Visibility for analytic rank one

Amod Agashe *

December 8, 2007

Abstract

Let E be an optimal elliptic curve of conductor N, 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. The Gross-Zagier theorem gives a formula that expresses the Birch and Swinnerton-Dyer conjectural order the Shafarevich-Tate group of E over K as a rational number. We extract an integer factor from this formula and relate it to certain congruences of the newform associated to E with eigenforms of odd analytic rank bigger than one. We use the theory 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^2 divides the actual order of the Shafarevich-Tate group. This provides theoretical evidence for the Birch and Swinnerton-Dyer conjecture in the analytic rank one case.

1 Introduction and results

Let N be a positive integer. Let $X = X_0(N)$ denote the modular curve over $\mathbf{Q}$ associated to $\Gamma_0(N)$, and let $J = J_0(N)$ denote the Jacobian of X, which is an abelian variety over $\mathbf{Q}$. If g is an eigenform of weight 2 on $\Gamma_0(N)$, we call the order of vanishing of the L-function $L(g,s)$ at $s = 1$ the *analytic rank of* g. Let f be a newform of weight 2 on $\Gamma_0(N)$ whose analytic rank is one. 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 $p \mid N$). Let $I_f = \mathrm{Ann}_{\mathbf{T}} f$ and let A_f denote the newform quotient J/I_fJ, which is an abelian variety over $\mathbf{Q}$. We denote the quotient map

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

$J \to A_f$ by π. For the sake of simplicity, we assume henceforth that A_f is an elliptic curve, and denote it by E (we expect that most of our discussion should hold with E replaced by A_f below as well).

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, hence 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 [GZ86, §V.2:(2.2)], the second part of the Birch and Swinnerton-Dyer (BSD) conjecture becomes:

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

$$|E(K)/\pi(\mathbf{T}P)| = c_E \cdot \prod_{p \mid N} c_p(E) \cdot |\text{Ш}(E/K)|^{1/2}, \tag{1}$$

where c_E is the Manin constant of E (conjectured to be one), and $c_p(E)$ is the arithmetic component group of E at the prime p.

Note that $\pi(\mathbf{T}P) = \mathbf{Z}\pi(P)$ and that the index on the left side of (1) is finite since the analytic rank of f is one (by [GZ86, p.311–313]). Also the order of $\text{Ш}(E/K)$ is finite, by work of Kolyvagin (see, e.g., [Gro91, Thm 1.3]). The theory of Euler systems can be used to show that the actual value of the order of $\text{Ш}(E/K)$ divides the order predicted by the conjectural formula (1) (equivalently, that the right side of (1) divides the left side), under certain hypotheses, and staying away from certain primes (see, e.g., [Gro91, Thm 1.3]). Our goal is to try to prove results towards divisibility in the opposite direction, i.e., that the left side of (1) divides the right side.

Let $B = \ker \pi$, which is an abelian subvariety of $J_0(N)$. If g is an eigenform of weight 2 on $\Gamma_0(N)$, then we shall denote the dual abelian variety of A_g by $A_g^\vee$; it is an abelian subvariety of $J_0(N)$. If H is a subgroup of a finitely-generated abelian group G, then the *saturation* H in G is the largest subgroup of G containing H with finite index. Let $\widehat{\mathbf{T}P}$ denote the saturation of $\mathbf{T}P$ in $J(K)$. The following result expresses the integer $|E(K)/\pi(\mathbf{T}P)|$ on the left side of (1) as a product of three integers:

Proposition 1.2. *We have*

$$|E(K)/\pi(\mathbf{T}P)| = \left|\frac{J(K)}{B(K)+\widehat{\mathbf{T}P}}\right| \cdot \left|\frac{B(K)+\widehat{\mathbf{T}P}}{B(K)+\mathbf{T}P}\right| \cdot \left|\ker\big(H^1(K,B) \to H^1(K,J)\big)\right|.$$

We give the proof of this proposition in Section 2. Let D denote the abelian subvariety of $J_0(N)$ generated by $A_g^\vee$ where g ranges over all eigenforms other than f of weight 2 on $\Gamma_0(N)$ and having analytic rank one.

