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

Amod Agashe *

February 20, 2009

Abstract

Let E be an optimal elliptic curve over $\mathbf{Q}$ of conductor N having analytic rank one, i.e., such that the L-function $L_E(s)$ of E vanishes to order one at $s = 1$. Let K be a quadratic imaginary field in which all the primes dividing N split and such that the L-function of E over K vanishes to order one 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 one and whose associated newform is congruent to the newform associated to E modulo an integer r. The theory of visibility then shows that under certain additional hypotheses, r divides the product of the order of the Shafarevich-Tate group of E over K and the orders of the arithmetic component groups of E. We extract an explicit integer factor from 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 one 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

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

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 $L(f, s)$. The analytic rank of A_f is then the analytic rank of f times the dimension of A_f. Now suppose that the newform f has integer Fourier coefficients. Then A_f is an elliptic curve, and we denote it by E instead. Since E has dimension one, it has analytic rank one.

Let K be a quadratic imaginary field of discriminant not equal to -3 or -4, and such that all primes dividing N split in K. Choose an ideal $\mathcal{N}$ of the ring of integers $\mathcal{O}_K$ of K such that $\mathcal{O}_K/\mathcal{N} \cong \mathbf{Z}/N\mathbf{Z}$. Then the complex tori $\mathbf{C}/\mathcal{O}_K$ and $\mathbf{C}/\mathcal{N}^{-1}$ define elliptic curves related by a cyclic N-isogeny, and thus give a complex valued point x of $X_0(N)$. This point, called a Heegner point, is defined over the Hilbert class field H of K. Let $P \in J(K)$ be the class of the divisor $\sum_{\sigma \in \mathrm{Gal}(H/K)} ((x) - (\infty))^\sigma$, where H is the Hilbert class field of K.

By [Wal85], we may choose K so that $L(E/K, s)$ vanishes to order one at $s = 1$. Hence, by [GZ86, §V.2:(2.1)], $\pi(P)$ has infinite order, and by work of Kolyvagin, $E(K)$ has rank one and the order of the Shafarevich-Tate group $Ш(E/K)$ of E over K is finite (e.g., see [Kol90, Thm. A] or [Gro91, Thm. 1.3]). In particular, the index $[E(K) : \mathbf{Z}\pi(P)]$ is finite. By [GZ86, §V.2:(2.2)] (or see [Gro91, Conj. 1.2]), the second part of the Birch and Swinnerton-Dyer (BSD) conjecture becomes:

Conjecture 1.1 (Birch and Swinnerton-Dyer, Gross-Zagier)**.**

$$|E(K)/\mathbf{Z}\pi(P)| \stackrel{?}{=} c_E \cdot \prod_{\ell | N} c_\ell(E) \cdot \sqrt{|Ш(E/K)|}, \tag{1}$$

where c_E is the Manin constant of E, $c_\ell(E)$ denotes the arithmetic component group of E at the prime ℓ, and the question mark above the equality sign emphasizes that this equality is conjectural.

Note that the Manin constant c_E is conjectured to be one, and one knows 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]).

Now suppose that f is congruent modulo a prime p to another newform g with integer Fourier coefficients, whose associated elliptic curve F has Mordell-Weil rank over $\mathbf{Q}$ bigger than one. 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 $\prod_{\ell | N} c_\ell(E) \cdot \sqrt{|Ш(E/K)|}$,

which in turn divides the right side of (1); we give precise results along these lines in Section 3. When this happens, the conjectural formula (1) says that r should also divide the index $|E(K)/\mathbf{Z}\pi(P)|$, which is the left side of (1). In Section 4, we extract an explicit integer factor from the index $|E(K)/\mathbf{Z}\pi(P)|$ (see Corollary 4.3), and under hypotheses similar to the ones made in the results coming from visibility, we show that r divides this integer factor (see Theorem 4.4). In fact, the only primes that can divide this factor are the ones modulo which f and g are congruent. Finally, in Section 5 we give the proof of our main result (Theorem 4.4). Section 2 is concerned with proving some results about the equality of r-torsion in the duals of E and F under a certain multiplicity one hypotheses; these results in turn are used to give examples where certain hypotheses in Sections 3 and 4 hold. The reader who is interested in seeing only the precise statements of our main results may read Sections 2, 3, and 4, skipping proofs and remarks. Note that in each section, we continue to use the notation introduced in earlier sections (unless mentioned otherwise).

Acknowledgements: We would like to thank the Tata Institute of Fundamental Research for their kind hospitality during a visit when the author worked on this paper.

