Visibility and the Birch and Swinnerton-Dyer conjecture for analytic rank zero

Amod Agashe *

Abstract

Let E be an optimal elliptic curve over $\mathbf{Q}$ of conductor N having analytic rank zero, i.e., such that the L-function $L_E(s)$ of E does not vanish at $s = 1$. Suppose there is another optimal elliptic curve over $\mathbf{Q}$ of the same conductor N whose Mordell-Weil rank is greater than zero and whose associated newform is congruent to the newform associated to E modulo a power r of a prime p. The theory of visibility then shows that under certain additional hypotheses involving p, r divides the product of the order of the Shafarevich-Tate group of E and the orders of the arithmetic component groups of E. We extract an explicit integer factor from the the Birch and Swinnerton-Dyer *conjectural* formula for the product mentioned above, and under some hypotheses similar to the ones made in the situation above, we show that r divides this integer factor. This provides theoretical evidence for the second part of the Birch and Swinnerton-Dyer conjecture in the analytic rank zero case.

1 Introduction

Let N be a positive integer. Let $X_0(N)$ be the modular curve over $\mathbf{Q}$ associated to $\Gamma_0(N)$, and let $J = J_0(N)$ denote the Jacobian of $X_0(N)$, which is an abelian variety over $\mathbf{Q}$. Let $\mathbf{T}$ denote the Hecke algebra, which is 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 $p \mid N$). If f is a newform of weight 2 on $\Gamma_0(N)$, then let $I_f = \mathrm{Ann}_{\mathbf{T}} f$ and let A_f denote the associated *newform quotient* $J/I_f J$, which is an abelian variety over $\mathbf{Q}$. Let π denote the quotient map $J \to J/I_f J = A_f$. By the *analytic rank* of f, we mean the order of vanishing at $s = 1$ of $L(f, s)$. Now suppose that the newform f has

*This material is based upon work supported by the National Science Foundation under Grant No. 0603668.

integer Fourier coefficients. Then A_f is an elliptic curve, and we denote it by E instead. The analytic rank of E is the same as the analytic rank of f.

Now suppose that $L_E(1) \neq 0$ (i.e., f has analytic rank zero). Then by [KL89], E has Mordell-Weil rank zero, and the Shafarevich-Tate group $Ш(E)$ of E is finite. Let $\mathcal{E}$ denote the Néron model of E over $\mathbf{Z}$ and let $\mathcal{E}^0$ denote the largest open subgroup scheme of $\mathcal{E}$ in which all the fibers are connected. Let Ω_E denote the volume of $E(\mathbf{R})$ with respect to the measure given by a generator of the rank one $\mathbf{Z}$-module of invariant differentials on $\mathcal{E}$. If p is a prime number, then the group of $\mathbf{F}_p$-valued points of the quotient $\mathcal{E}_{\mathbf{F}_p}/\mathcal{E}^0_{\mathbf{F}_p}$ is called the (arithmetic) component group of A and its order is denoted $c_p(A)$. Throughout this article, we use the symbol $\stackrel{?}{=}$ to denote a conjectural equality.

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

Conjecture 1.1 (Birch and Swinnerton-Dyer)**.**

$$\frac{L_E(1)}{\Omega_E} \stackrel{?}{=} \frac{|Ш(E)| \cdot \prod_{p|N} c_p(E)}{|E(\mathbf{Q})|^2} \ . \tag{1}$$

It is known that $L_E(1)/\Omega_E$ is a rational number. The importance of the second part of the Birch and Swinnerton-Dyer conjecture is that it gives a conjectural value of $|Ш(E)|$ in terms of the other quantities in (1) (which can often be computed). Let us denote this conjectural value of $|Ш(E)|$ by $|Ш(E)|_{\mathrm{an}}$ (where "an" stands for "analytic"). The theory of Euler systems has been used to bound $|Ш(E)|$ from above in terms $|Ш(A_f)|_{\mathrm{an}}$ 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 $|Ш(A_f)|_{\mathrm{an}}$ divides $|Ш(E)|$. In both of the methods above, one may have to stay away from certain primes.

The conjectural formula (1) may be rewritten as follows:

$$|E(\mathbf{Q})|^2 \cdot \frac{L_E(1)}{\Omega_E} \stackrel{?}{=} |Ш(E)| \cdot \prod_{p|N} c_p(E) \ . \tag{2}$$

We shall refer to the formula above as the Birch and Swinnerton-Dyer conjectural formula.

