Journal of Number Theory 130 (2010) 2078–2091

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Symmetric square L-values and dihedral congruences for cusp forms[☆]

Neil Dummigan[a,*], Bernhard Heim[b]

[a] University of Sheffield, Department of Pure Mathematics, Hicks Building, Hounsfield Road, Sheffield, S3 7RH, UK
[b] German University of Technology in Oman (GUtech), Department of Applied Information Technology, PO Box 1816 Athaibah, PC 130, Corner of Beach Road and Wadi Athaibah Way, Sultanate of Oman

ARTICLE INFO

Article history:
Received 4 January 2010
Available online 1 April 2010
Communicated by David Goss

MSC:
11F67
11B68
11E41
11F33
11F80

Keywords:
Modular form
L-function
Bloch–Kato conjecture

ABSTRACT

Let $p \equiv 3 \pmod 4$ be a prime, and $k = (p+1)/2$. In this paper we prove that two things happen if and only if the class number $h(\sqrt{-p}) > 1$. One is the non-integrality at p of a certain trace of normalised critical values of symmetric square L-functions, of cuspidal Hecke eigenforms of level one and weight k. The other is the existence of such a form g whose Hecke eigenvalues satisfy "dihedral" congruences modulo a divisor of p (e.g. $p = 23$, $k = 12$, $g = \Delta$). We use the Bloch–Kato conjecture to link these two phenomena, using the Galois interpretation of the congruences to produce global torsion elements which contribute to the denominator of the conjectural formula for an L-value. When $h(\sqrt{-p}) = 1$, the trace turns out always to be a p-adic unit.

1. Introduction

Let $S_k(\Gamma)$ be the vector space of cuspidal modular forms of integer weight k with respect to $\Gamma := \mathrm{SL}_2(\mathbb{Z})$. Let $\| \ \|$ be the Petersson norm. Let $g \in S_k(\Gamma)$ be a primitive Hecke eigenform with Fourier expansion $g(\tau) = q + \sum_{n=2}^{\infty} a_n q^n$ ($q := e^{2\pi i\tau}$ as usual). The Satake parameters α_p, β_p are the roots of the polynomial $x^2 - a_p x + p^{k-1}$. Then the symmetric square L-function of g is defined by the Euler product

[☆] This work was partly supported by the *Max-Planck-Institut für Mathematik*, Bonn.

[*] Corresponding author. Fax: +44 (0)114 222 3809.
E-mail addresses: n.p.dummigan@shef.ac.uk (N. Dummigan), bernhard.heim@gutech.edu.om (B. Heim).

0022-314X/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2010.01.012

$$L\big(\mathrm{Sym}^2(g),s\big) := \prod_p \big\{\big(1-\alpha_p^2 p^{-2s}\big)\big(1-\alpha_p\beta_p p^{-2s}\big)\big(1-\beta_p^2 p^{-2s}\big)\big\}^{-1}. \tag{1.1}$$

The completion of this L-function at infinity is given by

$$\widehat{L}\big(\mathrm{Sym}^2(g),s\big) := \Gamma_{\mathbb{R}}(s-k+2)\Gamma_{\mathbb{C}}(s)L\big(\mathrm{Sym}^2(g),s\big), \tag{1.2}$$

where $\Gamma_{\mathbb{R}}(s) := \pi^{-s/2}\Gamma(s/2)$ and $\Gamma_{\mathbb{C}}(s) := 2(2\pi)^{-s}\Gamma(s)$. By a theorem of Shimura [Sh], it has an analytical continuation to the whole of $\mathbb{C}$, and it follows from a theorem of Rankin [Ra] that it satisfies a functional equation

$$\widehat{L}\big(\mathrm{Sym}^2(g),2k-1-s\big) = \widehat{L}\big(\mathrm{Sym}^2(g),s\big).$$

It is well known that $s = 2k-2$ is the rightmost critical value in the sense of Deligne [De1]. It is paired with $s = 1$ by the functional equation. Then we define

$$\widehat{L}\big(\mathrm{Sym}^2(g),1\big)_{\mathrm{alg}} = \widehat{L}\big(\mathrm{Sym}^2(g),2k-2\big)_{\mathrm{alg}} := \frac{\widehat{L}(\mathrm{Sym}^2(g),2k-2)}{\pi^{\frac{k}{2}-1}\|g\|^2}, \tag{1.3}$$

which is known to be a non-zero, totally real algebraic number [Sh,Z1]. If $\kappa := 2^{-2k+3}(\frac{k}{2}-1)!(2k-3)!$, then

$$\widehat{L}\big(\mathrm{Sym}^2(g),2k-2\big) = \pi^{3-3k}\kappa L\big(\mathrm{Sym}^2(g),2k-2\big).$$

If p is a prime larger than $2k-2$, then the normalisation factor κ has no influence on the appearance or disappearance of p in the numerator or denominator of

$$\mathrm{trace}_k\big(\widehat{L}\big(\mathrm{Sym}^2,2k-2\big)_{\mathrm{alg}}\big) := \sum_g \widehat{L}\big(\mathrm{Sym}^2(g),2k-2\big)_{\mathrm{alg}} \in \mathbb{Q}, \tag{1.4}$$

where g runs through a primitive Hecke eigenbasis of $S_k(\Gamma)$. The functional equation implies that this is equal to

$$\mathrm{trace}_k\big(\widehat{L}\big(\mathrm{Sym}^2,1\big)_{\mathrm{alg}}\big). \tag{1.5}$$

The traces are interesting arithmetic objects. They can be explicitly calculated. The doubling method related to Siegel type Eisenstein series [Ga] provides a good way to do this (as in Section 2.3 below). For example let $k = 12, 16, 18, 20, 22, 24$. Then we have for the traces (1.5) the values (see also Table 1 in Section 2.4):

$$\begin{gathered}
\left(\frac{2^{24}\cdot 3\cdot 5\cdot 7}{23\cdot 691}\right)_{k=12} \qquad \left(\frac{2^{30}\cdot 3^2\cdot 5\cdot 7^3\cdot 11}{31\cdot 3617}\right)_{k=16} \\
\left(\frac{2^{37}\cdot 5^3\cdot 7\cdot 11\cdot 13}{43867}\right)_{k=18} \qquad \left(\frac{2^{36}\cdot 3^3\cdot 7^3\cdot 11\cdot 71^2}{283\cdot 617}\right)_{k=20} \\
\left(\frac{2^{42}\cdot 3\cdot 5^3\cdot 7^2\cdot 13\cdot 17\cdot 61\cdot 103}{11\cdot \underline{43}\cdot 131\cdot 593}\right)_{k=22} \qquad \left(\frac{2^{42}\cdot 11^2\cdot 59\cdot 691\cdot 2294824233197}{3\cdot 13\cdot 47\cdot 103\cdot 2294797}\right)_{k=24}.
\end{gathered}$$

Here the $\underline{43}$ indicates that the prime 43 does not occur and hence the numerator and denominator of the trace in the case $k = 22$ are coprime to 43. In all the other cases above, whenever $2k-1$ is a prime, this prime occurs in the denominator. The other *big* primes in the denominators are irregular primes related to the k-th Bernoulli number. Let p be a prime. Then we denote by $h(\sqrt{-p})$ the class number of $\mathbb{Q}(\sqrt{-p})$ and $\mathbb{Z}_{(p)}$ the localisation of $\mathbb{Z}$ at p.

Theorem I: Appearance of primes. *Let p be a prime $(p \geqslant 23)$ and $p \equiv 3 \pmod 4$. Then*

$$\operatorname{trace}_{\frac{p+1}{2}}\left(\widehat{L}\left(\mathrm{Sym}^2, 1\right)\right)_{\mathrm{alg}} \in p^{-1}\mathbb{Z}_{(p)}^{\times} \tag{1.6}$$

if and only if $h(\sqrt{-p}) > 1$.

