A visible factor of the special L-value

Amod Agashe[*]

October 1, 2008

Abstract

Let A be a quotient of $J_0(N)$ associated to a newform f such that the special L-value of A (at $s = 1$) is non-zero. We give a formula for the ratio of the special L-value to the real period of A that expresses this ratio as a rational number. We extract an integer factor from the numerator of this formula; this factor is non-trivial in general and is related to certain congruences of f with eigenforms of positive analytic rank. We use the techniques of visibility to show that, under certain hypotheses (which includes the first part of the Birch and Swinnerton-Dyer conjecture on rank), if an odd prime q divides this factor, then q divides either the order of the Shafarevich-Tate group or the order of a component group of A. Suppose p is an odd prime such that p^2 does not divide N, p does not divide the order of the rational torsion subgroup of A, and f is congruent modulo a prime ideal over p to an eigenform whose associated abelian variety has positive Mordell-Weil rank. Then we show that p divides the factor mentioned above; in particular, p divides the numerator of the ratio of the special L-value to the real period of A. Both of these results are as implied by the second part of the Birch and Swinnerton-Dyer conjecture, and thus provide theoretical evidence towards the conjecture.

1   Introduction

Mazur introduced the notion of visibility in order to better understand geometrically the elements of the Shafarevich-Tate group of an abelian variety. The corresponding theory, which we call the theory of visibility, has been used to show the existence of non-trivial elements of the Shafarevich-Tate group of abelian varieties and motives (e.g., see [CM00], [AS02], [DSW03]).

The second part of the Birch and Swinnerton-Dyer conjecture gives a formula for the order of the Shafarevich-Tate group, and one might wonder how much of this conjectural order can be explained by the theory of visibility, as well as whether, when the theory of visibility implies that the Shafarevich-Tate group is non-trivial, the Birch and Swinnerton-Dyer conjectural order of the Shafarevich-Tate group is non-trivial as well. While this issue has been investigated computationally (e.g., see [CM00], [AS05]), to our knowledge there have been no general theoretical results that directly link visibility to the Birch and Swinnerton-Dyer conjecture.

In this paper, for abelian subvarieties of $J_0(N)$ associated to newforms and having analytic rank zero, we take the first step in theoretically linking visibility to the second part of the Birch and Swinnerton-Dyer conjecture. Firstly, when the newform associated to such an abelian variety is congruent to an eigenform whose associated abelian variety has positive Mordell-Weil rank, the theory of visibility shows that the actual Shafarevich-Tate group of such an abelian variety is non-trivial (subject to some other minor hypotheses). We prove that in this situation, under some additional hypotheses, the Birch and Swinnerton-Dyer conjectural order of the Shafarevich-Tate group is non-trivial as well. Secondly, following an idea of L. Merel, we extract an integer factor from the Birch and Swinnerton-Dyer conjectural formula for the order of the Shafarevich-Tate group. This factor is a variant of the notion of the modular degree and is divisible by certain congruence primes associated to the newform. We show, using the theory of visibility, that if an odd prime divides this factor, then it also divides the actual order of the Shafarevich-Tate group under certain assumptions (the strongest assumption being the first part of the Birch and Swinnerton-Dyer formula on ranks of Mordell-Weil groups). We now describe our results more precisely.

Let N be a positive integer. Let $X_0(N)$ denote the modular curve over $\mathbf{Q}$ associated to $\Gamma_0(N)$, and let $J_0(N)$ be its Jacobian, which is an abelian variety over $\mathbf{Q}$. Let f be a newform of weight 2 on $\Gamma_0(N)$. We will denote by $L(f,s)$ the L-function associated to f. 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 $p \mid N$). Let $I_f = \mathrm{Ann}_{\mathbf{T}} f$. Let A_f denote the quotient abelian variety $J_0(N)/I_f J_0(N)$ over $\mathbf{Q}$, which was introduced by Shimura in [Shi73]. If f has integer Fourier coefficients, then A_f is just an elliptic curve, and the reader may assume this for simplicity; in any casse, in the proof of our main results, the dimension of A_f does not play a major role. Let $L_{A_f}(s)$ denote the L-function associated to A_f.

The order of vanishing of $L_{A_f}(s)$ at $s = 1$ is called the *analytic rank* of A_f, and the order of vanishing of $L(f,s)$ at $s = 1$ is called the *analytic rank*

of f. The rank of the finitely generated abelian group $A_f(\mathbf{Q})$ is called the *Mordell-Weil rank* of A_f. The first part of the Birch and Swinnerton-Dyer conjecture is the following:

Conjecture 1.1 (Birch and Swinnerton-Dyer). *The analytic rank of A_f is equal to its Mordell-Weil rank.*

Now suppose that $L_{A_f}(1) \neq 0$. Then by [KL89], A_f has Mordell-Weil rank zero, and the Shafarevich-Tate group $\text{Ш}(A_f)$ of A_f is finite. Let $\mathcal{A}$ denote the Néron model of A_f over $\mathbf{Z}$ and let $\mathcal{A}^0$ denote the largest open subgroup scheme of $\mathcal{A}$ in which all the fibers are connected. Let $d = \dim A_f$, and let D be a generator of the d-th exterior power of the group of invariant differentials on $\mathcal{A}$. Let Ω_{A_f} denote the volume of $A_f(\mathbf{R})$ with respect to the measure given by D. If p is a prime number, then the group of $\mathbf{F}_p$-valued points of the quotient $\mathcal{A}_{\mathbf{F}_p}/\mathcal{A}^0_{\mathbf{F}_p}$ is called the (arithmetic) component group of A and its order is denoted $c_p(A)$. If A is an abelian variety, then we denote by $A^\vee$ the dual abelian variety of A. Throughout this article, we use the symbol $\stackrel{?}{=}$ to denote a conjectural equality.

Considering that $L_{A_f}(1) \neq 0$, the second part of the Birch and Swinnerton-Dyer conjecture says the following:

Conjecture 1.2 (Birch and Swinnerton-Dyer).

$$\frac{L_{A_f}(1)}{\Omega_{A_f}} \stackrel{?}{=} \frac{|\text{Ш}(A_f)| \cdot \prod_{p|N} c_p(A_f)}{|A_f(\mathbf{Q})| \cdot |A_f^\vee(\mathbf{Q})|}. \tag{1}$$

It is known that $L_{A_f}(1)/\Omega_{A_f}$ is a rational number (this also follows from Theorem 2.1 below) and we call this number the algebraic part of the special L-value of A_f. The importance of the second part of the Birch and Swinnerton-Dyer conjecture is that it gives a conjectural value of $|\text{Ш}(A_f)|$ in terms of the other quantities in (1) (which can often be computed). Let us denote this conjectural value of $|\text{Ш}(A_f)|$ by $|\text{Ш}(A_f)|_{\text{an}}$ (where "an" stands for "analytic"). The theory of Euler systems has been used to bound $|\text{Ш}(A_f)|$ from above in terms $|\text{Ш}(A_f)|_{\text{an}}$ as in the work of Kolyvagin and of Kato (e.g., see [Rub98, Thm 8.6]). Also, the Eisenstein series method is being used by Skinner-Urban (as yet unpublished) to try to show that $|\text{Ш}(A_f)|_{\text{an}}$ divides $|\text{Ш}(A_f)|$. In both of the methods above, one may have to stay away from certain primes.

In order to explain our results, for the sake of simplicity, we assume for the moment that N is prime. Suppose q is a prime such that f is congruent modulo a prime ideal over q to a newform $g \in S_2(\Gamma_0(N), \mathbf{C})$ such that A_g

has positive Mordell-Weil rank. Then the theory of visibility often implies the existence of non-trivial elements of $\mathrm{III}(A_f)$ of order q (for example, this happens if $q \nmid N(N-1)$ – see the proof of Theorem 6.1 below; this kind of result is well known). Now if the second part of the Birch and Swinnerton-Dyer conjecture is true, then q should also divide $|\mathrm{III}(A_f)|_{\mathrm{an}}$. We show that this is indeed the case:

Theorem 1.3. *Recall that we are assuming that N is prime. Suppose q is an odd prime such that f is congruent modulo a prime ideal over q to a newform $g \in S_2(\Gamma_0(N), \mathbf{C})$ such that A_g has positive Mordell-Weil rank. Then q divides $|\mathrm{III}(A_f)|_{\mathrm{an}}$.*

The theorem follows from Corollary 5.5 below. Thus, in certain situations, when the theory of visibility implies that $|\mathrm{III}(A_f)|$ is non-trivial, we show that $|\mathrm{III}(A_f)|_{\mathrm{an}}$ is non-trivial as well, which provides theoretical evidence towards the second part of the Birch and Swinnerton-Dyer conjecture based on the theory of visibility.

Our other contribution towards the second part of the Birch and Swinnerton-Dyer conjecture is that we extract a factor of $|\mathrm{III}(A_f)|_{\mathrm{an}}$ that can be related to $|\mathrm{III}(A_f)|$, as we now explain. Let $H = H_1(J_0(N), \mathbf{Z})$ and let π_* denote the map $H_1(J_0(N), \mathbf{Q}) \to H_1(A_f, \mathbf{Q})$ induced by the quotient map $\pi : J_0(N) \to A_f$. Let K denote the kernel of π_* restricted to H. Let $e \in H_1(J_0(N), \mathbf{Q})$ denote the winding element (whose definition is recalled below in Section 2) and let I_e denote the annihilator of e under the action of $\mathbf{T}$. Let $\Im$ denote the annihilator, under the action of $\mathbf{T}$, of the divisor $(0) - (\infty)$, considered as an element of $J_0(N)(\mathbf{C})$. There is a complex conjugation involution acting on H, and if G is a group on which it induces an involution, then by G^+ we mean the subgroup of elements of G fixed by the involution. By Lemma 3.1 below, $\Im e \subseteq H[I_e]^+$. We show (see the discussion preceding formula (14) at the end of Section 3):

$$|\mathrm{III}(A_f)|_{\mathrm{an}} = \left| \frac{H^+}{H[I_e]^+ + K^+} \right| \cdot \left| \frac{H[I_e]^+}{\Im e + H[I_e]^+ \cap K^+} \right|. \tag{2}$$

Our long term goal is to show that $|\mathrm{III}(A_f)|_{\mathrm{an}}$ divides $|\mathrm{III}(A_f)|$. We have the following partial result towards this:

Theorem 1.4. *Recall that we are assuming that N is prime.*
(i) An odd prime q divides $\left| \frac{H^+}{H[I_e]^+ + K^+} \right|$ if and only if there is a normalized eigenform $g \in S_2(\Gamma_0(N), \mathbf{C})$ such that $L(g, 1) = 0$ and f is congruent to g modulo a prime ideal lying over q in the ring of integers of the number field

4

generated by the Fourier coefficients of f and g.

(ii) Assume that the first part of the Birch and Swinnerton-Dyer conjecture holds for all newform quotients of $J_0(N)$ of positive analytic rank. Let q be a prime such that $q \nmid N(N-1)$. If q divides the factor $|\frac{H^+}{H[I_e]^+ + K^+}|$ of $|\text{III}(A_f)|_{\text{an}}$, then q^2 divides $|\text{III}(A_f)|$.

Part (i) of the theorem follows from Corollary 5.6 below. Note that this part shows that the factor $|\frac{H^+}{H[I_e]^+ + K^+}|$ is non-trivial in general (cf. Remark 6.8). Part (ii) follows from part (i) using the theory of visibility (see Theorem 6.1 below). Thus one may say that we relate a piece of $|\text{III}(A_f)|_{\text{an}}$ to $|\text{III}(A_f)|$ using the theory of visibility. Apart from providing additional theoretical evidence towards the second part of the Birch and Swinnerton-Dyer conjecture, part (ii) of the theorem also shows some consistency between the the implications of the two parts of the Birch and Swinnerton-Dyer conjecture. Also, we remark that part (i) of the theorem proves Theorem 1.3 above, in view of the comments preceding Theorem 1.3 and the fact that if A_g has positive Mordell-Weil rank, then it has positive analytic rank by [KL89] (note that the proof of Theorem 1.4 does not use Theorem 1.3).

We also have results similar to the ones above when N is not assumed to be prime, as we will explain soon. Before doing that, we pause to comment on how our result fits into a potential approach towards proving the second part of the Birch and Swinnerton-Dyer conjecture. The Euler system method gives results of the type that $|\text{III}(A_f)|$ divides $|\text{III}(A_f)|_{\text{an}}$ (at present under certain hypotheses, and staying away from certain primes). In view of this, what one would like to show the reverse divisibility, i.e., that $|\text{III}(A_f)|_{\text{an}}$ divides $|\text{III}(A_f)|$. The Eisenstein ideal method of Skinner-Urban works in this direction, as does the theory of visibility. Our Theorem 1.4 may be seen as a first step in the approach using visibility to try to show that $|\text{III}(A_f)|_{\text{an}}$ divides $|\text{III}(A_f)|$. We hope to show in future work (using ideas similar to those in [Aga08]) that the entire factor $|\frac{H^+}{H[I_e]^+ + K^+}|$ of $|\text{III}(A_f)|_{\text{an}}$ divides $|\text{III}(A_f)|$, perhaps staying away from certain primes, and under certain hypotheses, including the first part of the Birch and Swinnerton-Dyer conjecture. One major hurdle that remains is to relate the other factor $|\frac{H[I_e]^+}{\Im e + H[I_e]^+ \cap K^+}|$ in (2) to $|\text{III}(A_f)|$. It is our hope that this factor can be explained by "visibility at higher level" (see Remark 6.10(3) below).