2 Multiplicity one

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 $J_0(N)$. The goal of this section is to give conditions under which $E^\vee[r] = F^\vee[r]$, which is a hypothesis that is used in Sections 3 and 4. This section may be of interest independent of results in the rest of this article.

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.

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 (*).

Proof. If $p \nmid N$, then the claim follows from Theorem 5.2(b) of [Rib90], so let us assume that $p||N$. Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}$ with residue characteristic p that is in the support of $J_0(N)[I_f+I_g]$. Then $\mathfrak{m}$ contains I_f+I_g, hence it also contains I_f and I_g. By the proof of Corollary 1.4 of [Aga08a], the hypothesis that either $E[p]$ or $F[p]$ is irreducible implies that the canonical semi-simple representation $\rho_{\mathfrak{m}}$ associated to $\mathfrak{m}$ (see, e.g., [Rib90, Prop. 5.1] for the definition of $\rho_{\mathfrak{m}}$) is irreducible. In view of this, Proposition 1.3 of [Aga08a] tells us that $\mathfrak{m}$ satisfies multiplicity one. □

Lemma 2.2. *Suppose p satisfies hypothesis (*). Then $E^\vee[r] = F^\vee[r]$, and both are direct summands of $E^\vee \cap F^\vee$ as $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules.*

Proof. By [Eme03, Cor. 2.5], if $\mathfrak{m}$ satisfies multiplicity one and I is any saturated ideal of $\mathbf{T}$, then the $\mathfrak{m}$-adic completion of the group of connected components of $J_0(N)[I]$ is trivial. If $L \to M$ is a homomorphism of two $\mathbf{T}$-modules, then we say that $L = M$ *away from* a given set of maximal ideals if the induced map on the $\mathfrak{m}$-adic completions is an isomorphism for all maximal ideals $\mathfrak{m}$ that are not in the prescribed set. Thus, the inclusions $E^\vee \subseteq J_0(N)[I_f]$ and $F^\vee \subseteq J_0(N)[I_g]$ are equalities away from maximal ideals that do not satisfy multiplicity one.
Claim: Then $E^\vee \cap F^\vee \subseteq J_0(N)[I_f + I_g]$ is an equality away from maximal ideals that do not satisfy multiplicity one.

Proof. Consider the natural map $F^\vee \cap J_0(N)[I_f] \to J_0(N)[I_f]/E^\vee$. It's kernel is $F^\vee \cap J_0(N)[I_f] \cap E^\vee = F^\vee \cap E^\vee$, and hence we have an injection:

$$\frac{F^\vee \cap J_0(N)[I_f]}{F^\vee \cap E^\vee} \hookrightarrow \frac{J_0(N)[I_f]}{E^\vee}. \tag{2}$$

Also, the natural map $J_0(N)[I_f + I_g] = J_0(N)[I_g][I_f] \to J_0(N)[I_g]/F^\vee$ has kernel $F^\vee \cap J_0(N)[I_g][I_f] = F^\vee \cap J_0(N)[I_f]$, and hence we have an injection

$$\frac{J_0(N)[I_f + I_g]}{F^\vee \cap J_0(N)[I_f]} \hookrightarrow \frac{J_0(N)[I_g]}{F^\vee} \tag{3}$$

The claim follows from equations (2) and (3), considering that the Hecke modules on the right sides of the two equations are supported on the set of maximal ideals of $\mathbf{T}$ that do not satisfy multiplicity one (by the statment just before the claim). □

Now $E^\vee \cap F^\vee \subseteq E^\vee[I_f + I_g] \subseteq J_0(N)[I_f + I_g]$. Hence if m denotes the largest integer such that f and g are congruent modulo m, then $E^\vee \cap F^\vee \subseteq$

$E^\vee[I_f + I_g] = E^\vee[m]$ is an equality away from the maximal ideals in the support of $J_0(N)[I_f + I_g]$ that do not satisfy multiplicity one. Similarly $E^\vee \cap F^\vee \subseteq F^\vee[I_f + I_g] = F^\vee[m]$ is an equality away from the maximal ideals in the support of $J_0(N)[I_f + I_g]$ that do not satisfy multiplicity one. From the hypotheses (*) on p and the definition of r, it follows then that $(E^\vee \cap F^\vee)[p^\infty] = E^\vee[r] = F^\vee[r]$. Thus $E^\vee[r]$ and $F^\vee[r]$ are identical and are direct summands of $E^\vee \cap F^\vee$ as $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules. □

3 Results from the theory of visibility

Proposition 3.1. *(i) Suppose that p is coprime to*

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

Then r divides $\prod_{\ell|N} c_\ell(E) \cdot \sqrt{|Ш(E/K)|}$, which in turn divides the right hand side of the Birch and Swinnerton-Dyer conjectural formula (1).
(ii) Suppose that f is congruent to g modulo an odd prime q such that $E[q]$ and $F[q]$ are irreducible and q does not divide

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

Also, assume that f is not congruent modulo q to a newform of a level dividing N/ℓ for some prime ℓ that divides N (for Fourier coefficients of index coprime to Nq), and either $q \nmid N$ or for all primes ℓ that divide N, $q \nmid (\ell - 1)$. Then q divides $|Ш(E/K)|$.