In a way, the p in the denominator has nothing to do with the class number. Ultimately it comes from a factor $\zeta(3-2k)$ in the constant term of the un-normalised Eisenstein series of degree 2. But when $h(\sqrt{-p}) = 1$, a subtle cancellation occurs:

Theorem II: Disappearance of primes. *Let p be a prime $(p \geqslant 23)$, $p \equiv 3 \pmod 4$, and the class number $h(\sqrt{-p}) = 1$. Then*

$$\operatorname{trace}_{\frac{p+1}{2}}\left(\widehat{L}\left(\mathrm{Sym}^2, 1\right)\right)_{\mathrm{alg}} \in \mathbb{Z}_{(p)}^{\times}. \tag{1.7}$$

Next we turn to congruences of modular forms. Let $\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n$ be the unique normalised cusp form of weight 12 for $\mathrm{SL}_2(\mathbb{Z})$. Wilton [Wi] proved the following congruences. Let $\ell \neq 23$ be a prime.

$$\tau(\ell) \equiv \begin{cases} 0 \pmod{23} & \text{if } (\frac{\ell}{23}) = -1; \\ 2 \pmod{23} & \text{if } (\frac{\ell}{23}) = 1 \text{ and } \ell = u^2 + 23v^2; \\ -1 \pmod{23} & \text{otherwise.} \end{cases}$$

Swinnerton-Dyer [SD] considered more generally a normalised, cuspidal Hecke eigenform $g = \sum_{n=1}^{\infty} a_n q^n$ for $\mathrm{SL}_2(\mathbb{Z})$, of weight k. For simplicity suppose that the a_n are rational. This probably means that $k = 12, 16, 18, 20, 22$ or 26. He showed that if p is a prime, and if for all primes ℓ such that $(\frac{\ell}{p}) = -1$ we have $a_\ell \equiv 0 \pmod p$, then necessarily $p < 2k$. In the case $p = 2k-1$ (if it is prime), he observed that such congruences hold for $k = 12$ ($p = 23$, i.e. Wilton's case), and also for $k = 16$ ($p = 31$), but not for $k = 22$ ($p = 43$). In fact, we shall prove the following.

Theorem III: Dihedral congruences. *Let k be an even integer such that $p := 2k-1$ is prime. There exist a normalised, cuspidal Hecke eigenform $g = \sum_{n=1}^{\infty} a_n q^n$ for $\mathrm{SL}_2(\mathbb{Z})$, of weight k, and a prime $\mathfrak{p} \mid p$ of $\mathbb{Q}(\{a_n\})$ such that $a_\ell \equiv 0 \pmod{\mathfrak{p}}$ for all primes ℓ with $(\frac{\ell}{p}) = -1$, if and only if $h(\sqrt{-p}) > 1$.*

Theorems I and III may appear to describe two unrelated consequences of the condition $h(\sqrt{-p}) > 1$. In this paper, aside from proving these theorems, we shall show how they may be linked using the Bloch–Kato conjecture on special values of L-functions. The Galois representation behind Theorem III is used to produce a non-zero $\mathfrak{p}$-torsion element in some "global torsion" group whose order appears in the denominator of the conjectural formula for the ratio of $L(\mathrm{Sym}^2(g), 1)$ to a canonical Deligne period. This may be viewed as explaining the non-integrality in Theorem I.

Section 2 contains the proofs of Theorems I and II. We exploit the appearance of the $L(\mathrm{Sym}^2(g), 1)_{\mathrm{alg}}$ as coefficients in a formula for the pullback to the diagonal of an Eisenstein series of degree 2. We also use formulas for the Fourier coefficients of this Eisenstein series, in terms of values of the Riemann zeta function and quadratic Dirichlet L-functions, and a congruence $h(\sqrt{-p}) \equiv -2B_{(p+1)/2} \pmod p$. Section 3 contains the proof of Theorem III. The non-triviality of the class number enables us to construct, using class field theory, a 2-dimensional, (mod p), dihedral Galois representation, ramified only at p. Known results on Serre's conjecture then provide the required cuspidal Hecke eigenform of weight k and level 1. In Section 4 we state the Bloch–Kato conjecture in the case of critical values of $L(\mathrm{Sym}^2(g), s)$, analyse some Tamagawa factors, then produce the global torsion element mentioned above. The computations in this paper have been performed by the computational package PARI, which is available at

```
http://pari.math.u-bordeaux.fr/
```

The authors' collaboration on this paper grew out of discussions between them at the workshop "Automorphic representations, automorphic L-functions and arithmetic" at Kyoto R.I.M.S. in January 2009 (where the first-named author was supported by an E.P.S.R.C. overseas travel grant). They would like to thank the organiser, Prof. Y. Ishikawa.

2. Proofs of Theorems I and II

To prove the theorems we use the explicit arithmetic of Fourier coefficients of Eisenstein series and related special values of Dirichlet L-functions.

2.1. Special values of Dirichlet L-functions

Let χ be a Dirichlet character modulo m. We define the generalised Bernoulli numbers $B_{n,\chi}$ by the generating series

$$\sum_{n=0}^{\infty} B_{n,\chi}\frac{t^n}{n!} := \frac{(\sum_{a=1}^{m-1}\chi(a)te^{at})}{e^{mt}-1} \tag{2.1}$$

(see also [Wa, Section 4]). This definition has the advantage that it is easily implemented by a computer program. If $\chi = 1$ (Dirichlet character mod 1) then $B_n := B_{n,1}$ $(n > 1)$ are the Bernoulli numbers, where $B_0 = 1$ and $B_1 = \frac{1}{2}$. Usually one finds the following definition in the literature:

$$\sum_{n=0}^{\infty} B_n\frac{t^n}{n!} := \frac{t}{e^t-1}.$$

The Dirichlet series $L(\chi, s)$ is defined by

$$L(\chi, s) := \sum_{n=1}^{\infty}\chi(n)n^{-s}, \qquad \mathrm{Re}(s) > 1. \tag{2.2}$$

This holomorphic function has a meromorphic continuation to the complex plane, and

$$L(\chi, 1-n) = -\frac{B_{n,\chi}}{n} \quad (n > 1). \tag{2.3}$$

Let $D < 0$ be a fundamental discriminant, i.e., either $D \equiv 1 \pmod 4$, with D square free, or $D \equiv 0 \pmod 4$, with $\frac{D}{4}$ square free and $\frac{D}{4} \equiv 2, 3 \pmod 4$. Then the quadratic Dirichlet characters χ with $\chi(-1) = -1$ are the χ_D, where χ_D is essentially the Legendre symbol $(\frac{D}{\cdot})$. The first fundamental discriminants are given by

$$-3, -4, -7, -8, -11, -15, -19, -20, \ldots.$$

Let $L_D(s) := L(\chi_D, s)$. Since χ_D is odd we have $B_{n,\chi_D} \neq 0$ if and only if n is odd. Hence we have for all even integers $k > 2$: $L_D(2-k) = -\frac{B_{k-1,\chi}}{k-1} \neq 0$.

2.2. Fourier coefficients of Eisenstein series

The group $\mathrm{Sp}(2n)(\mathbb{R})$ of real points of the symplectic group scheme $\mathrm{Sp}(2n)$ acts transitively on the Siegel upper half-space $\mathbb{H}_n$ of degree n by:

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}(Z) := (AZ+B)(CZ+D)^{-1}.$$

Let k be a positive even integer such that $k > n+1$. Then we denote by

$$E_k^n(Z) := \sum_{g \in \mathrm{Sp}(2n)_\infty \backslash \mathrm{Sp}(2n)(\mathbb{Z})} 1|_k g, \tag{2.4}$$

the (normalised) Siegel type Eisenstein series of degree n, weight k and level 1. Here $|_k$ symbolises the usual Petersson slash operator and $\mathrm{Sp}(2n)_\infty$ the stabiliser of $1|_k$ in $\mathrm{Sp}(2n)(\mathbb{Z})$. This holomorphic periodic function has a Fourier expansion:

$$\sum_{T \geqslant 0} A_k^n(T) e^{2\pi i \operatorname{tr}(TZ)}, \tag{2.5}$$

where T runs through the set of all positive semi-definite symmetric half-integral matrices. Note that $A_k^n(0) = 1$. It is well known that Fourier coefficients $A_k^n(T)$ for singular matrices T are related to Fourier coefficients of Eisenstein series of lower degree. The parametrisation $T \geqslant 0$ is given in the case $n = 1$ by the set of non-negative integers, and in the case $n = 2$ by the binary positive semi-definite quadratic forms $T = \begin{pmatrix} n & \frac{r}{2} \\ \frac{r}{2} & m \end{pmatrix}$. We put $T = (n, r, m)$ to simplify notation. In the case $n = 1$, $E_k^1(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$.

We recall now a formula for Fourier coefficients of Eisenstein series of degree 2. Let the content of $T = (n, r, m)$, the greatest common divisor of n, r, m, be one. Then the value of $A_k^2(T)$ $(T > 0)$ depends only on the discriminant $D := r^2 - 4nm$ of T. We put $A_k(D) := A_k^2(T)$. For D a fundamental discriminant we have

$$A_k(D) = 2\frac{L_D(2-k)}{\zeta(1-k)\zeta(3-2k)}. \tag{2.6}$$

See for example [Z2].

2.3. Pullback of Eisenstein series

There are several ways to study special values of the symmetric square L-function [Z1]. Here we apply the method given by the pullback of Siegel type Eisenstein series of degree 2 (see [Ga] for details).

