Squareness in the special L-value

Amod Agashe*
Department of Mathematics, Florida State University
Tallahassee, FL 32306, U.S.A.
agashe@math.fsu.edu

Received (Day Month Year)
Accepted (Day Month Year)

Communicated by xxx

Let N be a prime and let A be a quotient of $J_0(N)$ over $\mathbf{Q}$ associated to a newform f such that the special L-value of A (at $s = 1$) is non-zero. Suppose that the algebraic part of the special L-value of A is divisible by an odd prime q such that q does not divide the numerator of $\frac{N-1}{12}$. Then the Birch and Swinnerton-Dyer conjecture predicts that q^2 divides the algebraic part of special L value of A as well as the order of the Shafarevich-Tate group. Under a mod q non-vanishing hypothesis on special L-values of twists of A, we show that q^2 does indeed divide the algebraic part of the special L-value of A and the Birch and Swinnerton-Dyer conjectural order of the Shafarevich-Tate group of A. We also give a formula for the algebraic part of the special L-value of A over suitable quadratic imaginary fields in terms of the free abelian group on isomorphism classes of supersingular elliptic curves in characteristic N (equivalently over conjugacy classes of maximal orders in the definite quaternion algebra over $\mathbf{Q}$ ramified at N and ∞) which shows that this algebraic part is a perfect square away from two.

Keywords: Abelian variety; Special L-value; Shafarevich-Tate group.

Mathematics Subject Classification 2000: 11xxx, 11xxx, 11xxx

1. Introduction and results

Let A be an abelian variety over a number field F. Let $L(A/F, s)$ denote the associated L-function, and assume that $L(A/F, 1) \neq 0$. Let $\Omega(A/F)$ denote the quantity $C_{A,\infty}$ in [Lan91, § III.5]; it is the "archimedean volume" of A over embeddings of F in $\mathbf{R}$ and $\mathbf{C}$ (e.g., if $F = \mathbf{Q}$, then it is the volume of $A(\mathbf{R})$ computed using invariant differentials on the Néron model of A). Let M_{fin} denote the set of finite places of F. Let $\mathcal{A}$ denote the Néron model of A over the ring of integers of F and let $\mathcal{A}^0$ denote the largest open subgroup scheme of $\mathcal{A}$ in which all the fibers are connected. If $v \in M_{\text{fin}}$, then let $\mathbf{F}_v$ denote the associated residue class field and let $c_v(A/F) = [\mathcal{A}_{\mathbf{F}_v}(\mathbf{F}_v) : \mathcal{A}^0_{\mathbf{F}_v}(\mathbf{F}_v)]$, the orders of the arithmetic component groups. Let $Ш(A/F)$ denote the Shafarevich-Tate group of A over F. If $F = \mathbf{Q}$, then we

*The author was partially supported by National Science Foundation Grant No. 0603668.

will often drop the symbol "$/F$" in the notation (thus $Ш(A/\mathbf{Q})$ will be denoted $Ш(A)$, etc.). If B is an abelian variety over F, then we denote by $B^\vee$ the dual abelian variety of B, and by $B(F)_{\mathrm{tor}}$ the torsion subgroup of $B(F)$. Suppose that $L(A/F,1) \neq 0$. Then the second part of the Birch and Swinnerton-Dyer conjecture says the following (see [Lan91, § III.5]):

Conjecture 1.1 (Birch and Swinnerton-Dyer).

$$\frac{L(A/F,1)}{\Omega(A/F)} = \frac{|Ш(A/F)| \cdot \prod_{v \in M_{\mathrm{fin}}} c_v(A/F)}{|A(F)_{\mathrm{tor}}| \cdot |A^\vee(F)_{\mathrm{tor}}|}. \tag{1.1}$$

We denote by $|Ш(A/F)|_{\mathrm{an}}$ the order of $|Ш(A/F)|$ predicted by the conjecture above, and call it the *analytic order* of $|Ш(A/F)|$. Thus

$$|Ш(A/F)|_{\mathrm{an}} = \frac{L(A/F,1)}{\Omega(A/F)} \cdot \frac{|A(F)_{\mathrm{tor}}| \cdot |A^\vee(F)_{\mathrm{tor}}|}{\prod_{v \in M_{\mathrm{fin}}} c_v(A/F)} \quad .$$

If N is a positive integer, then let $X_0(N)$ denote the modular curve over $\mathbf{Q}$ associated to $\Gamma_0(N)$, and let $J_0(N)$ be its Jacobian. Let $\mathbf{T}$ denote the subring of endomorphisms of $J_0(N)$ generated by the Hecke operators (usually denoted T_ℓ for $\ell \nmid N$ and U_p for $p \,|\, N$). If f is a newform in $S_2(\Gamma_0(N), \mathbf{C})$, then let $I_f = \mathrm{Ann}_{\mathbf{T}} f$ and let A_f denote the quotient abelian variety $J_0(N)/I_f J_0(N)$ over $\mathbf{Q}$. We also denote by $L(f,s)$ the L-function associated to f and by $L(A_f,s)$ the L-function associated to A_f.