Now suppose that f is congruent modulo a prime p to another newform g that has integer Fourier coefficients and whose associated elliptic curve has positive Mordell-Weil rank. Let r denote the highest power of p modulo which this congruence holds. Then the theory of visibility (e.g., as

in [CM00]) often shows that r divides $|Ш(E)| \cdot \prod_{p|N} c_p(E)$, the right side of the Birch and Swinnerton-Dyer conjectural formula (2); we give precise results along these lines in Section 2 (see, e.g., Prop. 2.2(i) below). When this happens, the conjectural formula (2) says that r should also divide the left side of (2), which is $|E(\mathbf{Q})|^2 \cdot \frac{L_E(1)}{\Omega_E}$ (since it is not known that the rational number $|E(\mathbf{Q})|^2 \cdot \frac{L_E(1)}{\Omega_E}$ is an integer, what we mean here and henceforth is that the order at p of this rational number is at least $\mathrm{ord}_p r$). In Section 3, we show that this does happen under somewhat similar hypotheses (see, e.g., Cor. 3.3). Note that while we have stated results mostly when r is a power of a prime p, this implies similar results when r is any integer, provided that the primes that divide r satisfy the hypotheses involving p in several results in this article (in particular, see Cor. 2.3 and Cor. 3.4). In Section 4, we give the proof of our main result (Theorem 3.2); in the proof, we actually extract an explicit integer factor from $|E(\mathbf{Q})|^2 \cdot \frac{L_E(1)}{\Omega_E}$, and under certain hypotheses, we show that r divides this integer factor. The reader who is interested in seeing only the precise statements of our main results may read Sections 2 and 3, skipping proofs. In each section, we continue to use the notation introduced in earlier sections (unless mentioned otherwise).

We remark that the results of this article are very analogous to the results obtained in [Aga09], where we treated the case where E had analytic rank one. We also take the opportunity to point out some mistakes in [Aga09] (see Remark 4.4). Finally, our results for the case where $r = p$ (i.e., if f and g are congruent modulo p, but not modulo p^2), are covered to some extent in [Aga]. In fact, the present article arose from our efforts to generalize some of the results in [Aga], where we proved that the prime p divided certain quantities (in this article, we deal with powers of p dividing certain quantities).

Acknowledgements: We are grateful to M. Emerton for pointing out some errors related to the statement of Lemma 4.3 in an earlier version of this article.

2 Visibility and the right side of the Birch and Swinnerton-Dyer conjectural formula

Let F denote the elliptic curve associated to the newform g. If A is an abelian variety, then we denote its dual abelian variety by $A^\vee$. If h is a newform of weight 2 on $\Gamma_0(N)$, then by taking the dual of the quotient

map $J_0(N) \to A_h$ and using the self-duality of $J_0(N)$, we may view $A_h^\vee$ as an abelian subvariety of $J_0(N)$. In particular, we may view $E^\vee$ and $F^\vee$ as abelian subvarieties of $J_0(N)$. We say that a maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ satisfies *multiplicity one* if $J_0(N)[\mathfrak{m}]$ is two dimensional over $\mathbf{T}/\mathfrak{m}$. Consider the following hypothesis on p:
(*) if $\mathfrak{m}$ is a maximal ideal of $\mathbf{T}$ with residue characteristic p and $\mathfrak{m}$ is in the support of $J_0(N)[I_f + I_g]$, then $\mathfrak{m}$ satisfies multiplicity one.

The following lemma is Lemma 2.1 from [Aga09]; we repeat the statement here since we shall refer to it several times.

Lemma 2.1. *Suppose p is odd, and either*
(i) $p \nmid N$ or
(ii) $p \| N$ and $E[p]$ or $F[p]$ is irreducible.
Then p satisfies hypothesis (*).

Proposition 2.2. *(i) Suppose that p is coprime to*

$$N \cdot |(J_0(N)/F^\vee)(\mathbf{Q})_{\mathrm{tor}}| \cdot |F(\mathbf{Q})_{\mathrm{tor}}| \cdot \prod_{\ell | N} \big(c_\ell(F) \cdot c_\ell(E)\big).$$

Then r divides $|Ш(E)|$.
(ii) Suppose that p is odd, that $E[p]$ and $F[p]$ are irreducible, and that p does not divide

$$N \cdot |(J_0(N)/F^\vee)(\mathbf{Q})_{\mathrm{tor}}| \cdot |F(\mathbf{Q})_{\mathrm{tor}}|.$$

Then p divides $|Ш(E)| \cdot \prod_{\ell | N} c_\ell(E)$, the right hand side of the Birch and Swinnerton-Dyer formula (2). If we assume moreover that f is not congruent modulo a prime ideal over p to a newform of a level dividing N/ℓ for some prime ℓ that divides N (for Fourier coefficients of index coprime to Np), and that either $p \nmid N$ or for all primes ℓ that divide N, $p \nmid (\ell - 1)$, then p divides $|Ш(E/\mathbf{Q})|$.

