Symmetric Square L-Functions
and Shafarevich–Tate Groups

Neil Dummigan

CONTENTS

We use Zagier's method to compute the critical values of the
symmetric square L-functions of six cuspidal eigenforms of level
one with rational coefficients. According to the Bloch–Kato
conjecture, certain large primes dividing these critical values
must be the orders of elements in generalised Shafarevich–Tate
groups. We give some conditional constructions of these ele-
ments. One uses Heegner cycles and Ramanujan-style congru-
ences. The other uses Kurokawa's congruences for Siegel mod-
ular forms of degree two. The first construction also applies to
the tensor product L-function attached to a pair of eigenforms of
level one. Here the critical values can be both calculated and
analysed theoretically using a formula of Shimura.

1. INTRODUCTION

Bloch and Kato [1990] formulated a general con-
jecture on the values at integer points of the L-
functions attached to motives. Previous conjectures
of Deligne, Beilinson and Bloch had predicted these
values only up to rational multiples. Bloch and Kato
provided strong evidence for their conjecture in the
case of the Riemann zeta function, and for the L-
functions of complex-multiplication elliptic curves at
$s = 2$ (for $s \geq 2$ see [Kings 2001]). Evidence is also
provided by the work of Kolyvagin and others on the
Birch and Swinnerton-Dyer conjecture for abelian
varieties (at $s = 1$), of Diamond, Flach and Guo
[Diamond et al. $\geq$ 2001] on the symmetric square
motives attached to modular forms of weight k (at
$s = k$), and of Huber and Kings [2000] on Dirichlet
L-functions. See also [Guo 1996; Han 1997; Harri-
son 1994] for results concerning Hecke L-functions.

The "critical values" that appear in Deligne's con-
jecture [1979] perhaps offer a good opportunity for
testing the Bloch–Kato conjecture, since no com-
plicated regulators get in the way. The value of a
motivic L-function at a (noncentral) critical point

is conjecturally just a local volume at infinity (determinant of a period matrix times a power of $2\pi i$) times some nonzero rational number (if the motive has rational coefficient field). Separating out the local volume and the rational number could be a problem. However, the local volume at infinity is the same (up to a power of $2\pi i$) at different critical points of the same parity, and it should cancel when we take the ratio of L-values at those points. Removing the power of π, evidence for the Bloch–Kato conjecture should survive in the factorization of the rational ratio. This is exactly what happens for the L-functions attached to the cuspidal eigenforms on $SL_2(\mathbb{Z})$ with rational coefficients (weights $k = 12, 16, 18, 20, 22$ and 26), as described in [Dummigan 2000].

In these cases the Bloch–Kato conjecture predicts the existence of nontrivial elements in certain Shafarevich–Tate groups, but the prospects for finding such elements appear bleak. In the present paper we find that in certain cases we have much better luck with the symmetric square L-functions attached to these modular forms (but only at one or two of the critical points). We are unable to deal with the local fudge factors appearing in the Bloch–Kato conjecture without restricting ourselves to forms of level one.

The critical values (right of the central point) are at the points $s = r + k - 1$ for odd r with $1 \leq r \leq k - 1$. They may be calculated by a method due to Zagier [1977]. Each is equal to a power of π times the norm of the cusp form f with respect to the Petersson inner product, times a nonzero rational number. Large primes occurring in the numerators of these rational numbers should be the orders of elements in the associated Shafarevich–Tate groups. Our restriction to $k = 12, 16, 18, 20, 22$ and 26 is not really necessary, but makes things a little simpler.

When $k = 18, 22$ or 26 (so $k/2$ is odd) and $r = k/2$, the irregular prime divisors of the Bernoulli number B_k are such large prime divisors. This striking fact appears to have no elementary explanation. Allowing an assumption, we construct the predicted elements of Shafarevich–Tate groups using Nekovář's work [1995] on Heegner cycles, together with the Galois-theoretic interpretation of Ramanujan-style congruences [Serre 1969] (see also [Swinnerton-Dyer 1973]). For this we need to check

that the first derivative of the p-adic L-function attached to f does not vanish at $s = k/2$. Actually, we are only able to check this nonvanishing in the cases $k = 22, p = 131$ or 593, due to the enormous size of the computation that would be necessary for the larger primes $p = 43867$ and 657931. A precise theorem is stated at the end of Section 6.

Cremona and Mazur [2000] 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 order m. In most cases they find another elliptic curve, often of the same conductor, whose m-torsion is Galois-isomorphic to that of the first one, and which has rank two. The rational points on the second elliptic curve produce classes in the common $H^1(\mathbb{Q}, E[m])$. They expect 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. In somewhat similar fashion, our construction produces an element of order p in a Shafarevich–Tate group for the symmetric square of a modular form, which is explained in terms of a rational algebraic cycle on the motive for the modular form. The "p-torsion" of this motive is Galois isomorphic to a twist of a submodule of that of the symmetric square motive, thanks to the Ramanujan-style congruence.

We briefly discuss what ought to happen for higher symmetric powers of modular forms, assuming not only Bloch–Kato, but also the Beilinson–Bloch conjecture [Bloch 1984], which relates vanishing at the central point to the existence of certain algebraic cycles. There is presently a single piece of computational evidence for our suspicions, concerning the symmetric fourth power of the discriminant form.

To a pair of cuspidal Hecke eigenforms, f of weight k' and g of weight k, with $k' > k$, one may attach a tensor product L-function. We assume that both f and g have level one, that $k'/2$ is odd, and also that $k' > 2k$ (so that $s = (k'/2) + k - 1$ is critical). A construction like that mentioned above should provide elements of Shafarevich–Tate groups in this case, so we expect to find appropriate irregular primes dividing the norms of certain algebraic numbers coming from ratios of critical values.

The only known case where all the Fourier coefficients of f and g are rational is $k' = 26$, $k = 12$. In this case we compute a partial Euler product to find an approximation close to a simple rational number with the expected $p = 691$ in the numerator. But we can do much better than this, using Shimura's formula for the L-function as a Rankin–Selberg integral, combined with Sturm's holomorphic projection operator. Not only does it allow us to compute the critical values without resorting to approximation, under certain mild conditions it allows us to prove the occurrence of the irregular primes in the critical values, even for examples of higher weight where the Fourier coefficients are not rational. Not surprisingly, Ramanujan-style congruences make an appearance in this proof.

This analysis applies also to Hilbert modular forms (of scalar weight) for a totally real field F of narrow class number one, but only when the degree $[F : \mathbb{Q}]$ is odd. In the light of the Beilinson–Bloch conjecture, this condition on the degree is precisely what we would expect, since it forces the L-function of f to vanish at the central point (as long as we continue to insist that $k'/2$ is odd). Conjecturally, this provides us with the algebraic cycles we need for our construction.

We return now to consideration of the symmetric square L-function for a Hecke eigenform f of level one with rational coefficients. Associated to f is its Klingen–Eisenstein series $[f]$, a noncuspidal Siegel modular eigenform of degree two [Klingen 1967]. Kurokawa [1979] conjectured that the Hecke eigenvalues of $[f]$ are congruent to those of some cuspidal Siegel modular eigenform F, of degree two, modulo certain primes dividing the critical value for $r = k - 1$. Kurokawa proved a congruence modulo 71^2 when $k = 20$ and Mizumoto [1986] proved the general conjecture. These primes modulo which there is a congruence should, as large prime divisors of critical values, be the orders of elements in certain Shafarevich–Tate groups. The well-known connection between the deformation theory of Galois representations and Selmer groups for symmetric square motives suggests that the existence of the desired element should be a fairly direct consequence of the existence of the congruence. If the Galois representation attached to F by Weissauer [$\geq$ 2001] is absolutely irreducible and takes values in $GSp_4(\mathbb{Q}_p)$,

then we can use a construction based on work of Urban [1998], (though we are unable to confirm that the local condition at p is satisfied).

Hence, in the $r = k - 1$ case we have a direct explanation leading from divisibility of a critical value, via a congruence, to a probable element in a Shafarevich–Tate group.

2. CALCULATING THE CRITICAL VALUES

For the basics on modular forms see [Serre 1973], for example. Let f be a normalised Hecke eigenform of weight k for $SL_2(\mathbb{Z})$. Let $f = \sum_{n=1}^{\infty} a_n q^n$, where $q = e^{2\pi i z}$, for z in the upper half plane, and $a_1 = 1$. We now assume that $k = 12, 16, 18, 20, 22$ or 26. In these cases f is unique and the Fourier coefficients a_n are rational integers. For example, when $k = 12$, f is the discriminant function

$$\Delta = \sum \tau(n) q^n = q \prod_{n=1}^{\infty} (1 - q^n)^{24}.$$

Associated with f is the L-function

$$L_f(s) = \sum a_n n^{-s}$$

for $\mathrm{Re}\, s$ sufficiently large, continuable to a holomorphic function on the whole complex plane by means of the integral formula

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

It satisfies the functional equation

$$\Lambda_f(s) = (-1)^{k/2} \Lambda_f(k - s).$$

Since f is a Hecke eigenform, the L-function has an Euler product

$$L_f(s) = \prod_p (1 - a_p p^{-s} + p^{k-1-2s})^{-1},$$

the product taken over all prime numbers. For each p let α_p and β_p be the roots of the polynomial $x^2 - a_p x + p^{k-1}$. Then the symmetric square L-function $D_f(s)$ attached to f is defined by the Euler product

$$D_f(s) = \prod_p \left((1 - \alpha_p^2 p^{-s})(1 - \beta_p^2 p^{-s})(1 - \alpha_p \beta_p p^{-s})\right)^{-1}.$$

The Euler product converges only when $\mathrm{Re}\, s$ is sufficiently large, but there is again a holomorphic continuation to the whole complex plane. This was proved first by Shimura [1975], and later (using a different method) by Zagier [1977], together with

the functional equation

$$\mathfrak{D}(s) = \mathfrak{D}(2k-1-s),$$

where

$$\mathfrak{D}(s) = \Gamma(s)(2\pi)^{-s}\Gamma((s+2-k)/2)\pi^{-(s+2-k)/2}D_f(s).$$

Let (f, f) be the norm of f with respect to the Petersson inner product, and for odd r with $1 \le r \le k-1$ define

$$D_f^*(r+k-1) = D_f(r+k-1)/(f, f)\pi^{2r+k-1}.$$

These are rational numbers and we now describe the calculation of these numbers, which is justified by the contents of [Zagier 1977]. See especially formulas (5), (24) and (28) of that paper.