Now fix a prime N and a newform f on $\Gamma_0(N)$ such that $L(A_f,1) \neq 0$. Then by [KL89], $A_f(\mathbf{Q})$ has rank zero, and $Ш(A_f)$ is finite. Thus the second part of the Birch and Swinnerton-Dyer conjecture becomes:

Conjecture 1.2 (Birch and Swinnerton-Dyer).

$$\frac{L(A_f,1)}{\Omega(A_f)} = \frac{|Ш(A_f)| \cdot c_N(A_f)}{|A_f(\mathbf{Q})| \cdot |A_f^\vee(\mathbf{Q})|}, \tag{1.2}$$

It is known that $\frac{L(A_f,1)}{\Omega(A_f)}$ is a rational number and we call this number the *algebraic part* of the special L-value of A_f. Let q be an odd prime that does not divide the numerator of $\frac{N-1}{12}$ but divides $\frac{L(A_f,1)}{\Omega(A_f)}$. Note that the denominator of $\frac{L(A_f,1)}{\Omega(A_f)}$ divides the numerator of $\frac{N-1}{12}$ (by [Aga07, §1]), and so it makes sense to talk about whether q divides $\frac{L(A_f,1)}{\Omega(A_f)}$ or not.

Proposition 1.3. *Let q be as above. Then q divides $|Ш(A_f)|_{\mathrm{an}}$. If the Birch and Swinnerton-Dyer conjecture (1.2) is true, then q^2 divides $|Ш(A_f)|$ as well as $\frac{L(A_f,1)}{\Omega(A_f)}$.*

Proof. By [Eme03, Theorem B] (and considering that the order of the cuspidal subgroup of $J_0(N)$ is the numerator of $\frac{N-1}{12}$ when N is prime), q does not divide $\prod_{p|N} c_p(A_f)$ or $|A_f(\mathbf{Q})| \cdot |A_f^\vee(\mathbf{Q})|$. Thus if q divides $\frac{L(A_f,1)}{\Omega(A_f)}$ then q divides $|Ш(A)|_{\mathrm{an}}$. Now assume the Birch and Swinnerton-Dyer conjecture (1.2), so that q divides $|Ш(A)|$. As mentioned towards the end of §7.3 in [DSW03], if $A_f^\vee[\mathfrak{q}]$ is irreducible for all maximal ideals $\mathfrak{q}$ of $\mathbf{T}$ with residue field of characteristic q, then the q primary part of $Ш(A_f^\vee)$ (and hence that of $Ш(A_f)$) has order a perfect square. In our case, this irreducibility holds by [Maz77, Prop. 14.2], and thus q^2 divides the value of $|Ш(A_f)|$. Moreover, as mentioned above, q does not divide any of the other quantities on the right side of (1.2), hence we see that q^2 divides $\frac{L(A_f,1)}{\Omega(A_f)}$, which is the left side. □

Thus by Proposition 1.3, if q divides $\frac{L(A_f,1)}{\Omega(A_f)}$ or $|Ш(A_f)|_{\rm an}$, but does not divide the numerator of $\frac{N-1}{12}$, then q^2 (not just q) is expected to divide $\frac{L(A_f,1)}{\Omega(A_f)}$ and $|Ш(A_f)|_{\rm an}$.

Let K be a quadratic imaginary field and let $-D$ be its discriminant. . Let $\epsilon_D = (\frac{-D}{\cdot})$ denote the associated quadratic character. Suppose that D is coprime to N. Then $f \otimes \epsilon_D$ is a modular form of level ND^2. By a refinement of a theorem Waldspurger (see [LR97]), there exist infinitely many prime-to-N discriminants $-D$ such that $L(A_{f\otimes\epsilon_D}, 1) \neq 0$. Suppose D is such that $L(A_{f\otimes\epsilon_D}, 1) \neq 0$.

If $\langle\ ,\ \rangle : M \times M' \to \mathbf{C}$, is a pairing between two $\mathbf{Z}$-modules M and M', each of the same rank m, and $\{\alpha_1, \ldots, \alpha_m\}$ and $\{\beta_1, \ldots, \beta_m\}$ are bases of M and M' (respectively), then by $\mathrm{disc}(M \times M' \to \mathbf{C})$, we mean the absolute value of $\det(\langle\alpha_i, \beta_j\rangle)$; this value is independent of the choices of bases made in its definition. We have a pairing

$$H_1(X_0(N), \mathbf{Z}) \otimes \mathbf{C} \times S_2(\Gamma_0(N), \mathbf{C}) \to \mathbf{C} \qquad (1.3)$$

given by $(\gamma, g) \mapsto \langle\gamma, g\rangle = \int_\gamma 2\pi i g(z)dz$ and extended $\mathbf{C}$-linearly. At various points in this article, we will consider pairings between two $\mathbf{Z}$-modules; unless otherwise stated, each such pairing is obtained in a natural way from (1.3).

We have an involution induced by complex conjugation on $H_1(A_f, \mathbf{Z})$, and we denote by $H_1(A_f, \mathbf{Z})^-$ the subgroup of elements of $H_1(A_f, \mathbf{Z})$ on which the involution acts as -1. Let $S_f = S_2(\Gamma_0(N), \mathbf{Z})[I_f]$, and let $\Omega^-_{A_f} = \mathrm{disc}(H_1(A_f, \mathbf{Z})^- \times S_f \to \mathbf{C})$. Then $\frac{L(A_{f\otimes\epsilon_D},1)}{(i\sqrt{D})^d \Omega^-_{A_f}}$ is an integer (e.g., by Prop 2.1 below).