Proof. The proof is similar to the proof of Proposition 3.1 in [Aga09]. Both parts of the proposition above follow essentially from Theorem 3.1 of [AS02], which uses the theory of visibility. For Part (i), take $A = E^\vee$, $B = F^\vee$, and $n = r$ in [AS02, Thm. 3.1], and note that $F^\vee[r] \subseteq E^\vee$ by Lemma 2.1 and [Aga09, Lemma 2.2] (for the application of Lemma 2.1, note that $p \nmid N$ by hypothesis, and for the application of Lemma 2.2 of [Aga09], note that the analytic ranks of f and g do not play any role in the proof of Lemma 2.2 of loc. cit.). Then [AS02, Thm. 3.1] says that there is a map $F^\vee(\mathbf{Q})/rF^\vee(\mathbf{Q}) \to Ш(E^\vee)$, whose kernel has order at most r raised to the power the Mordell-Weil rank of E. This proves Part (i).

For the first statement in Part (ii), take $A = E^\vee$, $B = F^\vee$, and $n = p$ in [AS02, Thm. 3.1], and note that the congruence of f and g modulo p forces $F^\vee[p] = E^\vee[p]$ by [Rib90, Thm. 5.2] (cf. [CM00, p. 20]). For the second statement in Part (ii), note that the additional hypotheses imply that p does not divide $c_\ell(E)$ or $c_\ell(F)$ for any prime ℓ that divides N, as we now indicate. By [Eme03, Prop. 4.2], if p divides $c_\ell(E)$ for some prime ℓ that divides N, then for some maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ having characteristic p and containing I_f, $\rho_\mathfrak{m}$ is either finite or reducible (here, $\rho_\mathfrak{m}$ is the canonical two dimensional representation associated to $\mathfrak{m}$, e.g., as in [Rib90, Prop. 5.1]). Since $E[p]$ is irreducible, this can happen only if $\rho_\mathfrak{m}$ is finite. But this is not possible by [Rib90, Thm. 1.1], in view of the hypothesis that f is not congruent modulo p to a newform of a level dividing N/ℓ for any prime ℓ that divides N (for Fourier coefficients of index coprime to Np), and either $p \nmid N$ or for all primes ℓ that divide N, $p \nmid (\ell - 1)$. Thus p does not divide $c_\ell(E)$ for any prime ℓ that divides N. Similarly, p does not divide $c_\ell(F)$ for any prime ℓ that divides N, considering that the hypothesis that f is not congruent modulo p to a newform of a level dividing N/ℓ for any prime ℓ that divides N (for Fourier coefficients of index coprime to Np) applies to g as well, since g is congruent to f modulo p. This finishes the proof of the proposition. □

Part (i) of the proposition above implies:

Corollary 2.3. *Recall that f and g are two newforms in $S_2(\Gamma_0(N), \mathbf{C})$ with integer Fourier coefficients. Suppose that f and g are congruent modulo an integer n such that n is coprime to*

$$N \cdot |(J_0(N)/F^\vee)(\mathbf{Q})_{\mathrm{tor}}| \cdot |F(\mathbf{Q})_{\mathrm{tor}}| \cdot \prod_{\ell | N} \big(c_\ell(F) \cdot c_\ell(E)\big).$$

Then n divides $|Ш(E)|$.

We refer the reader to [CM00] or [AS05] for examples where the theory of visibility proves the existence of non-trivial elements of the Shafarevich-Tate group of an elliptic curve of analytic rank zero.

3 Congruences and the left side of the Birch and Swinnerton-Dyer conjectural formula

Considering that under certain hypotheses, the theory of visibility (more precisely Proposition 2.2(i)) implies that r divides $|Ш(E)|$, which divides the

right hand side of the Birch and Swinnerton-Dyer conjectural formula (2), under similar hypotheses, one should be able to show that r also divides $|E(\mathbf{Q})|^2 \cdot \frac{L_E(1)}{\Omega_E}$, which is the left hand side of (2). The theory of Euler systems says under certain hypotheses that the order of $Ш(E)$ divides its Birch and Swinnerton-Dyer conjectural order (e.g., as in the work of Kolyvagin and Kato). Thus, in conjunction with Proposition 2.2(i), the theory of Euler systems shows that under certain additional hypotheses, r does divide $|E(\mathbf{Q})|^2 \cdot \frac{L_E(1)}{\Omega_E}$. For example, we have the following:

Proposition 3.1. *Suppose that p is coprime to*

$$2 \cdot N \cdot |(J_0(N)/F^\vee)(\mathbf{Q})_{\mathrm{tor}}| \cdot |F(\mathbf{Q})_{\mathrm{tor}}| \cdot \prod_{\ell | N} \big(c_\ell(F) \cdot c_\ell(E)\big).$$

Assume that the image of the absolute Galois group of $\mathbf{Q}$ acting on $E[p]$ is isomorphic to $\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$. Then r divides $|E(\mathbf{Q})|^2 \cdot \frac{L_E(1)}{\Omega_E}$ and the Birch and Swinnerton-Dyer conjectural order of $Ш(E)$.