Let $p_{k,r}(t, m)$ be the coefficient of x^{k-r-1} in $(1 - tx + mx^2)^{-r}$. For fixed k and r let $c_0 = p_{k,r}(0, 1)$, $c_1 = p_{k,r}(1, 1) + p_{k,r}(-1, 1)$ and $c_2 = p_{k,r}(2, 1) + p_{k,r}(-2, 1)$. For $D \equiv 0$ or $1 \pmod 4$ let χ_D be the quadratic character associated to the quadratic order of discriminant D. Let $L(s, \chi_D)$ be the associated Dirichlet L-function. Let $\zeta(s)$ be the Riemann zeta function.

For $r = 1$ we have $D_f^*(k) = 2^{2k-1}/(k-1)!$. For odd $r \ge 3$ we have

$$D_f^*(r+k-1) = -\frac{4^{r+k-2}(k-r-1)!}{(r+k-2)!(k-2)!}\beta,$$

where β is given by

$$c_0L(1-r, \chi_{-4}) + c_1L(1-r, \chi_{-3}) + c_2\zeta(1-2r)$$

if $r < k-1$, and by

$$c_0L(1-r, \chi_{-4}) + c_1L(1-r, \chi_{-3}) + (c_2+2k/B_k)\zeta(1-2r)$$

if $r = k-1$. Recall that $L(1-r, \chi) = -B_{r,\chi}/r$ and $\zeta(1-2r) = -B_{2r}/2r$, where, for a character χ of conductor m, the generalised Bernoulli number is $B_{r,\chi} = m^{r-1}\sum_{a=1}^m \chi(a)B_r(a/m)$. The Bernoulli polynomials are defined by

$$\sum B_n(x)t^n/n! = te^{tx}/(e^t - 1),$$

and the Bernoulli numbers are $B_n = B_n(0)$.

3. TABLES OF RESULTS

Table 1 shows the values of

$$D_f^*(r+k-1) = D_f(r+k-1)/(f, f)\pi^{2r+k-1}$$

for odd r with $1 \le r \le k-1$. These calculations were performed using Maple.

4. AN OBSERVATION

Ramanujan's famous congruence

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}$$

generalises to

$$a_n \equiv \sigma_{k-1}(n) \pmod p,$$

where $f = \sum a_n q^n$ is the unique normalised cusp form (on $SL_2(\mathbb{Z})$) of weight $k = 12, 16, 18, 20, 22$ or 26 and p is a prime divisor of $B_k/2k$, where B_k is a Bernoulli number. We shall refer to such a p as an Eisenstein prime, since the q-expansion of f is congruent to that of an un-normalized Eisenstein series, modulo p. See [Swinnerton-Dyer 1973] for a discussion of congruences, and [Manin 1973] for a proof of the congruences above using periods of f. The Eisenstein primes are $p = 691$ (when $k = 12$), $p = 3617$ (when $k = 16$), $p = 43867$ (when $k = 18$), $p = 283$ or 617 (when $k = 20$), $p = 131$ or 593 (when $k = 22$) and $p = 657931$ (when $k = 26$).

Surveying the numbers in Table 1 on the next page, one notices that for $k = 18, 22$ or 26, the numerator of $D_f^*((k/2) + k - 1)$ is divisible by the Eisenstein prime divisors of B_k. The formulas used to calculate $D_f^*(r + k - 1)$ appear not to offer any elementary explanation for this phenomenon.

Since r must be odd, it is natural that we should be looking at those values of k for which $k/2$ is odd, but the significance of the $k/2$ is that it is the central point of symmetry for the functional equation of $L_f(s)$. It is precisely when $k/2$ is odd that the functional equation forces $L_f(s)$ to have odd order of vanishing at $s = k/2$, and in particular to vanish there. We shall see later how this, together with the Ramanujan-style congruences, may be used to explain the observation.

5. GALOIS REPRESENTATIONS

Let $f = \sum a_n q^n$ be one of the normalised eigenforms already introduced. A special case of a theorem of Deligne [1969] implies the existence, for each prime l, of a continuous representation

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

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

1. ρ_l is unramified at p for all primes $p \ne l$, and

$k = 16$

$r = 1$	$2^{20}/3^6.5^3.7^2.11.13$
3	$2^{18}.179/3^7.5^3.7^3.11.13^2.17$
5	$2^{22}/3^8.5^3.7^2.11.13^2.17.19$
7	$2^{22}.23^2/3^{11}.5^5.7^3.11^2.13^2.17.19$
9	$2^{21}.2243/3^{13}.5^5.7^3.11^2.13^2.17.19.23$
11	$2^{24}.839/3^{12}.5^8.7^5.11^3.13^2.17.19.23$
13	$2^{28}.373/3^{14}.5^8.7^5.11^3.13^2.17.19.23$
15	$2^{30}/3^{13}.5^6.7^2.11.13^2.17.19.23.29.31.3617$

$k = 12$

$r = 1$	$2^{15}/3^4.5^2.7.11$
3	$2^{17}/3^5.5^2.7^2.11.13$
5	$2^{16}/3^7.5^3.7^2.11.13$
7	$2^{19}/3^9.5^4.7^2.11.13.17$
9	$2^{23}/3^8.5^5.7^4.11.13.17.19$
11	$2^{24}/3^9.5^4.7^2.11.13.17.19.23.691$

$k = 18$

$r = 1$	$2^{20}/3^6.5^3.7^2.11.13.17$
3	$2^{20}/3^8.5^3.7^3.13.17.19$
5	$2^{22}/3^{10}.5^4.7^3.11^2.17.19$
7	$2^{22}/3^9.5^4.7^3.11^2.13.17.19.23$
9	$2^{21}.\mathbf{43867}/3^{12}.5^7.7^5.11^2.13^2.17.19.23$
11	$2^{24}.1951/3^{17}.5^7.7^4.11^2.13^2.17.19.23$
13	$2^{28}.19501/3^{18}.5^9.7^5.11^2.13^2.17.19.23.29$
15	$2^{30}.541.2879/3^{17}.5^7.7^7.11^4.13^3.17.19.23.29.31$
17	$2^{32}/3^{17}.5^5.7^4.11^2.13.17.19.23.29.31.43867$

$k = 20$

$r = 1$	$2^{23}/3^8.5^3.7^2.11.13.17.19$
3	$2^{25}/3^{10}.5^4.7^3.11.17^2.19$
5	$2^{27}/3^{12}.5^4.7^2.11.13.17^2.19.23$
7	$2^{26}.2593/3^{12}.5^7.7^3.11^2.13^2.17^2.19.23$
9	$2^{28}.8831/3^{15}.5^7.7^5.11^2.13^2.17^2.19.23$
11	$2^{27}.304793977/3^{19}.5^8.7^5.11^3.13^3.17^2.19.23.29$
13	$2^{25}.40706077/3^{20}.5^9.7^5.11^2.13^2.17^2.19.23.29.31$
15	$2^{28}.9385577/3^{19}.5^9.7^7.11^3.13^2.17^2.19.23.29.31$
17	$2^{32}.439367/3^{19}.5^{11}.7^5.11^4.13^3.17^2.19.23.29.31$
19	$2^{32}.\mathbf{71^2}/3^{18}.5^9.7^3.11^2.13^2.17^2.19.23.29.31.37.283.617$

$k = 22$

$r = 1$	$2^{25}/3^9.5^4.7^3.11.13.17.19$
3	$2^{28}/3^{10}.5^5.7^2.11^2.17.19^2.23$
5	$2^{26}.59/3^{11}.5^6.7^3.11^2.13.17.19^2.23$
7	$2^{28}.239/3^{15}.5^8.7^3.11^2.13^2.19^2.23$
9	$2^{28}.25537/3^{16}.5^8.7^4.11^2.13^2.17.19^2.23.29$
11	$2^{28}.\mathbf{131.593}/3^{17}.5^9.7^5.11.13^2.17.19^2.23.29.31$
13	$2^{28}.2436904891/3^{20}.5^{10}.7^5.11^4.13^2.17^2.19^2.23.29.31$
15	$2^{32}.98513941/3^{22}.5^{10}.7^6.11^4.13^2.17^2.19^2.23.29.31$
17	$2^{34}.545715463/3^{21}.5^{12}.7^7.11^4.13^2.17^2.19^2.23.29.31.37$
19	$2^{37}.281.286397/3^{21}.5^{10}.7^7.11^4.13^4.17^3.19^2.23.29.31.37$
21	$2^{37}.\mathbf{61.103}/3^{21}.5^8.7^4.11^4.13^2.17.19^2.23.29.31.37.41.131.593$

$k = 26$

$r = 1$	$2^{29}/3^{10}.5^6.7^3.11^2.13.17.19.23$
3	$2^{30}/3^{13}.5^6.7^4.11^2.13^2.23^2$
5	$2^{33}/3^{15}.5^6.7^3.11^2.13^2.19.23^2.29$
7	$2^{32}.3373/3^{16}.5^8.7^4.11^3.13^2.17.23^2.29.31$
9	$2^{31}.3308551/3^{17}.5^8.7^6.11^3.13^2.17^2.19.23^2.29.31$
11	$2^{30}.6560341/3^{20}.5^{10}.7^5.11^3.13^2.17^2.19.23^2.29.31$
13	$2^{35}.1559.\mathbf{657931}/3^{22}.5^{10}.7^6.11^4.13^2.17^2.19^2.23^2.29.31.37$
15	$2^{32}.83.1681092571/3^{22}.5^9.7^8.11^4.13^4.17^2.19^2.23^2.29.31.37$
17	$2^{30}.1097.1249037.129901/3^{25}.5^{12}.7^6.11^5.13^4.17^2.19^2.23^2.29.31.37.41$
19	$2^{33}.78750222771431/3^{27}.5^{11}.7^8.11^4.13^4.17^2.19^2.23^2.29.31.37.41.43$
21	$2^{38}.47.160217.4157.54377/3^{27}.5^{14}.7^{10}.11^5.13^4.17^2.19^2.23^2.29.31.37.41.43$
23	$2^{39}.4598642018203/3^{27}.5^{12}7^7.11^6.13^4.17^3.19^3.23^2.29.31.41.43.47$
25	$2^{41}.\mathbf{163.187273}/3^{26}.5^{10}.7^7.11^4.13^2.17^2.19.23^2.29.31.37.41.43.47.657931$

TABLE 1. Values of $D_f^*(r+k-1) = D_f(r+k-1)/(f,f)\pi^{2r+k-1}$ for odd r with $1 \le r \le k-1$.

2. If Frob_p is an arithmetic Frobenius element at p then the characteristic polynomial of Frob_p^{-1} acting on V_l is $x^2 - a_p x + p^{k-1}$.