Proof. Both results follow essentially from Theorem 3.1 of [AS02]. For the first part, 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 Lemmas 2.1 and 2.2, considering that $p \nmid N$ by hypothesis, and that the rank of $E^\vee(K)$ is less than the rank of $F^\vee(K)$. For the second part, take $A = E^\vee$, $B = F^\vee$, and $n = q$ in [AS02, Thm. 3.1], and note that the congruence of f and g modulo q forces $F^\vee[q] = E^\vee[q]$ by [Rib90, Thm. 5.2] (cf. [CM00, p. 20]), and that the hypotheses imply that q 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 q divides $c_\ell(E)$ for some prime ℓ that divides N, then for some maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ having characteristic q and containing I_f, either $\rho_\mathfrak{m}$ is finite or reducible. Since $E[q]$ 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 q to a newform of a level dividing N/ℓ for any prime ℓ that divides N (for Fourier coefficients

of index coprime to Nq), and either $q \nmid N$ or for all primes ℓ that divide N, $q \nmid (\ell - 1)$. Thus q does not divide $c_\ell(E)$ for any prime ℓ that divides N. Similarly, q does not divide $c_\ell(F)$ for any prime ℓ that divides N, considering that the hypothesis that f is not congruent modulo q to a newform of a level dividing N/ℓ for any prime ℓ that divides N (for Fourier coefficients of index coprime to Nq) applies to g as well, since g is congruent to f modulo q. This finishes the proof of the proposition. □

Remark 3.2. One might wonder how often it happens in numerical data that visibility explains the Shafarevich-Tate group of an elliptic curve of analytic rank one. Since it is difficult to compute the actual order of the Shafarevich-Tate group, we looked at the Birch and Swinnerton-Dyer conjectural orders in Cremona's online "Elliptic curve data" [Cre]. For levels up to 30000, we found only one optimal elliptic curve of Mordell-Weil rank one for which the conjectural order of the Shafarevich-Tate group was divisible by an odd prime: the curve with label 28042A, for which the conjectural order of the Shafarevich-Tate group is 9. At the same level, the curve 28042B has Mordell-Weil rank 3 and the newforms corresponding to 28042A and 28042B have Fourier coefficients that are congruent modulo 3 for every prime index up to 100. While this is not enough to conclude that the newforms are congruent modulo 3 for all Fourier coefficients (cf. [AS]), it is quite likely that this is true and that this congruence explains the nontrivial Shafarevich-Tate group, although we have not checked the details (in particular whether the hypotheses of Proposition 3.1 are satisfied), since our goal in this paper is to prove *theoretical* results. It would be interesting to do systematic computations to see how much of the Birch and Swinnerton-Dyer conjectural order of the Shafarevich-Tate group is explained by visibility for elliptic curves of analytic rank one (similar to the computations in [AS05] for the analytic rank zero case).

4 A visible factor

Considering that under certain hypotheses, the theory of visibility (more precisely Proposition 3.1(i)) implies that r divides divides $\prod_{\ell | N} c_\ell(E) \cdot \sqrt{|Ш(E/K)|}$, which in turn divides the right hand side of the Birch and Swinnerton-Dyer conjectural formula (1), under similar hypotheses, one should be able to show that r also divides $|E(K)/\mathbf{Z}\pi(P)|$, which is the left hand side of (1). Now the theory of Euler systems says under certain hypotheses that the order of $Ш(E/K)$ divides its Birch and Swinnerton-Dyer conjectural order (e.g., see [Kol90, Thm. A]). Thus, in conjunction with Proposition 3.1, the

theory of Euler systems shows that under certain additional hypotheses, r does divides $|E(K)/\mathbf{Z}\pi(P)|$. For example, we have the following:

Proposition 4.1. *Suppose that p is coprime to*

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

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

Proof. Proposition 3.1, which uses the theory of visibility, implies that r divides $\prod_{\ell|N} c_\ell(E) \cdot \sqrt{|Ш(E/K)|}$. The result now follows from [Jet07, Cor. 1.5], which uses the theory of Euler systems. □