We now drop the assumption that N is prime, and describe more general results as well as discuss the organization of the paper, which in turn will

also indicate the steps in the proofs of our main results. In Section 2, we give a formula that expresses the left hand side $L_{A_f}(1)/\Omega_{A_f}$ of the Birch and Swinnerton-Dyer conjectural formula (1) as a rational number. Using this formula, in Section 3, we show (Theorem 3.2 below) that

$$\frac{L_{A_f}(1)}{\Omega_{A_f}} = \frac{|\frac{H^+}{H[I_e]^+ + K^+}| \cdot |\frac{H[I_e]^+}{\Im e + H[I_e]^+ \cap K^+}|}{|\pi_*(\mathbf{T}e)/\pi_*(\Im e)|}, \tag{3}$$

up to powers of 2 and powers of primes whose squares divide N. Hence the Birch and Swinnerton-Dyer conjectural formula (1) becomes:

$$\frac{|\frac{H^+}{H[I_e]^+ + K^+}| \cdot |\frac{H[I_e]^+}{\Im e + H[I_e]^+ \cap K^+}|}{|\pi_*(\mathbf{T}e)/\pi_*(\Im e)|} \stackrel{?}{=} \frac{|\text{Ш}(A_f)| \cdot \prod_{p|N} c_p(A_f)}{|A_f(\mathbf{Q})| \cdot |A_f^\vee(\mathbf{Q})|}, \tag{4}$$

up to powers of 2 and powers of primes whose squares divide N. By Lemma 3.3 below, $|\pi_*(\mathbf{T}e)/\pi_*(\Im e)|$ divides $|A_f(\mathbf{Q})|$. In particular, the second part of the Birch and Swinnerton-Dyer conjecture implies that the first factor $|\frac{H^+}{H[I_e]^+ + K^+}|$ in the numerator of the right side of formula (3), divides $|\text{Ш}(A_f)| \cdot \prod_{p|N} c_p(A_f)$, up to powers of 2 and powers of primes whose squares divide N. Our goal is to prove results towards this implication.

In Section 4, we relate the factor $|\frac{H^+}{H[I_e]^+ + K^+}|$ to the order of the intersection of certain abelian variety subquotients of $J_0(N)$. Then in Section 5, we relate the order of this intersection to certain congruences of f with eigenforms of positive analytic rank. In particular, we show that if q is an odd prime such that $q^2 \nmid N$, then q divides $|\frac{H^+}{H[I_e]^+ + K^+}|$ if and only if there is a normalized eigenform $g \in S_2(\Gamma_0(N), \mathbf{C})$ such that $L(g, 1) = 0$ and f is congruent to g modulo a prime ideal lying over q in the ring of integers of the number field generated by the Fourier coefficients of f and g (see Corollary 5.6 below). Thus we obtain the following byproduct (for details, see Proposition 5.4 and its proof):

Proposition 1.5. *Let q be an odd prime such that $q^2 \nmid N$ and q does not divide $|A_f(\mathbf{Q})_{\text{tor}}|$. Suppose that there is a normalized eigenform $g \in S_2(\Gamma_0(N), \mathbf{C})$ such that $L(g, 1) = 0$ and g is congruent to f modulo a prime ideal over q in the ring of integers of the number field generated by the Fourier coefficients of f and g. Then q divides $\frac{L_{A_f}(1)}{\Omega_{A_f}}$, and in particular, $\frac{L_{A_f}(1)}{\Omega_{A_f}} \equiv \frac{L_{A_g}(1)}{\Omega_{A_g}} \bmod q$.*

A result similar to the one above is proved in [DSW03] using ideas from [Vat99] (our proof is different). These results fall under the general

philosophy that congruences between eigenforms should lead to congruences between algebraic parts the special L-values (e.g., see [Vat99], and the references therein for more instances).

In Section 6, we use the theory of visibility to relate congruences as in Proposition 1.5 to the product of the order of the Shafarevich-Tate group and the orders of the component groups of A_f, as we now explain. Suppose q and g are as in Proposition 1.5. Assume the first part of the Birch and Swinnerton-Dyer conjecture for all newform quotients; then the rank of $A_g(\mathbf{Q})$ is positive (considering that $L(g,1) = 0$). In this situation, a "visibility theorem" of [DSW03] shows that under certain other technical hypotheses, the congruence prime q divides $|\text{Ш}(A_f)| \cdot \prod_{p|N} c_p(A_f)$. The precise result we obtain is as follows (see Theorem 6.7):

Theorem 1.6. *Let q be a prime such that q divides $|\frac{H^+}{H[I_e]^+ + K^+}|$.*
Suppose that $q \nmid 2N$, and for all maximal ideals $\mathfrak{q}$ of $\mathbf{T}$ with residue characteristic q, $A_f[\mathfrak{q}]$ is irreducible. Assume that for all newforms g of level dividing N, if $L(g,1) = 0$, then the rank of $A_g(\mathbf{Q})$ is positive (this would hold if the first part of the Birch and Swinnerton-Dyer conjecture is true). Suppose that for all primes $p \mid N$, $p \not\equiv -w_p \pmod q$, where w_p is the sign of the Atkin-Lehner involution acting on f, and $p \not\equiv -1 \pmod q$ if $p^2 \mid N$. Suppose either that f is not congruent modulo a prime ideal over q to a newform of lower level (for Fourier coefficients of index coprime to Nq), or that there is a prime p dividing N and a maximal ideal $\mathfrak{q}$ of $\mathbf{T}$ with residue characteristic q such that f is congruent modulo $\mathfrak{q}$ to a newform h of level dividing N/p (for Fourier coefficients of index coprime to Nq), with $p^2 \nmid N$, $w_p = -1$, and $A_h[\mathfrak{q}]$ irreducible.
Then q divides $|\text{Ш}(A_f)| \cdot \prod_{p|N} c_p(A_f)$.

Thus, under certain hypotheses, we show that if a prime divides $|\frac{H^+}{H[I_e]^+ + K^+}|$, then it divides $|\text{Ш}(A_f)| \cdot \prod_{p|N} c_p(A_f)$, which, as mentioned earlier, is as implied by the second part of the Birch and Swinnerton-Dyer conjecture. Also, in some sense, one may say that our approach uses visibility to link the first part of the Birch and Swinnerton-Dyer conjecture to the second.

Note that if N is not prime, then the arithmetic component groups intervene in trying to explain the Shafarevich-Tate group using the theory of visibility. In fact, in Example 6.9 below, a prime divides the factor $|\frac{H^+}{H[I_e]^+ + K^+}|$, but does not divide the Birch and Swinnerton-Dyer conjectural order of $\text{Ш}(A_f)$, and instead divides $\prod_{p|N} c_p(A_f)$. As opposed to some of the other approaches to the second part of the Birch and Swinnerton-Dyer conjecture, our approach gives information about $\prod_{p|N} c_p(A_f)$ vis-a-vis the

7

conjecture. In fact, our result seems to indicate that instead of considering the quantities $|\text{Ш}(A_f)|$ and $\prod_{p|N} c_p(A_f)$ separately, one should consider the product $|\text{Ш}(A_f)| \cdot \prod_{p|N} c_p(A_f)$ in approaches towards the second part of the Birch and Swinnerton-Dyer conjecture (at least in the approaches that use the theory of visibility).

We would also like to mention some of our speculations on how to understand the second part of the Birch and Swinnerton-Dyer conjecture based on our formula (3) for $L_{A_f}(1)/\Omega_{A_f}$ even when the level N is not prime. Let C_f denote the subgroup of $A_f(\mathbf{Q})$ generated by the image of $\pi((0)-(\infty))$. By Lemma 3.3, $\pi_*(\mathbf{T}e)/\pi_*(\Im e) = C_f$, and so $|\pi_*(\mathbf{T}e)/\pi_*(\Im e)| = |C_f|$. For simplicity, assume that N is square free and that A_f is an elliptic curve. Then, by (4) and the discussion above, away from the prime 2, the second part of the Birch and Swinnerton-Dyer conjecture becomes:

$$\Big| \frac{H^+}{H[I_e]^+ + K^+} \Big| \cdot \Big| \frac{H[I_e]^+}{\Im e + H[I_e]^+ \cap K^+} \Big| \cdot \Big| \frac{A_f(\mathbf{Q})}{C_f} \Big| \cdot |A_f(\mathbf{Q})|$$
$$\overset{?}{=} |\text{Ш}(A_f)| \cdot \prod_{p|N} c_p(A_f) \ . \tag{5}$$

One would like to understand how the various quantities on the left are related to the quantities on the right. Based on some numerical data and theoretical results, we suspect that the product $\big(|(A_f(\mathbf{Q})/C_f)| \cdot |A_f(\mathbf{Q})| \big)$ divides $\prod_{p|N} c_p(A_f)$ (cf. [Aga07]). For example, when N is prime, then by [Eme03],
$$|C_f| = c_N(A_f) = |A_f(\mathbf{Q})|,$$
and so the two quantities $\big(|(A_f(\mathbf{Q})/C_f)| \cdot |A_f(\mathbf{Q})| \big)$ and $\prod_{p|N} c_p(A_f)$ are actually equal. If N is not prime, then we do not expect equality (e.g., see Example 6.9 below), but we expect that the ratio of $\prod_{p|N} c_p(A_f)$ to $\big(|(A_f(\mathbf{Q})/C_f)| \cdot |A_f(\mathbf{Q})| \big)$ is explained by congruences of f with newforms of lower level having positive analytic rank (cf. Proposition 6.3 and Remark 6.4 below). Thus we suspect that the product $|(A_f(\mathbf{Q})/C_f)| \cdot |A_f(\mathbf{Q})|$ on the left side of (5) contributes to part of $\prod_{p|N} c_p(A_f)$ in the product $|\text{Ш}(A_f)| \cdot \prod_{p|N} c_p(A_f)$ on the right side of (5), and the rest of the product $|\text{Ш}(A_f)| \cdot \prod_{p|N} c_p(A_f)$ is explained by the product $|\frac{H^+}{H[I_e]^+ + K^+}| \cdot |\frac{H[I_e]^+}{\Im e + H[I_e]^+ \cap K^+}|$ on the left side of (5), via congruences of f with eigenforms of positive analytic rank, possibly of some higher level (cf. Remark 6.10(3) below).

While the picture above is largely speculative at this stage and may need some extra conditions for it to be true (e.g., one may have to stay away

from certain primes), there are several reasons for mentioning it. Firstly, our Theorem 1.6 may be seen as a first step in proving results towards our speculations above, and shows that the theorem fits into a bigger picture (albeit speculative). Secondly, as opposed to other approaches to the second part of the Birch and Swinnerton-Dyer conjecture, our approach predicts more explicitly how non-trivial elements in the various quantities on the right side of the second part of the Birch and Swinnerton-Dyer conjectural formula (1) "arise". We hope that this may lead to a better understanding of the conjecture, even if it were proven by some other means. Lastly, we hope that the broader speculative picture above may help motivate computations or theoretical results regarding parts of it.

We end our paper with an appendix in Section 7, where we prove that for a prime p, the prime-to-p parts of the component group at p used in the Birch and Swinnerton-Dyer conjecture and the component group at p used in the formulation of the Bloch-Kato conjecture are equal. While the result is well known, to our knowledge, it has not been proven as such in the literature.

We remark that throughout this article, the notation introduced in one section is carried over to the next.

2 A formula for the ratio of special L-value to real volume for newform quotients

The goal of this section is to give a formula (formula (6) below) that expresses $L_{A_f}(1)/\Omega_{A_f}$, the left hand side of (1), as a rational number.

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 (see [Lan95, § IV.1]). 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 $\mathbf{T}e \subseteq H_1(X_0(N), \mathbf{Z})^+ \otimes \mathbf{Q}$. If the torsion-free group $\pi_*(\mathbf{T}e)$ has rank equal to d (= dim A_f), then let $[H_1(A_f, \mathbf{Z})^+ : \pi_*(\mathbf{T}e)]$ denote the absolute value of the determinant of an automorphism of $H_1(A_f, \mathbf{Q})$ that takes the lattice $H_1(A_f, \mathbf{Z})^+$ isomorphically onto the lattice $\pi_*(\mathbf{T}e)$; otherwise, define $[H_1(A_f, \mathbf{Z})^+ : \pi_*(\mathbf{T}e)]$ to be zero.

Let $g_1, \ldots, g_d$ be a $\mathbf{Z}$-basis of $S_2(\Gamma_0(N), \mathbf{Z})[I_f]$, and for $j = 1, \ldots, d$, consider $\omega_j = 2\pi i g_j(z) dz$ as differentials in $H^0(A_f, \Omega_{A_f/\mathbf{Q}})$. There exists $c \in \mathbf{Q}^*$ such that $D = c \cdot \wedge_j \omega_j$. As in [ARS06], we call the absolute value of c the Manin constant of A_f, and denote it by c_{A_f}. Let $c_\infty(A)$ denote the number of connected components of $A(\mathbf{R})$.

The following theorem is similar to Theorem 4.5 in [AS05] and the key idea behind the proof goes back to [Aga99].

Theorem 2.1.

$$\frac{L_{A_f}(1)}{\Omega_{A_f}} = \frac{[H_1(A_f, \mathbf{Z})^+ : \pi_*(\mathbf{T}e)]}{c_{A_f} \cdot c_\infty(A_f)}. \tag{6}$$

The rest of this section is devoted to proving the theorem above, and apart from Lemma 2.2, none of the discussion in the rest of this section will be used later.