Let $\mathbb{H} \times \mathbb{H} \hookrightarrow \mathbb{H}_2$ be the diagonal imbedding given by $(z, w) \mapsto \begin{pmatrix} z & 0 \\ 0 & w \end{pmatrix}$, where $\mathbb{H} := \mathbb{H}_1$. Let $(g_i)_i$ be a primitive Hecke eigenbasis of $S_k(\Gamma)$. Then

$$E_k^2|_{\mathbb{H}\times\mathbb{H}} = E_k \otimes E_k + \sum_{i=1}^{\dim S_k(\Gamma)} \alpha_i g_i \otimes g_i, \tag{2.7}$$

where the coefficients are totally real algebraic numbers given by:

$$\alpha_i = \mu_k^{-1}\widehat{L}\big(\mathsf{Sym}^2(g_i), 1\big)_{\mathsf{alg}},$$
$$\mu_k^{-1} = -2^{5-2k}\frac{k!}{(\frac{k}{2}-1)!}\frac{1}{B_k B_{2k-2}}. \tag{2.8}$$

Recall that $p \geqslant 23$ is a prime, with $p \equiv 3 \pmod 4$, and that $k := \frac{p+1}{2}$.

Lemma 2.1. $h(\sqrt{-p}) \equiv -2B_k \pmod p$.

This remarkable fact appears to be due to Carlitz ((5.2) of [C1]). A proof is also given in [IR], following Proposition 15.2.3, and it is Exercise 4 in 5.8 of [BS]. It is a consequence of the analytic class number formula and Kummer's congruences.

Lemma 2.2. $\mathrm{ord}_p(B_k) = 0$.

Proof. This follows from the lemma above, since the possibility that $p \mid h(\sqrt{-p})$ is excluded by the well-known fact that $h(\sqrt{-p}) < \sqrt{p}\log p$ (see for example [Wa, Ex. 5.9]). □

Proof of Theorem I. By comparing Fourier coefficients on both sides of the formula (2.7), we obtain

$$A_k^2(1,0,1) + 2A_k^2(1,1,1) + 2A_k^2(1,2,1) = \big(A_k^1(1)\big)^2 + (\mu_k)^{-1}\sum_{g_i}\widehat{L}\big(\mathsf{Sym}^2(g_i), 1\big)_{\mathsf{alg}}.$$

Let $a_k(1) := A_k^1(1)$ be the first Fourier coefficient of E_k, i.e. $a_k(1) = -2k/B_k$. Since $x^2 + 2xy + y^2 = (x+y)^2$, $A_k^2(1,2,1) = A_k^2(1,0,0)$, and it follows from the fact that $\Phi(E_k^2) = E_k^1$ (where Φ is Siegel's operator) that $A_k^2(1,0,0) = A_k^1(1)$ (see also Klingen [Kl, Section 5, proof of Proposition 8]). Hence $A_k^2(1,2,1) = a_k(1)$, and we have

$$\mathsf{trace}_k\big(\widehat{L}\big(\mathsf{Sym}^2, 1\big)\big)_{\mathsf{alg}} = \mu_k\big(A_k(-4) + 2A_k(-3) + 2a_k(1) - a_k(1)^2\big). \tag{2.9}$$

First we claim that $\mathrm{ord}_p(\mu_k) = -1$. Given Lemma 2.2, it suffices to show that $\mathrm{ord}_p(B_{2k-2}) = -1$, but since $2k-2 = p-1$, this is a direct consequence of the v. Staudt–Clausen theorem.

Next we claim that

$$\mu_k\big(A_k(-4) + 2A_k(-3)\big) \in \mathbb{Z}_{(p)}. \tag{2.10}$$

Recall from (2.6) that $A_k(D) = 2\frac{L_D(2-k)}{\zeta(1-k)\zeta(3-2k)}$. First, μ_k cancels with $\zeta(1-k)\zeta(3-2k)$, up to p-units. Then, Leopoldt's generalisation, to generalised Bernoulli numbers, of the v. Staudt–Clausen theorem [L] shows that $L_{-4}(2-k), L_{-3}(2-k) \in \mathbb{Z}_{(p)}$ (see also [RV] or [C2]).

To prove the theorem, it remains to show that $2a_k(1) - a_k(1)^2$, i.e. $a_k(1)(2 - a_k(1))$, belongs to $p\mathbb{Z}_{(p)}$ if $h(\sqrt{-p}) = 1$ but to $\mathbb{Z}_{(p)}^\times$ if $h(\sqrt{-p}) > 1$. By Lemma 2.2, $a_k(1) \in \mathbb{Z}_{(p)}^\times$. In fact, $a_k(1) = -2k/B_k$, but $2k = p+1 \equiv 1 \pmod p$, so $a_k(1) \equiv -1/B_k \pmod p$. With Lemma 2.1, this gives

$$2 - a_k(1) \equiv 2 - 2\,h(\sqrt{-p})^{-1} \pmod p$$

(note again that $h(\sqrt{-p}) < \sqrt{p}\log p < p$), from which we get what we want. □

Table 1

$p \equiv 3(4)$	$k = \frac{p+1}{2}$	$\mathrm{trace}_k \widehat{L}(\mathrm{Sym}^2, 1)_{\mathrm{alg}}$	$h(\sqrt{-p})$
3	2	–	1
7	4	–	1
11	6	–	1
19	10	–	1
23	12	$\frac{2^{24}\cdot 3\cdot 5\cdot 7}{23\cdot 691}$	3
31	16	$\frac{2^{30}\cdot 3^2\cdot 5\cdot 7^3\cdot 11}{31\cdot 3617}$	3
43	22	$\frac{2^{42}\cdot 3\cdot 5^3\cdot 7^2\cdot 13\cdot 17\cdot 61\cdot 103}{11\cdot 131\cdot 593}$	1
47	24	$\frac{2^{42}\cdot 11^2\cdot 59\cdot 691\cdot 2294824233197}{3\cdot 13\cdot 47\cdot 103\cdot 2294797}$	5
59	30	$\frac{2^{55}\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17^3\cdot 47\cdot 673\cdot 947\cdot 2087\cdot 958033842197}{3^4\cdot 19\cdot 59\cdot 1721\cdot 10012559881}$	3
67	34	$\frac{2^{62}\cdot 5\cdot 7\cdot 11\cdot 13\cdot 2083\cdot 2297\cdot 12811671172550037934783691}{3^3\cdot 17\cdot 19\cdot 23^2\cdot 151628697551}$	1
71	36	$\frac{2^{60}\cdot 23\cdot 47\cdot 353\cdot 431\cdot 260209\cdot 1520443\cdot 11314293544039\cdot 21560654759317409}{3^5\cdot 5^2\cdot 13\cdot 19\cdot 71\cdot 26315271553053477373}$	7
79	40	$\frac{2^{66}\cdot 179\cdot 20543\cdot 57844169585314072393284932599819687679553675399737}{3^4\cdot 5^3\cdot 23\cdot 29\cdot 79\cdot 137616929\cdot 1897170067619}$	5
83	42	$\frac{2^{72}\cdot 661\cdot 7417\cdot 115631553691\cdot 406193020940899943\cdot 30247154657851042934148779}{3^6\cdot 7\cdot 11^2\cdot 23\cdot 31\cdot 83\cdot 1520097643918070802691}$	3
103	52	$\in 103^{-1}\mathbb{Z}_{(103)}^{\times}$	5
107	54	$\frac{2^{90}\cdot 13\cdot 613\cdot 23068751315342507\cdot p_1}{3^9\cdot 5\cdot 7^3\cdot 19\cdot 29\cdot 31\cdot 37\cdot 43\cdot 107\cdot 39409\cdot 660183281\cdot 1120412849144121779}$	3
127	64	$127^{-1}\mathbb{Z}_{(127)}^{\times}$	5
131	66	$131^{-1}\mathbb{Z}_{(131)}^{\times}$	5
139	70	$139^{-1}\mathbb{Z}_{(139)}^{\times}$	3
151	76	$151^{-1}\mathbb{Z}_{(151)}^{\times}$	7
163	82	$\equiv 20 \pmod{163}$	1
167	84	$167^{-1}\mathbb{Z}_{(167)}^{\times}$	11

$$p_1 = 272604077981898503203628532273822570762$$

$$9174901615890777892164701437945309129$$

2.4. *Proof of Theorem II*

We already know, from the proof above, that if $h(\sqrt{-p}) = 1$ then

$$\mathrm{trace}_{\frac{p+1}{2}}\left(\widehat{L}\left(\mathrm{Sym}^2, 1\right)\right)_{\mathrm{alg}} \in \mathbb{Z}_{(p)}.$$

We can prove that it is a unit simply by inspecting Table 1, since the Heegner–Stark theorem tells us all the imaginary quadratic fields of class number one. Since $p \geqslant 23$ (otherwise $\dim S_{\frac{p+1}{2}}(\Gamma) = 0$), only $p = 43, 67, 163$ have to be considered. □

Table 1 contains the first cases where $2k - 1$ is a prime. One can see that frequently small primes appear in the denominator. The large primes in denominators are always divisors of the B_k.