For $N \geq 3$ let M_N be the modular scheme over $\mathbb{Z}[1/N]$ parametrising elliptic curves, each with a given basis for the group of points of order N. Let X_N be the universal elliptic curve over M_N. Let $\overline{M}_N$ be the compactification of M_N and let $\overline{X}_N$ be the universal generalised elliptic curve over $\overline{M}_N$. Let $\overline{X}_N^{k-2}$ be the $(k-2)$-fold fibre product of $\overline{X}_N$ over $\overline{M}_N$ and let

$$X = \overline{X}_N^{k-2}$$

be Deligne's canonical desingularisation. The variety X is proper and smooth over $\mathbb{Z}[1/N]$, though not geometrically irreducible.

We shall now fix $N = 3$. Following Scholl [1990], V_l may be constructed as the l-adic realisation of a Grothendieck motive. $V_l = P_f H_{et}^{k-1}(X \otimes \overline{\mathbb{Q}}, \mathbb{Q}_l)$, where P_f is a suitable projector, in our case in the group ring of the automorphism group of X. (Setting $N = 3$ certainly ensures that the rational coefficients of this projector are integral at any prime greater than $k-2$.) Let

$$V_l(j) = P_f H_{et}^{k-1}(X \otimes \overline{\mathbb{Q}}, \mathbb{Q}_l(j)),$$

the Tate twist as a Galois representation. For each prime l let $T_l(j) = P_f H_{et}^{k-1}(X \otimes \overline{\mathbb{Q}}, \mathbb{Z}_l(j))$ modulo torsion. Let $A_l(j) = V_l(j)/T_l(j)$.

For the symmetric square motive let

$$V_l' = \mathrm{Sym}^2(V_l), \quad T_l' = \mathrm{Sym}^2(T_l), \quad A_l' = V_l'/T_l'.$$

They have rank 3. We sometimes drop the subscript when it is convenient to do so. For an integer j of the form $r + k - 1$ or $k - r$, with r odd and $1 \leq r \leq k-1$ define the set of global points $\Gamma_{\mathbb{Q}}(j) = \bigoplus_l H^0(\mathbb{Q}, A_l'(j))$.

Following [Bloch and Kato 1990], for $p \neq l$ let

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

Here D_p is a decomposition subgroup at a prime above p, I_p denotes the inertia subgroup, and the cohomology is for continuous cocycles and coboundaries. For $p = l$ let

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

where B_{cris} is Fontaine's ring; see [Bloch and Kato 1990] for a definition. The subscript f stands for "finite part". Let $H_f^1(\mathbb{Q}, V_l'(j))$ be the subspace of elements of $H^1(\mathbb{Q}, V_l'(j))$ whose local restrictions lie in $H_f^1(\mathbb{Q}_p, V_l'(j))$ for all primes p. See the remark after Proposition 9.1.

There is a natural exact sequence

$$0 \longrightarrow T_l'(j) \longrightarrow V_l'(j) \xrightarrow{\pi} A_l'(j) \longrightarrow 0$$

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

$$\text{Ш}(j) = \bigoplus_l H_f^1(\mathbb{Q}, A_l'(j))/\pi_* H_f^1(\mathbb{Q}, V_l'(j)).$$

Of course, we could also define all these things with V_l', T_l' and A_l' replaced by V_l, T_l and A_l.

6. THE BLOCH–KATO CONJECTURE

Let M be the Grothendieck motive attached to f. Let j be of the form $r + k - 1$ with r odd and $1 \leq r \leq k - 1$. The Bloch–Kato conjecture for the twisted symmetric square motive $\mathrm{Sym}^2 M(j)$ predicts that

$$D_f(j) = \left(\prod_p c_p(j)\right) \frac{\mathrm{vol}_\infty(j) \, \#\text{Ш}(j)}{\#\Gamma_{\mathbb{Q}}(j) \, \#\Gamma_{\mathbb{Q}}(2k-1-j)}.$$

The $c_p(j)$ and $\mathrm{vol}_\infty(j)$ are defined similarly to those in [Dummigan 2000, Section 4], but note that the definition of $\mathrm{vol}_\infty(j)$ given there is mistaken, what is actually defined being $1/\mathrm{vol}_\infty(j)$. The Hodge filtration of the deRham realisation of the motive $\mathrm{Sym}^2 M$ has $F^0 = \mathrm{Sym}^2(P_f H_{\mathrm{dR}}^{k-1}(X))$, $F^1 = \cdots = F^{k-1} = P_f H_{\mathrm{dR}}^{k-1}(X) P_f H^0(X, \Omega^{k-1})$, $F^k = \cdots = F^{2k-2} = P_f H^0(X, \Omega^{k-1}) \otimes P_f H^0(X, \Omega^{k-1})$, $F^{2k-1} = \{0\}$.

The dimension of $\mathrm{Sym}^2 M$ is $2k-2$, and the length of its Hodge filtration is $2k - 1$. It then follows as in [Dummigan 2000, Section 7] that $c_p(j) = 1$ for all primes $p > 2k$, by an application of Faltings's comparison theorem [Faltings 1989] and [Bloch and Kato 1990, Theorem 4.1(iii)]. (We are unable to do this without restricting to forms of level one.) Also, each $c_p(j)$ (for $p < 2k$) is a power of p.

Since $F^k = \cdots = F^{2k-2}$ and $k \leq j \leq 2k - 2$ with all the j of the same parity, it follows as in

[Dummigan 2000, Section 4] that the $\text{vol}_\infty(j)$ for different j are the same, up to an appropriate power of $2\pi i$.

If the Bloch–Kato conjecture is true, and looking at the prime factorisation of $D_f^*(j)/D_f^*(j')$, with $j \neq j'$, any primes $p > 2k$ must be accounted for by elements of order p in Shafarevich–Tate groups and/or groups of global points, for j and j'. Now suppose that a prime $p > 2k$ occurs in the numerator of precisely one of the $D_f^*(j)$'s. Then according to the Bloch–Kato conjecture, either $\text{III}(j)$ contains an element of order p or, for all other critical j', p divides $\#\Gamma_\mathbb{Q}(j')\#\Gamma_\mathbb{Q}(2k-1-j')$. But the p-torsion subgroup $A'[p]$ cannot have so many twists with Galois-fixed lines, since it has at most three distinct composition factors as a Galois module. Therefore the Bloch–Kato conjecture predicts that there must be an element of order p in $\text{III}(j)$. In Table 1 we marked in boldface those primes p for which we will construct the predicted elements of $\text{III}(j)$. We give a precise statement here of what is actually proved in the next few sections.

Theorem 6.1. *When $k = 22$ and $p = 131$ or 593, if $H_f^1(\mathbb{Q}, V'((k/2)+k-1))$ and $H_f^1(\mathbb{Q}, V'(k/2))$ are both trivial, then $\text{III}((k/2)+k-1)$ (for $\text{Sym}^2(M)$) contains an element of order p. For $k = 18$, $p = 43867$, or $k = 26$, $p = 657931$, one obtains the same conclusion with the additional hypothesis that the first derivative of the p-adic L-function attached to f does not vanish at $s = k/2$.*

7. HEEGNER CYCLES

For a detailed description of the Heegner cycles of codimension $k/2$ on X, see [Nekovář 1992]. They project to Heegner divisors on the modular curve M_N, and involve products of graphs of endomorphisms of CM elliptic curves. Via the p-adic Abel–Jacobi map, a Heegner cycle gives rise to a class in $H^1(\mathbb{Q}, V_p(k/2))$, (for any prime p), and Nekovář [1992] shows that it is in fact in the subspace

$$H_f^1(\mathbb{Q}, V_p(k/2)).$$

See also [Nekovář 1995, 0.13].

Now suppose that $k = 18, 22$ or 26. The vanishing of the complex L-function $L_f(s)$ at $s = k/2$ implies the vanishing of the p-adic L-function $L_{p,f}(s)$ at $s = k/2$. (For the construction of this p-adic L-function

see [Mazur et al. 1986].) According to [Nekovář 1995, Theorem C], if the first derivative $L'_{p,f}(s)$ does not vanish at $s = k/2$ then $H_f^1(\mathbb{Q}, V_p(k/2))$ is one-dimensional, generated by the classes of Heegner cycles. We would like to check this nonvanishing for Eisenstein primes p. From now on, p will be one of these primes ($p = 43867$ when $k = 18$, 131 or 593 when $k = 22$ and 657931 when $k = 26$).

We refer to [Mazur et al. 1986] for more details on the p-adic L-function and calculations with modular symbols which we will not explain fully here. What we need to show is that

$$\int_{\mathbb{Z}_p^*} x^r \log_p(x) d\mu_{f,\alpha} \neq 0,$$

where $r = (k/2) - 1$ (which is even), α is a root of $X^2 - a_p X + p^{k-1}$ chosen so that $\text{ord}_p(\alpha) < k - 1$, $\log_p$ is the p-adic logarithm and $d\mu_{f,\alpha}$ is a certain p-adic measure. Manin [1973] showed that integrals such as this one converge when $\text{ord}_p(\alpha) = 0$. Such an α exists in the ordinary case, when p does not divide a_p. In [Amice and Vélu 1975] and [Vishik 1976] the condition is relaxed to $\text{ord}_p(\alpha) < k - 1$ (see [Mazur et al. 1986]), and there always exists such an α, but we are in the ordinary case anyway since $a_p \equiv \sigma_{k-1}(p) \equiv 1 \pmod{p}$.

To cut a long story short, calculating with modular symbols and approximating the integrand by a step function locally constant on discs of radius p^{-2}, it suffices to show that

$$\sum_{a,b=1}^{p-1} a^{2r} b[m_1^r + m_2^r + \cdots + 1^r] \neq 0 \pmod{p}.$$

Here we have used sequences of integers $a_0 > a_1 > \cdots > a_t = 0$ and $m_0 > m_1 > \cdots > m_t = 1$ (t depends on a and b) with $m_0 = p^2$, $1 \leq a_0 < p^2$, $a_0 \equiv a^p(1+bp) \pmod{p^2}$, $a_j m_{j+1} \equiv 1 \pmod{m_j}$ and $a_{j+1} = (a_j m_{j+1} - 1)/m_j$. Alternatively we could take the m_j to be the denominators of the convergents to the continued fraction for $a^p(1+bp)/p^2$.

This drastic simplification of the appropriate Riemann sum is made possible by the fact that p divides the even period ratios for f (see the table in [Manin 1973]), a fact which was one of the main concerns of [Dummigan 2000], and is the basis of that proof of the Ramanujan-style congruences to which we have already referred.

We ran a simple Maple program to evaluate this sum modulo p. When $k = 22$ and $p = 131$ the answer came out to 12, after 129 seconds of computer time. When $k = 22$ and $p = 593$ it came out to 167, after 83 minutes of computer time. For $p = 43867$ or 657931 the computation would have taken millions of minutes, so we did not start it.