In this section, we extract an explicit integer factor from $|E(K)/\mathbf{Z}\pi(P)|$, and show that under certain hypotheses, r divides this factor. These hypotheses in particular do not include the hypotheses needed in the theory of Euler systems that $p \nmid N$, that p divides at most one $c_\ell(E)$, and that the image of the absolute Galois group of $\mathbf{Q}$ acting on $E[p]$ is isomorphic to $\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$, nor the hypotheses needed in the theory of visibility that p does not divide $N \cdot |F(K)_{\mathrm{tor}}| \cdot \prod_{\ell|N} c_\ell(F)$. Also, our proof 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 one.

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'. Thus we have the following diagram:

$$\begin{array}{ccccccccc} & & & & J & & & & \\ & & & & \downarrow{\scriptstyle \pi''} & \searrow{\scriptstyle \pi} & & & \\ 0 & \longrightarrow & F' & \longrightarrow & J' & \xrightarrow{\pi'} & E & \longrightarrow & 0 \end{array}$$

Proposition 4.2. *We have*

$$|E(K)/\pi(\mathbf{T}P)| = \left| \frac{J'(K)}{F'(K) + \pi''(\mathbf{T}P)} \right| \cdot |\ker\big(H^1(K, F') \to H^1(K, J')\big)|. \quad (4)$$

Proof. Consider the exact sequence $0 \to F' \to J' \to E \to 0$. Part of the associated long exact sequence of Galois cohomology is

$$0 \to F'(K) \to J'(K) \xrightarrow{\pi'} E(K) \xrightarrow{\delta} H^1(K, F') \to H^1(K, J') \to \cdots, \tag{5}$$

where δ denotes the boundary map. Note that in this proof, the letters π' and π'' denote π' and π'' restricted to the K-valued points in their domain. Since $\pi''(\mathbf{T}P) \subseteq J'(K)$, by the exactness of (5) we see that $\delta(\pi'(\pi''(\mathbf{T}P))) = 0$. Using the exactness of (5) again, we see that δ thus induces a surjection

$$\phi : E(K)/\pi'(\pi''(\mathbf{T}P)) \to \ker\big(H^1(K, F') \to H^1(K, J')\big).$$

Since $\pi'(J'(K)) \subseteq \ker(\delta)$, we see that π' induces a natural map $\psi : J'(K) \to \ker(\phi)$.

Claim: ψ is surjective and its kernel is $F'(K) + \pi''(\mathbf{T}P)$.

Proof. Let $x \in J'(K)$. Then

$$\begin{aligned} x \in \ker(\psi) &\iff \pi'(x) = 0 \in \ker(\phi) \hookrightarrow E(K)/\pi'(\pi''(\mathbf{T}P)) \\ &\iff \pi'(x) \in \pi'(\pi''(\mathbf{T}P)) \\ &\iff \exists t \in \mathbf{T} : x - \pi''(tP) \in \ker(\pi') = F'(K) \\ &\iff x \in F'(K) + \pi''(\mathbf{T}P). \end{aligned}$$

Thus $\ker(\psi) = F'(K) + \pi''(\mathbf{T}P)$. To prove surjectivity of ψ, note that given an element of $\ker(\phi)$, we can write the element as $y + \pi'(\pi''(\mathbf{T}P))$ for some $y \in E(K)$ such that $\delta(y) = 0$. Then by the exactness of (5), $y \in \mathrm{Im}(\pi')$, hence $y + \pi'(\pi''(\mathbf{T}P)) \in \mathrm{Im}(\psi)$. This proves the claim. □

By the discussion above, we get an exact sequence:

$$0 \to \frac{J'(K)}{F'(K) + \pi''(\mathbf{T}P)} \xrightarrow{\psi'} \frac{E(K)}{\pi'(\pi''(\mathbf{T}P))} \xrightarrow{\phi} \ker\big(H^1(K, F') \to H^1(K, J')\big) \to 0, \tag{6}$$

where ψ' is the natural map induced by ψ. Now

$$|E(K)/\pi'(\pi''(\mathbf{T}P))| = |E(K)/\pi(\mathbf{T}P)|,$$

and the latter group is finite in our situation. Hence all groups in (6) are finite, and Proposition 4.2 now follows from the exactness of (6). □

Let E' denote the image of $E^\vee \subseteq J$ in J' under the quotient map $\pi'' : J \to J'$ and let $\pi''(\mathbf{T}P)_f$ denote the free part of $\pi''(\mathbf{T}P)$. The following result is essentially repeated from [Aga08b]:

Corollary 4.3. *We have $\pi''(\mathbf{T}P)_f \subseteq E'(K)$ with finite index, and*

$$\begin{aligned} & |E(K)/\pi(\mathbf{T}P)| \qquad (7) \\ = & \left|\frac{J'(K)}{F'(K)+E'(K)}\right| \cdot \left|\ker\big(H^1(K,F')\to H^1(K,J')\big)\right| \cdot \frac{\left|\frac{F'(K)+E'(K)}{F'(K)+\pi''(\mathbf{T}P)_f}\right|}{\left|\frac{F'(K)+\pi''(\mathbf{T}P)}{F'(K)+\pi''(\mathbf{T}P)_f}\right|} \ . \end{aligned}$$

Proof. If h is an eigenform of weight 2 on $\Gamma_0(N)$, then $\mathbf{T}P \cap A_h^\vee(K)$ is infinite if and only if h has analytic rank one (this follows by [GZ86, Thm 6.3] if h has analytic rank bigger than one, and the fact that $A_h^\vee(K)$ is finite if h has analytic rank zero, by [KL89]). The composite $E^\vee \stackrel{\pi''}{\to} E' \stackrel{\pi'}{\to} E$ is an isogeny, and so J' is isogenous to $E' \oplus F'$. Considering that F' has analytic rank greater than one, we see that the free part of $E'(K)$ contains $\pi''(\mathbf{T}P)_f$. The corollary now follows from equation (4). We remark that the transition from equation (4) to equation (7) is analogous to the situation in the rank one case (cf. Theorem 3.1 of [Aga07] and its proof), where the idea is due to L. Merel. □

The reason for the factoring $|E(K)/\pi(\mathbf{T}P)|$, which is the left side of the Birch and Swinnerton-Dyer conjectural formula (1), as in equation (7) is the following:

Theorem 4.4. *Suppose that $E^\vee[r] = F^\vee[r]$, and both are direct summands of $E^\vee \cap F^\vee$ as $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules. Then r divides the product*

$$\left|\frac{J'(K)}{F'(K)+E'(K)}\right| \cdot \left|\ker\big(H^1(K,F')\to H^1(K,J')\big)\right| \ . \qquad (8)$$

We will prove this theorem in Section 5. We remark that by Prop. 1.3 of our companion paper [Aga08b], if a prime q divides the product above, then q divides the order of the intersection $E^\vee \cap F^\vee$; in particular, f and g are congruent modulo q (e.g., by [ARS06, Thm 3.6(a)]), which is a partial converse to the theorem above. Also, by Theorem 1.4 of [Aga08b], if a prime q divides the product in (8), then under certain hypotheses (the most serious of which is the first part of the Birch and Swinnerton-Dyer conjecture on rank), it follows from the theory of visibility that q divides $\sqrt{|Ш(E/K)|} \cdot \prod_{\ell|N} c_\ell(E)$. For this reason we call the product in (8) a visible factor, and this is the factor we alluded to in the abstract.

Corollary 4.5. *(i) Suppose that the prime p satisfies hypothesis (*) and that p is coprime to the order of the torsion subgroup of the projection of $\mathbf{T}P$ in $J_0(N)/(I_f \cap I_g)J_0(N)$. Then r divides $|E(K)/\mathbf{Z}\pi(P)|$, which is the left*

hand side of the Birch and Swinnerton-Dyer conjectural formula (1).
(ii) Suppose p is odd, p is coprime to the order of the torsion subgroup of the projection of $\mathbf{T}P$ in $J_0(N)/(I_f \cap I_g)J_0(N)$, and either
(a) $p \nmid N$ or
(b) $p||N$ and $E[p]$ or $F[p]$ is irreducible.
Then r divides $|E(K)/\mathbf{Z}\pi(P)|$, which is the left hand side of the Birch and Swinnerton-Dyer conjectural formula (1).