Theorem 1.4. *Recall that the level N is assumed to be prime, and q is an odd prime which does not divide the numerator of $\frac{N-1}{12}$, but divides $\frac{L(A_f,1)}{\Omega(A_f)}$. Assume that q satisfies the following hypothesis:*
(*) there exists a fundamental discriminant $-D$ that is coprime to N such that $L(A_{f\otimes\epsilon_D}, 1) \neq 0$ and q does not divide $\frac{L(A_{f\otimes\epsilon_D},1)}{(i\sqrt{D})^d \Omega^-_{A_f}}$.
Then q^2 divides $\frac{L(A_f,1)}{\Omega(A_f)}$ and $|Ш(A_f)|_{\rm an}$.

We shall prove Theorem 1.4 in Section 2. Assuming hypothesis (*), in view of Proposition 1.3, Theorem 1.4 provides theoretical evidence towards the Birch and Swinnerton-Dyer conjectural formula (1.2).

We now give some heuristic and computational evidence for why hypothesis (*) might always hold when A_f is an elliptic curve, which we denote by E. In this case, $\frac{L(A_{f\otimes\epsilon_D},1)}{(i\sqrt{D})^d\Omega^-_{A_f}}$ is the special L-value of the twisted elliptic curve E_{-D} up to powers of 2 (because the Manin constant of E_{-D} is a power of 2, by [Maz78, Cor. 4.1]). As mentioned before, by [Eme03, Theorem B], q does not divide the orders of the arithmetic component groups of E, and hence by [Pra08, Lem. 2.1], q does not divide the orders of the arithmetic component groups of E_{-D} either. Thus if one assumes the second part of the Birch and Swinnerton-Dyer conjecture for E_{-D}, then the only way q can divide $\frac{L(E_{f\otimes\epsilon_D},1)}{(i\sqrt{D})^d\Omega^-_{A_f}}$ is if q divides the order of $Ш(E_{-D})$. Now there is no clear reason for q to divide the order of $Ш(E_{-D})$ for *every* D. Kolyvagin has asked whether for any prime q there is a twist of E such that q does not divide the order of the Shafarevich-Tate group of the twist (see Question A in [Pra08]). We are interested in the same question, but with the added restrictions that the twist is by a negative discriminant and that the special L-value of the twist is nonzero. There is some numerical evidence that the answer should be yes even with the added restriction. In [Che04], Chen reports on compuations to find how often certain small primes divide the analytic orders of the Shafarevich-Tate group for twists of certain elliptic curves. For example, consider the elliptic curve E of conductor 11 given by $y^2 + y = x^3 - x^2$, which has trivial Shafarevich-Tate group and analytic rank zero. Chen computes the analytic orders of the Shafarevich-Tate group of E_{-D} for $1 \leq D \leq 13,000,000$ such that D is coprime to 44 and the analytic rank of E_{-D} is zero (p. 5–7 of loc. cit.). She finds that for all primes q between 2 and 37, there is a positive fraction of D's such that q divides the analytic order of the Shafarevich-Tate group of E_{-D}. For each such pair (q, E_{-D}), we have an example of an elliptic curve E_{-D} for which the odd prime q divides the analytic order of the Shafarevich-Tate group, and which has a twist by $\mathbf{Q}(\sqrt{-D})$, viz. E itself, such that q does not divide the analytic order of the Shafarevich-Tate group of the twist. There is a similar example involving the curve $y^2 + xy + y = x^3 - x$ in p. 8–9 of loc. cit. Of course we have to assume the second part of the Birch and Swinnerton-Dyer conjecture to pass from analytic orders of the Shafarevich-Tate groups to their actual orders. The careful reader would have noticed that we want to apply hypothesis (*) to give evidence for the second part of the Birch and Swinnerton-Dyer conjecture, and at the same time we are assuming the conjecture to give some credence to the hypothesis. While this may sound like circular reasoning, the point is that the conjecture is being applied in different contexts, and also our reasoning is not intended in any way to be a part of a proof.

One would of course hope that hypothesis (*) is proved independent of the second part of the Birch and Swinnerton-Dyer conjecture. While it is known that hypothesis (*) does hold for all but finitely many primes q (e.g., see [OS98, Cor. 1]), it is not clear what that finite list of primes is. Also, in [BO03, p.167-168], one finds a criterion for how big q needs to be, but the period they use (cf. [Bru99, §5]) differs from the period we use by an unknown algebraic number (cf. the discussion in [Koh85, Cor. 2], and [Pra08, Conj. 5.1]). Thus unfortunately the theoretical results mentioned in this paragraph do not help us much regarding hypothesis (*).

Proposition 1.5. *Recall again that the level N is assumed to be prime. Suppose q is an odd prime that does not divide the numerator of $\frac{N-1}{12}$ and there is a normalized eigenform $g \in S_2(\Gamma_0(N), \mathbf{C})$ such that $L(A_g, 1) = 0$ and f is congruent to g modulo a prime ideal over q in the ring of integers of the number field generated by the Fourier coefficients of f and g.*
(i) If the first part of the Birch and Swinnerton-Dyer conjecture is true for A_g, then q^2 divides $|\text{Ш}(A_f)|$.
(ii) Suppose q satisfies hypothesis (*) of Theorem 1.4. Then q^2 divides $\frac{L(A_f,1)}{\Omega(A_f)}$ and the Birch and Swinnerton-Dyer conjectural value of $|\text{Ш}(A_f)|$. In particular $\frac{L(A_f,1)}{\Omega(A_f)} \equiv \frac{L(A_g,1)}{\Omega(A_g)} \bmod q^2$.