We start by giving some lemmas that will be used in the proof of the theorem. Let $S_f = S_2(\Gamma_0(N), \mathbf{Z})[I_f]$. There is a perfect pairing

$$\mathbf{T} \times S_2(\Gamma_0(N), \mathbf{Z}) \to \mathbf{Z} \tag{7}$$

which associates to (T, f) the first Fourier coefficient $a_1(f\,|\,T)$ of the modular form $f\,|\,T$ (see [Rib83, (2.2)]); this induces a pairing

$$\psi : \mathbf{T}/I_f \times S_f \to \mathbf{Z}.$$

Lemma 2.2. *The pairing ψ above is a perfect pairing.*

Proof. Both $\mathbf{T}/I_f$ and S_f are free $\mathbf{Z}$-modules of the same rank. So it suffices to prove that the induced maps $S_f \to \mathrm{Hom}(\mathbf{T}/I_f, \mathbf{Z})$ and $\mathbf{T}/I_f \to \mathrm{Hom}(S_f, \mathbf{Z})$ are injective. The injectivity of the first map follows from the perfectness of the pairing (7). Suppose the image of $T \in \mathbf{T}$ in $\mathbf{T}/I_f$ maps to the trivial element of $\mathrm{Hom}(S_f, \mathbf{Z})$. Then $a_1(f \,|\, T) = 0$. But f is an eigenform for T; suppose the eigenvalue is λ. Then $0 = a_1(f \mid T) = \lambda a_1(f) = \lambda$. Thus $f \,|\, T = 0$, i.e., $T \in I_f$. Thus the map $\mathbf{T}/I_f \to \mathrm{Hom}(S_f, \mathbf{Z})$ is injective and we are done. $\qquad\square$

Lemma 2.3. *The map $\mathbf{T} \to \mathbf{T}e$ given by $t \mapsto te$ induces an isomorphism $\mathbf{T}/I_f \xrightarrow{\cong} \mathbf{T}e/I_f e$.*

Proof. It is clear that the map $\mathbf{T} \to \mathbf{T}e/I_f e$ given by $t \mapsto te$ is surjective. All we have to show is that the kernel of this map is I_f. It is clear that the kernel contains I_f. Conversely, if t is in the kernel, then $te \in I_f e$; let $i \in I_f$ be such that $te = ie$. Then $(t-i)e = 0$, and thus $\int_{(t-i)e} \omega_f = 0$, i.e., $\int_e \omega_{(t-i)f} = 0$. If the eigenvalue of f under $(t-i)$ is λ, then this means $\lambda \cdot L(f,1) = 0$, i.e., $\lambda = 0$. Thus $(t-i) \in I_f$, i.e., $t \in I_f$. $\qquad\square$

We have a pairing

$$H_1(X_0(N), \mathbf{Z}) \otimes \mathbf{C} \times S_2(\Gamma_0(N), \mathbf{C}) \to \mathbf{C} \tag{8}$$

given by $(\gamma, f) \mapsto \langle \gamma, f \rangle = \int_\gamma \omega_f$ and extended $\mathbf{C}$-linearly. At various points below in this section, we will consider pairings between two $\mathbf{Z}$-modules; unless otherwise stated, each such pairing is obtained in a natural way from (8). 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.

Lemma 2.4. $\Omega_{A_f} = c_{A_f} \cdot c_\infty(A_f) \cdot \mathrm{disc}(H_1(A_f, \mathbf{Z})^+ \times S_f \to \mathbf{C})$.

Proof. Let $A(\mathbf{R})^0$ denote the component of $A(\mathbf{R})$ containing the identity. Then

$$\begin{aligned}
\Omega_{A_f} &= \int_{A(\mathbf{R})} D = c_\infty(A_f) \cdot \int_{A(\mathbf{R})^0} D = c_\infty(A_f) \cdot c_{A_f} \cdot \int_{A(\mathbf{R})^0} \wedge_j \omega_j \\
&= c_\infty(A_f) \cdot c_{A_f} \cdot \mathrm{disc}(H_1(A(\mathbf{R})^0, \mathbf{Z}) \times S_f \to \mathbf{C}) \\
&= c_\infty(A_f) \cdot c_{A_f} \cdot \mathrm{disc}(H_1(A_f, \mathbf{Z})^+ \times S_f \to \mathbf{C}),
\end{aligned}$$

11

where the last equality follows from the canonical isomorphism $H_1(A(\mathbf{R})^0, \mathbf{Z}) \cong H_1(A_f, \mathbf{Z})^+$ (see, e.g., [AS05, Lemma 4.4]; note that several of the $A(\mathbf{R})$'s in Section 4.2 of [AS05] should really be $A(\mathbf{R})^0$'s). $\qquad\square$

Proof of Theorem 2.1. Let $\{f_i\}$, for $i = 1, 2, \ldots d$, denote the set of Galois conjugates of f. By [Shi94, Thm. 7.14] and [Car86], $L_{A_f}(s) = \prod_i L(f_i, s) = \prod_i \langle e, f_i \rangle$. Hence, using Lemma 2.4,

$$
\begin{aligned}
c_{A_f} \cdot c_\infty(A_f) \cdot \frac{L_{A_f}(1)}{\Omega_{A_f}} &= \frac{\prod_i \langle e, f_i \rangle}{\mathrm{disc}(H_1(A_f, \mathbf{Z})^+ \times S_f \to \mathbf{C})} \\
&= \frac{\prod_i \langle e, f_i \rangle}{\mathrm{disc}(\mathbf{T}e/I_f e \times S_f \to \mathbf{C})} \cdot \left[H_1(A_f, \mathbf{Z})^+ : \pi_*(\mathbf{T}e) \right].
\end{aligned}
$$

To prove the theorem, it suffices to prove that

$$
\frac{\prod_i \langle e, f_i \rangle}{\mathrm{disc}(\mathbf{T}e/I_f e \times S_f \to \mathbf{C})} = 1. \tag{9}
$$

In what follows, $i, j, k,$ and ℓ are indices running from 1 to d. Let $\{g_k\}$ be a $\mathbf{Z}$-basis of S_f and let $\{t_j\}$ be the corresponding dual basis of $\mathbf{T}/I_f$ under the perfect pairing ψ in Lemma 2.2 above. Then by Lemma 2.3, $\{t_j e\}$ is a basis for $\mathbf{T}e/I_f e$. Now $g_k = \sum_k a_{ki} f_i$ for some $\{a_{ki} \in \mathbf{C}\}$. Let A be the matrix having (k, i)-th entry a_{ki}, and let $(a^{-1})_{i\ell}$ denote the (i, ℓ)-th element of the inverse of A. Then

$\mathrm{disc}(\mathbf{T}e/I_f e \times S_f \to \mathbf{C})$
$= \det\{\langle t_j e, g_k \rangle\} = \det\{\langle e, g_k | t_j \rangle\} = \det\{\langle e, (\sum_i a_{ki} f_i) | t_j \rangle\}$
$= \det\{\langle e, \sum_i a_{ki} a_1(f_i | t_j) f_i \rangle\}$ (since f_i's are eigenvectors)
$= \det\{\langle e, \sum_i a_{ki} \sum_\ell (a^{-1})_{i\ell} a_1(g_\ell | t_j) f_i \rangle\}$ (using $f_i = \sum_\ell (a^{-1})_{i\ell} g_\ell$)
$= \det\{\langle e, \sum_i a_{ki} (a^{-1})_{ij} f_i \rangle\}$ (using $a_1(g_\ell | t_j) = \delta_{\ell j}$)
$= \det\{\sum_i a_{ki} (a^{-1})_{ij} \langle e, f_i \rangle\} = \det\{\sum_i a_{ki} \langle e, f_i \rangle (a^{-1})_{ij}\}$
$= \det(A \Delta A^{-1})$ (where $\Delta = \mathrm{diag}(\langle e, f_i \rangle)$)
$= \det(\Delta) = \prod_i \langle e, f_i \rangle$.

This proves (9), and finishes the proof of the theorem. $\qquad\square$

3   Extracting an integer factor

The goal of this section is to rewrite the right hand side of formula (6) so that it can be better compared to the formula given by the Birch and Swinnerton-Dyer conjecture (Conjecture 1.2). We also extract the factor $|\frac{H^+}{H[I_e]^+ + K^+}|$

from $\frac{L_{A_f}(1)}{\Omega_{A_f}}$. Recall that $H = H_1(J_0(N), \mathbf{Z})$, I_e is the annihilator ideal of e, K denotes the kernel of π_* restricted to H, and $\Im$ denotes the annihilator ideal of the divisor $(0) - (\infty)$.

Lemma 3.1. $\Im e \subseteq H[I_e]^+$.

Proof. By [Maz77, II.18.6], we have $\Im e \subseteq H^+$ (note that in loc. cit., the definition of $\Im$ is different and N is assumed to be prime; but the only essential property of $\Im$ that is used in the proof is that $\Im$ annihilates the divisor $(0) - (\infty)$, and the assumption that N is prime is not used). Also, e is killed by I_e, hence so is $\Im e$, and the lemma follows. $\square$

Theorem 3.2. *Up to a power of* 2,

$$c_{A_f} \cdot c_\infty(A_f) \cdot \frac{L_{A_f}(1)}{\Omega_{A_f}} = \frac{|\frac{H^+}{H[I_e]^+ + K^+}| \cdot |\frac{H[I_e]^+}{\Im e + H[I_e]^+ \cap K^+}|}{|\pi_*(\mathbf{T}e)/\pi_*(\Im e)|}. \tag{10}$$

Proof. Since $\Im e \subseteq H^+$, and the map $\pi_* : H \to H_1(A_f, \mathbf{Z})$ is surjective (as the kernel of $J \to A_f$ is connected), from Theorem 2.1, we have

$$c_{A_f} \cdot c_\infty(A_f) \cdot \frac{L_{A_f}(1)}{\Omega_{A_f}} = [\pi_*(H)^+ : \pi_*(\mathbf{T}e)] = \frac{|\pi_*(H)^+/\pi_*(\Im e)|}{|\pi_*(\mathbf{T}e)/\pi_*(\Im e)|}. \tag{11}$$

Now $\pi_*(H) = H/K$ and up to a power of 2, $(H/K)^+ = H^+/K^+$. Also, $\pi_*(\Im e) = \Im e/(\Im e \cap K^+)$ and the kernel of the natural injective map $\Im e \to (\Im e + K^+)/K^+$ is $\Im e \cap K^+$; so $\pi_*(\Im e) = (\Im e + K^+)/K^+$. Thus up to a power of 2,

$$|\pi_*(H)^+/\pi_*(\Im e)| = \left|\frac{H^+}{K^+ + \Im e}\right|. \tag{12}$$

Now $\Im e \subseteq H[I_e]^+$, and so we have

$$\left|\frac{H^+}{K^+ + \Im e}\right| = \left|\frac{H^+}{H[I_e]^+ + K^+}\right| \cdot \left|\frac{H[I_e]^+ + K^+}{\Im e + K^+}\right|.$$

We have a map $H[I_e]^+ \to (H[I_e]^+ + K^+)/(\Im e + K^+)$ given by $h \mapsto h + (\Im e + K^+)$. It is clearly a surjection, and its kernel is precisely $\Im e + H[I_e]^+ \cap K^+$. So we have

$$\left|\frac{H^+}{K^+ + \Im e}\right| = \left|\frac{H^+}{H[I_e]^+ + K^+}\right| \cdot \left|\frac{H[I_e]^+}{\Im e + H[I_e]^+ \cap K^+}\right|.$$

Putting this in (12) and using (11), we get the theorem. $\square$

By [ARS06], if a prime p divides c_{A_f}, then $p = 2$ or $p^2 \mid N$. Also, $c_\infty(A_f)$ is a power of 2. Hence, in view of Theorem 3.2, the second part of the Birch and Swinnerton-Dyer conjecture (Conjecture 1.2) just says that up to powers of 2 and powers of primes whose squares divide N, we have

$$\frac{\left|\frac{H^+}{H[I_e]^+ + K^+}\right| \cdot \left|\frac{H[I_e]^+}{\Im e + H[I_e]^+ \cap K^+}\right|}{|\pi_*(\mathbf{T}e)/\pi_*(\Im e)|} \overset{?}{=} \frac{|\text{Ш}(A_f)| \cdot \prod_{p|N} c_p(A_f)}{|A_f(\mathbf{Q})| \cdot |A_f^\vee(\mathbf{Q})|}. \tag{13}$$

Lemma 3.3 (A-Stein). $\pi_*(\mathbf{T}e)/\pi_*(\Im e)$ *is the subgroup of* $A_f(\mathbf{Q})$ *generated by the image of* $\pi((0) - (\infty))$ *and so* $|\pi_*(\mathbf{T}e)/\pi_*(\Im e)|$ *divides* $|A_f(\mathbf{Q})|$.

Proof. The first claim follows from the proof of Prop. 4.6 of [AS05] and the second claim follows from the first by Lagrange's theorem that the order of a subgroup divides the order of the group. $\square$

Thus the second part of the Birch and Swinnerton-Dyer conjecture implies that up to powers of 2 and powers of primes whose square divides N, the factor $\left|\frac{H^+}{H[I_e]^+ + K^+}\right|$ divides $|\text{Ш}(A_f)| \cdot \prod_{p|N} c_p(A_f)$.

If N is prime, then things simplify significantly, since c_{A_f} is a power of 2 by [ARS06] and by [Eme03], we have $|\pi_*(\mathbf{T}e)/\pi_*(\Im e)| = c_N(A_f) = |A_f(\mathbf{Q})| = |A_f^\vee(\mathbf{Q})|$. Hence if N is prime, the Birch and Swinnerton-Dyer conjecture says that up to powers of 2,

$$\left|\frac{H^+}{H[I_e]^+ + K^+}\right| \cdot \left|\frac{H[I_e]^+}{\Im e + H[I_e]^+ \cap K^+}\right| \overset{?}{=} |\text{Ш}(A_f)|. \tag{14}$$

In particular, we note the following result for easy reference:

Proposition 3.4. *If* N *is prime, then the second part of the Birch and Swinnerton-Dyer conjecture implies that the odd part of* $\left|\frac{H^+}{H[I_e]^+ + K^+}\right|$ *divides* $|\text{Ш}(A_f)|$.