Proof. We first prove part (i). By Lemma 2.2, the hypothesis that p satisfies (*) implies the hypothesis in Theorem 4.4 that $E^\vee[r] = F^\vee[r]$ and both are direct summands of $E^\vee \cap F^\vee$ as $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules. The second hypothesis on p implies that r is coprime to the term $\left|\frac{F'(K)+\pi''(\mathbf{T}P)}{F'(K)+\pi''(\mathbf{T}P)_f}\right|$ in equation (7). Part (i) now follows from equation (7) and Theorem 4.4. Part (ii) follows from Part (i) considering that the hypothesis (*) is satisfied, in view of Lemma 2.1. □

Corollary 4.6. *Suppose q is an odd prime such that $q^2 \nmid N$, $E[q]$ and $F[q]$ are irreducible, and q does not divide $|J_0(N)(K)_{\mathrm{tor}}|$. Let m denote the highest power of q modulo which f and g are congruent. Then m divides $|E(K)/\mathbf{Z}\pi(P)|$. If moreover, f is not congruent modulo q to a newform of a level dividing N/ℓ for some prime ℓ that divides N (for Fourier coefficients of index coprime to Nq), and either $q \nmid N$ or for all primes ℓ that divide N, $q \nmid (\ell - 1)$, then m divides the Birch and Swinnerton-Dyer conjectural order of $Ш(E/K)$.*

Proof. Take $p = q$ in Corollary 4.5(i). By Lemma 2.1, q satisfies hypothesis (*). The hypothesis that q does not divide $|J_0(N)(K)_{\mathrm{tor}}|$ implies the hypothesis in Corollary 4.5(i) that p is coprime to the order of the torsion subgroup of the projection of $\mathbf{T}P$ in $J_0(N)/(I_f \cap I_g)J_0(N)$. Hence by Corollary 4.5(i), m divides $|E(K)/\mathbf{Z}\pi(P)|$. As explained in the proof of Proposition 3.1(ii), the hypotheses imply that q does not divide $c_\ell(E)$ for any prime ℓ. Also, by [Maz78, Cor. 4.1], q does not divide the Manin constant c_E. Hence, by (1), m divides the Birch and Swinnerton-Dyer conjectural order of $Ш(E/K)$. □

In view of Proposition 3.1, Corollaries 4.5(ii) and 4.6 provide theoretical evidence towards the Birch and Swinnerton-Dyer conjectural formula (1). We remark that Corollary 4.5(ii) is to be compared to part (i) of Proposition 3.1 and Corollary 4.6 to part (ii) of Proposition 3.1. Regarding the hypothesis in Corollary 4.6 that q does not divide $|J_0(N)(K)_{\mathrm{tor}}|$, we do not know of any results that would give some criteria on q which would imply

that this hypothesis holds (unlike the similar situation over $\mathbf{Q}$, where at least for prime N, we know by [Maz77, Thm (1)] that $|J_0(N)(\mathbf{Q})_{\mathrm{tor}}|$ equals the numerator of $\frac{N-1}{12}$). As in Corollary 4.5, we could have replaced this hypothesis by the requirement that p is coprime to the order of the torsion subgroup of the projection of $\mathbf{T}P$ in $J_0(N)/(I_f \cap I_g)J_0(N)$. Note that there is some similarity between these hypotheses and the hypothesis in Proposition 3.1 that p does not divide $|(J_0(N)/F^\vee)(K)_{\mathrm{tor}}|$. In any case, our discussion just above emphasizes the need to study the torsion in $J_0(N)$ and its quotients over number fields other than $\mathbf{Q}$.

Our Corollary 4.5(ii) may be compared to the similar Proposition 4.1 that uses the theory of visibility and the theory of Euler systems. Note that in our corollary, we do not assume the following hypotheses of Proposition 4.1: $p \nmid N$ (although we do need that $p^2 \nmid N$), p divides at most one $c_\ell(E)$, p does not divide $|F(K)_{\mathrm{tor}}| \cdot \prod_{\ell|N} c_\ell(F)$, and the image of the absolute Galois group of $\mathbf{Q}$ acting on $E[p]$ is isomorphic to $\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$. We do have the hypothesis in Corollary 4.5(ii) that p is coprime to the order of the torsion subgroup of the projection of $\mathbf{T}P$ in $J_0(N)/(I_f \cap I_g)J_0(N)$, but this is somewhat similar to the hypothesis in in Proposition 4.1 that p does not divide $|(J_0(N)/F^\vee)(K)_{\mathrm{tor}}|$.