In any case, if we have a nonzero class in $H^1_f(\mathbb{Q}, V_p(k/2))$ then by continuity we may assume, after multiplication by a power of p if necessary, that it lies in $H^1(\mathbb{Q}, T_p(k/2))$ but not in $H^1(\mathbb{Q}, pT_p(k/2))$, then by reduction modulo p we get a nonzero class $c \in H^1(\mathbb{Q}, A[p](k/2))$. Here $A[p]$ is the p-torsion subgroup of A_p. (We know for certain that this class exists when $k = 22$, $p = 131$ or 593.)

8. RAMANUJAN CONGRUENCES AND SHAFAREVICH–TATE GROUPS

For p as above, there is a congruence $a_n \equiv \sigma_{k-1}(n)$ (mod p), for all $n \geq 1$. It follows that for prime $l \neq p$, the trace of Frob_l^{-1} acting on $A[p]$ is $1 + l^{k-1}$. It then follows from the Brauer–Nesbitt theorem that $A[p]$ contains a Galois submodule isomorphic to either $\mathbb{F}_p$ or the twist $\mathbb{F}_p(1 - k)$. (Whichever one it is, the quotient is isomorphic to the other one.) In [Dummigan 2000], assuming the latter led to an explanation (via Bloch–Kato) of the occurrence of Eisenstein primes in the numerators of even period ratios. We shall make the same assumption for the moment, though we shall see later that it is unnecessary. Now if $A[p]$ has a submodule isomorphic to $\mathbb{F}_p(1 - k)$ then the three-dimensional $A'[p]$ has a two-dimensional submodule isomorphic to $A[p](1-k)$, with trivial one-dimensional quotient. Twisting, $A'[p]((k/2) + k - 1)$ has a submodule isomorphic to $A[p](k/2)$.

The element Frob_l^{-1} acts as $l^{1-k-(k/2)}$ on the quotient $Q \simeq \mathbb{F}_p((k/2) + k - 1)$, so $H^0(\mathbb{Q}, Q)$ is trivial and $H^1(\mathbb{Q}, A[p](k/2))$ injects into

$$H^1(\mathbb{Q}, A'[p]((k/2)+k-1)),$$

sending the Heegner cycle class c to a nonzero class c'.

There is an exact sequence

$$0 \longrightarrow A'[p]((k/2)+k-1) \longrightarrow A'((k/2)+k-1) \overset{p}{\longrightarrow}$$
$$A'((k/2)+k-1) \longrightarrow 0$$

and $H^0(\mathbb{Q}, A'((k/2)+k-1)) = 0$ (since $k > 2$ so $k-1 \neq k/2$, and the composition factors of $A'[p]$ are $\mathbb{F}_p, \mathbb{F}_p(1-k)$ and $\mathbb{F}_p(2-2k)$), so

$$H^1(\mathbb{Q}, A'[p]((k/2)+k-1))$$

injects into $H^1(\mathbb{Q}, A'((k/2)+k-1))$, and we get a nonzero class $d \in H^1(\mathbb{Q}, A'((k/2)+k-1))$. Since $(k/2) + k - 1$ is a noncentral critical point, conjecturally $H^1_f(\mathbb{Q}, V'((k/2)+k-1))$ should be trivial. Admitting this assumption, to show we have constructed an element of order p in $\mathrm{III}((k/2)+k-1)$ we just have to show that $d \in H^1_f(\mathbb{Q}, A'((k/2)+k-1))$.

Notice that the occurrence in $A'[p]$ of a submodule isomorphic to $\mathbb{F}_p(2 - 2k)$ fits well with Bloch–Kato and the Eisenstein prime in the denominator of $D^*_f(2k-2)$ (see Section 3). Of course, the presence of that Eisenstein prime has a simple explanation since there is a Bernoulli number in the calculation.

Any element of order p in $\mathrm{III}(k/2)$ for M should produce an element of order p in $\mathrm{III}((k/2)+k-1)$ for $\mathrm{Sym}^2(M)$, independent of that produced by the Heegner cycle. Since (for $k = 18, 22, 26$) the numerator of $D^*_f((k/2)+k-1)$ is not divisible by the square of the Eisenstein prime p, there should not be any elements of order p in $\mathrm{III}(k/2)$ (for M). Kolyvagin's method [Nekovář 1992] is unable to confirm this for such exceptional p, for which the map from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is not surjective.

9. CHECKING THE LOCAL CONDITIONS

Proposition 9.1. *For all primes $l \neq p$,*

$$\mathrm{res}_l \, d \in H^1_f(\mathbb{Q}_l, A'((k/2)+k-1)).$$

Proof. We know that $\mathrm{res}_l \, c \in H^1(\mathbb{Q}_l^{ur}/\mathbb{Q}_l, A[p](k/2))$, so that $\mathrm{res}_l \, c' \in H^1(\mathbb{Q}_l^{ur}/\mathbb{Q}_l, A'[p]((k/2)+k-1))$ and then $\mathrm{res}_l \, d \in H^1(\mathbb{Q}_l^{ur}/\mathbb{Q}_l, A'((k/2)+k-1))$. But it follows from the fact that A' is unramified at l that

$$H^1(\mathbb{Q}_l^{ur}/\mathbb{Q}_l, A'((k/2)+k-1))$$
$$= H^1_f(\mathbb{Q}_l, A'((k/2)+k-1)),$$

so we have what we want (see the proof of [Flach 1990, Theorem 3]). $\square$

Incidentally,

$$H^1_f(\mathbb{Q}_l, V'((k/2)+k-1))$$
$$\simeq V'((k/2)+k-1)/(1-\mathrm{Frob}_l)V'((k/2)+k-1),$$

$(V'$ is unramified at l), which is zero by the Weil conjectures, l being a prime of good reduction since f has level one. Hence $H^1_f(\mathbb{Q}_l, A'((k/2)+k-1))$ is actually trivial.

Proposition 9.2. $\mathrm{res}_p d \in H^1_f(\mathbb{Q}_p, A'((k/2)+k-1))$.

Proof. Bloch and Kato [1990, Lemma 4.4] construct a cohomological functor $\{h^i\}_{i\geq 0}$ on the Fontaine–Lafaille category of filtered Dieudonné modules over $\mathbb{Z}_p$. It satisfies $h^i(D) = 0$ 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.
    Let

$$D = P_f H^{k-1}_{\mathrm{dR}}(X \otimes \mathbb{Z}_p) \quad \text{and} \quad D' = \mathrm{Sym}^2(D).$$

By [Bloch and Kato 1990, Lemma 4.5(c)] and the application of [Faltings 1989] described in [Dummigan 2000, Section 7], we have

$$h^1(D) \simeq H^1_e(\mathbb{Q}_p, T),$$

where

$$H^1_e(\mathbb{Q}_p, T)$$
$$= \ker\big(H^1(\mathbb{Q}_p, T) \to H^1(\mathbb{Q}_p, V)/H^1_e(\mathbb{Q}_p, V)\big)$$

and

$$H^1_e(\mathbb{Q}_p, V) = \ker\big(H^1(\mathbb{Q}_p, V) \to H^1(\mathbb{Q}_p, B^{f=1}_{\mathrm{cris}} \otimes V)\big).$$

Note that D and D' are torsion-free, by [Dummigan 2000, Section 7].
    For an integer j let $D(j)$ be D with the Hodge filtration shifted by j. Then

$$h^1(D(j)) \simeq H^1_e(\mathbb{Q}_p, T(j))$$

(as long as $k-p+1 < j < p-1$, so that $D(j)$ satisfies the hypotheses of [Bloch and Kato 1990, Lemma 4.5]). By [Bloch and Kato 1990, Corollary 3.8.4],

$$H^1_f(\mathbb{Q}_p, V(j))/H^1_e(\mathbb{Q}_p, V(j))$$
$$\simeq D(j) \otimes \mathbb{Q}_p/(1-f)D(j) \otimes \mathbb{Q}_p,$$

where f is the Frobenius operator on crystalline cohomology. By [Scholl 1990, 1.2.4(ii)] and the Weil conjectures, $H^1_e(\mathbb{Q}_p, V(j)) = H^1_f(\mathbb{Q}_p, V(j))$, since $j \neq (k-1)/2$. Similarly,

$$H^1_e(\mathbb{Q}_p, V'(j)) = H^1_f(\mathbb{Q}_p, V'(j))$$

unless $j = k-1$.
    We have then $h^1(D(k/2)) \simeq H^1_f(\mathbb{Q}_p, T(k/2))$ and $h^1(D'((k/2)+k-1)) \simeq H^1_f(\mathbb{Q}_p, T'((k/2)+k-1))$.

The exact sequence in [Bloch and Kato 1990, p. 366, middle] gives us a commutative diagram

$$
\begin{array}{ccccc}
h^1\big(D(\tfrac{k}{2})\big) & \xrightarrow{\ p\ } & h^1\big(D(\tfrac{k}{2})\big) & \longrightarrow & h^1\big(D(\tfrac{k}{2})/pD(\tfrac{k}{2})\big) \\
\downarrow & & \downarrow & & \downarrow \\
H^1\big(\mathbb{Q}_p, T(\tfrac{k}{2})\big) & \longrightarrow & H^1\big(\mathbb{Q}_p, T(\tfrac{k}{2})\big) & \longrightarrow & H^1\big(\mathbb{Q}_p, A[p](\tfrac{k}{2})\big)
\end{array}
$$

The vertical arrows are all inclusions and we know that the image of $h^1(D(k/2))$ in $H^1(\mathbb{Q}_p, T(k/2))$ is exactly $H^1_f(\mathbb{Q}_p, T(k/2))$. The top right horizontal map is surjective since $h^2(D(k/2)) = 0$.
    The Heegner cycle class $c \in H^1(\mathbb{Q}_p, A[p](k/2))$ is in the image of $H^1_f(\mathbb{Q}_p, T(k/2))$ (by [Nekovář 1992]) and is thus in the image of $h^1(D(k/2)/pD(k/2))$. Recall that $A'[p]((k/2) + k - 1)$ has a Galois submodule isomorphic to $A[p](k/2)$. By the fullness of the Fontaine–Lafaille functor [1982] (see [Bloch and Kato 1990, Theorem 4.3]),

$$D'((k/2)+k-1)/pD'((k/2)+k-1)$$

has a subobject isomorphic to $D(k/2)/pD(k/2)$.
    It follows that the class

$$c' \in H^1(\mathbb{Q}_p, A'[p]((k/2)+k-1))$$

is in the image of

$$h^1\big(D'((k/2)+k-1)/pD'((k/2)+k-1)\big)$$

by the vertical map in the exact sequence analogous to the above. Since the map from

$$h^1\big(D'((k/2)+k-1)\big)$$

to $h^1(D'((k/2)+k-1)/pD'((k/2)+k-1))$ is surjective, c' lies in the image of $H^1_f(\mathbb{Q}_p, T'((k/2)+k-1))$. From this it follows that

$$d \in H^1_f(\mathbb{Q}_p, A'((k/2)+k-1)),$$

as desired. $\qquad\square$

So far, we have assumed that $A[p]$ has a Galois submodule isomorphic to $\mathbb{F}_p(1-k)$. In the other case, it has a Galois submodule isomorphic to $\mathbb{F}_p$. Then we similarly obtain an element of order p in $\mathrm{III}(k/2)$. Using Flach's generalisation [1990] of the Cassels–Tate pairing, we can reflect this across the central point to get an element of order p in $\mathrm{III}(k - 1 + (k/2))$, as desired. Our only assumption is of the triviality of $H^1_f(\mathbb{Q}, V'_p(k/2))$.