4 Relating the factor to an intersection

In this section, we will relate the factor $\left|\frac{H^+}{H[I_e]^+ + K^+}\right|$ to the order of the intersection of certain subquotients of J.

We first need the following lemma, which is an adaptation of [AS05, Prop. 3.2]. Suppose J is an abelian variety over $\mathbf{Q}$, and A and B are abelian subvarieties of J. Let $(A \cap B)^0$ denote the connected component of $A \cap B$ that contains the identity; it is an abelian variety over $\mathbf{Q}$. Let $(A \cap B)^c$ denote the component group of $A \cap B$, i.e., $(A \cap B)/(A \cap B)^0$. If G is a finitely generated abelian group, then we denote its torsion part by G_{tor}.

Lemma 4.1. *With notation as above, there is a natural isomorphism of groups*

$$(A \cap B)^c \cong \left(\frac{H_1(J, \mathbf{Z})}{H_1(A, \mathbf{Z}) + H_1(B, \mathbf{Z})} \right)_{\text{tor}}.$$

Proof. If E is an abelian variety over $\mathbf{Q}$, then let T_E denote the vector space $\text{Hom}_{\mathbf{C}}(H^0(E_{\mathbf{C}}, \Omega^1), \mathbf{C})$, and let H_E denote $H_1(E(\mathbf{C}), \mathbf{Z})$. There is a natural inclusion $H_E{\to}T_E$, and the complex torus $E(\mathbf{C})$ is isomorphic to T_E/H_E. There is also a natural inclusion of T_A and T_B in T_J, and we have $H_A = H_J \cap T_A$ and $H_B = H_J \cap T_B$.

The exact sequence

$$0{\to}A \cap B{\to}A \oplus B{\to}J$$

fits into the following diagram obtained from complex analytic uniformization.

$$
\begin{array}{ccccccc}
& & 0 & & 0 & & \\
& & \downarrow & & \downarrow & & \\
H_{(A\cap B)^0} & \longrightarrow & H_A \oplus H_B & \longrightarrow & H_J & \longrightarrow & H_J/(H_A + H_B) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
T_{(A\cap B)^0} & \longrightarrow & T_A \oplus T_B & \longrightarrow & T_J & \longrightarrow & T_J/(T_A + T_B) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
A \cap B & \longrightarrow & A \oplus B & \longrightarrow & J & \longrightarrow & J/(A + B) \\
& & \downarrow & & \downarrow & & \\
& & 0 & & 0 & &
\end{array}
$$

Using the snake lemma, which connects the kernel $A \cap B$ of $A \oplus B{\to}J$ to the cokernel of $H_A \oplus H_B{\to}H_J$, we obtain an exact sequence

$$0{\to}T_{(A\cap B)^0}/H_{(A\cap B)^0}{\to}A \cap B{\to}H_J/(H_A + H_B){\to}T_J/(T_A + T_B).$$

Now $T_{(A\cap B)^0}/H_{(A\cap B)^0} = (A \cap B)^0$, so the exact sequence becomes

$$0{\to}(A \cap B)^c{\to}H_J/(H_A + H_B){\to}T_J/(T_A + T_B).$$

Since $T_J/(T_A + T_B)$ is a $\mathbf{C}$-vector space, the torsion part of $H_J/(H_A + H_B)$ must map to 0. No non-torsion in $H_J/(H_A + H_B)$ could map to 0, because if it did then $(A \cap B)^c$ would not be finite. The lemma follows. $\qquad\square$

15

In this paragraph and the next, the symbol g stands for a newform of level N_g dividing N. Let S'_g denote the subspace of $S_2(\Gamma_0(N), \mathbf{C})$ spanned by the forms $g(dz)$ where d ranges over the divisors of N/N_g. If n is a positive integer, then let $\sigma_0(n)$ denote the number of divisors of n. Then S'_g has dimension $\sigma_0(N/N_g)$. Let $[g]$ denote the Galois orbit of g, and let $S_{[g]}$ denote the $\mathbf{Q}$-subspace of forms in $\oplus_{h \in [g]} S'_h$ with rational Fourier coefficients. We have $S_2(\Gamma_0(N), \mathbf{Q}) = \oplus_{[g]} S_{[g]}$, where the sum is over Galois conjugacy classes of newforms of some level dividing N.

Let B_g denote the abelian subvariety of $J_0(N_g)$ associated to g by Shimura [Shi94, Thm. 7.14], and let J_g be the sum of the images of B_g in $J = J_0(N)$ under the usual degeneracy maps. Then J_g is isogenous to $B_g^{\sigma_0(N/N_g)}$. If J' is an abelian subvariety of J that is preserved by $\operatorname{End} J$, then by $\operatorname{Ann}_{\mathbf{T} \otimes \mathbf{Q}} J'$ we mean the kernel of the image of $\mathbf{T} \otimes \mathbf{Q}$ in $\operatorname{End} J' \otimes \mathbf{Q}$. Note that $\operatorname{End} J$ preserves J_g (e.g., see [ARS07, § 3]) and $\operatorname{Ann}_{\mathbf{T} \otimes \mathbf{Q}} J_g = \operatorname{Ann}_{\mathbf{T} \otimes \mathbf{Q}} S_{[g]}$. If T is a subset of the set of Galois conjugacy classes of newforms of some level dividing N, then let $S_T = \oplus_{[g] \in T} S_{[g]}$, $I_T = \operatorname{Ann}_{\mathbf{T}} S_T$, and let J_T denote the abelian subvariety of J generated by the J_g for all $[g] \in T$. Then J_T is isogenous to $\prod_{[g] \in T} J_g$, hence is preserved by $\operatorname{End} J$ and moreover, $\operatorname{Ann}_{\mathbf{T} \otimes \mathbf{Q}} J_T = \operatorname{Ann}_{\mathbf{T} \otimes \mathbf{Q}} S_T$. Intersecting with $\mathbf{T}$, we get

Lemma 4.2. $\operatorname{Ann}_{\mathbf{T}} J_T = \operatorname{Ann}_{\mathbf{T}} S_T = I_T$.

We say that a subgroup G' of a finitely generated abelian group G is *saturated* (in G) if the quotient G/G' is torsion-free. Recall that $H = H_1(J_0(N), \mathbf{Z})$.

Lemma 4.3. $H_1(J_T, \mathbf{Z}) = H[I_T]$.

Proof. We have $H_1(J_T, \mathbf{Z}) = H \cap \operatorname{Hom}_{\mathbf{C}}(H^0(J_T(\mathbf{C}), \Omega^1), \mathbf{C})$. Hence $H_1(J_T, \mathbf{Z})$ is saturated in H and it is clear by Lemma 4.2 that $H_1(J_T, \mathbf{Z}) \subseteq H[I_T]$. So it suffices to show that the inclusion $H_1(J_T, \mathbf{Z}) \otimes \mathbf{Q} \subseteq H[I_T] \otimes \mathbf{Q}$ is an equality, for which in turn, it suffices to check that the two $\mathbf{Q}$-vector spaces have the same dimension. Now $H \otimes \mathbf{Q}$ is free of rank 2 over $\mathbf{T} \otimes \mathbf{Q}$, and thus, $\dim_{\mathbf{Q}} H[I_T] = 2 \cdot \dim_{\mathbf{Q}}(\mathbf{T}/I_T \otimes \mathbf{Q})$. We have

$\dim_{\mathbf{Q}}(H_1(J_T, \mathbf{Z}) \otimes \mathbf{Q})$
$= 2 \cdot \dim J_T = 2 \cdot \dim_{\mathbf{Q}} H^0(J_T(\mathbf{Q}), \Omega_{J_T(\mathbf{Q})/\mathbf{Q}})$
$= 2 \cdot \sum_{[g] \in T} \dim_{\mathbf{Q}} H^0(J_g(\mathbf{Q}), \Omega_{J_g(\mathbf{Q})/\mathbf{Q}}) = 2 \cdot \sum_{[g] \in T} \dim_{\mathbf{Q}} T_{[g]}$
$= 2 \cdot \dim_{\mathbf{Q}} S_T = 2 \cdot \dim_{\mathbf{Q}}(\mathbf{T}/I_T \otimes \mathbf{Q}),$

where the last equality follows since $S_2(\Gamma_0(N), \mathbf{Q})$ is free of rank one over $\mathbf{T} \otimes \mathbf{Q}$. Thus $\dim_{\mathbf{Q}} H_1(J_T, \mathbf{Z}) \otimes \mathbf{Q} = \dim_{\mathbf{Q}} H[I_T] \otimes \mathbf{Q}$, and we are done. $\square$

Let T_1, T_2, and T_3 be the sets of Galois conjugacy classes of newforms of level dividing N of analytic rank zero, of classes not in $[f]$, and of classes of newforms of analytic rank zero except those in $[f]$ respectively. Let $A = J_{T_1}$, $B = J_{T_2}$, and $C = J_{T_3}$. Also for simplicity, we will write I_A for I_{T_1}, I_B for I_{T_2}, and I_C for I_{T_3}, as well as S_A for S_{T_1}, S_B for S_{T_2}, and S_C for S_{T_3}. Note that both I_A and I_B are contained in I_C, and C is an abelian subvariety of both A and B. The differentials on A/C and B/C correspond respectively to the space generated by the conjugates of f and the space generated by eigenforms of analytic rank greater than zero.

Lemma 4.4.
$$\left| \frac{H}{H[I_e] + K} \right| = |(A/C) \cap (B/C)| ,$$

where the latter intersection is considered in J/C.

Proof. Claim 1: $H_1(A, \mathbf{Z}) = H[I_e]$.

Proof. By Lemma 4.3, it suffices to show that $I_A = I_e$. It follows from Lemma 3.10 in [Par99] that $I_e \subseteq I_A$. We next prove the reverse inclusion. Let $t \in \mathbf{T}$. By the first statement in the proof of Lemma 3.10 in [Par99], if f is a newform with analytic rank greater than zero of level M dividing N, and $g \in S'_f$, then $\langle e, g \rangle = 0$; hence $\langle te, f \rangle = \langle e, tf \rangle = 0$. If moreover $t \in I_A$, then for all newforms g of analytic rank zero, $\langle te, g \rangle = \langle e, tg \rangle = \langle e, 0 \rangle = 0$. Thus te is orthogonal to all of $S_2(\Gamma_0(N), \mathbf{C})$, and so $te = 0$, i.e., $t \in I_e$, which shows that $I_A \subseteq I_e$, and we are done. $\square$

Recall that K denotes the kernel of $\pi_* : H_1(J_0(N), \mathbf{Q}) \to H_1(A_f, \mathbf{Q})$ restricted to H.

Claim 2: $H_1(B, \mathbf{Z}) = K$.

Proof. Now B is easily seen to be the kernel of the map $J \to A_f$, and so we have a short exact sequence $0 \to B \to J \to A_f \to 0$, and part of the associated long exact sequence of homology is:

$$\ldots \to H_1(B, \mathbf{Z}) \to H_1(J, \mathbf{Z}) \stackrel{\pi_*}{\to} H_1(A_f, \mathbf{Z}) \to 0 \to \ldots$$

Hence it is clear that $H_1(B, \mathbf{Z}) \subseteq K$. Since $H_1(B, \mathbf{Z})$ is saturated in H, it suffices to show that $H_1(B, \mathbf{Z}) \otimes \mathbf{Q} = K \otimes \mathbf{Q}$, i.e., that $H_1(B, \mathbf{Z})$ and K have the same rank. If G is a free abelian group, then we denote its rank by $\mathrm{rk}(G)$. Now

$$\mathrm{rk}(K) = 2 \cdot \dim J - 2 \cdot \dim A_f = 2 \cdot \dim_{\mathbf{Q}} S_2(\Gamma_0(N), \mathbf{Q}) - 2 \cdot \dim_{\mathbf{Q}} S_{[f]}$$
$$= 2 \cdot \dim_{\mathbf{Q}} S_{T_2} = 2 \cdot \dim_{\mathbf{Q}} B = \mathrm{rk}(H_1(B, \mathbf{Z})).$$

This proves the claim. $\qquad\square$

Also, $(A \cap B)^0 = C$, and so $(A \cap B)^c = |(A/C) \cap (B/C)|$. The desired result now follows by Lemma 4.1 in view of the two claims above. $\qquad\square$

5 Relating the intersection to certain congruences

If T is a subset of the set of Galois conjugacy classes of newforms of some level dividing N, then let T' denote its complement. For simplicity, we will write $I_{A'}$ for $I_{T_1'}$, $I_{B'}$ for $I_{T_2'}$, and $I_{C'}$ for $I_{T_3'}$, as well as $S_{A'}$ for $S_{T_1'}$, $S_{B'}$ for $S_{T_2'}$, and $S_{C'}$ for $S_{T_3'}$. Note that since T_2' is the set of Galois conjugacy classes of newforms of level dividing N that are in $[f]$, we have $I_{B'} = I_f$. Let S be short for $S_2(\Gamma_0(N), \mathbf{Z})$. Recall that the exponent of a finite group G is the smallest positive integer that annihilates G.