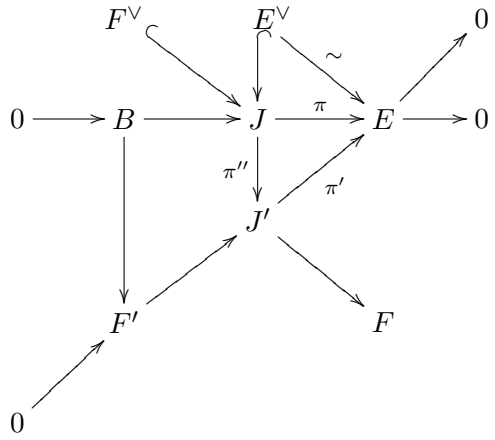
5 Proof of Theorem 4.4

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). 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 $J' = J/(I_f \cap I_g)J$, E' is the image of $E^\vee$ in J' under the projection map $\pi'' : J \to J'$, π' denotes the projection $J' \to A_f = E$, and $F' = \ker \pi'$. Our goal is to show that r divides

$$\left| \frac{J'(K)}{F'(K) + E'(K)} \right| \cdot \left| \ker\big(H^1(K, F') \to H^1(K, J')\big) \right| . \tag{9}$$

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):

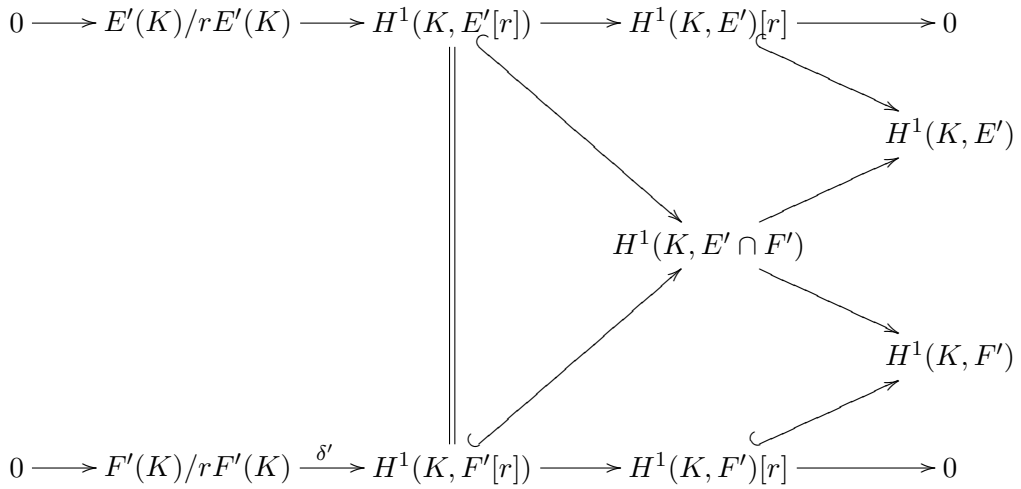


Now F' is connected, since it is a quotient of B (as a simple diagram chase above shows) and B is connected. Thus, by looking at dimensions, one sees that F' is the image of $F^\vee$ under π''. Since the composite $F^\vee \hookrightarrow J \to J' \to F$ is an isogeny, the the quotient map $J' \to F$ induces an isogeny $\pi''(F^\vee) \sim F$, and hence an isogeny $F' \sim F$. Thus F' and F have the same rank (over $\mathbf{Q}$ or over K). 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. Thus E' and E have the same rank (over $\mathbf{Q}$ or over K).

Now we impose the assumption that f and g have integer Fourier coefficients, so that E and F are elliptic curves. Recall that we are assuming that $E^\vee[r] = F^\vee[r]$ and that 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. In particular, the natural maps $H^1(K, E'[r]) \to H^1(K, E' \cap F')$ and $H^1(K, F'[r]) \to H^1(K, E' \cap F')$ are injections. Recall that E has analytic rank one and F has Mordell-Weil rank more than one. Then the abelian group $F(K)$ has rank more than one, and as remarked just before Conjecture 1, the abelian group $E(K)$ has rank one. Also, note that the newform g has analytic rank greater than one, since otherwise the Mordell-Weil rank of F would be at most one. With an eye towards potential generalizations, we remark that after this paragraph, we will not explicitly use the fact that E and F have dimension one (i.e., are elliptic curves). Thus if the conclusions of this paragraph are satisfied, then the rest of the argument would go through even if E and F have dimension greater than one.

Consider the following commutative diagram, where the top and bottom rows are the Kummer exact sequences of E' and F' respectively, and the

other maps are the obvious natural maps:



Let Q be a generator for the free part of $E'(K)$ (which is isomorphic to the free part of $E(K)$). Then from the top exact sequence in the diagram above, we see that Q gives rise to a non-trivial element σ in $H^1(K, E'[r])$.