3. Dihedral congruences for cusp forms of level one

Our goal in this section is to prove Theorem III. In the following theorem, p is not necessarily equal to $2k - 1$.

Theorem 3.1 *(Deligne [De2]). Let $g=\sum_{n=1}^{\infty}a_nq^n$ be a normalised newform of weight $k\geqslant 2$ and character ϵ, for $\Gamma_1(N)$. Let $K=\mathbb{Q}(\{a_n\})$, and let $\mathfrak{p}\mid p$ be some prime of the ring of integers O_K, with completions $K_{\mathfrak{p}}$ and $O_{\mathfrak{p}}$. There exists a continuous representation*

$$\rho_g=\rho_{g,\mathfrak{p}}:\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\to \mathrm{GL}_2(K_{\mathfrak{p}}),$$

unramified outside pN, such that if $\ell\nmid pN$ is a prime, and Frob_ℓ *is an arithmetic Frobenius element, then*

$$\mathrm{Tr}\big(\rho_g\big(\mathrm{Frob}_\ell^{-1}\big)\big)=a_\ell,\qquad \det\big(\rho_g\big(\mathrm{Frob}_\ell^{-1}\big)\big)=\epsilon(\ell)\ell^{k-1}.$$

One can conjugate so that ρ_g takes values in $\mathrm{GL}_2(O_{\mathfrak{p}})$, then reduce (mod $\mathfrak{p}$) to get a continuous representation $\bar{\rho}_g=\bar{\rho}_{g,\mathfrak{p}}:\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\to\mathrm{GL}_2(\overline{\mathbb{F}}_p)$, which, if it is irreducible, is independent of the choice of invariant $O_{\mathfrak{p}}$-lattice. If $c\in\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is a complex conjugation, then necessarily $\det(\rho_g(c))=-1$, i.e. ρ_g is *odd*. Serre ($(3.2.3)_?$ of [Se1]) conjectured that, conversely, any odd, irreducible, continuous representation $\rho:\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\to\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ is isomorphic to some $\bar{\rho}_g$ as above. Moreover ($(3.2.4)_?$ of [Se1]), he conjectured an optimal level, character and weight. The level is the (prime-to-p) Artin conductor $N(\rho)$, while the weight depends on the restriction of ρ to an inertia subgroup I_p. Khare [K] has proved Serre's conjecture in the case $N(\rho)=1$.

Proposition 3.2. *Let $p\equiv 3 \pmod 4$ be a prime, and let $k:=(p+1)/2$. Suppose that $h(\sqrt{-p})>1$. Then there exist a normalised, cuspidal Hecke eigenform $g=\sum_{n=1}^{\infty}a_nq^n$ for $\mathrm{SL}_2(\mathbb{Z})$, of weight k, and a prime $\mathfrak{p}\mid p$ of $\mathbb{Q}(\{a_n\})$ such that $\bar{\rho}_{g,\mathfrak{p}}:\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\to\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ has dihedral image, factoring through $\mathrm{Gal}(E/\mathbb{Q})$, where E is any unramified, cyclic extension of $\mathbb{Q}(\sqrt{-p})$.*

Proof. Let E be any (non-trivial) unramified, cyclic extension of $F:=\mathbb{Q}(\sqrt{-p})$, say $[E:F]=r$. It exists by class field theory, since $h(\sqrt{-p})>1$. Let $\tau:\mathrm{Gal}(E/F)\to\overline{\mathbb{F}}_p^\times$ be a character of order r, and let $\rho:\mathrm{Gal}(E/\mathbb{Q})\to\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ be $\mathrm{Ind}_F^{\mathbb{Q}}\tau$. We also denote by ρ the inflation to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This ρ is easily seen to be continuous, odd and irreducible. Since E/F is unramified, and $F/\mathbb{Q}$ is ramified only at p, the Artin conductor of ρ is equal to 1. By Khare's theorem, ρ is of the form $\bar{\rho}_{g,\mathfrak{p}}$ for some level-one cuspidal eigenform g. It remains to show that the Serre weight of ρ is k. Bearing in mind that E/F is unramified, the restriction of ρ to an inertia subgroup I_p is tamely ramified, and decomposes as a sum of the trivial character and the quadratic character χ_{-p}. These are both "level-one" characters of the tame quotient of I_p, and writing them in the form χ^a,χ^b, with χ the inverse-cyclotomic character and $0\leqslant a\leqslant b\leqslant p-2$, we have $a=0$, $b=(p-1)/2$. The weight is given by $1+pa+b$ (as in 2(a) of 1.7 of [E]), which is equal to $(p+1)/2=k$. □

Strictly speaking, one does not need the full force of Khare's theorem. One can produce a complex-multiplication form f (of weight 1, level p and quadratic character) such that $\bar{\rho}_f\simeq\rho$. Then one can use the fact that the weak Serre conjecture implies the strong Serre conjecture to replace f by something of the correct level and weight. In fact, in the cases $k=12$ and $k=16$, this f is the linear combination of binary theta series on the right-hand side of (26) or (27) in [SD]. Note that $h(\sqrt{-p})$ is necessarily odd, so the character τ in the proof above has odd order.

Corollary 3.3. *Let k be an even integer such that $p:=2k-1$ is prime. Suppose that $h(\sqrt{-p})>1$. Then there exist a normalised, cuspidal Hecke eigenform $g=\sum_{n=1}^{\infty}a_nq^n$ for $\mathrm{SL}_2(\mathbb{Z})$, of weight k, and a prime $\mathfrak{p}\mid p$ of $\mathbb{Q}(\{a_n\})$ such that $a_\ell\equiv 0 \pmod{\mathfrak{p}}$ for all primes ℓ with $(\frac{\ell}{p})=-1$.*

One uses $a_\ell\equiv\mathrm{Tr}(\rho_g(\mathrm{Frob}_\ell^{-1}))\pmod{\mathfrak{p}}$. According to a remark at the end of [Ri], which refers to a footnote about Δ^2 in [Wi], the case $k=24$, $p=47$ may be proved using Wilton's methods.

Wilton and Swinnerton-Dyer also had something to say about primes ℓ such that $(\frac{\ell}{p})=1$. Such a prime splits in O_F, say $(\ell)=\mathfrak{l}\bar{\mathfrak{l}}$. By class field theory, we may view the character τ in the above proof as a character of the ideal class group of O_F. Then a consequence of $a_\ell \equiv \mathrm{Tr}(\rho_g(\mathrm{Frob}_\ell^{-1})) \pmod{\mathfrak{p}}$ is that $a_\ell \equiv \tau([\mathfrak{l}]) + \tau^{-1}([\mathfrak{l}]) \pmod{\mathfrak{p}}$. In particular, if $\mathfrak{l}$ is principal (i.e. if $\ell = u^2 + pv^2$, when $p \equiv 7 \pmod 8$, or more generally if $\ell = u^2 + uv + \frac{p+1}{4}v^2$), then $a_\ell \equiv 2 \pmod{\mathfrak{p}}$. In the cases $k = 12$ and $k = 16$, where $h(\sqrt{-p}) = 3$, there is only one possible non-trivial choice of $\{\tau, \tau^{-1}\}$.

To complete the proof of Theorem III, it suffices to prove the following.

Proposition 3.4. *Let k be an even integer such that $p := 2k - 1$ is prime. Suppose that there exist a normalised, cuspidal Hecke eigenform $g = \sum_{n=1}^{\infty} a_n q^n$ for $\mathrm{SL}_2(\mathbb{Z})$, of weight k, and a prime $\mathfrak{p} \mid p$ of $\mathbb{Q}(\{a_n\})$ such that $a_\ell \equiv 0 \pmod{\mathfrak{p}}$ for all primes ℓ with $(\frac{\ell}{p}) = -1$. Then $h(\sqrt{-p}) > 1$.*

Proof. Similarly to 3.2 of [Se2], the only possibility compatible with the congruence is that the image of $\overline{\rho}_g(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ in $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$ is dihedral. Since g has level one, so that $\overline{\rho}_g$ is unramified away from p, it must be the case that the image of $\overline{\rho}_g(\mathrm{Gal}(\overline{\mathbb{Q}}/F))$ in $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$ is cyclic, where $F = \mathbb{Q}(\sqrt{-p})$.

We claim that the restriction of $\overline{\rho}_g$ to $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ must be unramified at (the prime dividing) p. Suppose that it is not. Then, if I_p is an inertia subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the image of $\overline{\rho}_f(I_p)$ in $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$ is dihedral, and certainly the restriction of $\overline{\rho}_g$ to $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ is irreducible (hence semi-simple). But then $\overline{\rho}_g|_{I_p}$ would be a sum of two characters (as on p. 214 of [E]), contrary to $\overline{\rho}_g(I_p)$ being non-abelian. Thus the claim is established. But the restriction of $\overline{\rho}_g$ to $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ is not trivial, so factors through the Galois group of a non-trivial extension E/F, which was already unramified away from p, but, we know now, is also unramified above p. By class field theory, we must have $h(\sqrt{-p}) > 1$. □

In principle, the above proposition could be proved by inspection, since there are only finitely many p to consider.