10. HIGHER SYMMETRIC POWERS

Let f be one of the cuspidal eigenforms we are concerned with in this paper (level one, rational coefficients). For $n \geq 1$ one may define an n-th symmetric power L-function

$$L_{n,f}(s) := \prod_p \prod_{i=0}^{n} (1 - \alpha_p^i \beta_p^{n-i} p^{-s})^{-1}.$$

The Euler product converges for $\operatorname{Re} s > n(k-1)/2 + 1$ but conjecturally there is an analytic continuation to the whole complex plane, with a functional equation relating the values at s and $(n-1)(k-1)+k-s$. This is known for $n \leq 3$, the case $n = 3$ being due to Garrett [1987], who shows that the sign in the functional equation is -1.

This forces the symmetric cube L-function $L_{3,f}(s)$ to vanish at the central point $s = (k-1) + k/2$. According to the conjecture of Beilinson and Bloch [Bloch 1984], there should consequently be a rationally defined, null-homologous algebraic cycle, of infinite order in the $((k-1)+k/2)$-th Chow group of the symmetric cube of the motive attached to f. An explicit construction of a candidate for such a cycle is easily obtained by generalising the (unmodified) diagonal cycle considered in [Gross and Schoen 1995] (where $k = 2$).

The Abel–Jacobi image of this cycle should give us (for any prime p), a nonzero element of

$$H_f^1(\mathbb{Q}, \operatorname{Sym}^3(A)(k-1+(k/2)).$$

Admitting this, in the case where p is an Eisenstein prime (for any k), arguments analogous to those of Sections 8 and 9 will then give us a nonzero element of $H_f^1(\mathbb{Q}, \operatorname{Sym}^4(A)(2(k-1)+(k/2)))$, which ought to be isomorphic to the appropriate Shafarevich–Tate group.

The right-of-centre critical points for $L_{4,f}(s)$ are of the form $s = 2(k-1)+r$ with even $2 \leq r \leq k-2$. Therefore when $k/2$ is even (i.e. for $k = 12, 16$ or 20), the Bloch–Kato conjecture leads us to expect that the ratio of $L_{4,f}(2(k-1)+(k/2))$ to any other critical value is an appropriate power of π times a rational number with p in the numerator.

For $k = 12$ ($f = \Delta$), highly accurate computations of approximate critical values for $L_{4,f}(s)$ were made, using over a thousand terms of the Euler product. The results of these computations, made

by G. Köckritz and R. Schillo on an IBM 370/168, were reported in [Zagier 1977]. The ratios of the approximate critical values turned out to be extremely close to powers of π times fairly simple rational numbers. It is very nice to see that in these rational numbers, the factor of $p = 691$ is there, exactly where we expect it to be. See the entry for $s = 28$ in the table at the end of Section 1 of [Zagier 1977].

In general, when n is odd the critical points are $s = ((n-1)/2)(k-1)+r$ with integer $1 \leq r \leq k-1$. When n is even the right-of-centre critical points are even integers of the form $s = (n/2)(k-1)+r$ with $1 \leq r \leq k-1$. Thus, r is odd when $n \equiv 2 \pmod 4$, but even when $n \equiv 0 \pmod 4$.

For any $k = 12, 16, 18, 20, 22$ or 26 and any Eisenstein p, we seem to have an element of order p in the Shafarevich–Tate group $\text{Ш}(2(k-1)+(k/2))$ for $\operatorname{Sym}^4(M)$. Using Flach's generalisation of the Cassels–Tate pairing [Flach 1990], we can reflect this across the central point to get an element of order p in $\text{Ш}(k-1+(k/2))$. Then, using twice the Ramanujan congruence trick of Section 8, we (hopefully) get an element of order p in $\text{Ш}(3(k-1)+(k/2))$ for $\operatorname{Sym}^6(M)$. Again, if it is $A[p]$ rather than $A[p](k-1)$ which has a trivial submodule, we may apply these steps in the opposite order to achieve the same result. Repetition of this process should give elements of order p in $\text{Ш}((n/2)(k-1)+(k/2))$ for $\operatorname{Sym}^n(M)$, for any even n. If $p > n(k-1)+2$ then we know that $c_p = 1$. So if $n < (p-2)/(k-1)$ and if $n/2$ and $k/2$ have the same parity, then we expect the ratio of $L_{n,f}((n/2)(k-1)+(k/2))$ to the other critical values to be an appropriate power of π times a rational number with p dividing the numerator.

Using the table in [Deligne 1979, 5.3], we find that for odd n, the sign in the functional equation of $L_{n,f}(s)$ is predicted to be -1 precisely when $n \equiv 3 \pmod 8$, or $n \equiv 1 \pmod 8$ and $k/2$ is odd, or $n \equiv 5 \pmod 8$ and $k/2$ is even. Hence when $n \equiv 5 \pmod 8$ or $n \equiv 7 \pmod 8$ we cannot be led to our expectations concerning divisibility of critical values for $\operatorname{Sym}^{n+1}(M)$ more directly by using cycles for $\operatorname{Sym}^n(M)$.

We have no experimental evidence for the above when $n > 4$ or $k > 12$. A recurrence relation described in [Watson 1949] (see also [Ramanujan 1916, Section 17]) allows the first N coefficients of Δ to be computed in time which grows like $N^{3/2}$. But for

$n = 8$ and $k = 12$, too many terms of the Euler product are required to get the necessary accuracy. For $k > 12$, Δ must be multiplied by Eisenstein series, and the time to get the first N coefficients grows like N^2. This makes it too difficult to get enough terms of the Euler product, even when $n = 4$. (Using all primes less than $N = 3000$ was not enough.) However, there is one more place to look for evidence of a similar phenomenon, where it turns out that the computational difficulties are not too great.

11. A TENSOR PRODUCT L-FUNCTION

Consider the forms of weights $k = 12$ and $k' = 26$ and form their tensor product L-function

$$L(s) := \prod_p \Big((1 - \alpha\alpha' p^{-s})(1 - \alpha\beta' p^{-s})$$
$$\times (1 - \beta\alpha' p^{-s})(1 - \beta\beta' p^{-s}) \Big)^{-1},$$

with the obvious notation for roots of Hecke polynomials.

The critical points for the associated motive are integers s such that $k - 1 < s \leq k' - 1$. Then $s = k - 1 + (k'/2)$ is critical iff $k' > 2k$, and we have chosen the only example for which both spaces of cusp forms are one-dimensional. Using Heegner cycles for $k' = 26$ and the Ramanujan congruence for $k = 12$, we would expect that $\pi^2 L(24)/L(25)$ is a rational number with $p = 691$ in the numerator.

Using Maple to multiply together all terms of the Euler product for primes less than 1000, we found an approximation whose continued fraction has partial quotients

$$[9, 1, 6, 1, 3, 1, 1, 22253370239262, \ldots].$$

This suggests that the exact value has continued fraction $[9, 1, 6, 1, 3, 2]$. This rational number is precisely $691/70$.

Actually, in the next section we will use a different method to recover this rational number $691/70$ without any need for approximation. Then we will look at tensor product L-functions for level-one forms of higher weights, and give an analytic reason to expect the occurrence of Eisenstein primes in the critical values, using Ramanujan-style congruences.

12. SHIMURA'S DIFFERENTIAL OPERATORS AND HOLOMORPHIC PROJECTION

For a positive integer k, let M_k be the space of holomorphic modular forms for $SL_2(\mathbb{Z})$, and let S_k be the subspace of cusp forms. Let G_k be the space of C^∞ complex-valued functions on the upper half plane, not necessarily holomorphic but satisfying the same transformation law as modular forms of weight k.

Shimura defined differential operators $\delta_\lambda : G_\lambda \to G_{\lambda+2}$, and more generally $\delta_\lambda^{(r)} : G_\lambda \to G_{\lambda+2r}$, by

$$\delta_\lambda = \frac{1}{2\pi i}\Big(\frac{\lambda}{2iy} + \frac{\partial}{\partial z} \Big)$$

and $\delta_\lambda^{(r)} = \delta_{\lambda+2r-2} \ldots \delta_{\lambda+2}\delta_\lambda$, where

$$\frac{\partial}{\partial z} = \frac{1}{2}\Big(\frac{\partial}{\partial x} - i\frac{\partial}{\partial y} \Big).$$

Given $f, g \in G_k$ whose product is zero at infinity, the Petersson inner product is defined by

$$(f, g) = \int_{\mathcal{F}} f(z)\overline{g(z)}y^{k-2}dy,$$

where $\mathcal{F}$ is a fundamental domain. Sturm [1980a] defined a "holomorphic projection" operator which, given $g \in G_k$ satisfying certain conditions (which we never need to worry about; but see [Sturm 1980a] or [Gross and Zagier 1986, pp. 288–290]) produces $\mathrm{Hol}\, g \in S_k$ with the property that $(f, g) = (f, \mathrm{Hol}\, g)$ for all $f \in S_k$. If $g = \sum_{m=0}^{\infty} a_m(y)q^m$ and $\mathrm{Hol}\, g = \sum_{m=1}^{\infty} a_m q^m$ then

$$a_m = \frac{(4\pi m)^{k-1}}{(k-2)!}\int_0^\infty a_m(y)e^{-4\pi my}y^{k-2}dy.$$

The effect is to delete the constant term and to replace $y^{-j}q^m$ by

$$\frac{(k-2-j)!}{(k-2)!}(4\pi m)^j q^m.$$

Let E_k be the normalised Eisenstein series of weight k. Its q-expansion is

$$E_k = 1 - (2k/B_k)\sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n,$$

where $\sigma_r(n) = \sum_{d|n, d>0} d^r$.