Lemma 5.1. *The exponent of the group $(A/C) \cap (B/C)$ divides the exponent of the group $\frac{S[I_{C'}]}{S[I_{B'}] + S[I_{A'}]}$. Moreover, if ℓ is a prime such that $\ell^2 \nmid N$, then ℓ does not divide the ratio of the exponent of $\frac{S[I_{C'}]}{S[I_{B'}] + S[I_{A'}]}$ to the exponent of $(A/C) \cap (B/C)$.*

Proof. Both parts of the lemma are generalizations of results in [ARS07].

The proof of the first part is a generalization of the proof of Theorem 3.6(a) in [ARS07] which says that the modular exponent divides the congruence exponent. Note that $\mathrm{End}\, J_0(N)$ preserves A, B, and C, and hence A/C and B/C, and that the image of $\mathbf{T}$ acting on $J_0(N)/C$ is $\mathbf{T}_{C'}$ (since $\mathrm{Ann}_{\mathbf{T} \otimes \mathbf{Q}} J/C = \mathrm{Ann}_{\mathbf{T} \otimes \mathbf{Q}} S_2(\mathbf{Q})/S_C = \mathrm{Ann}_{\mathbf{T} \otimes \mathbf{Q}} S_{C'}$). We have a perfect $\mathbf{T}$-equivariant bilinear pairing $\mathbf{T} \times S \to \mathbf{Z}$ given by $(t, g) \mapsto a_1(t(g))$.

Claim: The induced pairing

$$\mathbf{T}/I_{C'} \times S[I_{C'}] \to \mathbf{Z} \qquad (15)$$

is perfect.

Proof. We follow the proof of Lemma 2.2, and the only thing that one has to show differently is that the map $\mathbf{T}/I_{C'} \to \mathrm{Hom}(S[I_{C'}], \mathbf{Z})$ is injective. Suppose the image of $T \in \mathbf{T}$ in $\mathbf{T}/I_{C'}$ is in the kernel of this map. Then if $h \in S[I_{C'}]$, we have $a_1(h \mid T) = 0$. But then $a_n(h \mid T) = a_1((h \mid T) \mid T_n) = a_1((h \mid T_n) \mid$

$T) = 0$ for all n (considering that $h|T_n \in S[I_{C'}]$), and hence $h|T = 0$ for all $h \in S[I_{C'}]$. Hence T annihilates $S[I_{C'}] = S \cap S_{C'}$, and so it annihilates $S_{C'}$. Thus $T \in I_{C'}$, which proves the injectivity. $\qed$

Using this pairing, $\mathrm{Hom}(\mathbf{T}_{C'}/\mathrm{Ann}_{\mathbf{T}_{C'}}(A/C), \mathbf{Z})$ may be viewed as a saturated subgroup of $S[I_{C'}]$. Now $\mathrm{Ann}_{\mathbf{T}_{C'} \otimes \mathbf{Q}} A/C = \mathrm{Ann}_{\mathbf{T}_{C'} \otimes \mathbf{Q}} S_A/S_C = I_f/I_{C'} \otimes \mathbf{Q} = I_{B'}/I_{C'} \otimes \mathbf{Q}$ and thus on tensoring with $\mathbf{Q}$, $\mathbf{T}_{C'}/\mathrm{Ann}_{\mathbf{T}_{C'}}(A/C)$ is dual, under the pairing (15), to $S[I_{B'}]$, which is itself saturated in $S[I_{C'}]$. Hence

$$\mathrm{Hom}(\mathbf{T}_{C'}/\mathrm{Ann}_{\mathbf{T}_{C'}}(A/C), \mathbf{Z}) = S[I_{B'}].$$

Similarly,

$$\mathrm{Hom}(\mathbf{T}_{C'}/\mathrm{Ann}_{\mathbf{T}_{C'}}(B/C), \mathbf{Z}) = S[I_{A'}].$$

Bearing all this in mind, and making the following changes in Sections 3–4 of [ARS07]: replace J by $J_0(N)/C$, A by A/C, B by B/C, $\mathbf{T}$ by $\mathbf{T}_{C'} = \mathbf{T}/I_{C'}$, the proof in loc. cit. that the modular exponent divides the congruence exponent (with the changes mentioned above) gives us the first statement in the lemma.

The proof of the second part of the lemma is a generalization of the proof of Theorem 3.6(a) in [ARS07], which says that if ℓ is a prime such that $\ell^2 \nmid N$, then ℓ does not divide the ratio of the congruence exponent to the modular exponent, as we now explain. Let $\mathbf{T}_{A/C}$ and $\mathbf{T}_{B/C}$ denote the images of $\mathbf{T}_{C'}$ acting on A/C and B/C respectively. Let $\pi_{A/C}$ and $\pi_{B/C}$ denote the maps $\mathbf{T}_{C'} \to \mathbf{T}_{A/C}$ and $\mathbf{T}_{C'} \to \mathbf{T}_{B/C}$ respectively. Let $R_{C'} = \pi_{A/C}(\ker(\pi_{B/C}))$ and let $S_{C'}$ be the annihilator in $\mathbf{T}_{A/C}$ of $(A/C) \cap (B/C)$. By a reasoning as in [ARS07, §5.1], except replacing J by $J_0(N)/C$, A by A/C, B by B/C, $\mathbf{T}$ by $\mathbf{T}_{C'}$, R by $R_{C'}$, and S by $S_{C'}$ in loc. cit., we get the following: $R_{C'} \subseteq S_{C'}$, the exponent of $\frac{S[I_{C'}]}{S[I_{B'}] + S[I_{A'}]}$ is the exponent of $\mathbf{T}_{A/C}/R_{C'}$, and multiplication by the exponent of $(A/C) \cap (B/C)$ annihilates $\mathbf{T}_{A/C}/S_{C'}$. Let $\mathbf{T}'_{C'}$ be the saturation of $\mathbf{T}_{C'}$ in $\mathrm{End}\,(J/C)$. Then in a manner similar to loc. cit. (with the changes mentioned above), we get an injection $S_{C'}/R_{C'} \hookrightarrow \mathbf{T}'_{C'}/\mathbf{T}_{C'}$ and to prove the second part of our lemma, it suffices to show that $\mathbf{T}_{C'} = \mathbf{T}'_{C'}$ locally at all maximal ideals of $\mathbf{T}_{C'}$ with residue characteristic ℓ that contain the annihilator of A/C, which is $I_f/I_{C'}$ (since $\mathrm{Ann}_{\mathbf{T} \otimes \mathbf{Q}} A/C = \mathrm{Ann}_{\mathbf{T} \otimes \mathbf{Q}} S_A/S_C = \mathrm{Ann}_{\mathbf{T} \otimes \mathbf{Q}} S_{[f]}$). Considering that $\mathbf{T}_{C'} = \mathbf{T}/I_{C'}$, it suffices to show that $\mathbf{T} = \mathbf{T}'$ for all maximal ideals of $\mathbf{T}$ with residue characteristic ℓ which contain I_f (where $\mathbf{T}'$ is the saturation of $\mathbf{T}$ in $\mathrm{End}\,J$). But this is proved in [ARS07, §5.1]. $\qed$

If g and h are eigenforms in $S_2(\Gamma_0(N), \mathbf{C})$ and $\mathfrak{q}$ is an ideal in the ring of integers of a number field that contains all the Fourier coefficients of g and h, then we will say that g is congruent to h modulo $\mathfrak{q}$ and write $g \equiv h \pmod{\mathfrak{q}}$ if $a_n(g) \equiv a_n(h) \pmod{\mathfrak{q}}$ for all $n \in \mathbf{N}$, where as usual if $g' \in S_2(\Gamma_0(N), \mathbf{C})$, then $a_n(g')$ denotes the n-th Fourier coefficient of g'.

Lemma 5.2. *A prime q divides the order of the group*

$$\frac{S[I_{C'}]}{S[I_{B'}] + S[I_{A'}]}$$

if and only if there is a normalized eigenform $g \in S_2(\Gamma_0(N), \mathbf{C})$ with $L(A_g, 1) = 0$ such that g is congruent to f modulo a prime ideal $\mathfrak{q}$ over q in the ring of integers of the number field generated by the Fourier coefficients of f and g.

Proof. This follows from a slight modification of [Rib83, §1] and we only indicate the changes that need to be made in loc. cit. Replacing S by $S_2(\mathbf{C})[I_{C'}]$ and letting $X = S[I_{B'}] \otimes \mathbf{C}$ and $Y = S[I_{A'}] \otimes \mathbf{C}$ in loc. cit., by the discussion on p. 194-196 of loc. cit., there exist normalized eigenforms $f' \in S[I_{B'}] = S[I_f]$ and $g' \in S[I_{A'}]$ such that $f' \equiv g'$ modulo a prime ideal over q in the ring of integers of the number field generated by the Fourier coefficients of f' and g'. By the definitions of $I_{C'}$, $I_{A'}$, and $I_{B'} = I_f$, it is clear that f' is a Galois conjugate of f by some $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, and $L(g', 1) = 0$. Applying the inverse of σ, and letting $g = \sigma^{-1}(g')$, we get the statement in the lemma. $\square$

Proposition 5.3. *If an odd prime q divides $|\frac{H^+}{H[I_e]^+ + K^+}|$, then there is a normalized eigenform $g \in S_2(\Gamma_0(N), \mathbf{C})$ with $L(g, 1) = 0$ such that g is congruent to f modulo a prime ideal over q in the ring of integers of the number field generated by the Fourier coefficients of f and g.*

Proof. Note that $|\frac{H^+}{H[I_e]^+ + K^+}|$ differs from $|\frac{H}{H[I_e] + K}|$ only in powers of 2. The proposition now follows from Lemmas 4.4, 5.1, and 5.2. $\square$

Proposition 5.4. *Let q be an odd prime such that $q^2 \nmid N$. Suppose that there is a normalized eigenform $g \in S_2(\Gamma_0(N), \mathbf{C})$ with $L(g, 1) = 0$ such that g is congruent to f modulo a prime ideal over q in the ring of integers of the number field generated by the Fourier coefficients of f and g. Then q divides $|\frac{H^+}{H[I_e]^+ + K^+}|$. Suppose moreover that q does not divide $|A_f(\mathbf{Q})_{\mathrm{tor}}|$. Then q divides $L_{A_f}(1)/\Omega_{A_f}$, and in particular, $\frac{L_{A_f}(1)}{\Omega_{A_f}} \equiv \frac{L_{A_g}(1)}{\Omega_{A_g}} \bmod q$.*

Proof. The first part of the proposition follows from Lemma 4.4, the second statement in Lemma 5.1, and the fact that $|\frac{H^+}{H[I_e]^+ + K^+}|$ differs from $|\frac{H}{H[I_e]+K}|$ only in powers of 2. The second part follows from Theorem 3.2, in view of the following facts: $|\pi_*(\mathbf{T}e)/\pi_*(\Im e)|$ divides $|A_f(\mathbf{Q})_{\text{tor}}|$ (by Lemma 3.3), $q \nmid c_\infty(A_f)$ (since q is odd), $q \nmid c_{A_f}$ (by [ARS06], considering that $q^2 \nmid N$), and $L_{A_g}(1) = 0$ (since $L(g,1) = 0$). $\square$

Corollary 5.5. *Let q be an odd prime such that $q^2 \nmid N$. Suppose that there is a normalized eigenform $g \in S_2(\Gamma_0(N), \mathbf{C})$ such that A_g has positive Mordell-Weil rank and g is congruent to f modulo a prime ideal over q in the ring of integers of the number field generated by the Fourier coefficients of f and g. Then the second part of the Birch and Swinnerton-Dyer conjecture implies that q divides $|\text{III}(A_f)| \cdot \prod_{p|N} c_p(A_f)$. If moreover, N is prime, then the conjecture implies that q divides $|\text{III}(A_f)|$.*

Proof. By [KL89], since A_g has positive Mordell-Weil rank, $L(g,1) = 0$. Hence by Proposition 5.4, q divides $|\frac{H^+}{H[I_e]^+ + K^+}|$. The first conclusion of the Corollary now follows from formula (13) and Lemma 3.3, and the second conclusion (for N prime) follows from Proposition 3.4. $\square$

We also have the following characterization of certain primes that divide the factor $|\frac{H^+}{H[I_e]^+ + K^+}|$.

Corollary 5.6. *Suppose q is an odd prime such that $q^2 \nmid N$. Then q divides $|\frac{H^+}{H[I_e]^+ + K^+}|$ if and only if there is a normalized eigenform $g \in S_2(\Gamma_0(N), \mathbf{C})$ with $L(g,1) = 0$ such that g is congruent to f modulo a prime ideal over q in the ring of integers of the number field generated by the Fourier coefficients of f and g.*

Proof. This follows from Propositions 5.3 and 5.4. $\square$

6 Visibility: relating the congruence to the Shafarevich-Tate group and the component group

In this section, we finally relate the factor $|\frac{H^+}{H[I_e]^+ + K^+}|$ in the numerator of our formula (6) for $L_{A_f}(1)/\Omega_{A_f}$ to the numerator $|\text{III}(A_f)| \cdot \prod_{p|N} c_p(A_f)$ of the Birch and Swinnerton-Dyer conjectural formula (1) for $L_{A_f}(1)/\Omega_{A_f}$. Recall that since $L(A_f, 1) \neq 0$, by [KL89], $\text{III}(A_f)$ is finite and $A_f(\mathbf{Q})$ has rank zero. At several instances below, we will consider the torsion group $A_f[\mathfrak{q}]$ where $\mathfrak{q}$ is a prime ideal in a number field L containing the Fourier

coefficients of f and another eigenform – this makes sense if A_f has the full action of the ring of integers of L. If not, then we merely replace $\mathfrak{q}$ by a prime of fusion, which is a maximal ideal of $\mathbf{T}$ (see, e.g., [Rib83, p.196] and [Gha02, §2]) that is contained in $\mathfrak{q}$, and all the arguments go through. We have preferred to consider prime ideals of L instead of maximal ideals of $\mathbf{T}$ simply to keep the notation similar to the one in the article [DSW03], which we will often refer to in this section. If p is a prime that divides N, then we denote by w_p the eigenvalue of the Atkin-Lehner involution W_p acting on f. Similarly w_N denotes the eigenvalue of the Atkin-Lehner involution W_N acting on f (so that w_N is the product over all primes that divide N of the w_p's).