Proof. Proposition 2.2(i), which uses the theory of visibility, implies that r divides $|Ш(E)|$. The result now follows by [SW08, Theorem 13], which uses the theory of Euler systems and is an extension of a theorem of Kato. □

The pullback of a generator of the rank one $\mathbf{Z}$-module of invariant differentials on the Néron model of E to $X_0(N)$ (under the modular parametrization) is a multiple of the differential $2\pi i f(z) dz$ by a rational number; this number is called the Manin constant of E, and we shall denote it by c_E. It is conjectured that c_E is one, and one knows that c_E is an integer, and that if p is a prime such that $p^2 \nmid 4N$, then p does not divide c_E (by [Maz78, Cor. 4.1] and [AU96, Thm. A]).

Theorem 3.2. *Suppose that p is odd and satisfies the hypothesis (*). Assume that f and g are not congruent modulo a prime ideal over p to any other newforms of level dividing N (for Fourier coefficients of index coprime to Np). Suppose that either $p^2 \nmid N$ or that the Manin constant c_E is one (as is conjectured). Then r divides $|E(\mathbf{Q})|^2 \cdot \frac{L_E(1)}{\Omega_E}$, the left side of the Birch and Swinnerton-Dyer conjectural formula (2).*

We shall prove this theorem in Section 4.

Corollary 3.3. *Suppose that p is odd, that f and g are not congruent modulo a prime ideal over p to any other newforms of level dividing N (for Fourier coefficients of index coprime to Np), and that either*

(a) $p \nmid N$ or
(b) $p || N$ and $E[p]$ or $F[p]$ is irreducible.
Then r divides $|E(\mathbf{Q})|^2 \cdot \frac{L_E(1)}{\Omega_E}$ and the Birch and Swinnerton-Dyer conjectural order of $Ш(E)$.

Proof. The statement that r divides $|E(\mathbf{Q})|^2 \cdot \frac{L_E(1)}{\Omega_E}$ follows from the theorem above, considering that the hypothesis (*) is satisfied, in view of Lemma 2.1. By the hypothesis that f and g are not congruent modulo a prime ideal over p to any other newforms of level dividing N (for Fourier coefficients of index coprime to Np), as explained in the proof of Proposition 2.2(ii), p does not divide $c_\ell(E)$ for any prime ℓ. Hence, by (2), r divides the Birch and Swinnerton-Dyer conjectural order of $Ш(E)$. □

The corollary above implies:

Corollary 3.4. *Recall that f and g are two newforms in $S_2(\Gamma_0(N), \mathbf{C})$ with integer Fourier coefficients. Suppose that f and g are congruent modulo an integer n such that for every prime p dividing n, f and g are not congruent modulo a prime ideal over p to any other newforms of level dividing N (for Fourier coefficients of index coprime to Np), and that either*
(a) $p \nmid N$ or
(b) $p || N$ and $E[p]$ or $F[p]$ is irreducible.
Then n divides $|E(\mathbf{Q})|^2 \cdot \frac{L_E(1)}{\Omega_E}$ and the Birch and Swinnerton-Dyer conjectural order of $Ш(E)$.

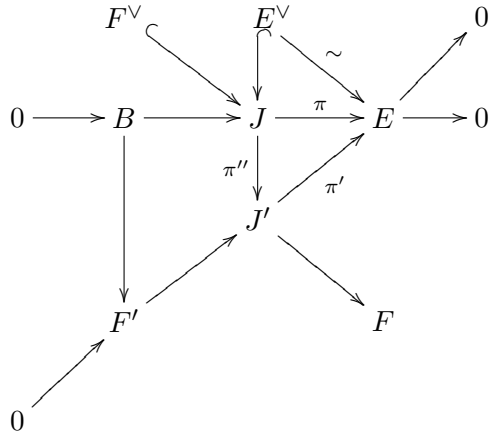
In view of Proposition 2.2, Corollary 3.3 provides theoretical evidence towards the Birch and Swinnerton-Dyer conjectural formula (2). Corollary 3.3 may also be compared to the similar Proposition 3.1 that uses the theory of visibility and the theory of Euler systems. Note that in Corollary 3.3, we do not assume the following hypotheses of Proposition 3.1: $p \nmid N$ (although we do need that $p^2 \nmid N$), p does not divide $|(J_0(N)/F^\vee)(\mathbf{Q})_{\mathrm{tor}}| \cdot |F(\mathbf{Q})_{\mathrm{tor}}| \cdot \prod_{\ell | N} c_\ell(F)$, and the image of the absolute Galois group of $\mathbf{Q}$ acting on $E[p]$ is isomorphic to $\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$. However, in Corollary 3.3, we do have the extra hypothesis that f and g are not congruent modulo a prime ideal over p to any other newforms of level dividing N (for Fourier coefficients of index coprime to Np). This hypothesis is used only via Lemma 4.3 below, and so if it could be removed from that lemma, then it can be removed from Theorem 3.2 and Corollary 3.3. In any case, our proof of Theorem 3.2 does not use the theory of visibility or the theory of Euler systems, and is much more elementary than either theories. In fact, our approach may be considered an alternative to the theory of Euler systems in the context where

the theory of visibility predicts non-triviality of Shafarevich-Tate groups for analytic rank zero.