Given cuspidal eigenforms $f = \sum a_n q^n$ of weight k' and $g = \sum b_n q^n$ of weight k, let's say both of level

one, with $k' > k$, let $L(s)$ be the tensor product L-function defined in the previous section. It is known [Shimura 1976] that

$$L(s) = \zeta(2s + 2 - k - k')D(s, f, g),$$

where ζ is the Riemann zeta function and

$$D(s, f, g) = \sum_{n=1}^{\infty} a_n b_n n^{-s}$$

is the Rankin convolution. Now when $s = (k'/2) + k - 1$ we find $2s + 2 - k - k' = k$, and $\zeta(k)$ gives us the Eisenstein prime factor we are looking for. To show that it is not cancelled by a factor in the value of the Rankin convolution at another point, we use [Shimura 1976, Theorem 2], which tells us that

$$D(k' - 1 - r, f, g) = c\pi^{k'-1}(f, g\delta_\lambda^{(r)}E_\lambda),$$

where

$$c = \frac{(k' - k - 2r - 1)!}{(k' - 2 - r)! \, (k' - k - r - 1)!}(-1)^r 4^{k'-1},$$

$r \geq 0$ is an integer such that $k + 2r < k'$, and $\lambda = k' - k - 2r$. (In all the cases we consider, λ will be comfortably greater than 2.)

We re-examine the case $k' = 26$, $k = 12$, and evaluate the ratio $\pi^2 L(24)/L(25)$. For $s = 24$ we have $26 - 1 - r = 24$ so $r = 1$ and $\lambda = 26 - 12 - 2 = 12$.

$$E_{12} = 1 + \tfrac{65520}{691}(q + 2049q^2 + \cdots)$$

so

$$\delta_{12}E_{12} = \tfrac{65520}{691}(q + 4098q^2 + \cdots)$$
$$- \frac{3}{\pi y}\left(1 + \tfrac{65520}{691}(q + 2049q^2 + \cdots)\right).$$

Now $g = q - 24q^2 + \cdots$, so $g\delta_{12}E_{12} = (-3/(\pi y))q + \cdots$ and

$$\mathrm{Hol}(g\delta_{12}E_{12}) = \frac{-3}{\pi}4\pi\frac{1}{24}q + \cdots = (-1/2)q + \cdots.$$

Since S_{26} is one-dimensional $\mathrm{Hol}(g\delta_{12}E_{12})$ must be equal to $-\tfrac{1}{2}f$. Hence

$$D(24, f, g) = \frac{-(11!)}{23! \, 12!}(4\pi)^{25}(-1/2)(f, f).$$

For $s = 25$ we have $r = 0, \lambda = 14$ and $gE_{14} = q + \cdots$, so $gE_{14} = f$. Hence

$$D(25, f, g) = \frac{13!}{24! \, 13!}(4\pi)^{25}(f, f)$$

and we find that

$$\frac{D(24, f, g)}{D(25, f, g)} = \frac{-24 \cdot 13}{13 \cdot 12}(-1/2) = 1.$$

Then

$$\pi^2 \frac{L(24)}{L(25)} = \pi^2 \frac{\zeta(12)}{\zeta(14)} = \frac{2^{12}B_{12}/12!}{2^{14}B_{14}/14!} = \frac{691}{70}.$$

13. ANOTHER CALCULATION

We shall see that the calculation of the previous section was a very special case and did not really give a fair indication of what is going on in general. This time let $k = 12$ again, but let $k' = 34$. The dimension of S_{34} is 2, and the two normalised cuspidal eigenforms are

$$f_1 = q + (-60840 + 72\sqrt{2356201})q^2 + \cdots$$

and

$$f_2 = q + (-60840 - 72\sqrt{2356201})q^2 + \cdots.$$

In this case $(k'/2) + k - 1 = 17 + 11 = 28$. We will use Shimura's formula to calculate $D(28, f_1, g)$ and $D(30, f_1, g)$. (Again, g is the normalised cusp form of weight 12.)

Let $L(s)$ be the tensor product L-function attached to f_1 and g. Then

$$L(s) = \zeta(2s - 44)D(s, f_1, g),$$

so

$$L(30) = \zeta(16)D(30, f_1, g),$$
$$L(28) = \zeta(12)D(28, f_1, g).$$

Since 3617 divides the numerator of B_{16}, we might then expect 3617 to divide the numerator of the rational number $L(30)/\pi^4 L(28)$. Let us see how this fails to happen.

For $s = 30$, $r = k' - 1 - 30 = 3$. We have

$$D(30, f_1, g) = c\pi^{33}(f_1, \mathrm{Hol}(g\delta_{16}^{(3)}E_{16})),$$
$$E_{16} = 1 + \tfrac{16320}{3617}(q + 32769q^2 + \cdots),$$
$$\delta_{16}^{(3)}E_{16} = \frac{-153}{2\pi^3 y^3}$$
$$+ \tfrac{16320}{3617}\left(1 - \frac{27}{2\pi y} + \frac{459}{8\pi^2 y^2} - \frac{153}{2\pi^3 y^3}\right)q + \cdots,$$
$$\mathrm{Hol}(g\delta_{16}^{(3)}E_{16}) = -\tfrac{29!}{32!}(4896q - \tfrac{3405187584}{3617}q^2 + \cdots).$$

Since f_1 and f_2 span S_{34} there exist α and β such that

$$\mathrm{Hol}(g\delta_{16}^{(3)}E_{16}) = \tfrac{-29!}{32!}(\alpha f_1 + \beta f_2).$$

Then $D(30, f_1, g) = c\pi^{33}(\frac{-29!}{32!})\alpha$. Letting

$$\gamma = -60840 + 72\sqrt{2356201},$$
$$\gamma' = -60840 - 72\sqrt{2356201},$$

we solve the equations for the first two coefficients:

$$\alpha + \beta = 4896,$$
$$\gamma\alpha + \gamma'\beta = -\frac{3405187584}{3617},$$

to find

$$\alpha, \beta = \frac{20862783833616 \pm 7458334384\sqrt{2356201}}{479 \cdot 4919 \cdot 3617}.$$

The norm of the numerator is

$$2^{13}.5^2.7^2.17^2.479.522887.85133.4919.$$

The 3617 in the denominator of α will completely cancel the 3617 in the numerator of $\zeta(16)/\pi^{16}$. The prime 3617 is inert in the field $\mathbb{Q}(\sqrt{2356201})$. We have just seen that 3617 does not divide the algebraic number $L(30)/\pi^{49}(f_1, f_1)$.

For $L(28)$ we do not want the factor of 691 in the numerator of $\zeta(12)/\pi^{12}$ to be cancelled, yet looking at the previous calculation it appears likely that something similar will occur. This time $r = 5$.

$$E_{12} = 1 + \frac{65520}{691}(q + 2049q^2 + \cdots).$$

We find that

$$g\delta_{12}^{(5)}E_{12} = -\frac{4095}{8\pi^5 y^5}q$$
$$+ \frac{65520}{691}\left(1 - \frac{20}{\pi y} + \frac{150}{\pi^2 y^2} - \frac{525}{\pi^3 y^3} + \frac{6825}{8\pi^4 y^4} - \frac{6117}{16\pi^5 y^5}\right)q^2$$
$$+ \cdots,$$

but then a miracle occurs, because

$$\text{Hol}(g\delta_{12}^{(5)}E_{12}) = -\frac{27!}{32!}(4193280q - 402554880q^2 + \cdots),$$

without any 691 in the denominator of the second coefficient. It is natural to suspect that this has something to do with Ramanujan's congruence, and we shall see in the next section that this is indeed the case.

If

$$\text{Hol}(g\delta_{12}^{(5)}E_{12}) = -\frac{27!}{32!}(\alpha f_1 + \beta f_2)$$

then

$$\alpha, \beta = \frac{4940105264640 \pm 1768865280\sqrt{2356201}}{479 \cdot 4919}.$$

This time the norm of the numerator (excluding the factorial) is

$$2^{21}.3^2.5^2.7^3.13^2.479.264283.4919,$$

again a very smooth number. Note that the primes 479 and 4919 are bad because they divide 2356201. We have seen that the algebraic number

$$\frac{L(28)}{\pi^{45}(f_1, f_1)}$$

does manage to be divisible by 691.

14. TENSOR PRODUCT L-FUNCTIONS FOR HIGHER WEIGHTS

Let $f = \sum a_n q^n$ and $g = \sum b_n q^n$ be normalised cuspidal eigenforms of level one and weights k', k respectively, with $k' > k$ and $k'/2$ odd. Let $L(s)$ be their tensor product L-function. Recall that

$$L(s) = \zeta(2s + 2 - k - k')D(s, f, g),$$

and

$$D(k' - 1 - r, f, g) = c\pi^{k'-1}(f, g\delta_\lambda^{(r)}E_\lambda),$$

where

$$c = \frac{(k' - k - 2r - 1)!}{(k' - 2 - r)!(k' - k - r - 1)!}(-1)^r 4^{k'-1},$$

$r \geq 0$ is an integer such that $k + 2r < k'$, and $\lambda = k' - k - 2r$.

The point we are most interested in is $s = (k'/2) + k - 1$. This corresponds to $r = (k'/2) - k$ (which is odd) and $\lambda = k$.

Let $g = g^{(1)}, g^{(2)}, \ldots, g^{(d)}$ be the distinct conjugates of g under the action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the Fourier coefficients. Write $g^{(i)} = \sum_{n=1}^{\infty} b_n^{(i)}q^n$. Let K_g be the field generated by the coefficients of g. It has been conjectured by Maeda that (for level one), the conjugates of g always span the whole of S_k. This has been confirmed for $k \leq 2000$; see [Buzzard 1996; Farmer and James $\geq$ 2001]. If it is the case, and if $B_k/2k$ has a prime divisor p, then the next proposition shows that the coefficients of g satisfy a Ramanujan-style congruence.

Proposition 14.1. *Let p be a prime dividing the numerator of $B_k/2k$. Let $\mathfrak{p}$ be a prime ideal dividing p, in the ring of integers of the field generated by the coefficients of all the cuspidal eigenforms of weight k. Then there exists a cuspidal eigenform $\sum c_n q^n$ of weight k such that $c_n \equiv \sigma_{k-1}(n) \pmod{\mathfrak{p}}$ for all $n \geq 1$.*

This is precisely [Datskovsky and Guerzhoy 1996, Theorem 2]. Note that if all the cuspidal eigenforms

are Galois conjugate, the coefficients of g satisfy the same congruence modulo some conjugate of $\mathfrak{p}$.