Proof. If the first part of the Birch and Swinnerton-Dyer conjecture (on rank) is true for A_g, then considering that $L(A_g, 1) = 0$, we see that A_g has positive Mordell-Weil rank. Part (i) now follows from [Aga07, Thm 6.1]. By [Aga07, Prop. 1.3], the hypotheses of the proposition implies that q divides $L(A_f, 1)/\Omega(A_f)$. Thus part (ii) follows from the Theorem above. □

Subject to hypothesis (*), the proposition above shows some consistency between the predictions of the two parts of the Birch and Swinnerton-Dyer conjecture. There is a general philosophy that congruences between eigenforms should lead to congruences between algebraic parts the corresponding special L-values, and there are theorems in this direction (see [Vat99] and the references therein for more instances). However, these theorems prove congruences modulo primes, but not their powers. To our knowledge, part (ii) of Proposition 1.5 above is the first result of of a form in which the algebraic parts of the special L-value are congruent modulo the *square* of a congruence prime.

Let $\{E_0, E_1, \ldots, E_g\}$ be a set of representatives for the isomorphism classes of supersingular elliptic curves in characteristic N, where g is the genus of $X_0(N)$. We denote the class of E_i by $[E_i]$. Let $\mathcal{P}$ denote the divisor group supported on the $[E_i]$ and let $\mathcal{P}^0$ denote the subgroup of divisors of degree 0. For $i = 1, 2, \ldots, g$, let $R_i = \text{End } E_i$. Each R_i is a maximal order in the definite quaternion algebra ramified at N and ∞, which we denote by $\mathcal{B}$ and in fact, the R_i's are representatives of the conjugacy classes of maximal orders of $\mathcal{B}$. Moreover, setting $I_i = \text{Hom}(E_0, E_i)$, we see that the I_i are representatives for the isomorphism classes of right locally free rank one modules over R_0. Let $\mathcal{O}_{-D}$ denote the quadratic order of discriminant $-D$, $h(-D)$ the number of classes of $\mathcal{O}_{-D}$, $u(-D)$ the order of $\mathcal{O}^*_{-D}/\langle \pm 1 \rangle$, and $h_i(-D)$ the number of optimal embeddings of $\mathcal{O}_{-D}$ in R_i modulo conjugation by R_i^*. Following [Gro87], we define

$$\chi_D = \frac{1}{2u(-D)} \sum_{i=0}^{g} h_i(-D)[E_i] \in \mathcal{P} \otimes \mathbf{Q}.$$

Let $w_i = |\mathrm{Aut} E_i| = |R_i^*/\langle \pm 1 \rangle|$. Define the Eisenstein element in $\mathcal{P} \otimes \mathbf{Q}$ as $a_E = \sum_{i=0}^{g} \frac{[E_i]}{w_i}$. Let $\chi_D^0 = \chi_D - \frac{12}{p-1} \deg(e_D) a_E$. Let $n = \mathrm{numr}(\frac{p-1}{12})$; then $n\chi_D^0 \in \mathcal{P}^0$. The key step in proving Theorem 1.4 is the following result, which is also proved in Section 2:

Theorem 1.6. *Recall that the level N is prime. Let K be a quadratic imaginary field with discriminant $-D$ that is coprime to N. If $L(A_f/K, 1) \neq 0$, then up to powers of 2,*

$$\frac{L(A_f/K,1)}{\Omega(A/K)} = \frac{\left|\pi\left(\frac{\mathcal{P}^0}{\mathbf{T} n \chi_D^0}\right)\right|^2}{n^2} \quad .$$

In particular, $\frac{L(A_f/K,1)}{\Omega(A/K)}$ is a perfect square away from the prime 2.

This addresses the issue raised in [Reb06, p. 236] that as of the writing of loc. cit., one did not have a way of expressing special L-values in terms of the module $\mathcal{P}$. Also, it may be possible to use the formula above for computations using Brandt matrices (cf. [Koh]). Note that up to powers of 2, $\frac{L(A_f/K,1)}{\Omega(A_f/K)}$ equals $\frac{L(A_f,1)}{\Omega(A_f)} \cdot \frac{L(A_{f\otimes\epsilon_D},1)}{(i\sqrt{D})^d \Omega_{A_f}^-}$. Thus if the formula in Theorem 1.6 could be used for computations, then considering that one already knows how to compute $\frac{L(A_f,1)}{\Omega(A_f)}$ (see [AS05]), one could compute $\frac{L(A_{f\otimes\epsilon_D},1)}{(i\sqrt{D})^d \Omega_{A_f}^-}$ systematically and check whether hypothesis (*) holds in the computations.

2. Proofs

In this section, we prove Theorems 1.4 and 1.6. We continue to use the notation introduced so far. We shall be using results from [Reb06], and details of some of the facts we use here routinely may be found in loc. cit.