4 Proof of Theorem 3.2

We work in slightly more generality in the beginning and assume that f and g are any newforms (whose Fourier coefficients need not be integers), with f having analytic rank zero and g having analytic rank greater than zero. Thus the associated newform quotients A_f and A_g need not be elliptic curves, but we will still denote them by E and F (respectively) for simplicity of notation.

Recall that $I_g = \mathrm{Ann}_{\mathbf{T}} g$. Let $J' = J/(I_f \cap I_g)J$ and let π'' denote the quotient map $J \to J'$. Then the quotient map $J \xrightarrow{\pi} E$ factors through J'; let π' denote the map $J' \to E$ in this factorization. Let F' denote the kernel of π'. Let E' denote the image of $E^\vee \subseteq J$ in J' under the quotient map $\pi'' : J \to J'$. Let B denote the kernel of the projection map $\pi : J \to E$; it is the abelian subvariety $I_f J$ of J. We have the following diagram, in which the two sequences of four arrows are exact (one horizontal and one upwards diagonal):



Now F' is connected, since it is a quotient of B (as a simple diagram chase above shows) and B is connected. Thus, by looking at dimensions, one sees that F' is the image of $F^\vee$ under π''. Since the composite $F^\vee \hookrightarrow J \to J' \to F$ is an isogeny, the quotient map $J' \to F$ induces an isogeny $\pi''(F^\vee) \sim F$, and hence an isogeny $F' \sim F$. Let E' denote $\pi''(E^\vee)$. Since π induces an isogeny from $E^\vee$ to E, we see that π' also induces an isogeny from E' to E.

Let $\Im$ denote the annihilator, under the action of $\mathbf{T}$, of the divisor $(0)-(\infty)$, considered as an element of $J_0(N)(\mathbf{C})$. 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 [Maz77, II.18.6], we have $\Im e\subseteq H_1(X_0(N),\mathbf{Z})=H_1(J_0(N),\mathbf{Z})$ (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). If ϕ is a map of abelian varieties over $\mathbf{Q}$, then we denote the induced map on the first homology groups by ϕ_*.

Lemma 4.1. $\pi''_*(\Im e)\subseteq H_1(E',\mathbf{Z})$.

Proof. Since J' is isogenous to $E'\oplus F'$, we have $H_1(J',\mathbf{Z})\otimes\mathbf{Q}\cong H_1(E',\mathbf{Z})\otimes\mathbf{Q}\oplus H_1(F',\mathbf{Z})\otimes\mathbf{Q}$. Viewing $\pi''_*(\Im e)$ as a subset of $H_1(J',\mathbf{Z})\otimes\mathbf{Q}$, it suffices to show that $\pi''_*(\Im e)\cap(H_1(F',\mathbf{Z})\otimes\mathbf{Q})=0$. Suppose $x\in\pi''_*(\Im e)\cap(H_1(F',\mathbf{Z})\otimes\mathbf{Q})$; we need to show that then $x=0$. For some integer n, we have $nx\in H_1(F',\mathbf{Z})$, and for some $t\in\Im$, we have $t\pi''_*(e)=nx$. Let ω be a differential over $\mathbf{Q}$ on F', which we may view as a differential on J'. Then $\pi''^*(\omega)$, when viewed as a differential on $X_0(N)$, is of the form $2\pi i h(z)dz$ for some h in $S_2(\Gamma_0(N),\mathbf{Q})[I_g]$. Thus $\int_{nx}\omega=\int_{t\pi''_*(e)}\omega=\int_{te}2\pi i h(z)dz=\int_e 2\pi i(th)(z)dz$. Now $th\in S_2(\Gamma_0(N),\mathbf{Q})[I_g]$, and so th is a $\mathbf{Q}$-linear combination of the Galois conjugates of g. Hence $\int_e 2\pi i(th)(z)dz$ is a $\mathbf{Q}$-linear combination of of $\int_e 2\pi i g^\sigma(z)dz=L(g^\sigma,1)$ for various conjugates g^σ of g, where $\sigma\in\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Since g has positive analytic rank, $L(g,1)=0$, and so $L(g^\sigma,1)=0$ for all $\sigma\in\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, e.g., by [GZ86, Cor. V.1.3]. Thus, by the discussion above, we see that $\int_{nx}\omega=0$ for every differential ω over $\mathbf{Q}$ on F', and so $nx=0$ in $H_1(F',\mathbf{Z})\otimes\mathbf{Q}$. Hence $x=0$, as was to be shown. □