Let K_f be the field generated by the Fourier coefficients of f. Let $K = K_f K_g$ be the field generated by the Fourier coefficients of f and g. Let $\{f_1, \ldots, f_{d'}\}$ be an orthogonal basis for $S_{k'}$ consisting of normalised eigenforms. Let L be the field generated by the coefficients of $g, f_1, \ldots, f_{d'}$. Let $f_i = \sum a_{ij} q^j$.

Theorem 14.2. *Suppose that for all $n \geq 1$, $b_n \equiv \sigma_{k-1}(n)$ (mod $\mathfrak{p}$) (in the ring of integers of K_g), with $\mathfrak{p}$ dividing p, a prime divisor of $B_k/2k$, satisfying $p > k' - 2$. Let $\mathfrak{p}'$ be any prime ideal of the ring of integers of K, dividing $\mathfrak{p}$. Suppose that $\{f_1, \ldots, f_{d'}\}$ is linearly independent modulo any prime ideal dividing p (i.e., p is not a congruence prime for $S_{k'}$). Then*

$$\mathrm{ord}_{\mathfrak{p}'}(L((k'/2)+k-1)/(\pi^{k'+k-1}(f,f))) > 0.$$

(Note that this number is in K, by [Shimura 1976, Theorem 3].)

Proof. It suffices to show that

$$\mathrm{ord}_{\mathfrak{p}'}\left(\frac{-B_k}{2k}(f, g\delta_k^{(r)}E_k)/(f,f)\right) > 0.$$

By [Hida 1985, Lemma 5.3],

$$\mathrm{Hol}(g\delta_l^{(r)}g') = (-1)^r \mathrm{Hol}(g'\delta_k^{(r)}g)$$

for any $g' \in M_l$. Letting $g' = g$ and noting that r is odd, we find $\mathrm{Hol}(g\delta_k^{(r)}g) = 0$, therefore if we let $h = g + (B_k/(2k))E_k$, then it suffices to show that $\mathrm{ord}_{\mathfrak{p}'}((f, g\delta_k^{(r)}h)/(f,f)) > 0$. All (but one) of the coefficients of h are algebraic integers divisible by $\mathfrak{p}$, thanks to the Ramanujan-style congruence. Therefore, the coefficients of $h' := \mathrm{Hol}(g\delta_\lambda^{(r)}h)$ are all integral at $\mathfrak{p}$ and divisible by $\mathfrak{p}$. (Viewing the $(k'-2)!$ in the denominator of the formula for holomorphic projection, this is where we need $p > k' - 2$.) The linear independence assumption implies that if $h' = \sum_{i=1}^{d'} \alpha_i f_i$ then α_1 is divisible by $\mathfrak{p}'$, as required. $\square$

Of course, the interest of this theorem is that it accords with what is predicted by (the generalisation to nonrational coefficients of) the Bloch–Kato conjecture, since $\mathfrak{p}'$-torsion in some Shafarevich–Tate group can be constructed just as before. (To avoid primes which might be involved in fudge factors, suppose $p > k+k'$.) Since $k'/2$ is odd, $L_f(k'/2) = 0$

and we get the algebraic cycles we need if we assume the Beilinson–Bloch conjecture. We also have to assume that their Abel–Jacobi images are nonzero, and that the Shafarevich–Tate group (for the tensor product at $(k'/2)+k-1$) is the same as the Selmer group. To avoid divisors of p appearing in the denominators of the projectors used to construct the motives, we really should assume that p is not a congruence prime for S_k or $S_{k'}$.

For Hilbert modular forms (of scalar weights) over a totally real field F, the $(-1)^r$ in Hida's Lemma 5.3 would have to be replaced by $(-1)^{r[F:\mathbb{Q}]}$, so we need to assume that $[F : \mathbb{Q}]$ is odd. As noted in the introduction, this is precisely the condition we need to make $L_f(k'/2)$ vanish (retaining, of course, the assumption that $k'/2$ is odd). We also assume the narrow class number of F is one, so that there is only one cusp and therefore one Eisenstein series. In general, the factors $c_{\mathfrak{p}}(j)$ and $\#\Gamma_F(j)$ appearing in the Bloch–Kato conjecture are not as well understood as in the case $F = \mathbb{Q}$.

For the symmetric square,

$$D_f(s) = \frac{\zeta(2s+2-2k)}{\zeta(s+1-k)} \sum_{n=1}^{\infty} a_n^2 n^{-s},$$

a theta series, as well as an Eisenstein series (of half-integral weight), occurs in the Shimura–Rankin–Selberg integral for $\sum_{n=1}^{\infty} a_n^2 n^{-s}$; see [Sturm 1980b]. When $s = (k/2) + k - 1$ we have $2s + 2 - 2k = k$, and $\zeta(k)$ gives us an Eisenstein prime. While there does not seem to be any particular reason for this prime to get cancelled, we can see that this is not a satisfactory explanation. For example, when $k = 22$ and $r = k/2 = 11$, let's say $\zeta(22)$ puts factors of 131 and 593 into $D_f^*(r+k-1)$. Then when r goes up to 13, $\zeta(26)$ should put a factor of 657931 into $D_f^*(r+k-1)$, but there isn't one.

15. KLINGEN–EISENSTEIN SERIES AND KUROKAWA'S CONGRUENCES

Let f be one of the modular forms considered in Section 3. Associated to f is its Klingen–Eisenstein series $[f]$, a noncuspidal Siegel modular eigenform of weight k and degree two [Klingen 1967]. For us, the important fact about the relation between f and $[f]$ is that, if $L_{[f]}(s)$ is the L-function naturally

associated with the eigenform $[f]$, then $L_{[f]}(s) = L_f(s)L_f(s-(k-2))$.

Kurokawa [1979] proved that when $k = 20$ there exists a cuspidal Siegel eigenform F, of weight k and degree two, such that the Hecke eigenvalues of F and $[f]$ are congruent modulo 71^2. Mizumoto [1986] proved that when $k = 22$ there exists a cuspidal Siegel eigenform F, of weight k and degree two, such that the Hecke eigenvalues of F and $[f]$ are congruent modulo 61.103. In the case $k = 26$, the multiplicity-one result needed to apply Mizumoto's general theorem follows from the calculations in [Skoruppa 1992]. From the data in the same work we check that F must be $\gamma26a$ (when $p = 163$) or $\gamma26b$ (when $p = 187273$). In all the cases above, the Fourier coefficients and Hecke eigenvalues of F are rational.

The congruences result from the appearence of $D_f(2k-2)$ in the denominator of an expression for the Fourier coefficients of $[f]$ [Mizumoto 1981].

Let p be 71 (when $k = 20$), or 61 or 103 (when $k = 22$), or 163 or 187273 (when $k = 26$), and let F be as above. Thanks to Weissauer [$\geq$ 2001] we know there is a continuous representation

$$\theta_p : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(W_p)$$

(W_p is a four-dimensional vector space over $\overline{\mathbb{Q}}_p$), such that

1. θ_p is unramified at l for all primes $l \neq p$;
2. If Frob_l is a Frobenius element at l then the characteristic polynomial of Frob_l^{-1} acting on W_p is the degree four polynomial with roots reciprocal to those of the polynomial associated to the l-th Euler factor of $L_F(s)$.

(This θ_p exists for any prime p, not just our special choices.)

We make the following assumptions.

1. W_p is a four-dimensional vector space over $\mathbb{Q}_p$ itself.
2. θ_p is absolutely irreducible.
3. With respect to some symplectic form on W_p, the image of θ_p is contained in the group of symplectic similitudes $GSp_4(\mathbb{Q}_p)$.

The congruence between the Hecke eigenvalues of F and f, and the equality

$$L_{[f]}(s) = L_f(s)L_f(s-(k-2)),$$

force us to the conclusion that the reduction modulo p of any Galois-invariant $\mathbb{Z}_p$-lattice in W_p has composition factors isomorphic to $A[p]$ and $A[p](2-k)$. Note that these factors are irreducible (since the coefficients of f do not satisfy a congruence modulo p), and that we have used the Brauer–Nesbitt theorem.

Proposition 15.1. *Admitting the assumptions above, there exists a Galois-stable $\mathbb{Z}_p$ lattice S_p in W_p such that if $B := W_p/S_p$ then there is a nonsplit exact sequence of $\mathbb{F}_p[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-modules*

$$0 \longrightarrow A[p](2-k) \xrightarrow{i} B[p] \xrightarrow{\pi} A[p] \longrightarrow 0.$$

Moreover, letting s be a section for π as a map of $\mathbb{F}_p$-vector spaces, there exists a skew-symmetric form φ on $B[p]$ such that, for all $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and $v, w \in B[p]$, $\varphi(g.v, g.w) = \chi(g)\varphi(v, w)$. Here, χ is the $(2k-3)^{rd}$ power of the p-cyclotomic character. Further, $i(A[p](2-k))$ and $s(A[p])$ are isotropic subspaces for φ. There exists a basis $\{v_1, v_2\}$ for $A[p]$ with dual basis $\{w_1, w_2\}$ for $A[p](k-1)$ such that, when considered as bases for $i(A[p](2-k))$ and $s(A[p])$ respectively, we have $\varphi(v_i, w_j) = \delta_{ij}$.

All this follows from [Urban 1998, Proposition 1.1]. Now, following [Urban 1998, Section 3.4], we define a cocycle $C : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Hom}_{\mathbb{F}_p}(A[p], A[p](2-k))$ by

$$C(g)(w) = i^{-1}(s(w) - g.s(g^{-1}.w)).$$

This cocycle is not a coboundary since the exact sequence above is nonsplit. The choice of section s does not affect the cohomology class of C. Since $A[p]$ is dual to $A[p](k-1)$ as a Galois module, we have a nonzero element $c \in H^1(\mathbb{Q}, A[p] \otimes A[p](1))$ (because $(k-1) + (2-k) = 1$). In fact, just as in [Urban 1998, Section 3.4] (proof of Fact 2, which uses Proposition 15.1 above), we have

$$c \in H^1(\mathbb{Q}, (\mathrm{Sym}^2 A[p])(1)) = H^1(\mathbb{Q}, A'[p](1)).$$

Proposition 15.2. *The element c gives us a nonzero class $d \in H^1(\mathbb{Q}, A'(1))$.*

Proof. We need to show that $H^0(\mathbb{Q}, A'(1))$ is trivial, so that the map $H^1(\mathbb{Q}, A'[p](1)) \to H^1(\mathbb{Q}, A'(1))$ is injective. It suffices to prove that

$$H^0(\mathbb{Q}, (A[p] \otimes A[p])(1))$$

is trivial. Bearing in mind that $A[p]$ is dual to $A[p](k-1)$, an element of

$$H^0(\mathbb{Q}, \, (A[p] \otimes A[p])(1))$$

gives a Galois-equivariant map from $A[p]$ to $A[p](2-k)$, which must be trivial since these are nonisomorphic irreducible $\mathbb{F}_p[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-modules. $\square$