4. The Bloch–Kato conjecture

4.1. Statement of the conjecture

Let $\sum_{n=1}^{\infty} a_n q^n = g \in S_k(\Gamma)$ (necessarily for some even $k \geqslant 12$) be a normalised Hecke eigenform, $K = \mathbb{Q}(\{a_n\})$. Attached to g is a "premotivic structure" M_g over $\mathbb{Q}$ with coefficients in K. Thus there are 2-dimensional K-vector spaces $M_{g,B}$ and $M_{g,\mathrm{dR}}$ (the Betti and de Rham realisations) and, for each finite prime $\mathfrak{q}$ of O_K, a 2-dimensional $K_\mathfrak{q}$-vector space $M_{g,\mathfrak{q}}$, the $\mathfrak{q}$-adic realisation. These come with various structures and comparison isomorphisms, such as $M_{g,B} \otimes_K K_\mathfrak{q} \simeq M_{g,\mathfrak{q}}$. See 1.1.1 of [DFG] for the precise definition of a premotivic structure, and 1.6.2 of [DFG] for the construction of M_g. The $\mathfrak{q}$-adic realisation $M_{g,\mathfrak{q}}$ realises the representation $\rho_{g,\mathfrak{q}}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. For each prime number ℓ, the restriction to $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ may be used to define a local L-factor, and the Euler product is precisely $L(g, s)$. Let $M'_g := \mathrm{Sym}^2 M_g$. Then similarly from M'_g one obtains $L(\mathrm{Sym}^2(g), s)$.

On $M_{g,B}$ there is an action of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, and the eigenspaces $M^{\pm}_{g,B}$ are 1-dimensional. On $M_{g,\mathrm{dR}}$ there is a decreasing filtration, with F^j a 1-dimensional space precisely for $1 \leqslant j \leqslant k-1$. The de Rham isomorphism $M_{g,B} \otimes_K \mathbb{C} \simeq M_{g,\mathrm{dR}} \otimes_K \mathbb{C}$ induces isomorphisms between $M^{\pm}_{g,B} \otimes \mathbb{C}$ and $(M_{g,\mathrm{dR}}/F) \otimes \mathbb{C}$, where $F := F^1 = \cdots = F^{k-1}$. Define $\Omega^{\pm}$ to be the determinants of these isomorphisms. These depend on the choice of K-bases for $M^{\pm}_{g,B}$ and $M_{g,\mathrm{dR}}/F$, so should be viewed as elements of $\mathbb{C}^\times/K^\times$. Note that if we consider the twist $M_g(j)$ (with $1 \leqslant j \leqslant k-1$), then $(M_g(j))_B = (2\pi i)^j M_g$, so $(M_g(j))^+_B = (2\pi i)^j M^{(-1)^j}_{g,B}$ and the Deligne period of $M_g(j)$, as the determinant of the isomorphism from $(M_g(j))^+_B \otimes_K \mathbb{C}$ to $(M_g(j)_{\mathrm{dR}}/F^0 M_g(j)_{\mathrm{dR}}) \otimes_K \mathbb{C} = (M_{g,\mathrm{dR}}/F^j M_{g,\mathrm{dR}}) \otimes_K \mathbb{C}$, is $(2\pi i)^j \Omega^{(-1)^j}$.

The eigenspace $M'^{-}_{g,B}$ is 1-dimensional. On $M'_{g,\mathrm{dR}}$ there is a decreasing filtration, with F^t a 2-dimensional space precisely for $1 \leqslant t \leqslant k-1$. The de Rham isomorphism $M'_{g,B} \otimes_K \mathbb{C} \simeq M'_{g,\mathrm{dR}} \otimes_K \mathbb{C}$ induces an isomorphism between $M'^{-}_{g,B} \otimes \mathbb{C}$ and $(M'_{g,\mathrm{dR}}/F') \otimes \mathbb{C}$, where $F' := F^1 = \cdots = F^{k-1}$. Define $\Omega \in \mathbb{C}^\times/K^\times$ to be the determinant of this isomorphism. Note that t as above is critical only when it is odd, since this is when the dimension of $(M'_g(t))^+_B = (2\pi i)^t M'_{g,B}{}^{(-1)^t}$ matches that of $(M'_g(t))_{\mathrm{dR}}/F^0(M'_g(t))_{\mathrm{dR}} = M'_{g,\mathrm{dR}}/F^t M'_{g,\mathrm{dR}}$. In this case, the Deligne period of $M'_g(t)$ is $(2\pi i)^t \Omega$. Note that the remaining critical points, paired with these by the functional equation, are the even t such that $k \leqslant t \leqslant 2k-2$.

We shall choose an O_K-submodule $\mathfrak{M}_{g,B}$, generating $M_{g,B}$ over K, but not necessarily free, and likewise an $O_K[1/S]$-submodule $\mathfrak{M}_{g,\mathrm{dR}}$, generating $M_{g,\mathrm{dR}}$ over K, where S is the set of primes less than or equal to k. We take these as in 1.6.2 of [DFG]. They are part of the "S-integral premotivic structure" $\mathfrak{M}_g$ associated to g. Actually, it will be convenient to enlarge S so that $O_K[1/S]$ is a principal ideal domain, then replace $\mathfrak{M}_{g,B}$ and $\mathfrak{M}_{g,\mathrm{dR}}$ by their tensor products with the new $O_K[1/S]$. These will now be free, as will be any submodules and quotients. Choosing bases, and using these to calculate the above determinants, we pin down the values of $\Omega^\pm$ (up to S-units). Setting $\mathfrak{M}'_{g,B} := \mathrm{Sym}^2\mathfrak{M}_{g,B}$ and $\mathfrak{M}'_{g,\mathrm{dR}} := \mathrm{Sym}^2\mathfrak{M}_{g,\mathrm{dR}}$, similarly we pin down Ω (up to S-units). We just have to imagine not including in S any prime we care about (specifically $p = 2k-1$ if it is prime).

Lemma 4.1. $\Omega = \Omega^+\Omega^-$.

Proof. Let e^+ and e^- be generators of $\mathfrak{M}^+_{g,B}$ and $\mathfrak{M}^-_{g,B}$ respectively. Let $\{x, y\}$ be an $O_K[1/S]$-basis for $\mathfrak{M}_{g,\mathrm{dR}}$, with y generating the submodule F. Under the isomorphism $M_{g,B} \otimes_K \mathbb{C} \simeq M_{g,\mathrm{dR}} \otimes_K \mathbb{C}$ we have

$$e^+ \mapsto \Omega^+ x + \eta^+ y, \qquad e^- \mapsto \Omega^- x + \eta^- y,$$

for some η^+, η^-, so under the isomorphism between $M'^-_{g,B} \otimes \mathbb{C}$ and $(M'_{g,\mathrm{dR}}/F') \otimes \mathbb{C}$ we have

$$e^+e^- \mapsto \Omega^+\Omega^- x^2.$$

Hence $\Omega = \Omega^+\Omega^-$, as required. □

We shall need the elements $\mathfrak{M}_{g,\mathfrak{q}}$ of the S-integral premotivic structure, for each prime $\mathfrak{q}$ of O_K. These are as in 1.6.2 of [DFG]. For each $\mathfrak{q}$, $\mathfrak{M}_{g,\mathfrak{q}}$ is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable $O_{\mathfrak{q}}$-lattice in $M_{g,\mathfrak{q}}$. Taking symmetric squares, we get $\mathfrak{M}'_{g,\mathfrak{q}}$, a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable $O_{\mathfrak{q}}$-lattice in $M'_{g,\mathfrak{q}}$.

Let $A_{g,\mathfrak{q}} = A_{\mathfrak{q}} := M_{g,\mathfrak{q}}/\mathfrak{M}_{g,\mathfrak{q}}$, and $A[\mathfrak{q}] := A_{\mathfrak{q}}[\mathfrak{q}]$, the $\mathfrak{q}$-torsion subgroup. Similarly, let $A'_{g,\mathfrak{q}} = A'_{\mathfrak{q}} := M'_{g,\mathfrak{q}}/\mathfrak{M}'_{g,\mathfrak{q}}$, and $A'[\mathfrak{q}] = A'_{\mathfrak{q}}[\mathfrak{q}]$. Let $\check{A}'_{\mathfrak{q}} := \check{M}'_{g,\mathfrak{q}}/\check{\mathfrak{M}}'_{g,\mathfrak{q}}$, where $\check{M}'_{g,\mathfrak{q}}$ and $\check{\mathfrak{M}}'_{g,\mathfrak{q}}$ are the $K_{\mathfrak{q}}$-vector space and $O_{\mathfrak{q}}$-lattice dual to $M'_{g,\mathfrak{q}}$ and $\mathfrak{M}'_{g,\mathfrak{q}}$ respectively, with the natural $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action. Let $A' := \bigoplus_{\mathfrak{q}} A'_{\mathfrak{q}}$, etc.

