1) $E = 15A8 = [1,1,1,0,0]$. We have $\Delta = -15 < 0$. One finds that apparently $L(\mathrm{Sym}^{10} E,6)(2\pi)^9/(\Omega^+\Omega^-)^{15} = \mathbf{2^{26}541/(3^{15}5^{14})}$. According to Guess 4.3, $\mathrm{ord}_p(c_p) = -15$ for $p = 3$ or 5.

For the prime $p = 3$ of multiplicative reduction, $d_p = 1$ and $a = c = 0$ for $\ell = 5$. The equations (3) give

$$5a_{10} = 0,\ a_9 = a_8 = a_7 = 0,\ a_6 = 3a_{10},\ 5a_5 = 0,$$

$$a_4 = a_3 = 0,\ a_2 = a_{10},\ a_1 = -a_5.$$

The equations (4) impose the additional condition $a_5 = 0$, so that we have $\mathrm{ord}_5(c_3) = 1$. By Proposition 21 of [Se1] the natural map from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\mathrm{Aut}(E[5])$ is surjective. The ring of invariants for the natural action of $\mathrm{SL}_2(\mathbb{F}_5)$ on $\mathbb{F}_5[x, y]$ is generated by elements of degrees $\ell + 1 = 6$ and $\ell^2 - \ell = 20$, so $H^0(\mathbb{Q}, A'_5(5))$ and $H^0(\mathbb{Q}, A'_5(6))$ are trivial, see §5.6, Example 5 of [Sm]. We have successfully accounted for the correct power of 5.

For the prime $p = 5$ of multiplicative reduction, $d_p = 1$ and $a = c = 0$ for $\ell = 3$. The equations (3) give

$$a_{10} = 0,\ 9a_9 = 0,\ a_8 = 0,\ a_7 = 6a_9,\ 3a_6 = 0,\ a_5 = 3a_9,$$

$$a_4 = a_6,\ 3a_3 = 6a_9,\ a_2 = a_6,\ a_1 = -(a_3 + a_9).$$

The equations (4) impose the extra conditions $a_9 = 0$, $a_3 = a_6$, so that $\mathrm{ord}_3(c_5) = 1$. This can be balanced by a global torsion factor. The natural map from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\mathrm{Aut}(E[3])$ is surjective. The ring of invariants for the natural action of $\mathrm{SL}_2(\mathbb{F}_3)$ on $\mathbb{F}_3[x, y]$ is generated by elements of degrees $\ell + 1 = 4$ and $\ell^2 - \ell = 6$, and the one-dimensional space of invariants in degree 10 is spanned by $xy^9 - x^9y$, see §5.6, Example 5 of [Sm]. On $xy^9 - x^9y$ $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts via the cyclotomic character, so $H^0(\mathbb{Q}, A'_3(6))$ is trivial but $(xy^9 - x^9y)(-5)$ is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant element of $H^0(\mathbb{Q}, A'[3](5))$, showing that $\#H^0(\mathbb{Q}, A'_3(5)) \geq 3$.

Now let us try to account for the power of 2 using Conjecture 2.3. We get 2^{15} from (2), and $c_\infty = 2^5$ from Lemma 3.4. Both factors $\#H^0(\mathbb{Q}, A'_2(3))$ and $\#H^0(\mathbb{Q}, A'_2(4))$ are bounded below by 2^5, by Proposition 5.1, since $\#E[2](\mathbb{Q}) = 2$. In fact $\#H^0(\mathbb{Q}, A'_2(4))$ is bounded below by 2^6, as a consequence of E having a rational point of order 4. For the prime $p = 5$ of multiplicative reduction, we have $d_p = 1$, and with $\ell = 2$ we have $a = c = 0$. The equations (3) give

$$2a_{10} = 0,\ a_9 = a_{10},\ 8a_8 = 0,\ a_7 = 4a_8,\ 2a_6 = 4a_8,\ a_5 = a_6 - 2a_8,\ 4a_4 = 4a_8,$$

$$a_3 = 2a_4 + a_6 + a_{10},\ 2a_2 = 2a_4 + a_{10},\ a_1 = -a_2 - 3a_4 - a_6 + a_8 + a_{10}.$$

Examining these equations, one finds that $2a_i = 0$ whenever i is odd, and always $8a_i = 0$. It follows from this that the equations (4) do not impose any further conditions on $a_1, \ldots, a_{10}$. Hence $\mathrm{ord}_2(c_5(6)) = 1 + 3 + 1 + 2 + 1 = 8$. For the prime $p = 3$ of multiplicative reduction we have again $d_p = 1$, and $a = c = 0$ for $\ell = 2$, and similarly $\mathrm{ord}_2(c_3(6)) = 8$. We have then accounted for $2^{15+5-5-6+8+8} = 2^{25}$.

References

[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.

[CHT] L. Clozel, M. Harris, R. Taylor, Automorphy for some l-adic lifts of automorphic mod l Galois representations, preprint, http://abel.math.harvard.edu/~rtaylor/

[CS] J. Coates, C.G. Schmidt, Iwasawa theory for the symmetric square of an elliptic curve, *J. Reine Angew. Math.* **375/376** (1987), 104–156.