Proposition 15.3. *For any prime $l \neq p$,*

$$\mathrm{res}_l \, d \in H^1_f(\mathbb{Q}_l, \, A'(1)).$$

Proof. For any prime $l \neq p$, the restriction of c to $H^1(I_l, A'[p](1))$ is trivial, where I_l is an inertia group at l. This simply follows from the triviality of the $\mathbb{F}_p[I_l]$-modules $A[p](2-k)$, $B[p]$ and $A[p]$, which implies that the exact sequence giving rise to c splits as a sequence of $\mathbb{F}_p[I_l]$-modules. Hence $\mathrm{res}_l \, c \in H^1(\mathbb{Q}_l^{ur}/\mathbb{Q}_l, \, A'[p](1))$, so $\mathrm{res}_l \, d \in H^1(\mathbb{Q}_l^{ur}/\mathbb{Q}_l, A'(1))$, which is the same as $H^1_f(\mathbb{Q}_l, \, A'(1))$ since A' is unramified at l (see the proof of Theorem 3 of [Flach 1990]). $\square$

Though we have shown that d satisfies the local conditions at all primes $l \neq p$, we are unable to deal with the local condition at p. But if d does give us an element of order p in $\mathrm{III}(1)$ for $\mathrm{Sym}^2(M)$, then [Flach 1990] allows us to reflect across the central point $k - \frac{1}{2}$ and get an element of order p in $\mathrm{III}(2k-2)$. Recall that the existence of such an element was suggested by the Bloch–Kato conjecture and the results in Section 3.

ACKNOWLEDGEMENTS

REFERENCES

[Amice and Vélu 1975] Y. Amice and J. Vélu, "Distributions p-adiques associées aux séries de Hecke", pp. 119–131 in *Journées Arithmétiques de Bordeaux* (Bordeaux, 1974), Astérisque **24–25**, Soc. math. France, Paris, 1975.

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

[Bloch and Kato 1990] S. Bloch and K. Kato, "L-functions and Tamagawa numbers of motives", pp. 333–400 in *The Grothendieck Festschrift*, vol. I, Prog. Math. **56**, Birkhäuser, Boston, 1990.

[Buzzard 1996] K. Buzzard, "On the eigenvalues of the Hecke operator T_2", *J. Number Theory* **57**:1 (1996), 130–132.

[Cremona and Mazur 2000] J. E. Cremona and B. Mazur, "Visualizing elements in the Shafarevich-Tate group", *Experiment. Math.* **9**:1 (2000), 13–28.

[Datskovsky and Guerzhoy 1996] B. Datskovsky and P. Guerzhoy, "On Ramanujan congruences for modular forms of integral and half-integral weights", *Proc. Amer. Math. Soc.* **124**:8 (1996), 2283–2291.

[Deligne 1969] P. Deligne, "Formes modulaires et représentations l-adiques", pp. 139–172, exp. 355 in *Séminaire Bourbaki*, Lecture Notes in Math. **179**, Springer, 1969.

[Deligne 1979] P. Deligne, "Valeurs de fonctions L et périodes d'intégrales", pp. 313–346 in *Automorphic forms, representations and L-functions* (Corvallis, OR, 1977), vol. 2, edited by A. Borel and W. Casselman, Proc. Sympos. Pure Math. **33**, Amer. Math. Soc., Providence, 1979.

[Diamond et al. $\geq$ 2001] F. Diamond, M. Flach, and L. Guo, "On the Bloch–Kato conjecture for adjoint motives of modular forms", *Math. Res. Lett.*. To appear.

[Dummigan 2000] N. Dummigan, "Period ratios of modular forms", *Math. Ann.* **318**:3 (2000), 621–636.

[Faltings 1989] G. Faltings, "Crystalline cohomology and p-adic Galois-representations", pp. 25–80 in *Algebraic analysis, geometry, and number theory* (Baltimore, 1988), edited by J.-I. Igusa, Johns Hopkins Univ. Press, Baltimore, MD, 1989.

[Farmer and James $\geq$ 2001] D. W. Farmer and K. James, "The irreducibility of some level-1 Hecke polynomials", preprint. See http://www.math.clemson.edu/~kevja/PAPERS/FarmerJames2000.dvi. To appear in *Math. Comp.*

[Flach 1990] M. Flach, "A generalisation of the Cassels–Tate pairing", *J. Reine Angew. Math.* **412** (1990), 113–127.

[Fontaine and Laffaille 1982] J.-M. Fontaine and G. Laffaille, "Construction de représentations p-adiques", *Ann. Sci. École Norm. Sup.* (4) **15**:4 (1982), 547–608 (1983).

[Garrett 1987] P. B. Garrett, "Decomposition of Eisenstein series: Rankin triple products", *Ann. of Math.* (2) **125**:2 (1987), 209–235.

[Gross and Schoen 1995] B. H. Gross and C. Schoen, "The modified diagonal cycle on the triple product of a pointed curve", *Ann. Inst. Fourier (Grenoble)* **45**:3 (1995), 649–679.

[Gross and Zagier 1986] B. H. Gross and D. B. Zagier, "Heegner points and derivatives of *L*-series", *Invent. Math.* **84**:2 (1986), 225–320.

[Guo 1996] L. Guo, "On the Bloch-Kato conjecture for Hecke *L*-functions", *J. Number Theory* **57**:2 (1996), 340–365.

[Han 1997] B. Han, *On Bloch-Kato's Tamagawa number conjecture for Hecke characters of imaginary quadratic fields*, Ph.D. thesis, University of Chicago, 1997.

[Harrison 1994] M. C. Harrison, *On the conjecture of Bloch–Kato for Grossencharacters over* $\mathbb{Q}(i)$, Ph.D. thesis, Cambridge University, 1994.

[Hida 1985] H. Hida, "A *p*-adic measure attached to the zeta functions associated with two elliptic modular forms, I", *Invent. Math.* **79**:1 (1985), 159–195.

[Huber and Kings 2000] A. Huber and G. Kings, "Bloch–Kato conjecture and Main Conjecture of Iwasawa theory for Dirichlet characters", preprint, 2000. See http://www.math.uiuc.edu/Algebraic-Number-Theory/0279/.

[Kings 2001] G. Kings, "The Tamagawa number conjecture for CM elliptic curves", *Invent. Math.* **143**:3 (2001), 571–627.

[Klingen 1967] H. Klingen, "Zum Darstellungssatz für Siegelsche Modulformen", *Math. Z.* **102** (1967), 30–43. Correction in **105** (1968), 399–400.

[Kurokawa 1979] N. Kurokawa, "Congruences between Siegel modular forms of degree two", *Proc. Japan Acad. Ser. A Math. Sci.* **55**:10 (1979), 417–422.

[Manin 1973] Y. I. Manin, "Periods of parabolic forms and *p*-adic Hecke series", *Mat. Sbornik* **92** (1973), 371–393.

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

[Mizumoto 1981] S. Mizumoto, "Fourier coefficients of generalized Eisenstein series of degree two. I", *Invent. Math.* **65**:1 (1981), 115–135.

[Mizumoto 1986] S. Mizumoto, "Congruences for eigenvalues of Hecke operators on Siegel modular forms of degree two", *Math. Ann.* **275**:1 (1986), 149–161.

[Nekovář 1992] J. Nekovář, "Kolyvagin's method for Chow groups of Kuga-Sato varieties", *Invent. Math.* **107**:1 (1992), 99–125.

[Nekovář 1995] J. Nekovář, "On the *p*-adic height of Heegner cycles", *Math. Ann.* **302**:4 (1995), 609–686.

[Ramanujan 1916] S. Ramanujan, "On certain arithmetical functions", *Trans. Camb. Phil. Soc.* **22**:9 (1916), 159–184.

[Scholl 1990] A. J. Scholl, "Motives for modular forms", *Invent. Math.* **100**:2 (1990), 419–430.

[Serre 1969] J.-P. Serre, "Une interprétation des congruences relatives à la fonction τ de Ramanujan", fasc. 1, exp. 14 in *Séminaire Delange–Pisot–Poitou: 1967/68*, Secrétariat mathématique, Paris, 1969.

[Serre 1973] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Math. **7**, Springer, New York, 1973.

[Shimura 1975] G. Shimura, "On the holomorphy of certain Dirichlet series", *Proc. London Math. Soc.* (3) **31**:1 (1975), 79–98.

[Shimura 1976] G. Shimura, "The special values of the zeta functions associated with cusp forms", *Comm. Pure Appl. Math.* **29**:6 (1976), 783–804.

[Skoruppa 1992] N.-P. Skoruppa, "Computations of Siegel modular forms of genus two", *Math. Comp.* **58**:197 (1992), 381–398.

[Sturm 1980a] J. Sturm, "Projections of C^∞ automorphic forms", *Bull. Amer. Math. Soc. (N.S.)* **2**:3 (1980), 435–439.

[Sturm 1980b] J. Sturm, "Special values of zeta functions, and Eisenstein series of half integral weight", *Amer. J. Math.* **102**:2 (1980), 219–240. Addendum in **102**:4 (1980), 781–783.

[Swinnerton-Dyer 1973] H. P. F. Swinnerton-Dyer, "On *l*-adic representations and congruences for coefficients of modular forms", pp. 1–55 in *Modular functions of one variable III* (Antwerp, 1972), edited by W. Kuyk and J.-P. Serre, Lecture Notes in Math. **350**, Springer, Berlin, 1973.

[Urban 1998] E. Urban, "Selmer groups and the Eisenstein-Klingen Ideal", preprint, 1998. See http://www.math.uiuc.edu/Algebraic-Number-Theory/0107/.

[Vishik 1976] M. Vishik, "Nonarchimedean measures connected with Dirichlet series", *Math. USSR Sb.* **28** (1976), 216–228.

[Watson 1949] G. N. Watson, "A table of Ramanujan's function $\tau(n)$", *Proc. London Math. Soc.* (2) **51** (1949), 1–13.

[Weissauer ≥ 2001] R. Weissauer, "A special case of the fundamental lemma: the case GSp_4, I, II, III", preprints.

[Zagier 1977] D. Zagier, "Modular forms whose coefficients involve zeta-functions of quadratic fields", pp. 105–169 in *Modular functions of one variable VI* (Bonn, 1976), edited by J.-P. Serre and D. Zagier, Lecture Notes in Mathematics **627**, Springer, Berlin, 1977.

Neil Dummigan, Department of Pure Mathematics, University of Sheffield, Hicks Building, Hounsfield Road, Sheffield, S3 7RH, United Kingdom (n.p.dummigan@shef.ac.uk)