Let $-D$ be a fundamental discriminant prime to N such that $L(A_{f\otimes\epsilon_D}, 1) \neq 0$. Let H^+ and H^- denote the subgroup of elements of $H_1(X_0(N), \mathbf{Z})$ on which the complex conjugation involution acts as 1 and -1 respectively. The modular symbol $\sum_{b \bmod D} \epsilon_D(b)\{-\frac{b}{D}, \infty\}$ is an element of H^- and will be denoted by e_D. Since the level N is prime, the Hecke algebra $\mathbf{T}$ is semi-simple, and hence we have an isomorphism $\mathbf{T}\otimes\mathbf{Q} \cong \mathbf{T}/I_f \otimes \mathbf{Q} \oplus B$ of $\mathbf{T}\otimes\mathbf{Q}$-modules for some $\mathbf{T}\otimes\mathbf{Q}$-module B. Let π denote element of $\mathbf{T}\otimes\mathbf{Q}$ that is the projection on the first factor.

Proposition 2.1.

$$\frac{L(A_{f\otimes\epsilon_D},1)}{(i\sqrt{D})^d \Omega_{A_f}^-} = \left|\pi\left(\frac{H^-}{\mathbf{T} e_D}\right)\right|.$$

Proof. The proof is very similar to the proof of Theorem 2.1 in [Aga07]. The main thing to note is that if $f_1, \ldots, f_d$ are the Galois conjugates of f, then $L(A_{f\otimes\epsilon_D}, 1) = \prod_i L(f_i \otimes \epsilon_D, 1) = \prod_i \frac{\langle e_D, f_i\rangle}{i\sqrt{D}}$ (see, e.g., [Man71, Thm 9.9]). Hence, up to a power of 2,

$$\frac{L(A_{f\otimes\epsilon_D},1)}{(\sqrt{-D})^d\Omega^-_{A_f}} = \frac{\prod_i \langle e_D, f_i\rangle}{\mathrm{disc}(\pi(H^-)\times S_f \to \mathbf{C})}$$
$$= \frac{\prod_i \langle e_D, f_i\rangle}{\mathrm{disc}(\pi(\mathbf{T}e_D)\times S_f \to \mathbf{C})} \cdot |\pi(H^-) : \pi(\mathbf{T}e_D)|.$$

One can see in a manner similar to the proof of formula (6) in the proof of Theorem 2.1 in [Aga07] that the first factor above is 1 (in that proof, replace e by e_D and in the analog of the proof of Lemma 2.3 in [Aga07], use the fact that $L(f\otimes\epsilon, 1) \neq 0$). □

Let $\mathcal{H}$ denote the complex upper half plane, and let $\{0, i\infty\}$ denote the projection of the geodesic path from 0 to $i\infty$ in $\mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})$ to $X_0(N)(\mathbf{C})$. We have an isomorphism

$$H_1(X_0(N),\mathbf{Z}) \otimes \mathbf{R} \xrightarrow{\cong} \mathrm{Hom}_{\mathbf{C}}(H^0(X_0(N),\Omega^1),\mathbf{C}),$$

obtained by integrating differentials along cycles. Let e be the element of $H_1(X_0(N),\mathbf{Z}) \otimes \mathbf{R}$ that corresponds to the map $\omega \mapsto -\int_{\{0,i\infty\}}\omega$ under this isomorphism. It is called the *winding element*. By the Manin-Drinfeld Theorem, (see [Lan95, Chap. IV, Theorem 2.1] and [Man72]), $e \in H_1(X_0(N),\mathbf{Z}) \otimes \mathbf{Q}$. Also, since the complex conjugation involution on $H_1(X_0(N),\mathbf{Z})$ is induced by the map $z \mapsto -\overline{z}$ on the complex upper half plane, we see that e is invariant under complex conjugation. Thus $e \in H_1(X_0(N),\mathbf{Z})^+ \otimes \mathbf{Q}$.

Consider the $\mathbf{T}[1/2]$-equivariant isomorphism

$$\Phi : \mathcal{P}^0[1/2] \otimes_{\mathbf{T}[1/2]} \mathcal{P}^0[1/2] \to H^+[1/2] \otimes_{\mathbf{T}[1/2]} H^-[1/2] \tag{2.1}$$

obtained from [Reb06, Prop. 4.6] (which says that both sides of (2.1) are isomorphic to $S_2(\Gamma_0(N),\mathbf{Z})[1/2]$, and whose proof relies on results of [Eme02]). By [Reb06, Thm 0.2], we have $\Phi_{\mathbf{Q}}(\chi^0_D \otimes_{\mathbf{T_Q}} \chi^0_D) = e \otimes_{\mathbf{T_Q}} e_D$, where the subscript $\mathbf{Q}$ stands for tensoring with $\mathbf{Q}$ (this follows essentially from [Gro87, Cor 11.6], along with its generalization [Zha01, Thm 1.3.2]). Thus $\Phi_{\mathbf{Q}}$ induces an isomorphism

$$\mathbf{T}[1/2](n\chi^0_D \otimes_{\mathbf{T}[1/2]} n\chi^0_D) \cong \mathbf{T}[1/2]ne \otimes_{\mathbf{T}[1/2]} \mathbf{T}[1/2]ne_D. \tag{2.2}$$

Note that $ne \in H^+$ by II.18.6 and II.9.7 of [Maz77].