[Cr] J. Cremona, Elliptic curve data, http://www.warwick.ac.uk/~masgaj/ftp/data/INDEX.html .

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

[DFG] F. Diamond, M. Flach, L. Guo, The Tamagawa number conjecture of adjoint motives of modular forms, *Ann. Sci. École Norm. Sup. (4)* **37** (2004), 663–727.

[Du1] N. Dummigan, Tamagawa factors for certain semi-stable representations, *Bull. London Math. Soc.* **37** (2005), 835–845.

[Du2] N. Dummigan, Symmetric square L-functions and Shafarevich-Tate groups, *Experiment. Math.***10** (2001), 383–400.

[Fl1] M. Flach, The equivariant Tamagawa number conjecture: a survey, *in* Stark's conjectures: recent work and new directions, 79–125, Contemp. Math., **358**, Amer. Math. Soc., Providence, RI, 2004.

[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.

[Fl3] M. Flach, A generalisation of the Cassels-Tate pairing, *J. reine angew. Math.* **412** (1990), 113–127.

[Fo] J.-M. Fontaine, Valeurs spéciales des fonctions L des motifs, Séminaire Bourbaki, Vol. 1991/92. *Astérisque* **206** (1992), Exp. No. 751, 4, 205–249.

[FP] J.-M. Fontaine, B. Perrin-Riou, Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L, In: Motives, A.M.S. Proc. Symp. Pure Math. **55**, Part 1 (1994), 599–706.

[GH] P. B. Garrett, M. Harris, Special values of triple product L-functions, *Amer. Jour. Math.* **115** (1993), 161–240.

[GK] B. H. Gross, S. S. Kudla, Heights and the central critical values of triple product L-functions, *Compositio Math.* **81** (1992), 143–209.

[Gu] L. Guo, On the Bloch-Kato conjecture for Hecke L-functions, *J. Number Theory* **57** (1996), 340–365.

[H] E. Hecke, *Analysis und Zahlentheorie: Vorlesung Hamburg 1920* (German). [Analysis and Number Theory: Hamburg Lectures 1920.] Edited and with a foreword by P. Roquette. Dokumente zur Geschichte der Mathematik [Documents on the History of Mathematics], **3**. Friedr. Vieweg & Sohn, Braunschweig, (1987), 234pp. Also appears in *Mathematische Werke* (German). [Mathematical works.] With introductory material by B. Schoeneberg, C. L. Siegel and J. Nielsen. Third edition. Vandenhoeck & Ruprecht, Göttingen (1983), 960pp.

[HSBT] M. Harris, N. Shepherd-Barron, R. Taylor, A family of Calabi-Yau varieties and potential automorphy, preprint, http://abel.math.harvard.edu/~rtaylor/

[K] N. Katz, p-adic properties of modular schemes and modular forms, *Modular functions of one variable* III, Lect. Notes Math. **350** 69–190, Springer, 1973.

[KS] H. H. Kim, F. Shahidi, Cuspidality of symmetric powers with applications, *Duke Math. J.* **112** (2002), 177–197.

[Kr] C. Krattenthaler, Advanced determinant calculus. The Andrews Festschrift (Maratea, 1998). *Sém. Lothar. Combin.* **42** (1999) Art.B42q, 67pp. (electronic).

[MW] P. Martin, M. Watkins, *Symmetric powers of elliptic curve L-functions.* In *Algorithmic Number Theory,* Seventh International Symposium, ANTS-VII (Berlin 2006), F. Hess, S. Pauli, M. Pohst (ed.), 377–392, Lecture Notes in Computer Science, **4076**, Springer, 2006.

[Mz] B. Mazur, Rational isogenies of prime degree, *Invent. Math.* **44** (1978), 129–162.

[MO] J.-F. Mestre, J. Oesterlé, Courbes de Weil semi-stables de discriminant une puissance m-ième, J. reine angew. Math. **400** (1989), 173–184.

[P] PARI/GP, Université Bordeaux I, Bordeaux, France. Online at `pari.math.u-bordeaux.fr`

[Se1] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.

[Se2] J.-P. Serre, Facteurs locaux des fontions zêta des variétés algébriques (définitions et conjectures), Séminaire Delange-Pisot-Poitou, 1969/70, no. **19**.

[Sm] L. Smith, *Polynomial Invariants of Finite Groups*, Research Notes in Mathematics, Volume 6, A. K. Peters, Wellesley MA, 1995.

[St] A. Stacey, Determinants of matrices from Pascal's triangle, preprint, http://www.math.ntnu.no/~stacey/Research/Preprints/intmat.html

[T] R. Taylor, Automorphy for some l-adic lifts of automorphic mod l Galois representations. II, preprint, http://abel.math.harvard.edu/~rtaylor/

[W] M. Watkins, Computing the modular degree of an elliptic curve, *Experiment. Math.* **11** (2002), 487–502.

[Z] D. Zagier, Modular forms whose coefficients involve zeta-functions of quadratic fields, *Modular functions of one variable* VI, Lect. Notes Math. **627** 105–169, Springer, 1977.

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

Mark Watkins
School of Mathematics and Statistics F07
University of Sydney NSW 2006
Australia
E-mail: watkins@maths.usyd.edu.au