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

$$H^1_f\big(\mathbb{Q}_\ell, M'_{g,\mathfrak{q}}(t)\big) := \ker\big(H^1\big(D_\ell, M'_{g,\mathfrak{q}}(t)\big) \to H^1\big(I_\ell, M'_{g,\mathfrak{q}}(t)\big)\big).$$

Here D_ℓ is a decomposition subgroup at a prime above ℓ, I_ℓ is the inertia subgroup, and $M'_{g,\mathfrak{q}}(t)$ is a Tate twist of $M'_{g,\mathfrak{q}}$, etc. The cohomology is for continuous cocycles and coboundaries. For $\ell = q$ let

$$H^1_f\big(\mathbb{Q}_q, M'_{f,\mathfrak{q}}(t)\big) := \ker\big(H^1\big(D_q, M'_{f,\mathfrak{q}}(t)\big) \to H^1\big(D_q, M'_{f,\mathfrak{q}}(t) \otimes_{\mathbb{Q}_q} B_{\mathrm{crys}}\big)\big).$$

(See Section 1 of [BK], or Section 2 of [Fo], for the definition of Fontaine's ring B_{crys}.) Let $H^1_f(\mathbb{Q}, M'_{g,\mathfrak{q}}(t))$ be the subspace of those elements of $H^1(\mathbb{Q}, M'_{g,\mathfrak{q}}(t))$ which, for all primes ℓ, have local restriction lying in $H^1_f(\mathbb{Q}_\ell, M'_{g,\mathfrak{q}}(t))$. There is a natural exact sequence

$$0 \longrightarrow \mathfrak{M}'_{g,\mathfrak{q}}(t) \longrightarrow M'_{g,\mathfrak{q}}(t) \xrightarrow{\pi} A'_{\mathfrak{q}}(t) \longrightarrow 0.$$

Let $H^1_f(\mathbb{Q}_\ell, A'_{\mathfrak{q}}(t)) = \pi_* H^1_f(\mathbb{Q}_\ell, M'_{g,\mathfrak{q}}(t))$. Define the $\mathfrak{q}$-Selmer group $H^1_f(\mathbb{Q}, A'_{\mathfrak{q}}(t))$ to be the subgroup of elements of $H^1(\mathbb{Q}, A'_{\mathfrak{q}}(t))$ whose local restrictions lie in $H^1_f(\mathbb{Q}_\ell, A'_{\mathfrak{q}}(t))$ for all primes ℓ. Note that the condition at $\ell = \infty$ is superfluous unless $q = 2$. Define the Shafarevich–Tate group

$$Ш(t) = \bigoplus_{\mathfrak{q}} \frac{H^1_f(\mathbb{Q}, A'_{\mathfrak{q}}(t))}{\pi_* H^1_f(\mathbb{Q}, M'_{g,\mathfrak{q}}(t))}.$$

Conjecture 4.2 *(Case of Bloch–Kato). Suppose that $1 \leqslant t \leqslant k-1$ is odd. Then we have the following equality of fractional ideals of $O_K[1/S]$:*

$$\frac{L(\mathrm{Sym}^2(g), t)}{(2\pi i)^t \Omega} = \frac{\prod_{\ell \leqslant \infty} c_\ell(t)\ \#Ш(t)}{\#H^0(\mathbb{Q}, A'(t))\#H^0(\mathbb{Q}, \check{A}'(1-t))}. \tag{4.1}$$

The Tamagawa factors $c_\ell(t)$ will be defined in the next subsection. It is more convenient to use $\|g\|^2$ than Ω, so we consider the relation between the two. Calculating as in (5.18) of [Hi], using Lemma 5.1.6 of [De1] and the latter part of 1.5.1 of [DFG], one recovers the well-known fact that, up to S-units,

$$\|g\|^2 = i^{k-1}\Omega^+\Omega^- c(g), \tag{4.2}$$

where $c(g)$, the “cohomology congruence ideal”, is, as the cup-product of basis elements for $\mathfrak{M}_{g,B}$, an integral ideal. (It is certainly trivial in those cases for which $\dim(S_k) = 1$.) Recall that by Lemma 4.1 above,

$$\Omega = \Omega^+\Omega^-.$$

Via the duality $M_g \times M_g \to K(1-k)$, $\check{A}'_{g,\mathfrak{q}} \simeq A'_{g,\mathfrak{q}}(2k-2)$. (Recall that $K = \mathbb{Q}(\{a_n\})$, and here $K(1-k)$ is a twist of the trivial premotivic structure over $\mathbb{Q}$ with coefficients in K.) Therefore (4.1) becomes, for $1 \leqslant t \leqslant k-1$ odd, the conjecture that

$$\frac{L(\mathrm{Sym}^2(g), t)}{(2\pi i)^t i^{1-k}\|g\|^2} = \frac{\prod_{\ell \leqslant \infty} c_\ell(t)\ \#Ш(t)}{\#H^0(\mathbb{Q}, A'(t))\#H^0(\mathbb{Q}, A'(2k-1-t))c(g)}. \tag{4.3}$$

4.2. Tamagawa factors

The goal of this subsection is to show that if $p = 2k-1$ is prime, and $\mathfrak{p} \mid p$, then the factor $\prod_{\ell \leqslant \infty} c_\ell(t)$ contributes nothing to the $\mathfrak{p}$-part of the right-hand side of (4.3) in the case $t = 1$.

Let t be an integer with $1 \leqslant t < k-1$. (It is really the case $t = 1$ with which we are concerned, so for convenience we exclude the slightly awkward case $t = k-1$ at this point.) For a finite prime ℓ, let $H^1_f(\mathbb{Q}_\ell, \mathfrak{M}'_{g,\mathfrak{q}}(t))$ be the inverse image of $H^1_f(\mathbb{Q}_\ell, M'_{g,\mathfrak{q}}(t))$ under the natural map. Suppose now that $\ell \neq q$. If $H^0(\mathbb{Q}_\ell, M'_{g,\mathfrak{q}}(t))$ is trivial (which is certainly the case if $t < k-1$, since the eigenvalues of Frob_ℓ^{-1} acting on $M_{g,\mathfrak{q}}$ are algebraic integers with absolute value $\ell^{(k-1)/2}$) then, by inflation–restriction, we find that $H^1_f(\mathbb{Q}_\ell, M'_{g,\mathfrak{q}}(t)) \simeq (M'_{g,\mathfrak{q}}(t)^{I_\ell})/(1 - \mathrm{Frob}_\ell)(M'_{g,\mathfrak{q}}(t)^{I_\ell})$ is trivial, so $H^1_f(\mathbb{Q}_\ell, \mathfrak{M}'_{g,\mathfrak{q}}(t))$ is the torsion part of $H^1(\mathbb{Q}_\ell, \mathfrak{M}'_{g,\mathfrak{q}}(t))$. Again using the triviality of $H^0(\mathbb{Q}_\ell, M'_{g,\mathfrak{q}}(t))$, we identify $H^1_f(\mathbb{Q}_\ell, \mathfrak{M}'_{g,\mathfrak{q}}(t))$ with $H^0(\mathbb{Q}_\ell, A'_{\mathfrak{q}}(t))$. This has a subgroup that is given by $(M'_{g,\mathfrak{q}}(t)^{I_\ell}/\mathfrak{M}'_{g,\mathfrak{q}}(t)^{I_\ell})^{\mathrm{Frob}_\ell = \mathrm{id}}$, whose order is the $\mathfrak{q}$-part of $P_\ell(\ell^{-t})$, where

$P_\ell(\ell^{-s}) = \det(1 - \mathrm{Frob}_\ell^{-1}\,\ell^{-s} \mid {M'_{g,\mathfrak{q}}}^{I_\ell})$ is the Euler factor at ℓ in $L(\mathrm{Sym}^2(g), s)$ (strictly speaking, its reciprocal). When ℓ is a prime of "good reduction", so that $M'_{g,\mathfrak{q}}(t)^{I_\ell} = M'_{g,\mathfrak{q}}(t)$ maps surjectively to $A'_{\mathfrak{q}}(t)$, the subgroup is the whole of $H^0(\mathbb{Q}_\ell, A'_{\mathfrak{q}}(t))$, but in general we define the $\mathfrak{q}$-part of the Tamagawa factor $c_\ell(t)$ to be the index of the subgroup. For us, every ℓ is a prime of good reduction (i.e. $M'_{g,\mathfrak{q}}$ is unramified at ℓ), because g has level one, so we get the following straight from the definition.