Proposition 2.2.

$$\left|\pi\left(\frac{H^+[1/2]}{\mathbf{T}[1/2]ne}\right)\right| \cdot \left|\pi\left(\frac{H^-[1/2]}{\mathbf{T}[1/2]ne_D}\right)\right| = \left|\pi\left(\frac{H^+[1/2]\otimes_{\mathbf{T}} H^-[1/2])}{\mathbf{T}[1/2]ne \otimes_{\mathbf{T}} \mathbf{T}[1/2]ne_D}\right)\right|$$

Proof. By [Maz77, §15], if $\mathfrak{m}$ is a Gorenstein maximal ideal of $\mathbf{T}$ with odd residue characteristic, then $H^+_{\mathfrak{m}}$ and $H^-_{\mathfrak{m}}$ are free $\mathbf{T}_{\mathfrak{m}}$-modules of of rank one. Since the level is prime, the only non-Gorenstein ideals are the ones lying over 2, a prime that we are systematically inverting anyway.

Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}$ with odd residue characteristic. Let x be a generator of $H^+_{\mathfrak{m}}$ as a free $\mathbf{T}_{\mathfrak{m}}$-module, and let y be a generator of $H^-_{\mathfrak{m}}$ as a free $\mathbf{T}_{\mathfrak{m}}$-module. Then there exists $t_1 \in \mathbf{T}_{\mathfrak{m}}$ such that $ne = t_1 x$ and $t_2 \in \mathbf{T}_{\mathfrak{m}}$ such that $ne_D = t_2 y$. We have

$$\begin{aligned}\left|\frac{\pi(H^+_{\mathfrak{m}} \otimes_{\mathbf{T}_{\mathfrak{m}}} H^-_{\mathfrak{m}})}{\pi(\mathbf{T}_{\mathfrak{m}} ne \otimes_{\mathbf{T}_{\mathfrak{m}}} \mathbf{T}_{\mathfrak{m}} ne_D)}\right| &= \left|\frac{\pi(\mathbf{T}_{\mathfrak{m}} x \otimes_{\mathbf{T}_{\mathfrak{m}}} \mathbf{T}_{\mathfrak{m}} y)}{\pi(\mathbf{T}_{\mathfrak{m}} t_1 x \otimes_{\mathbf{T}_{\mathfrak{m}}} \mathbf{T}_{\mathfrak{m}} t_2 y)}\right| \\ &= \left|\frac{\pi(\mathbf{T}_{\mathfrak{m}}(x \otimes_{\mathbf{T}_{\mathfrak{m}}} y))}{t_1 t_2 \pi(\mathbf{T}_{\mathfrak{m}}(x \otimes_{\mathbf{T}_{\mathfrak{m}}} y))}\right| \\ &= \left|\frac{\pi(\mathbf{T}_{\mathfrak{m}})}{t_2 t_1 \pi(\mathbf{T}_{\mathfrak{m}})}\right| \\ &= \left|\frac{\pi(\mathbf{T}_{\mathfrak{m}})}{t_1 \pi(\mathbf{T}_{\mathfrak{m}})}\right| \cdot \left|\frac{\pi(t_1 \mathbf{T}_{\mathfrak{m}})}{t_2 \pi(t_1 \mathbf{T}_{\mathfrak{m}})}\right|.\end{aligned}$$

Claim:

$$\left|\frac{\pi(t_1 \mathbf{T}_{\mathfrak{m}})}{t_2 \pi(t_1 \mathbf{T}_{\mathfrak{m}})}\right| = \left|\frac{\pi(\mathbf{T}_{\mathfrak{m}})}{t_2 \pi(\mathbf{T}_{\mathfrak{m}})}\right| \quad .$$

Proof. Consider the map $\psi : \pi(\mathbf{T}_{\mathfrak{m}}) \rightarrow \pi(t_1 \mathbf{T}_{\mathfrak{m}})/t_2 \pi(t_1 \mathbf{T}_{\mathfrak{m}})$ given as follows: if $t \in \mathbf{T}_{\mathfrak{m}}$, then $\pi(t) \mapsto \pi(t_1 t)$. If $\pi(t)$ is in the kernel of ψ, then $\pi(t_1 t) = \pi(t_2 t_1 t')$ for some $t' \in \mathbf{T}_{\mathfrak{m}}$. Then $\pi(t_1(t - t_2 t')) = 0$, and since $\pi(t_1) \neq 0$ (as $L(A_f, 1) \neq 0$), we have $\pi(t) = \pi(t_2 t')$. Thus the kernel of ψ is $t_2 \pi(\mathbf{T}_{\mathfrak{m}})$, which proves the lemma. □