Theorem 1.3. *Let q be an odd prime that does not divide $J(K)_{\mathrm{tor}}$. Suppose that for no prime $p \mid N$ is f congruent to a newform h of level dividing N/p modulo a prime ideal over q in the ring of integers of the number field generated by the Fourier coefficients of f and h (for Fourier coefficients coprime to Nq). Assume that q does not divide $|E^\vee \cap D|$. Suppose that for all primes p dividing N, $p \not\equiv -w_p \bmod q$, with $p \not\equiv -1 \bmod q$, if $p^2 \mid N$. If q divides $\left|\frac{J(K)}{B(K)+\widehat{\mathbf{T}P}}\right|$, then:*
1) There is a newform g on $\Gamma_0(N)$ having odd analytic rank greater than one such that 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.
2) Assume the first part of the Birch and Swinnerton-Dyer conjecture for all $A_g^\vee$ such that g is an eigenform with odd analytic rank bigger than one. Then q^2 divides the order of $Ш(E/K)$.

Note that in particular, the prime q as above divides the right side of (1), which is as predicted by the conjecture of Birch and Swinnerton-Dyer in view of Proposition 1.2. Thus the theorem above provides theoretical evidence towards the Birch and Swinnerton-Dyer conjecture. We prove this theorem in Section 3. As mentioned in the abstract, the proof uses the theory of visibility. As far as we know, this is the first instance where the Birch and Swinnerton-Dyer conjectural order of the Shafarevich-Tate group has been related to its actual order using visibility for an abelian variety of analytic rank greater than zero, either theoretically or computationally (as opposed to the analytic rank zero case, where much work has been done: see, e.g., [CM00], [AS05], [Aga07]). This gives hope that the theory of visibility may give useful information even when the analytic rank is greater than zero. Also, while for analytic rank zero, there is work of Skinner-Urban that gives results opposite to those coming from the theory of Euler systems (for the Birch and Swinnerton-Dyer conjectural order of the Shafarevich-Tate group), for analytic rank greater than zero, we are not aware of any results that complement those coming from the theory of Euler systems other than our approach using visibility in this article.

We now make some remarks on the hypotheses of Theorem 1.3. While the hypothesis that q does not divide $J(K)_{\mathrm{tor}}$ can perhaps be weakened, one will mostly likely need the hypothesis that q does not divide $E(K)_{\mathrm{tor}}$, since if q divides $E(K)_{\mathrm{tor}}$, then q may divide the left side of (1) without dividing $|Ш(E/K)|$. The hypothesis that f is not congruent modulo a prime over q to a newform of lower level cannot be completely eliminated, since if it fails, then q could divide $c_p(E)$ for some prime p dividing N, and thus q need not divide $|Ш(E/K)|$ (if one believes formula (1)). The hypothesis that that q does not divide $|E^\vee \cap D|$ in Theorem 1.3 holds if f is not congruent modulo a prime over q to another newform on $\Gamma_0(N)$ having analytic rank one (in view of the hypothesis that f is not congruent modulo a prime over q to a newform of lower level). We expect that if this hypothesis fails, then q divides the factor $|\ker\big(H^1(K,B)\to H^1(K,J)\big)|$ of $|E(K)/\pi(\mathbf{T}P)|$ (cf. Proposition 1.2); however, the proof we have in mind requires a stronger "visibility theorem" than what exists in the literature, and will be the subject of a future paper. Finally, Neil Dummigan has informed us that the hypothesis that for all primes p dividing N, $p \not\equiv -w_p \bmod q$ can be eliminated from [DSW03, Thm. 6.1], and hence from Theorem 1.3.

The rest of this article is devoted to the proofs of the two results mentioned above. In each section, we continue using the notation introduced earlier.

Acknowledgement: We are grateful to Neil Dummigan for answering some questions regarding [DSW03].

2 Proof of Proposition 1.2

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

$$0\to B(K)\to J(K) \xrightarrow{\pi} E(K) \xrightarrow{\delta} H^1(K,B)\to H^1(K,J)\to \cdots . \tag{2}$$

Now $\delta(\pi(P)) = 0$, so δ induces a map

$$\phi : E(K)/\pi(\mathbf{T}P)\to\ker\big(H^1(K,B)\to H^1(K,J)\big).$$

By the exactness of (2), ϕ is a surjection and the kernel of ϕ is the image of π in $E(K)/\pi(\mathbf{T}P)$. Also, π induces a natural map $\psi : J(K)\to \ker(\phi)$.