Let r' be the smallest positive integer such that $r'\sigma \in \delta'(F'(K)/rF'(K))$ (where δ' is the boundary map in the Kummer exact sequence associated to F', as indicated in the diagram above). Thus r' divides r (since $r\sigma = 0 \in \delta'(F'(K)/rF'(K))$). Then, by the top and bottom exact sequences in the diagram above, $r'\sigma$ maps to the trivial element in both $H^1(K, E')[r]$ and $H^1(K, F')[r]$, and hence in $H^1(K, E')$ and $H^1(K, F')$. The image of $r'\sigma$ in $H^1(K, E' \cap F')$ is then a non-trivial element of order r/r' that dies in $H^1(K, F')$ and in $H^1(K, E')$. Thus we see that r/r' divides the order of $\ker(H^1(K, E' \cap F') \to H^1(K, E' \oplus F'))$.

Lemma 5.1. *We have*

$$\frac{J'(K)}{F'(K) + E'(K)} \cong \ker\big(H^1(K, E' \cap F') \to H^1(K, E' \oplus F')\big).$$

Proof. Following a similar situation in [CM00], consider the short exact sequence

$$0 \to E' \cap F' \to E' \oplus F' \to J' \to 0, \tag{10}$$

where the map $E' \cap F' \to E' \oplus F'$ is the anti-diagonal embedding $x \mapsto (-x, x)$ and the map $E' \oplus F' \to J'$ is given by $(x, y) \mapsto x + y$. Part of the associated

long exact sequence is

$$\cdots \to E'(K) \oplus F'(K) \to J'(K) \to H^1(K, E' \cap F') \to H^1(K, E' \oplus F') \to \cdots,$$

from which we get the lemma. □

By the lemma and the discussion preceding it, we see that r/r' divides $|\frac{J'(K)}{F'(K)+E'(K)}|$, which is the first factor in (9).

If $r' = 1$, then we are done, so let us assume that $r' > 1$. Then $\sigma \notin \delta'(F'(K)/rF'(K))$. So while the image of σ in $H^1(K, E')[r]$ is trivial by the top exact sequence in the diagram above, the image of σ in $H^1(K, F')[r]$ generates a subgroup of order r', by the lower exact sequence of the diagram above (recall that r' is the *smallest* positive integer such that $r'\sigma \in \delta'(F'(K)/rF'(K))$). Thus, from the same diagram, we see that σ, viewed as an element of $H^1(K, E' \cap F')$, maps to the trivial element of $H^1(K, E')$ but a nontrivial element σ' of $H^1(K, F')$ of order r'. Following a similar situation in [Maz99], considering the exactness of

$$H^1(K, E' \cap F') \to H^1(K, E') \oplus H^1(K, F') \to H^1(K, J'),$$

which is part of the long exact sequence associated to (10), we see that the element $(0, \sigma')$ in the middle group dies in the rightmost group, since it arises from the element σ in the leftmost group. Thus $\sigma' \in H^1(K, F')$ dies in $H^1(K, J')$, and thus is a nontrivial element of order r' of $\ker\big(H^1(K, F') \to H^1(K, J')\big)$. Hence r' divides the second factor in (9).

Thus r/r' divides the first factor in (9), and r' divides the second factor in (9), and so r divides the product in (9), as was to be shown.

References

[Aga07] A. Agashe, *A visible factor of the special L-value*, submitted (2007), available at arXiv:0810.2477 or `http://www.math.fsu.edu/~agashe/math.html`.

[Aga08a] ———, *The modular number, congruence number, and multiplicity one*, submitted (2008), available at arXiv:0810.5176 or `http://www.math.fsu.edu/~agashe/math.html`.

[Aga08b] ———, *A visible factor for analytic rank one*, submitted (2008), available at arXiv:0810.5177 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*, preprint (2006), available at
http://www.math.fsu.edu/~agashe/math.html.

[AS] A. Agashe and W. A. Stein, Appendix to Joan-C. Lario and René Schoof: *Some computations with Hecke rings and deformation rings*, submitted.

[AS02] ———, *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.

[Cre] J. E. Cremona, *Elliptic curve data,*
`http://www.warwick.ac.uk/staff/j.e.cremona/ftp/data/index.html`.

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

[Gro91] B. H. Gross, *Kolyvagin's work on modular elliptic curves*, *L*-functions and arithmetic (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, pp. 235–256.

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

[Jet07] D. Jetchev, *Global divisibility of heegner points and tamagawa numbers*, preprint (2007), available at arXiv:math/0703431.

[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.

[Kol90] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.

[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.

[Maz99] ———, *Visualizing elements of order three in the Shafarevich-Tate group*, Asian J. Math. **3** (1999), no. 1, 221–232. MR 2000g:11048

[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.

[Wal85] J.-L. Waldspurger, *Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie*, Compositio Math. **54** (1985), no. 2, 173–242. MR 87g:11061b