There is a complex conjugation involution acting on $H_1(X_0(N),\mathbf{C})$, 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. It is easy to see that e is fixed by the complex conjugation involution, and so by Lemma 4.1, we have $\pi''_*(\Im e)\subseteq H_1(E',\mathbf{Z})^+$. The following is an analog of [Aga, Theorem 3.2]:

Proposition 4.2. *Up to a power of* 2,

$$c_E\cdot c_\infty(E)\cdot\frac{L_E(1)}{\Omega_E}=\frac{\left|\frac{H_1(J',\mathbf{Z})^+}{H_1(F',\mathbf{Z})^+ + H_1(E',\mathbf{Z})^+}\right|\cdot\left|\frac{H_1(E',\mathbf{Z})^+ + H_1(F',\mathbf{Z})^+}{\pi''_*(\Im e)+H_1(F',\mathbf{Z})^+}\right|}{|\pi_*(\mathbf{T}e)/\pi_*(\Im e)|}. \qquad (3)$$

Proof. By [Aga, Thm. 2.1], we have

$$\frac{L_E(1)}{\Omega_E} = \frac{[H_1(E,\mathbf{Z})^+ : \pi_*(\mathbf{T}e)]}{c_E \cdot c_\infty(E)}\ , \tag{4}$$

where $[H_1(E,\mathbf{Z})^+ : \pi_*(\mathbf{T}e)]$ denotes the absolute value of the determinant of an automorphism of $H_1(E,\mathbf{Q})$ that takes the lattice $H_1(E,\mathbf{Z})^+$ isomorphically onto the lattice $\pi_*(\mathbf{T}e)$. Now π''_* and π'_* are both surjective, since the kernels of π'' and π' (respectively) are connected. Thus $H_1(E,\mathbf{Z}) = \pi'_*(H_1(J',\mathbf{Z}))$. Putting this in (4), and considering that $\pi''_*(\Im e) \subseteq H_1(J',\mathbf{Z})^+$ (since $\Im e \subseteq H_1(J_0(N),\mathbf{Z})^+$), we get

$$c_E \cdot c_\infty(E) \cdot \frac{L_E(1)}{\Omega_E} = [\pi'_*(H_1(J',\mathbf{Z}))^+ : \pi_*(\mathbf{T}e)] = \frac{|\pi'_*(H_1(J',\mathbf{Z}))^+/\pi'_*(\pi''_*(\Im e))|}{|\pi_*(\mathbf{T}e)/\pi_*(\Im e)|}. \tag{5}$$

The long exact sequence of homology associated to the short exact sequence $0 \to F' \to J' \to E \to 0$ is:

$$\ldots \to H_1(F',\mathbf{Z}) \to H_1(J',\mathbf{Z}) \stackrel{\pi'_*}{\to} H_1(E,\mathbf{Z}) \to 0 \to \ldots$$

Thus $H_1(F',\mathbf{Z}) \subseteq \ker(\pi'_*)$.

Claim: $H_1(F',\mathbf{Z}) = \ker(\pi'_*)$.

Proof. Since $H_1(F',\mathbf{Z})$ is saturated in $H_1(J',\mathbf{Z})$, it suffices to show that $H_1(F',\mathbf{Z}) \otimes \mathbf{Q} = \ker(\pi'_*) \otimes \mathbf{Q}$, i.e., that the free abelian groups $H_1(F',\mathbf{Z})$ and $\ker(\pi'_*)$ have the same rank. But

$\operatorname{rank}(\ker(\pi'_*)) = 2 \cdot \dim J' - 2 \cdot \dim E$
$= 2 \cdot \dim_{\mathbf{Q}} S_2(\Gamma_0(N),\mathbf{Q})[I_f \cap I_g] - 2 \cdot \dim_{\mathbf{Q}} S_2(\Gamma_0(N),\mathbf{Q})[I_f]$
$= 2 \cdot \dim_{\mathbf{Q}} S_2(\Gamma_0(N),\mathbf{Q})[I_g] = 2 \cdot \dim_{\mathbf{Q}} F' = \operatorname{rank}(H_1(F',\mathbf{Z}))$.

This proves the claim. □

The kernel of the natural map $H_1(J',\mathbf{Z}) \to \pi'_*(H_1(J',\mathbf{Z}))/\pi'_*(\pi''_*(\Im e))$ is $\ker(\pi'_*) + \pi''_*(\Im e) = H_1(F',\mathbf{Z}) + \pi''_*(\Im e)$, by the claim above Thus up to a power of 2,

$$|\pi_*(H_1(J',\mathbf{Z}))^+/\pi'_*(\pi''_*(\Im e))| = \Big|\frac{H_1(J',\mathbf{Z})^+}{H_1(F',\mathbf{Z})^+ + \pi''_*(\Im e)}\Big|. \tag{6}$$