Theorem 6.1. *Suppose N is prime, and q is a prime such that q divides $|\frac{H^+}{H[I_e]^+ + K^+}|$, and $q \nmid N(N-1)$. Assume that for all newforms g on $\Gamma_0(N)$, if $L(g,1) = 0$, then the rank of $A_g(\mathbf{Q})$ is positive. Then q divides $|\text{Ш}(A_f)|$. If moreover we assume the parity conjecture, then q^2 divides $|\text{Ш}(A_f)|$ (both the assumption on the rank and the parity conjecture hold if the first part of the Birch and Swinnerton-Dyer conjecture (Conjecture 1.1) is true).*

Proof. By Prop. 5.3, 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 $\mathfrak{q}$ over q in the ring of integers of the number field generated by the Fourier coefficients of f and g. By the hypothesis, the rank of $A_g(\mathbf{Q})$ is positive. By [Maz77, Prop. 14.2], since $q \nmid 2 \cdot \text{numr}(\frac{N-1}{12})$, it follows that $A_f^\vee[\mathfrak{q}]$ and $A_g^\vee[\mathfrak{q}]$ are irreducible. Also, since $L_{A_f}(1) \neq 0$, we have $w_N = -1$. Hence by hypothesis, $N \not\equiv -w_N \pmod q$. Thus the hypotheses of Theorem 6.1 of [DSW03] are satisfied and the conclusion of this theorem tells us that q divides $|\text{Ш}(A_f^\vee)|$ (in the notation of [DSW03], $r \geq 1$ since the dimension of $H_f^1(\mathbf{Q}, V_\mathfrak{q}'(1))$ is an upper bound for the rank of $A_g(\mathbf{Q})$; also given that $\text{Ш}(A_f^\vee)$ is finite, the q-primary part of $\text{Ш}(A_f^\vee)$ is the same as $H_f^1(\mathbf{Q}, A_\mathfrak{q}(1))$). By the perfectness of the Cassels-Tate pairing, q divides $|\text{Ш}(A_f)|$ as well. This proves the first assertion of the theorem.

Since q is odd, f and g have the same eigenvalue under the Atkin-Lehner involution, and hence the same sign in their functional equations (see, e.g., Remark 6.4). Thus if we assume the parity conjecture, then $A_g^\vee$ has even Mordell-Weil rank, and so $r \geq 2$ (where r is as in the statement of Theorem 6.1 of [DSW03]). Theorem 6.1 of [DSW03] in fact tells us that q^r divides $|\text{Ш}(A_f^\vee)|$, which gives the second assertion of our theorem. $\square$

As mentioned towards the end of Section 3, the second part of the Birch and Swinnerton-Dyer conjecture implies that when N is prime, if an odd

prime q divides $|\frac{H^+}{H[I_e]^++K^+}|$, then q divides $|\text{Ш}(A_f)|$. Thus Theorem 6.1 may be viewed as a partial result towards the second part of the Birch and Swinnerton-Dyer conjecture.

Example 6.2. Consider the prime level 389. From [Ste], one sees that the quotient associated the newform denoted **389E1** is the winding quotient $J_0(N)/I_e J_0(N)$ for $N = 389$ (the other newforms of level 389 have positive analytic rank). The factor $|\frac{H^+}{H[I_e]^++K^+}|$ was computed for this winding quotient in [Aga00, §3.3] and its odd part was found to be 5. Moreover, $5 \nmid 389(389-1)$, and hence if one assumes the first part of the Birch and Swinnerton-Dyer conjecture, Theorem 6.1 implies that 5 divides Ш(**389E**). In fact, it turns out that one can show 5 divides Ш(**389E**) without assuming the conjecture – see [AS02, §4.1].

The following proposition is easily extracted from §7.4 of [DSW03]; see also [Dum04, §7].

Proposition 6.3 (Dummigan-Stein-Watkins). *Let p be a prime such that $p||N$. Suppose that there is a newform h of level dividing N/p, and an odd prime $q \neq p$ such that modulo a prime ideal $\mathfrak{q}$ over q in some number field containing the Fourier coefficients of f and h, we have $f \equiv h$ (for Fourier coefficients of index coprime to Nq). Suppose $A_f[\mathfrak{q}]$ and $A_h[\mathfrak{q}]$ are irreducible and that $p \not\equiv -w_p \pmod{q}$. If $w_p = -1$, then $\mathrm{ord}_{\mathfrak{q}}(c_p(A_f)) > 0$.*

Proof. The proof is essentially given in the first example in §7.4 of [DSW03]; we repeat the argument here for clarity. We use the notation as in [DSW03].

Let $T''_{\mathfrak{q}}$, $V''_{\mathfrak{q}}$, and $A''_{\mathfrak{q}}$ be the objects attached to h, just as $T_{\mathfrak{q}}$, $V_{\mathfrak{q}}$, and $A_{\mathfrak{q}}$ have been attached to f. Since $p^2 \nmid N$, p does not divide the level of h, and so the representation $V''_{\mathfrak{q}}$ is unramified at p. Hence $H^0(I_p, A''[\mathfrak{q}])$ is two dimensional. Since $A_f[\mathfrak{q}]$ and $A_h[\mathfrak{q}]$ are irreducible, by the Chebotarev density theorem, they are isomorphic as Galois representations and thus $H^0(I_p, A[\mathfrak{q}])$ is also two dimensional. Since $p||N$, by [Car86], $H^0(I_p, V_{\mathfrak{q}})$ is one dimensional, and following the argument in Case (2) of the proof of Theorem 6.1 of [DSW03], we see that the eigenvalue of Frob_p^{-1} acting on $H^0(I_p, V_{\mathfrak{q}})$ is $\alpha = -w_p p^{(k/2)-1}$ (for us, $k = 2$). Hence Frob_p^{-1} acts as $\alpha = -w_p p^{(k/2)-1}$ on the subspace of $H^0(I_p, A[\mathfrak{q}])$ formed by the image of $H^0(I_p, V_{\mathfrak{q}})$. Since $\alpha\beta = p^{k-1}$, the other eigenvalue must be $\beta = -w_p p^{k/2}$. Twisting by $k/2$, we see that the corresponding eigenvalues of Frob_p^{-1} on $H^0(I_p, A[\mathfrak{q}](k/2))$ are $-w_p$ and $-w_p/p$. Since $p \not\equiv -w_p \pmod{q}$ and $w_p = -1$, the two eigenvalues are different. Hence the quotient of $H^0(I_p, A[\mathfrak{q}](k/2))$ by the image of $H^0(I_p, V_{\mathfrak{q}}(k/2))$ may be viewed as a subspace, and Frob_p^{-1} acts as $-w_p$

on the quotient. As $w_p = -1$, we have $\mathrm{ord}_{\mathfrak{q}}(c_p(k/2)) > 0$. Since $k = 2$, the prime-to-p parts of $c_p(k/2)$ (as defined in [DSW03, §4]) and $c_p(A_f)$ are the same (see the Appendix). □

Remark 6.4. In Proposition 6.3, f need not have analytic rank 0. Note that if $w_p = -1$, then the analytic rank of h has a different parity than that of f. This is because the sign in the functional equation of a newform (of weight 2) is the negative of the product of the eigenvalues of W_p over all primes p dividing the level of the form in question. If this sign is positive, then the analytic rank of the newform is even, and it is odd otherwise (see, e.g., [Sil01, Ex. 4.3.3]).

Proposition 6.5. *Let q be an odd prime such that $q \nmid N$. Suppose $g \in S_2(\Gamma_0(N), \mathbf{C})$ is an eigenform (for all the Hecke operators) such that $A_g(\mathbf{Q})$ has positive rank and f is congruent to g modulo a prime ideal $\mathfrak{q}$ over q in the ring of integers of the number field generated by the Fourier coefficients of f and g. Suppose that $A_f[\mathfrak{q}]$ is an irreducible representation of the absolute Galois group of $\mathbf{Q}$. Assume that for all primes $p | N$, $p \not\equiv -w_p \pmod q$ and $p \not\equiv -1 \pmod q$ if $p^2 | N$. We have two possibilities:*
Case (i) For all primes $p | N$, f is not congruent modulo $\mathfrak{q}$ to a newform of level dividing N/p (for Fourier coefficients of index coprime to Nq):
In this case, $\mathfrak{q}$ divides $|\mathrm{III}(A_f)|$.
Case (ii) f is congruent modulo $\mathfrak{q}$ to a newform of lower level (for Fourier coefficients of index coprime to Nq):
In this case, suppose that
(*) there is a prime p dividing N such that $p^2 \nmid N$, $w_p = -1$, $A_h[\mathfrak{q}]$ is irreducible, and f is congruent modulo $\mathfrak{q}$ to a newform h of level dividing N/p (for Fourier coefficients of index coprime to Nq).
Then $\mathfrak{q}$ divides $\prod_{p|N} c_p(A_f)$.

Proof. The first part follows from [DSW03, Thm. 6.1] (cf. the proof of Theorem 6.1 for details), and the second part follows from Proposition 6.3. □

In view of Corollary 5.5, the Proposition above provides theoretical evidence towards the second part of the Birch and Swinnerton-Dyer conjecture.

Remark 6.6. (1) In condition (*), the statement "f is congruent mod $\mathfrak{q}$ to a newform of level dividing N/p (for Fourier coefficients of index coprime to Nq)" may be replaced by the potentially weaker statement "$A[\mathfrak{q}]$ is unramified at p" (this can be seen from the proof of Prop. 6.3).
(2) Suppose h is a newform of level N/p for some prime $p||N$ with $w_p = 1$

such that $f \equiv h$ modulo a prime ideal with odd residue characteristic. This is one situation where the condition (*) does not hold. Then, as N. Dummigan pointed out to us, by the reasoning in Remark 6.4, the sign in the functional equation of $L(A_h, s)$ is the same as that of $L(A_f, s)$, i.e., it is positive. Thus A_h has even analytic rank. If the analytic rank of h is in fact zero, then since $h \equiv g \pmod{\mathfrak{q}}$, one expects that $\mathrm{III}(A_h)$ is non-trivial, and hence h should show up in the tables in [AS05]. With this in mind, we searched the tables in [AS05] and found only one potential example where (*) may fail because the condition on w_p does not hold: At level $N = 1994$, whose prime factorization is $2 \cdot 997$, the newform $f = \mathbf{1994D}$ is of rank 0 with $w_2 = 1$ ($w_{997} = -1$, but there are no cusp forms over $\Gamma_0(2)$). The newform f is congruent modulo a prime ideal over 3 to $g = \mathbf{997B}$ of positive analytic rank (this can be deduced from the table in [AS05] and the result of [ARS07] that the modular exponent divides the congruence exponent). Similarly, one finds that g is congruent modulo a prime ideal over 3 to $h = \mathbf{997H}$ of Mordell-Weil rank zero. However, we do not know if the congruences mentioned in the previous two sentences hold modulo the *same* ideal over 3.

Theorem 6.7. *Let q be a prime such that q divides $|\frac{H^+}{H[I_e]^+ + K^+}|$.*
Suppose that $q \nmid 2N$ and that for all maximal ideals $\mathfrak{q}$ of $\mathbf{T}$ with residue characteristic q, $A_f[\mathfrak{q}]$ is irreducible. Assume that for all newforms g of level dividing N, if $L(g, 1) = 0$, then the rank of $A_g(\mathbf{Q})$ is positive (this would hold if the first part of the Birch and Swinnerton-Dyer conjecture (Conjecture 1.1) is true). Suppose that for all primes $p \mid N$, $p \not\equiv -w_p$ (mod q) and $p \not\equiv -1$ (mod q) if $p^2 | N$. We have two possibilities:
Case (i) For all primes $p \mid N$, f is not congruent modulo a maximal ideal of $\mathbf{T}$ over q to a newform of level dividing N/p (for Fourier coefficients of index coprime to Nq):
In this case, q divides $|\mathrm{III}(A_f)|$.
Case (ii) For some prime p dividing N, f is congruent modulo a maximal ideal of $\mathbf{T}$ over q to a newform of level dividing N/p (for Fourier coefficients of index coprime to Nq):
In this case, suppose that
(*) there is a prime p dividing N and a maximal ideal $\mathfrak{q}$ of $\mathbf{T}$ over q such that $p^2 \nmid N$, $w_p = -1$, $A_h[\mathfrak{q}]$ is irreducible, and f is congruent modulo $\mathfrak{q}$ to a newform h of level dividing N/p (for Fourier coefficients of index coprime to Nq).
Then q divides $\prod_{p|N} c_p(A_f)$.