Lemma 4.3. *If ℓ is a finite prime, and $\mathfrak{q}$ divides $q \neq \ell$, and $1 \leqslant t < k-1$, then the $\mathfrak{q}$ part of $c_\ell(t)$ is trivial.*

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

$$\frac{(M'_{g,\mathfrak{q}}(t)/\mathfrak{M}'_{g,\mathfrak{q}}(t))^{\pm}}{M'_{g,\mathfrak{q}}(t)^{\pm}/\mathfrak{M}'_{g,\mathfrak{q}}(t)^{\pm}},$$

where $\pm = (-1)^t$. This is at worst a power of 2, so need not concern us.

It remains to consider the $\mathfrak{q}$-part of $c_\ell(t)$ in the case that $q = \ell$. It is known that $M'_{g,\mathfrak{q}}$ is a crystalline representation of $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$, as long as $q > k$. (Recall that the level $N = 1$ for us.) For a careful discussion, referring to [Fa], see 1.2.5 of [DFG]. Furthermore, $\mathbb{V}(\mathfrak{M}'_{g,\mathrm{dR}} \otimes O_{\mathfrak{q}}) = \mathfrak{M}'_{g,\mathfrak{q}}$. (Note that $\mathfrak{M}'_{g,\mathrm{dR}} \otimes O_{\mathfrak{q}}$ is really the crystalline realisation $\mathfrak{M}'_{g,\mathrm{crys}}$.) For the definitions of the modified Fontaine–Lafaille functor $\mathbb{V}$ and the categories $O_{\mathfrak{q}}$-$\mathfrak{MF}^a$ of filtered Dieudonné modules, see 1.1.2 of [DFG]. It now follows from Theorem 4.1(ii) of [BK] that the Bloch–Kato exponential map gives an isomorphism

$$\bigl(M'_{g,\mathrm{dR}} \otimes K_{\mathfrak{q}}\bigr)/F^t\bigl(M'_{g,\mathrm{dR}} \otimes K_{\mathfrak{q}}\bigr) \simeq H^1_f\bigl(\mathbb{Q}_q, M'_{g,\mathfrak{q}}(t)\bigr).$$

The norm of the $\mathfrak{q}$-part of the Tamagawa factor $c_q(t)$ is

$$\mu\bigl(H^1_f\bigl(\mathbb{Q}_q, \mathfrak{M}'_{g,\mathfrak{q}}(t)\bigr)\bigr)/\bigl|P_q\bigl(q^{-t}\bigr)\bigr|_q^{-1},$$

where μ is the Haar measure of $H^1_f(\mathbb{Q}_q, M'_{g,\mathfrak{q}}(t))$ induced via the exponential map from that measure on $(M'_{g,\mathrm{dR}} \otimes K_{\mathfrak{q}})/F^t(M'_{g,\mathrm{dR}} \otimes K_{\mathfrak{q}})$ giving $(\mathfrak{M}'_{g,\mathrm{dR}} \otimes O_{\mathfrak{q}})/F^t(\mathfrak{M}'_{g,\mathrm{dR}} \otimes O_{\mathfrak{q}})$ volume 1. The following is a direct consequence of Theorem 4.1(iii) of [BK].

Lemma 4.4. *If $q > 2k-1$, $\mathfrak{q} \mid q$ and $1 \leqslant t \leqslant 2k-2$, with $t \neq k-1$, then the $\mathfrak{q}$-part of $c_q(t)$ is trivial.*

(This $2k-1$ is the length of the Hodge filtration.) Since we are especially interested in the choice $q = p := 2k-1$ (when it is prime), this is just not quite good enough for our purposes. However, using the fact that $M'_g(k-1) \oplus K \simeq \mathrm{Hom}(M_g, M_g)$, a sufficiently good improvement is possible. The proposition below is a direct application of the proof of Proposition 2.16 of [DFG] (that part before the statement of Lemma 2.17), making the choices (in their notation) $\mathcal{D}_1 = \mathfrak{M}_{g,\mathrm{crys}}[k-1-t]$, $\mathcal{D}_2 = \mathfrak{M}_{g,\mathrm{crys}}$. In [DFG] the case $t = k-1$ (for which they require $q > k$) is considered, but they also look at the choice $\mathcal{D}_1 = \mathfrak{M}_{g,\mathrm{crys}}$, $\mathcal{D}_2 = \mathfrak{M}_{g,\mathrm{crys}}[1]$, for which they require $q > k+1$. (Their more careful definition of the Tamagawa factor allows the case $t = k-1$.) The proof of the following proposition is a simple generalisation of these cases.

Proposition 4.5. *For $1 \leqslant t < k-1$, the $\mathfrak{q}$-part of $c_q(t)$ is trivial as long as $q > 2k-1-t$.*

In [Du], one of us made do with Lemma 4.4, thus missing the significance of primes of the form $2k-1$, which was impressed upon him by the other author. The stated goal of this subsection has now been achieved.

4.3. Global torsion

Let $p \equiv 3 \pmod 4$ be a prime, and let $k := (p+1)/2$. Suppose that $h(\sqrt{-p}) > 1$. According to Theorem I,

$$\mathsf{trace}_k\big(\widehat{L}(\mathsf{Sym}^2, 1)\big)_{\mathsf{alg}} \in p^{-1}\mathbb{Z}_{(p)}^{\times}.$$

Hence there must exist a normalised, cuspidal Hecke eigenform $g = \sum_{n=1}^{\infty} a_n q^n$ for $\mathrm{SL}_2(\mathbb{Z})$, of weight k, and a prime $\mathfrak{p} \mid p$ of $\mathbb{Q}(\{a_n\})$ such that $\frac{L(\mathsf{Sym}^2(g),1)}{2\pi\|g\|^2}$ is not integral at $\mathfrak{p}$. For $t = 1$, one of the terms appearing in the denominator of (4.3) has $\mathfrak{p}$-part $H^0(\mathbb{Q}, A'_{g,\mathfrak{p}}(2k-2))$. So the following proposition is consistent with the Bloch–Kato conjecture, and seems to provide a link between Theorem I and Theorem III. Not knowing the $\mathfrak{p}$-part of Ш(1), it is not possible to strengthen this statement.

Proposition 4.6. *Let $p \equiv 3 \pmod 4$ be a prime, and let $k := (p+1)/2$. Suppose that $h(\sqrt{-p}) > 1$. Then there exist a normalised, cuspidal Hecke eigenform $g = \sum_{n=1}^{\infty} a_n q^n$ for $\mathrm{SL}_2(\mathbb{Z})$, of weight k, and a prime $\mathfrak{p} \mid p$ of $\mathbb{Q}(\{a_n\})$ such that $H^0(\mathbb{Q}, A'_{g,\mathfrak{p}}(2k-2))$ is non-trivial.*

Proof. By Proposition 3.2, there is a g such that $\overline{\rho}_{g,\mathfrak{p}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ has dihedral image, factoring through $\mathrm{Gal}(E/\mathbb{Q})$, where E is some unramified, cyclic extension of $F := \mathbb{Q}(\sqrt{-p})$. The representation $\overline{\rho}_{g,\mathfrak{p}}$ is induced from a character of $\mathrm{Gal}(E/F)$, of order r, say, and is realised on the space $A_g[\mathfrak{p}]$. Since $2k-2 = p-1$, and the $(p-1)$-power of the (mod p) cyclotomic character is trivial, $A'_g[\mathfrak{p}]$ is isomorphic to $A'_g[\mathfrak{p}](2k-2)$. Hence it suffices to produce a non-zero $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-fixed element of $A'_g[\mathfrak{p}] = \mathsf{Sym}^2 A_g[\mathfrak{p}]$.

The restriction of $\overline{\rho}_{g,\mathfrak{p}}$ to the cyclic subgroup $\mathrm{Gal}(E/F)$ is a sum of characters τ and τ^{-1}. Let $\{x, y\}$ be a basis of $A_g[\mathfrak{p}]$ such that $\mathrm{Gal}(E/F)$ acts on x and y by τ and τ^{-1} respectively. Then xy is the $\mathrm{Gal}(E/\mathbb{Q})$-invariant element we seek. (In the non-trivial coset of $\mathrm{Gal}(E/F)$ in $\mathrm{Gal}(E/\mathbb{Q})$, there is a representative that switches x and y.) □

We consider the other possible contributions to global torsion terms.