In view of Lemma 4.1,

$$\Big|\frac{H_1(J',\mathbf{Z})^+}{H_1(F',\mathbf{Z})^+ + \pi''_*(\Im e)}\Big| = \Big|\frac{H_1(J',\mathbf{Z})^+}{H_1(F',\mathbf{Z})^+ + H_1(E',\mathbf{Z})^+}\Big| \cdot \Big|\frac{H_1(E',\mathbf{Z})^+ + H_1(F',\mathbf{Z})^+}{\pi''_*(\Im e) + H_1(F',\mathbf{Z})^+}\Big|. \tag{7}$$

Putting (7) in (6), and then putting the result in (5), we get the formula in the proposition. □

Lemma 4.3. *Suppose that p satisfies hypothesis (*), and assume that f and g have integer Fourier coefficients (so $E^\vee$ and $F^\vee$ are elliptic curves). Assume moreover that f and g are not congruent modulo a prime ideal over p to any other newforms of level dividing N (for Fourier coefficients of index coprime to Np). Then $E'[r] = F'[r]$, and both are direct summands of $E' \cap F'$ as $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules.*

Proof. By the proof of [Aga09, Lemma 2.2], $(E^\vee \cap F^\vee)[p^\infty] = E^\vee[r] = F^\vee[r]$. The kernels of the surjective maps $E^\vee \to E'$, $F^\vee \to F'$, and $E^\vee \cap F^\vee \to E' \cap F'$ that are induced by π'' are all contained in $J'^\vee \cap IJ$. By [ARS06, Theorem 3.6(a)] with $A = J'^\vee$, if a prime ℓ divides the order of $J'^\vee \cap IJ$, then ℓ divides the congruence exponent of $J'^\vee$ (with notation as in loc. cit.). By the hypothesis that f and g are not congruent modulo a prime ideal over p to any other newforms of level dividing N (for Fourier coefficients of index coprime to Np), the congruence exponent of $J'^\vee$ is coprime to p. Hence the kernels of the maps mentioned above have orders coprime to p. Thus the maps $E^\vee \to E'$, $F^\vee \to F'$, and $E^\vee \cap F^\vee \to E' \cap F'$ are all isomorphisms on p^n torsion points for any positive integer n (this can be seen, e.g., by the snake lemma applied to the multiplication by p^n map on the corrsponding short exact sequence in each situation). In particular the maps $(E^\vee \cap F^\vee)[p^\infty] \to (E' \cap F')[p^\infty]$, $E^\vee[r] \to E'[r]$, and $F^\vee[r] \to F'[r]$ are isomorphisms. From this and the very first statement in this proof, we see that $(E' \cap F')[p^\infty] = E'[r] = F'[r]$. The lemma now follows from the conclusion of the previous sentence. □

Proof of Theorem 3.2. Note that since F has positive Mordell-Weil rank, g has positive analytic rank (by [KL89]), and so the discussion of this section applies. By Proposition 4.2, we see that up to a power of 2,

$$\begin{aligned} & |E(\mathbf{Q})|^2 \cdot \frac{L_E(1)}{\Omega_E} \qquad (8) \\ = \; & \frac{|\frac{H_1(J',\mathbf{Z})^+}{H_1(F',\mathbf{Z})^+ + H_1(E',\mathbf{Z})^+}| \cdot |\frac{H_1(E',\mathbf{Z})^+ + H_1(F',\mathbf{Z})^+}{\pi''_*(\Im e) + H_1(F',\mathbf{Z})^+}|}{c_E \cdot c_\infty(E)} \cdot \frac{|E(\mathbf{Q})|}{|\pi_*(\mathbf{T}e)/\pi_*(\Im e)|} \cdot |E(\mathbf{Q})|. \end{aligned}$$

By Lemma 4.3, we see that r^2 divides $|E' \cap F'|$. By [Aga, Lemma 4.1], we have $|\frac{H_1(J',\mathbf{Z})}{H_1(F',\mathbf{Z})+H_1(E',\mathbf{Z})}| = |E' \cap F'|$, and so r^2 divides $|\frac{H_1(J',\mathbf{Z})}{H_1(F',\mathbf{Z})+H_1(E',\mathbf{Z})}|$. If H is an abelian group on which the complex conjugation involution c acts, then let H^- denote the subgroup of elements x of H such that $cx = -x$. Let