Proof. By Prop. 5.3, there is a normalized eigenform $g \in S_2(\Gamma_0(N), \mathbf{C})$ such

that $L(g, 1) = 0$, and $f \equiv g$ modulo a prime ideal $\mathfrak{q}$ over q in the ring of integers of the number field generated by the Fourier coefficients of f and g. By the hypothesis, the rank of $A_g(\mathbf{Q})$ is positive. The theorem then follows by Proposition 6.5. □

As mentioned towards the end of Section 3, the second part of the Birch and Swinnerton-Dyer conjecture implies that the part of $|\frac{H^+}{H[I_e]^+ + K^+}|$ that is coprime to $|A_f(\mathbf{Q})|$ divides $|\text{Ш}(A_f)| \cdot \prod_{p|N} c_p(A_f)$ up to a power of 2 and powers of primes whose squares divide N. Thus Theorem 6.7(ii) is a partial result towards the second part of the Birch and Swinnerton-Dyer conjecture.

Remark 6.8. The factor $|\frac{H^+}{H[I_e]^+ + K^+}|$ is often non-trivial. In [AS05], one finds a table of all quotients associated to newforms f of level $N < 2333$ such that $L(f, 1) \neq 0$ and the conjectural value of $|\text{Ш}(A_f)|$ is bigger than 1. In all the cases when the entry under the column labelled "B" is *not* NONE, there is an odd prime q and a normalized eigenform $g \in S_2(\Gamma_0(N), \mathbf{C})$ such that $L(g, 1) = 0$, and $f \equiv g$ modulo a prime ideal lying over q. If $q^2 \nmid N$, then by Prop. 5.4, q divides $|\frac{H^+}{H[I_e]^+ + K^+}|$. Thus all such entries in the table give examples where the factor $|\frac{H^+}{H[I_e]^+ + K^+}|$ is non-trivial, and where a prime dividing this factor divides the conjectural order of $\text{Ш}(A_f)$. The first level where this happens (also the first level where an odd prime divides the Birch and Swinnerton-Dyer conjectural order of $\text{Ш}(A_f)$) is 389, where there is a newform quotient of dimension 20 for which 5 divides $|\frac{H^+}{H[I_e]^+ + K^+}|$. When the entry under the column labelled "B" is NONE, the factor $|\frac{H^+}{H[I_e]^+ + K^+}|$ is a (possibly trivial) power of 2.

Example 6.9. We now give an example where a prime divides the factor $|\frac{H^+}{H[I_e]^+ + K^+}|$, but does not divide the conjectural order of $\text{Ш}(A_f)$, and instead divides $\prod_{p|N} c_p(A_f)$. This example was obtained using W. Stein's "The Modular Forms Explorer" [Ste] and we use the notation as therein. The newform $f = \mathbf{1751C1}$ is of analytic rank 0 and the newform $h = \mathbf{103A1}$ has positive analytic rank (note that $1751 = 17 \cdot 103$). From [AS05, Table 2], we find that 505 divides the order of the intersection of $A_f^\vee$ with the abelian subvariety of $J_0(1751)$ generated by the images of $A_h^\vee$ under the degeneracy maps. Hence, by the result in [ARS07] that the modular exponent divides the congruence exponent, we conclude that f is congruent modulo a prime ideal over 101 to an eigenform g in the subspace generated by h and $B_{17}(h)$ (a similar result holds for the congruence prime 5). We conclude from Proposition 5.4 that 101 divides $|\frac{H^+}{H[I_e]^+ + K^+}|$. One finds that $w_{17} = -1$,

and since 103 is prime and $101 \nmid \text{numr}(\frac{103-1}{12})$, $A_f[\mathfrak{q}] \cong A_h[\mathfrak{q}]$ is irreducible. Hence, Theorem 6.5 implies that 101 divides $c_{17}(f)$ (a similar result holds for the congruence prime 5 replacing 101 as well). As a confirmation, one finds from [Ste] that $c_{17}(A_f) = 6565$ (which is divisible by 101 and 5). It turns out that 5 divides the conjectural value of $|\text{III}(A_f)|$, but 101 doesn't. Note that neither 5 nor 101 divides the order of either $A_f(\mathbf{Q})_{\text{tor}}$ or $A_f^\vee(\mathbf{Q})_{\text{tor}}$.

Remark 6.10. (1) By the comment just after the proof of Theorem 6.7, the Birch and Swinnerton-Dyer conjecture suggests that the extra hypothesis (*) is unnecessary in Proposition 6.5 and Theorem 6.7. There are other versions of "visibility theorems" similar to Theorem 6.5. In the version in [AS02] and that of Cremona and Mazur (see the appendix of [AS05]), instead of our hypothesis (*) in Proposition 6.5 there is the hypothesis that q does not divide $\prod_{p|N} c_p(A_g)$. It is not clear to us whether the two hypotheses are related (there is some difference in the other hypotheses of the theorems as well).

(2) In [AS05], whenever an odd prime q divides $|\frac{H^+}{H[I_e]^+ + K^+}|$ (cf. Remark 6.8) and the entry under the column labelled "Vis" is a number, one finds that q^2 divides $|\text{III}(A)|$. Note that in most of these cases, we do not expect q^2 to divide $|\frac{H^+}{H[I_e]^+ + K^+}|$ (roughly speaking, locally the homology is often of rank two over the Hecke algebra, and our factor captures only half of the homology; see also Example 6.2). This seems to suggest that if an odd prime q divides $|\frac{H^+}{H[I_e]^+ + K^+}|$, then it also divides the other factor $|\frac{H[I_e]^+}{\Im e + H[I_e]^+ \cap K^+}|$ in (10) (perhaps under some additional mild hypotheses).

(3) We have not said much about the factor $|\frac{H[I_e]^+}{\Im e + H[I_e]^+ \cap K^+}|$, except the remark just above, which indicates that this factor should be divisible by primes q such that f is congruent modulo a prime ideal over q to an eigenform in $S_2(\Gamma_0(N), \mathbf{C})$ with positive analytic rank. However, these are not all the primes that divide this factor in general. In most of the examples in [AS05] where the entry under the column B is NONE, this factor is non-trivial and is divisible by primes q such that there is no eigenform g congruent to f modulo a prime over q with $L(g, 1) = 0$. It is our guess, however, that the factor $|\frac{H[I_e]^+}{\Im e + H[I_e]^+ \cap K^+}|$ can be explained by "visibility at higher level", as we now explain. It can be shown that the non-trivial elements of $\text{III}(A_f^\vee)$ (whose order is the same as that of $\text{III}(A_f)$) whose existence is implied by Theorems 6.1 and 6.7 are in the kernel of the natural map $\text{III}(A_f^\vee) \to \text{III}(J_0(N))$ (this can be seen from the proof of [DSW03, Thm. 6.1], or better still, from the analogous Theorem 3.1 of [AS02]). In general, if J is an abelian variety with a map $A_f^\vee \to J$, then we say that an element of $\text{III}(A_f^\vee)$ is *visible*

in J if it is in the kernel of the induced map $\text{III}(A_f^\vee) \to \text{III}(J)$. If an element of $\text{III}(A_f^\vee)$ is visible in $J_0(N)$ under the natural inclusion $A_f^\vee \to J_0(N)$, we say that it is *visible at the same level.* Now one has certain natural degeneracy maps $J_0(N) \to J_0(NM)$ for every positive integer M. We say that an element of $\text{III}(A_f^\vee)$ is *visible at higher level* if it is visible in $J_0(NM)$ under a map $A_f^\vee \to J_0(N) \to J_0(NM)$ for some integer M bigger than one. In [AS02, §4.2], there is an example of a particular f for which an element of $\text{III}(A_f^\vee)$ is not visible at the same level, but becomes visible at a higher level. In fact, it has been conjectured that any element the Shafarevich-Tate group can be explained by visibility at some higher level (see Conjecture 7.1.1 in [JS07] for details and a precise statement). Thus there is hope that the factor $|\frac{H[I_e]^+}{\Im e + H[I_e]^+ \cap K^+}|$ may be interpreted by considerations of visibility at the same and higher levels. This also suggests that while our formula for $L_{A_f}(1)/\Omega_{A_f}$ was obtained via the parametrization of A_f by $J_0(N)$, perhaps one should try to prove and use a similar formula for $L_{A_f}(1)/\Omega_{A_f}$ obtained via a parametrization of A_f by $J_0(NM)$ for an integer M.

7 Appendix: component groups

The proofs of some of the results in Section 6 employ the language of representations (à la [BK90]) as opposed to the language of abelian varieties. In this appendix we show that if p is a prime, then the definitions of the prime to p part of the component group at p coincide in the two languages. This is well known to experts, and our aim is simply to provide some details that we could not find in the literature.

Let A be an abelian variety and $\mathcal{A}$ its Néron model. Let $\mathcal{A}^0$ denote the largest open subgroup scheme of $\mathcal{A}$ in which all the fibers are connected. Let p be a prime. In Section 1, we had defined $c_p(A) = [\mathcal{A}_p(\mathbf{F}_p) : \mathcal{A}_p^0(\mathbf{F}_p)]$, where the subscript p denotes the special fiber at p.

Let B be a group and ℓ is a prime. Consider the inverse system $\{B[\ell^n]\}_{n \in \mathbf{N}}$ where for each n, the map $B[\ell^{n+1}] \to B[\ell^n]$ is multiplication by ℓ. We denote by $T_\ell B$ the inverse limit of the this system, which is a $\mathbf{Z}_\ell$-module in a natural way. Let $V_\ell B = T_\ell B \otimes \mathbf{Q}_\ell$, and $W_\ell B = V_\ell B / T_\ell B$. The natural map $T_\ell B \otimes \mathbf{Q}_\ell \to T_\ell B \otimes \mathbf{Q}_\ell / \mathbf{Z}_\ell$ is surjective, with kernel $T_\ell B$; hence we have a canonical isomorphism $W_\ell B \cong T_\ell B \otimes \mathbf{Q}_\ell / \mathbf{Z}_\ell$.

For simplicity of notation, for the case $B = A(\overline{\mathbf{Q}})$, we simply write T_ℓ, V_ℓ, and W_ℓ for the corresponding objects. In [DSW03, §4], the authors define an integer $c_p(1)$ associated to A as follows: if I_p denotes the inertia

subgroup of the absolute Galois group of $\mathbf{Q}_p$ and $\ell \neq p$ is a prime, then

$$\operatorname{ord}_\ell(c_p(1)) = \#H^0(\mathbf{Q}_p, W_\ell^{I_p}) - \#H^0(\mathbf{Q}_p, V_\ell^{I_p}/T_\ell^{I_p}), \qquad (16)$$

(note that in their notation $T_\ell(1) = T_\ell A$, as mentioned at the end of §1 in [DSW03]). The definition of $\operatorname{ord}_p(c_p(1))$ is more complicated, and we shall not be concerned with it. Our first goal in this appendix is to show that if $\ell \neq p$ is a prime, then $\operatorname{ord}_\ell(c_p(1)) = \operatorname{ord}_\ell(c_p(A))$ (this is used in the proof of Prop. 6.3). The other goal of this appendix is to give some details of how the definition in (16) comes naturally from the formulation of the Bloch-Kato conjecture [BK90].

Henceforth, $\ell \neq p$ is a prime. The following lemma is well known:

Lemma 7.1. *Suppose the inverse system $\{B[\ell^n]\}_{n \in \mathbf{N}}$ is surjective, i.e., the multiplication by ℓ maps $B[\ell^{n+1}] \to B[\ell^n]$ are surjective for all n. Then one has a canonical isomorphism (of groups) $T_\ell B \otimes \mathbf{Q}_\ell/\mathbf{Z}_\ell = B[\ell^\infty]$.*

Proof. Our proof is inspired by [Gro72, IX.11]. Consider the direct system $\{\mathbf{Z}_\ell/\ell^n\mathbf{Z}_\ell\}_{n \in \mathbf{N}}$, where the maps $\mathbf{Z}_\ell/\ell^n\mathbf{Z}_\ell \to \mathbf{Z}_\ell/\ell^{n+1}\mathbf{Z}_\ell$ are multiplication by ℓ. The direct limit $\varinjlim_n \mathbf{Z}_\ell/\ell^n\mathbf{Z}_\ell$ of this system is the direct sum $\oplus(\mathbf{Z}_\ell/\ell^n\mathbf{Z}_\ell)$ modulo the subgroup generated by all elements of the form $(\ldots, 0, x_n, 0, \ldots, 0, x_m, 0, \ldots)$, such that $x_m = -\ell^{m-n}x_n$, where $m > n$ and x_n and x_m are the entries in the n-th and m-th position respectively. Then the assignment $(x_n) \in \oplus(\mathbf{Z}_\ell/\ell^n\mathbf{Z}_\ell)$ maps to $\sum \frac{x_n}{\ell^n}$ gives a canonical isomorphism $\varinjlim_n \mathbf{Z}_\ell/\ell^n\mathbf{Z}_\ell \cong \mathbf{Q}_\ell/\mathbf{Z}_\ell$.

Next, let $(t_i)_{i \in \mathbf{N}}$ be an element of $T_\ell B$. Let m be any positive integer. Using the construction of the inverse limit and the fact that $\{B[\ell^n]\}$ is a surjective system, one sees that the assignment $(t_i) \otimes 1 \mapsto t_m$ gives a canonical isomorphism $T_\ell B \otimes (\mathbf{Z}_\ell/\ell^m\mathbf{Z}_\ell) \cong B[\ell^m]$. This maps the direct system $\{T_\ell B \otimes (\mathbf{Z}_\ell/\ell^m\mathbf{Z}_\ell)\}_{m \in \mathbf{N}}$ with the multiplication by ℓ map on the second component and identity on the first isomorphically to the direct system $\{B[\ell^m]\}$ where the maps are the natural inclusion maps $B[\ell^m] \hookrightarrow B[\ell^{m+1}]$.