Proposition 4.7. *Suppose that $1 \leqslant t \leqslant k-1$ is odd, and that the $\mathfrak{q}$-part of $\#H^0(\mathbb{Q}, A'(t))\#H^0(\mathbb{Q}, A'(2k-1-t))$ is non-trivial. Then either $t = 1$ and $q = p = 2k-1$, with $h(\sqrt{-p}) > 1$, or $q \leqslant k+1$, or $\mathrm{ord}_q(B_k) > 0$. In the case $\mathrm{ord}_q(B_k) > 0$, if $q > 2k$ then $t = 1$ or $k-1$.*

Proof. It is equivalent to consider non-triviality of $\#H^0(\mathbb{Q}, A'[\mathfrak{q}](t))\#H^0(\mathbb{Q}, A'[\mathfrak{q}](2k-1-t))$. Now $H^0(\mathbb{Q}, A'[\mathfrak{q}](t)) \subset \mathrm{Hom}_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}(A[\mathfrak{q}](k-1-t), A[\mathfrak{q}])$ and $H^0(\mathbb{Q}, A'[\mathfrak{q}](2k-1-t)) \subset \mathrm{Hom}_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}(A[\mathfrak{q}], A[\mathfrak{q}](k-t))$. Recall that the twist is here multiplication by a power of the (mod q) cyclotomic character.

If $A[\mathfrak{q}]$ is irreducible then, in order to get a non-zero element of $H^0(\mathbb{Q}, A'[\mathfrak{q}](t))$ or $H^0(\mathbb{Q}, A'[\mathfrak{q}](2k-1-t))$, we require $A[\mathfrak{q}]$ to be isomorphic to a twist (by $k-1-t$ or $k-t$) of itself. Considering the determinant, that twist must be by either the trivial character or a quadratic character (necessarily χ_{-q}, the $\frac{q-1}{2}$-power of the cyclotomic character). In the first case, we are looking at $\mathrm{Hom}_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}(A[\mathfrak{q}], A[\mathfrak{q}])$, which consists of scalars, by Schur's lemma, but we need endomorphisms of trace zero, so we get nothing non-zero. In the latter case $a_\ell \equiv 0 \pmod{\mathfrak{q}}$ for all primes ℓ with $(\frac{\ell}{q}) = -1$, since $a_\ell \equiv \chi_{-q}(\ell)a_\ell \pmod{\mathfrak{q}}$. As we have seen, this implies that the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $A[\mathfrak{q}]$ factors through a dihedral extension. As before, the Serre weight is $1 + q(0) + (q-1)/2 = (q+1)/2$, so unless $q < k$ we get $k = (q+1)/2$, i.e. $q = 2k-1$. Since the twist $(q-1)/2 = k-1$, we must have $t = 1$. Also, by Proposition 3.4, this case only happens when $h(\sqrt{-p}) > 1$.

If $A[\mathfrak{q}]$ is reducible then its semi-simplification must be the sum of two powers of the inverse-cyclotomic character, χ^a and χ^b, with $0 \leqslant a < b \leqslant q-2$ and $a + b \equiv k-1 \pmod{q-1}$. It follows from a theorem of Swinnerton-Dyer [SD] (see also 3.2 of [Se2]) that either $q \leqslant k+1$ or $\mathrm{ord}_q(B_k) > 0$. (The generalisation to coefficients in a finite extension of $\mathbb{F}_q$ is completely straightforward.) Furthermore, in the latter case, if we assume $q > k$ then $a = 0$ and $b = k-1$. In that case the composition factors of $A'[\mathfrak{q}]$ are $\mathbb{F}_q$, $\mathbb{F}_q(1-k)$ and $\mathbb{F}_q(2-2k)$. If $q > 2k$ then the only r such that $1 \leqslant r \leqslant 2k-2$ and $A'[\mathfrak{q}](r)$ has a trivial composition factor are $r = k-1$ and $r = 2k-2$. □

In each of the cases for which $h(\sqrt{-p}) = 1$, one may check, using Stein's table [Ste], that p does not divide the discriminant of the characteristic polynomial of T_2 on $S_k(\Gamma)$. (When $p = 163$, one of the prime divisors of the discriminant has 133 digits.) It follows from this that the congruence ideal $c(g)$ is coprime to p. The previous proposition shows that the other terms in the denominator of the right-hand side of (4.3) are also coprime to p in these cases. This then accounts for the integrality at p of $\mathrm{trace}_k(\widehat{L}(\mathrm{Sym}^2, 1)_{\mathrm{alg}})$.

References

[BK] S. Bloch, K. Kato, L-functions and Tamagawa numbers of motives, in: The Grothendieck Festschrift, vol. I, in: Progr. Math., vol. 86, Birkhäuser, 1990, pp. 333–400.

[BS] Z.I. Borevich, I.R. Shafarevich, Number Theory, Academic Press, New York, 1966, transl. by N. Greenleaf.

[C1] L. Carlitz, The class number of an imaginary quadratic field, Comment. Math. Helv. 27 (1953) 338–345.

[C2] L. Carlitz, Some arithmetic properties of generalized Bernoulli numbers, Bull. Amer. Math. Soc. 65 (1959) 68–69.

[De1] P. Deligne, Valeurs de fonctions L et periodes d'integrales, Proc. Sympos. Pure Math., vol. 33, 1979, pp. 313–346 (part 2).

[De2] P. Deligne, Formes modulaires et représentations l-adiques, in: Sém. Bourbaki, éxp. 355, in: Lecture Notes in Math., vol. 179, Springer-Verlag, Berlin, 1969, pp. 139–172.

[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.

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

[E] B. Edixhoven, Serre's conjecture, in: G. Cornell, J.H. Silverman, G. Stevens (Eds.), Modular Forms and Fermat's Last Theorem, Springer-Verlag, New York, 1997, pp. 209–242.

[Fa] G. Faltings, Crystalline cohomology and p-adic Galois-representations, in: Algebraic Analysis, Geometry, and Number Theory, Johns Hopkins Univ. Press, Baltimore, 1989, pp. 25–80.

[Fo] J.-M. Fontaine, Le corps de périodes p-adiques, Astérisque 223 (1994) 59–111.

[Ga] P. Garrett, Pullbacks of Eisenstein series applications, in: Automorphic Forms of Several Variables, Katata, 1983, in: Progr. Math., vol. 46, Birkhäuser Boston, Boston, MA, 1984, pp. 114–137.

[Hi] H. Hida, Modular Forms and Galois Cohomology, Cambridge University Press, 2000.

[IR] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, second edition, Grad. Texts in Math., vol. 84, 1990.

[K] C. Khare, Serre's modularity conjecture: the level one case, Duke Math. J. 134 (2006) 557–589.

[Kl] H. Klingen, Introductory Lectures on Siegel Modular Forms, Cambridge Stud. Adv. Math., vol. 20, 1990.

[L] H.-W. Leopoldt, Eine Verallgemeinerung der Bernoullischen Zahlen, Abh. Math. Sem. Univ. Hamburg 22 (1958) 131–140.

[Ra] R.A. Rankin, Contributions to the theory of Ramanujan's function $\tau(n)$ and other similar arithmetical functions, I and II, Proc. Cambridge Philos. Soc. 35 (1939) 351–372.

[Ri] K.A. Ribet, On l-adic representations attached to modular forms, Invent. Math. 28 (1975) 245–275.

[RV] F. Rodriguez Villegas, The congruences of Clausen–von Staudt and Kummer for half-integral weight Eisenstein series, Math. Nachr. 162 (1993) 187–191.

[Se1] J.-P. Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. 54 (1987) 179–230.

[Se2] J.-P. Serre, Congruences et formes modulaires (d'après H.P.F. Swinnerton-Dyer), in: Séminaire Bourbaki No. 416, 1971/1972.

[Sh] G. Shimura, On the holomorphy of certain Dirichlet series, Proc. Lond. Math. Soc. (3) 31 (1975) 79–98.

[Ste] W. Stein, Characteristic polynomials of T_2 on $S_k(\mathrm{SL}_2(\mathbb{Z}))$, http://modular.fas.harvard.edu/Tables/charpoly_level1/t2/.

[SD] H.P.F. Swinnerton-Dyer, On l-adic representations and congruences for coefficients of modular forms, in: Modular Functions of One Variable, III, Proc. Internat. Summer School, Univ. Antwerp, 1972, in: Lecture Notes in Math., vol. 350, Springer-Verlag, Berlin, 1973, pp. 1–55.

[Wa] L. Washington, Introduction to Cyclotomic Fields, second edition, Grad. Texts in Math., vol. 83, Springer-Verlag, Berlin, 1997.

[Wi] J.R. Wilton, Congruence properties of Ramanujan's function $\tau(n)$, Proc. Lond. Math. Soc. (2) 31 (1930) 1–10.

[Z1] D. Zagier, Modular forms whose Fourier coefficients involve zeta-functions of quadratic fields, in: Modular Functions of One Variable, VI, Proc. Second Internat. Conf., Univ. Bonn, 1976, in: Lecture Notes in Math., vol. 627, Springer-Verlag, Berlin, 1977, pp. 105–169.

[Z2] D. Zagier, Sur la conjecture de Saito–Kurokawa (d'après H. Maass), in: Sém. Delange–Pisot–Poitou 1979/1980, in: Progr. Math., vol. 12, 1980, pp. 371–394.