H be a group as in the previous sentence. Then $(1+c)H \subseteq H^+$ and $(1-c)H \subseteq H^+$. Also, if $x \in H$, then $2x = (1+c)x + (1-c)x$ is in the sum of the subgroups $(1+c)H$ and $(1-c)H$; moreover, these latter two subgroups are isomorphic. Thus we see that on tensoring with $\mathbf{Z}[1/2]$, H^+ and H^- become isomorphic, and their sum becomes H. Applying this discussion with $H = H_1(J', \mathbf{Z}), H_1(F', \mathbf{Z})$, and $H_1(E', \mathbf{Z})$, we see that $|\frac{H_1(J', \mathbf{Z})}{H_1(F', \mathbf{Z}) + H_1(E', \mathbf{Z})}|$ is the square of $|\frac{H_1(J', \mathbf{Z})^+}{H_1(F', \mathbf{Z})^+ + H_1(E', \mathbf{Z})^+}|$, up to a power of 2. Considering that r is odd and r^2 divides $|\frac{H_1(J', \mathbf{Z})}{H_1(F', \mathbf{Z}) + H_1(E', \mathbf{Z})}|$, it follows that r divides the term $|\frac{H_1(J', \mathbf{Z})^+}{H_1(F', \mathbf{Z})^+ + H_1(E', \mathbf{Z})^+}|$ on the right side of (8). The theorem now follows from equation (8), in view of the facts that $|\pi_*(\mathbf{T}e)/\pi_*(\Im e)|$ divides $|E(\mathbf{Q})|$ (by [Aga, Lemma 3.3]), c_E is coprime to p if $p^2 \nmid N$ (by [Maz78, Cor. 4.1]), and $c_\infty(E)$ is a power of 2, hence coprime to r. □

Remark 4.4. We would like to take the chance to make some corrections to our earlier paper [Aga09]. First, the statement of the first part of Proposition 3.1 of loc. cit. should read:
"Suppose that p is coprime to

$$N \cdot |(J_0(N)/F^\vee)(K)_{\mathrm{tor}}| \cdot |F(K)_{\mathrm{tor}}| \cdot \prod_{\ell | N} \big(c_\ell(F) \cdot c_\ell(E)\big).$$

Then r divides $|Ш(E/K)|$".

The proof of the statement above is identical to the proof of Part (i) of Proposition 2.2 in this article, with $\mathbf{Q}$ replaced by K. As a result of this correction, the statement of Proposition 4.1 of [Aga09] should change to:
"Suppose that p is coprime to

$$2 \cdot N \cdot |(J_0(N)/F^\vee)(K)_{\mathrm{tor}}| \cdot |F(K)_{\mathrm{tor}}| \cdot \prod_{\ell | N} \big(c_\ell(F) \cdot c_\ell(E)\big).$$

Assume that the image of the absolute Galois group of $\mathbf{Q}$ acting on $E[p]$ is isomorphic to $\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$. Then r divides $|E(K)/\mathbf{Z}\pi(P)|^2$".

The statement above follows from the corrected version of Proposition 3.1 mentioned above, and from the paragraph just after the statement of Theorem 1.1 in [Jet08].

Finally, in the fourth paragraph of Section 5 of loc. cit., we claimed that "since $E^\vee[r] = F^\vee[r]$ and both are direct summands of $E^\vee \cap F^\vee$ as $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules, on applying π'' we find that $E'[r] = F'[r]$ and both are direct summands of $E' \cap F'$ as $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules". Since it may not

be true that $\pi''(E^\vee[r]) = E'[r]$ or $\pi''(F^\vee[r]) = F'[r]$, our claim was not justified. The claim does hold however, by Lemma 4.3, under the extra hypothesis that f and g are not congruent modulo a prime ideal over p to any other newforms of level dividing N for Fourier coefficients of index coprime to Np (note that in the proof of Lemma 4.3, the analytic or Mordell-Weil ranks of f and g do not play any role). As a result, the statements of Theorem 4.4, Corollary 4.5, and Corollary 4.6 of [Aga09] need the extra hypothesis mentioned in the previous sentence to be sure that they are valid.

References

[Aga] A. Agashe, *A visible factor of the special L-value*, to appear in J. Reine Angew. Math. (Crelle's journal), available at arXiv:0810.2477 or
`http://www.math.fsu.edu/~agashe/math.html`.

[Aga09] _____, *Visibility and the Birch and Swinnerton-dyer conjecture for analytic rank one*, Int. Math. Res. Not. (2009), doi: 10.1093/imrn/rnp036 (electronic; print version to appear); available at arXiv:0810.2487 or
`http://www.math.fsu.edu/~agashe/math.html`.

[ARS06] A. Agashe, K. Ribet, and W. A. Stein, *The modular degree, congruence primes, and multiplicity one*, to appear in a special volume in honor of Serge Lang (2006), available at
http://www.math.fsu.edu/~agashe/math.html.

[AS02] A. Agashe and W. A. 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.

[AU96] Ahmed Abbes and Emmanuel Ullmo, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires*, Compositio Math. **103** (1996), no. 3, 269–286. MR 97f:11038

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

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

[GZ86] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320. MR 87j:11057

[Jet08] Dimitar Jetchev, *Global divisibility of Heegner points and Tamagawa numbers*, Compos. Math. **144** (2008), no. 4, 811–826.

[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.

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

[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.

[Rib90] K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476.

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

[SW08] W. Stein and C. Wuthrich, *Computations about Tate-Shafarevich groups using Iwasawa theory*, preprint (2008), available at `http://modular.math.washington.edu/papers`.