Thus we see that $T_\ell B \otimes \mathbf{Q}_\ell/\mathbf{Z}_\ell = \varinjlim_m T_\ell B \otimes \mathbf{Z}_\ell/\ell^m\mathbf{Z}_\ell = \varinjlim_m B[\ell^m] = B[\ell^\infty]$. $\qquad\square$

We now apply this to the case $B = A(\overline{\mathbf{Q}})$. Note that since $\ell \neq p$, the reduction map gives an isomorphism of Galois modules

$$A[\ell^n]^{I_p} \cong \mathcal{A}_p(\overline{\mathbf{F}}_p)[\ell^n] \qquad (17)$$

(e.g., see [ST68, p. 495]).

Proposition 7.2. *We have isomorphisms* $H^0(\mathbf{Q}_p, W_\ell{}^{I_p}) \cong \mathcal{A}_p(\mathbf{F}_p)[\ell^\infty]$ *and* $H^0(\mathbf{Q}_p, V_\ell{}^{I_p}/T_\ell{}^{I_p}) \cong \mathcal{A}_p^0(\mathbf{F}_p)[\ell^\infty]$.

Proof. By lemma 7.1, $W_\ell \cong A[\ell^\infty]$, and from its proof, we see that this isomorphism respects the action of the absolute Galois group of $\mathbf{Q}_p$. Using (17), we get $W_\ell{}^{I_p} = A[\ell^\infty]^{I_p} \cong \mathcal{A}_p(\overline{\mathbf{F}}_p)[\ell^\infty]$. Hence $H^0(\mathbf{Q}_p, W_\ell{}^{I_p}) = H^0(\mathbf{Q}_p/I_p, W_\ell{}^{I_p}) \cong (\mathcal{A}_p(\overline{\mathbf{F}}_p)[\ell^\infty])^{\mathrm{Frob}_p} = \mathcal{A}_p(\mathbf{F}_p)[\ell^\infty]$, which gives the first isomorphism in the Proposition.

Next, note that since $\mathcal{A}_p^0$ is connected, the system $\mathcal{A}_p^0[\ell^n]$ is surjective. Moreover, since $\mathcal{A}_p^0$ is of finite index in $\mathcal{A}_p$, by the construction of inverse limits, we have $T_\ell\mathcal{A}_p = T_\ell\mathcal{A}_p^0$ (the only infinitely ℓ-divisible points in $\mathcal{A}_p(\overline{\mathbf{F}}_p)$ are those coming from $\mathcal{A}_p^0(\overline{\mathbf{F}}_p)$). Thus from (17), we have an isomorphism $(T_\ell A)^{I_p} = T_\ell(A^{I_p}) \cong T_\ell\mathcal{A}_p = T_\ell\mathcal{A}_p^0$. Thus

$$H^0(\mathbf{Q}_p, V_\ell{}^{I_p}/T_\ell{}^{I_p}) = H^0(\mathbf{Q}_p, T_\ell{}^{I_p} \otimes \mathbf{Q}_\ell/\mathbf{Z}_\ell)$$
$$= H^0(\mathbf{Q}_p/I_p, (T_\ell A)^{I_p} \otimes \mathbf{Q}_\ell/\mathbf{Z}_\ell) \cong H^0(\mathbf{Q}_p/I_p, (T_\ell\mathcal{A}_p^0)^{I_p} \otimes \mathbf{Q}_\ell/\mathbf{Z}_\ell)$$
$$= (\mathcal{A}_p^0(\overline{\mathbf{F}}_p)[\ell^\infty])^{\mathrm{Frob}_p} = \mathcal{A}_p^0(\mathbf{F}_p)[\ell^\infty].$$

$\square$

Thus it follows that $\mathrm{ord}_\ell(c_p(1)) = \#H^0(\mathbf{Q}_p, W_\ell{}^{I_p}) - \#H^0(\mathbf{Q}_p, V_\ell{}^{I_p}/T_\ell{}^{I_p}) = \mathrm{ord}_\ell\mathcal{A}_p(\mathbf{F}_p) - \mathrm{ord}_\ell\mathcal{A}_p^0(\mathbf{F}_p) = \mathrm{ord}_\ell(c_p(A))$, as was to be shown.

We next indicate how the definition in (16) arises naturally from the formulation of the Bloch-Kato conjecture [BK90]. Following the discussion on p.26-30 of [Fla93], if c_p denotes the Tamagawa measure of $A(\mathbf{Q}_\ell)$ defined in [BK90], then

$$\mathrm{ord}_\ell(c_p) = \#H^0(\mathbf{Q}_p, W_\ell) - \mathrm{ord}_\ell(P_p(p^{-1})), \tag{18}$$

where $P_p(p^{-s}) = \det(1 - \mathrm{Frob}_p^{-1}p^{-s} \mid H_{\mathrm{et}}^1(A \otimes \overline{\mathbf{Q}}, \mathbf{Q}_\ell))$ is the usual Euler factor at p. To see that the prime-to-p parts of c_p and $c_p(1)$ coincide, one only needs the following Proposition, whose proof is skipped in [Fla93].

Proposition 7.3. $\mathrm{ord}_\ell(P_p(p^{-1})) = \#H^0(\mathbf{Q}_\ell, V_\ell{}^{I_p}/T_\ell{}^{I_p})$.

Proof. We have the following isomorphisms of Galois modules: $H_{\mathrm{et}}^1(A \otimes \overline{\mathbf{Q}}, \mathbf{Q}_\ell) \cong \mathrm{Hom}(V_\ell, \mathbf{Q}_\ell) \cong V_\ell(-1)$, where the second isomorphism comes from the Weil pairing combined with a polarization map on $A^\vee$ (thus the isomorphism may not hold over $\mathbf{Z}_\ell$). Hence

$$\begin{aligned}
P_p(p^{-1}) &= \det(1 - \mathrm{Frob}_p^{-1}p^{-1} \mid H_{\mathrm{et}}^1(A \otimes \overline{\mathbf{Q}}, \mathbf{Q}_\ell)) \\
&= \det(1 - \mathrm{Frob}_p^{-1}p^{-1} \mid V_\ell(-1)) \\
&= \det(1 - \mathrm{Frob}_p^{-1} \mid V_\ell). \tag{19}
\end{aligned}$$

30

Now there is a $\mathbf{Z}_\ell$-basis $(e_1, \ldots, e_n)$ of $T_\ell^{I_p}$ and $a_1, \ldots, a_n \in \mathbf{Z}_\ell$ such that $(a_1 e_1, \ldots, a_n e_n)$ is a basis for the submodule $(1 - \mathrm{Frob}_p{}^{-1}) T_\ell^{I_p}$ (see, e.g., [Lan93, Thm. III.7.8]). Then $\# T_\ell^{I_p}/(1 - \mathrm{Frob}_p{}^{-1}) T_\ell^{I_p} = \mathrm{ord}_\ell(\prod_{i=1}^n a_i)$. The endomorphism $(1 - \mathrm{Frob}_p{}^{-1})$ may map $T_\ell^{I_p}$ to some basis of $(1 - \mathrm{Frob}_p{}^{-1}) T_\ell^{I_p}$ other than $(a_1 e_1, \ldots, a_n e_n)$, but the change of basis matrix has determinant invertible in $\mathbf{Z}_\ell$. Thus

$$
\begin{aligned}
\mathrm{ord}_\ell(\det(1 - \mathrm{Frob}_p{}^{-1} \mid V_\ell)) &= \mathrm{ord}_\ell(\prod_{i=1}^n a_i) \\
&= \# T_\ell^{I_p}/(1 - \mathrm{Frob}_p{}^{-1}) T_\ell^{I_p}. \quad (20)
\end{aligned}
$$

Next we need the following lemma:

Lemma 7.4. *The groups* $(V_\ell^{I_p}/T_\ell^{I_p})^{\mathrm{Frob}_p{}^{-1}}$ *and* $T_\ell^{I_p}/(1 - \mathrm{Frob}_p{}^{-1}) T_\ell^{I_p}$ *are isomorphic.*

Proof. If $v \in V_\ell^{I_p}$ is such that $v + T_\ell^{I_p} \in (V_\ell^{I_p}/T_\ell^{I_p})^{\mathrm{Frob}_p{}^{-1}}$, then $\mathrm{Frob}_p{}^{-1} v - v \in T_\ell^{I_p}$. This gives us a homomorphism $\phi : (V_\ell^{I_p}/T_\ell^{I_p})^{\mathrm{Frob}_p{}^{-1}} \to (V_\ell^{I_p}/T_\ell^{I_p})^{\mathrm{Frob}_p{}^{-1}}$, which we will show is an isomorphism.

For simplicity, let $F = \mathrm{Frob}_p{}^{-1}$, $T = (T_\ell A)^{I_p}$ and $V = (V_\ell A)^{I_p}$. By (17), $T \cong T_\ell \mathcal{A}_p(\overline{\mathbf{F}}_p)$; hence $T^F = T_\ell \mathcal{A}_p(\mathbf{F}_p)$. Thus T^F is trivial, and hence so is V^F. We have an exact sequence

$$
0 \to V^F \to V \xrightarrow{(1-F)} V \to V/(1-F)V \to 0.
$$

Since V^F is trivial, this shows that $V/(1-F)V$ is of dimension zero. Hence $T/(1-F)T$ is torsion. Thus if $t \in T$, then there is an integer n such that $nt \in (1-F)T$; so there is a $t' \in T$ such that $nt = (1-F)t'$. Then $v = t'/n \in V$ maps to t. Thus ϕ is surjective. Suppose $v \in V$ is such that $\phi(v) = 0$. Then $Fv - v = Ft - t$, for some $t \in T$, so $v - t$ is fixed by F. But $V^F = 0$, so $v = t \in T$. Thus ϕ is injective, and hence an isomorphism. $\qquad\square$

By (19), (20), and Lemma 7.4,

$$
\mathrm{ord}_\ell(P_p(p^{-1})) = \#(V_\ell/T_\ell)^{\mathrm{Frob}_p{}^{-1}} = \#(V_\ell/T_\ell)^{\mathrm{Frob}_p} = \# H^0(\mathbf{Q}_\ell, V_\ell^{I_p}/T_\ell^{I_p}),
$$

which proves the proposition. $\qquad\square$

References

[Aga99] A. Agashe, *On invisible elements of the Tate-Shafarevich group*, C. R. Acad. Sci. Paris Sér. I Math. **328** (1999), no. 5, 369–374.

[Aga00] _____, *The Birch and Swinnerton-Dyer formula for modular abelian varieties of analytic rank zero*, Ph.D. thesis, University of California, Berkeley (2000), available at `http://www.math.fsu.edu/~agashe/math.html`.

[Aga07] _____, *Letter to W. Stein*, available at `http://www.math.fsu.edu/~agashe/math.html`.

[Aga08] _____, *The modular number, congruence number, and multiplicity one*, preprint (2008), available at `http://www.math.fsu.edu/~agashe/math.html`.

[ARS06] Amod Agashe, Kenneth Ribet, and William A. Stein, *The Manin constant*, Pure Appl. Math. Q. **2** (2006), no. 2, 617–636.

[ARS07] A. Agashe, K. Ribet, and W. A. Stein, *The modular degree, congruence primes, and multiplicity one*, preprint (2007), available at `http://www.math.fsu.edu/~agashe/moddeg3.html`.

[AS02] Amod Agashe and William Stein, *Visibility of Shafarevich-Tate groups of abelian varieties*, J. Number Theory **97** (2002), no. 1, 171–185.

[AS05] _____, *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.

[BK90] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.

[Car86] H. Carayol, *Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert*, Ann. scient. Éc. Norm. Sup., 4[eb] série **19** (1986), 409–468.

32

[CM00]   J. E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experiment. Math. **9** (2000), no. 1, 13–28. MR 1 758 797

[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.

[Dum04] N. Dummigan, *Level-lowering for higher congruences of modular forms*, preprint (2004).

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

[Fla93]   Matthias Flach, *On the degree of modular parametrizations*, Séminaire de Théorie des Nombres, Paris, 1991–92, Progr. Math., vol. 116, Birkhäuser Boston, Boston, MA, 1993, pp. 23–36.

[Gha02]   Eknath Ghate, *An introduction to congruences between modular forms*, Currents trends in number theory (Allahabad, 2000), Hindustan Book Agency, New Delhi, 2002, pp. 39–58.

[Gro72]   A. Grothendieck, *Groupes de monodromie en géométrie algébrique. I*, Springer-Verlag, Berlin, 1972, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim, Lecture Notes in Mathematics, Vol. 288.

[JS07]   Dimitar P. Jetchev and William A. Stein, *Visibility of the Shafarevich-Tate group at higher level*, Doc. Math. **12** (2007), 673–696.

[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.

[Lan93]   S. Lang, *Algebra*, third ed., Addison-Wesley Publishing Co., Reading, Mass., 1993.

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

[Man72] J. I. Manin, *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).

[Par99] Pierre Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math. **506** (1999), 85–116.

[Rib83] Kenneth A. Ribet, *Mod p Hecke operators and congruences between modular forms*, Invent. Math. **71** (1983), no. 1, 193–205.

[Rub98] Karl Rubin, *Euler systems and modular elliptic curves*, Galois representations in arithmetic algebraic geometry (Durham, 1996), Cambridge Univ. Press, Cambridge, 1998, pp. 351–367.

[Shi73] G. Shimura, *On the factors of the jacobian variety of a modular function field*, J. Math. Soc. Japan **25** (1973), no. 3, 523–544.

[Shi94] ———, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kan Memorial Lectures, 1.

[Sil01] Alice Silverberg, *Open questions in arithmetic algebraic geometry*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, pp. 83–142. MR 2002g:11073

[ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517.

[Ste] W. A. Stein, *Modular forms database,*
http://modular.math.washington.edu/Tables/.

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