Using the claim and the series of equalities above, we have

$$\begin{aligned}\left|\frac{\pi(H^+_{\mathfrak{m}} \otimes_{\mathbf{T}_{\mathfrak{m}}} H^-_{\mathfrak{m}})}{\pi(\mathbf{T}_{\mathfrak{m}} ne \otimes_{\mathbf{T}_{\mathfrak{m}}} \mathbf{T}_{\mathfrak{m}} ne_D)}\right| &= \left|\frac{\pi(\mathbf{T}_{\mathfrak{m}})}{t_1 \pi(\mathbf{T}_{\mathfrak{m}})}\right| \cdot \left|\frac{\pi(\mathbf{T}_{\mathfrak{m}})}{t_2 \pi(\mathbf{T}_{\mathfrak{m}})}\right| \\ &= \left|\frac{\pi(\mathbf{T}_{\mathfrak{m}} x)}{t_1 \pi(\mathbf{T}_{\mathfrak{m}} x)}\right| \cdot \left|\frac{\pi(\mathbf{T}_{\mathfrak{m}} y)}{t_2 \pi(\mathbf{T}_{\mathfrak{m}} y)}\right| \\ &= \left|\frac{\pi(H^+_{\mathfrak{m}})}{\pi(\mathbf{T}_{\mathfrak{m}} ne)}\right| \cdot \left|\frac{\pi(H^-_{\mathfrak{m}})}{\pi(\mathbf{T}_{\mathfrak{m}} ne_D)}\right| \\ &= \left|\pi\left(\frac{H^+_{\mathfrak{m}}}{\mathbf{T}_{\mathfrak{m}} ne}\right)\right| \cdot \left|\pi\left(\frac{H^-_{\mathfrak{m}}}{\mathbf{T}_{\mathfrak{m}} ne_D}\right)\right| \quad .\end{aligned}$$

Since this is true for every $\mathfrak{m}$ with odd residue characteristic, we get the statement in the proposition.

Proposition 2.3.

$$\left|\pi\left(\frac{\mathcal{P}^0[1/2] \otimes_{\mathbf{T}[1/2]} \mathcal{P}^0[1/2]}{\mathbf{T}[1/2](n\chi^0_D \otimes_{\mathbf{T}[1/2]} n\chi^0_D)}\right)\right| = \left|\pi\left(\frac{\mathcal{P}^0[1/2]}{\mathbf{T}[1/2] n\chi^0_D}\right)\right|^2.$$

Proof. By [Eme02, Thm 0.5], if $\mathfrak{m}$ is a Gorenstein maximal ideal of $\mathbf{T}$, then $\mathcal{P}^0_{\mathfrak{m}}$ is a free $\mathbf{T}_{\mathfrak{m}}$-module of rank one; let x be a generator. Then $n\chi^0_D = tx$ for some

$t \in \mathbf{T}_{\mathfrak{m}}$. Hence in a manner similar to the steps in the proof of Proposition 2.2, we have

$$\left|\pi\left(\frac{\mathcal{P}^0_{\mathfrak{m}} \otimes_{\mathbf{T}[1/2]} \mathcal{P}^0_{\mathfrak{m}}}{\mathbf{T}_{\mathfrak{m}}(n\chi^0_D \otimes_{\mathbf{T}[1/2]} n\chi^0_D)}\right)\right| = \left|\pi\left(\frac{\mathbf{T}_{\mathfrak{m}} x \otimes_{\mathbf{T}[1/2]} \mathbf{T}_{\mathfrak{m}} x}{\mathbf{T}_{\mathfrak{m}}(tx \otimes_{\mathbf{T}[1/2]} tx)}\right)\right| = \left|\pi\left(\frac{\mathbf{T}_{\mathfrak{m}}}{t^2 \mathbf{T}_{\mathfrak{m}}}\right)\right|$$

$$= \left|\pi\left(\frac{\mathbf{T}_{\mathfrak{m}}}{t \mathbf{T}_{\mathfrak{m}}}\right)\right|^2 = \left|\pi\left(\frac{\mathcal{P}^0_{\mathfrak{m}}}{\mathbf{T}_{\mathfrak{m}} n\chi^0_D}\right)\right|^2.$$

Since this holds for every maximal ideal $\mathfrak{m}$ of odd residue characteristic, we get the proposition. □

By formula (2.1), formula (2.2), Proposition 2.2, and Proposition 2.3, we have

$$\left|\pi\left(\frac{H^+[1/2]}{\mathbf{T}[1/2]ne}\right)\right| \cdot \left|\pi\left(\frac{H^-[1/2]}{\mathbf{T}[1/2]ne_D}\right)\right| = \left|\pi\left(\frac{\mathcal{P}^0[1/2]}{\mathbf{T}[1/2]n\chi^0_D}\right)\right|^2 \tag{2.3}$$

Let $\Omega^+_{A_f} = \mathrm{disc}(H_1(A_f, \mathbf{Z})^+ \times S_f \to \mathbf{C})$; it differs from $\Omega(A_f)$ by a power of 2 (by [Aga07, Lemma 2.4]). By the proofs of Theorems 2.1 and 3.1 of [Aga07], we have

$$\left|\pi\left(\frac{H^+}{\mathbf{T}(ne)}\right)\right| = n \cdot \frac{L(A_f, 1)}{\Omega^+_{A_f}}.$$

Using this and Proposition 2.1, equation (2.3) says that up to powers of 2,

$$\frac{L(A_f/K, 1)}{\Omega(A/K)} = \frac{L(A_f, 1)}{\Omega^+_{A_f}} \cdot \frac{L(A_{f \otimes \epsilon_D}, 1)}{(i\sqrt{D})^d \Omega^-_{A_f}} = \frac{1}{n^2} \cdot \left|\pi\left(\frac{\mathcal{P}^0[1/2]}{\mathbf{T}[1/2]n\chi^0_D}\right)\right|^2. \tag{2.4}$$

This proves Theorem 1.6.

Also, if an odd prime q divides $\frac{L(A_f,1)}{\Omega(A_f)}$ (which differs from $\frac{L(A_f,1)}{\Omega^+_{A_f}}$ by a power of 2) and q does not divide $\frac{L(A_{f\otimes\epsilon_D},1)}{(i\sqrt{D})^d\Omega^-_{A_f}}$, then by (2.4), q^2 divides $\frac{L(A_f,1)}{\Omega(A_f)}$. By [Eme03, Theorem B], we have $|A_f(\mathbf{Q})| = |A^\vee_f(\mathbf{Q})|$ and this order divides the numerator of $\frac{N-1}{12}$. Thus if q does not divide the numerator of $\frac{N-1}{12}$, then from (1.2), q^2 divides the conjectured value of $|Ш(A_f)|$. This proves Theorem 1.4.

Acknowledgments

This paper owes its existence to Loic Merel. He pointed out to us that Gross' formula [Gro87] should have some implications for the squareness of the order of the Shafarevich-Tate group, and also indicated the relevance of [Reb06]. The author's task was to work out the details and see what precise implications could be drawn. We would like to thank Loic Merel for suggesting this project as well as for several discussions regarding it. We are also grateful to J. Brown, K. Ono, and K. Prasanna for some discussion regarding nonvanishing of twisted L-values modulo primes.

References

[Aga07] A. Agashe, *A visible factor of the special L-value*, submitted (2007), available at
`http://www.math.fsu.edu/~agashe/math.html`.

[AS05] Amod Agashe and William Stein, *Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero*, Math. Comp. **74** (2005), no. 249, 455–484 (electronic), With an appendix by J. Cremona and B. Mazur.

[BO03] Jan H. Bruinier and Ken Ono, *Coefficients of half-integral weight modular forms*, J. Number Theory **99** (2003), no. 1, 164–179.

[Bru99] Jan Hendrik Bruinier, *Nonvanishing modulo l of Fourier coefficients of half-integral weight modular forms*, Duke Math. J. **98** (1999), no. 3, 595–611.

[Che04] Jy-Ying Janet Chen, *The Tate-Shafarevich group in families of elliptic curves*, Senior honors thesis, Stanford university (2004), available at
`http://math.stanford.edu/theses/jchen-thesis.pdf`.

[DSW03] N. Dummigan, W. Stein, and M. Watkins, *Constructing elements in Shafarevich-Tate groups of modular motives*, Number theory and algebraic geometry, London Math. Soc. Lecture Note Ser., vol. 303, Cambridge Univ. Press, Cambridge, 2003, pp. 91–118.

[Eme02] Matthew Emerton, *Supersingular elliptic curves, theta series and weight two modular forms*, J. Amer. Math. Soc. **15** (2002), no. 3, 671–714 (electronic).

[Eme03] ———, *Optimal quotients of modular Jacobians*, Math. Ann. **327** (2003), no. 3, 429–458.

[Gro87] Benedict H. Gross, *Heights and the special values of L-series*, Number theory (Montreal, Que., 1985), CMS Conf. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 1987, pp. 115–187.

[KL89] V. A. Kolyvagin and D. Y. Logachev, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*, Algebra i Analiz **1** (1989), no. 5, 171–196.

[Koh] D. R. Kohel, *Hecke module structure of quaternions*, In K. Miyake, ed., *Class Field Theory – Its Centenary and Prospect*, The Advanced Studies in Pure Mathematics Series, Math Soc. Japan, to appear.

[Koh85] Winfried Kohnen, *Fourier coefficients of modular forms of half-integral weight*, Math. Ann. **271** (1985), no. 2, 237–268.

[Lan91] S. Lang, *Number theory. III*, Springer-Verlag, Berlin, 1991, Diophantine geometry. MR 93a:11048

[Lan95] ———, *Introduction to modular forms*, Springer-Verlag, Berlin, 1995, With appendixes by D. Zagier and W. Feit, Corrected reprint of the 1976 original.

[LR97] Wenzhi Luo and Dinakar Ramakrishnan, *Determination of modular forms by twists of critical L-values*, Invent. Math. **130** (1997), no. 2, 371–398. MR 98h:11059

[Man71] J. I. Manin, *Cyclotomic fields and modular curves*, Russian Math. Surveys **26** (1971), no. 6, 7–78.

[Man72] ———, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66.

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978).

[Maz78] ———, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[OS98] K. Ono and C. Skinner, *Fourier coefficients of half-integral weight modular forms* *modulo l*, Ann. of Math. (2) **147** (1998), no. 2, 453–470.

[Pra08] K. Prasanna, *On p-adic properties of central values of quadratic twists of an elliptic curve*, preprint (2008).

[Reb06] Marusia Rebolledo, *Module supersingulier et homologie des courbes modulaires*, J. Number Theory **121** (2006), no. 2, 234–264.

[Vat99] V. Vatsal, *Canonical periods and congruence formulae*, Duke Math. J. **98** (1999), no. 2, 397–419.

[Zha01] Shou-Wu Zhang, *Gross-Zagier formula for* GL_2, Asian J. Math. **5** (2001), no. 2, 183–290. MR 2003k:11101