Claim: ψ is surjective and its kernel is $B(K) + \mathbf{T}P$.

Proof. Let $x \in J(K)$. Then $x \in \ker(\psi) \iff \pi(x) = 0 \in \ker(\phi) \hookrightarrow E(K)/\pi(\mathbf{T}P) \iff \pi(x) \in \pi(\mathbf{T}P) \iff \exists t \in \mathbf{T} : x - tP \in \ker(\pi) = B(K) \iff x \in B(K) + \mathbf{T}P$. Thus $\ker(\psi) = B(K) + \mathbf{T}P$. To prove surjectivity of ψ, note that given an element of the codomain $\ker(\phi)$, we can write the element as $y + \pi(\mathbf{T}P)$ for some $y \in E(K)$ such that $\delta(y) = 0$. Then by the exactness of (2), $y \in \mathrm{Im}(\pi)$, hence $y + \pi(\mathbf{T}P) \in \mathrm{Im}(\psi)$. $\square$

By the discussion above, we get an exact sequence

$$0 \to \frac{J(K)}{B(K) + \mathbf{T}P} \xrightarrow{\psi'} \frac{E(K)}{\pi(\mathbf{T}P)} \xrightarrow{\phi} \ker\bigl(H^1(K,B) \to H^1(K,J)\bigr) \to 0, \tag{3}$$

where ψ' is the map induced by ψ.

Now

$$\left|\frac{J(K)}{B(K) + \mathbf{T}P}\right| = \left|\frac{J(K)}{B(K) + \widehat{\mathbf{T}P}}\right| \cdot \left|\frac{B(K) + \widehat{\mathbf{T}P}}{B(K) + \mathbf{T}P}\right|. \tag{4}$$

The proposition now follows from (3) and (4) above.

We remark that idea of factoring the term $|\frac{J(K)}{B(K)+\mathbf{T}P}|$ as in (4) is in analogy with the analytic rank zero case [Aga07], where the idea is due to Loïc Merel.

3 Proof of Theorem 1.3

Let C denote the abelian subvariety of $J_0(N)$ generated by $A_g^\vee$ where g ranges over all eigenforms of weight 2 on $\Gamma_0(N)$ having analytic rank one. If g is an eigenform of weight 2 on $\Gamma_0(N)$, then $\mathbf{T}P \cap A_g^\vee(K)$ is infinite if and only if g has analytic rank one (this follows by [GZ86, Thm 6.3] if g has analytic rank bigger than one, and the fact that $A_g^\vee(K)$ is finite if g has analytic rank one, by [KL89]). Thus we see that the free parts of $C(K)$ and of $\widehat{\mathbf{T}P}$ agree, and since q does not divide $J(K)_{\mathrm{tor}}$, so do their q-primary parts (as they are both trivial). Thus considering that q divides $|\frac{J(K)}{B(K)+\widehat{\mathbf{T}P}}|$, we see that q divides $|\frac{J(K)}{B(K)+C(K)}|$ as well.

Following a similar situation in [CM00], consider the short exact sequence $0 \to B \cap C \to B \oplus C \to J \to 0$, where the second map is the anti-diagonal embedding $x \mapsto (-x, x)$. Part of the associated long exact sequence is

$$\cdots \to B(K) \oplus C(K) \to J(K) \to H^1(K, B \cap C) \to H^1(K, B \oplus C) \to \cdots,$$

from which we get

$$\frac{J(K)}{B(K)+C(K)} = \ker\big(H^1(K, B\cap C)\to H^1(K, B\oplus C)\big). \tag{5}$$

Since q divides $|\frac{J(K)}{B(K)+C(K)}|$, there is an element σ of the right hand side of (5) of order q. Now D is seen to be the connected component of $C\cap B$; let Q be the quotient $(C\cap B)/D$, which is finite. Thus we have a short exact sequence $0\to D\to B\cap C\to Q\to 0$. Part of the associated long exact sequence is

$$\cdots\to H^1(K, D) \xrightarrow{i} H^1(K, B\cap C)\to H^1(K, Q)\to\cdots \tag{6}$$

Let m be the exponent of Q. Then $m\sigma \in i(H^1(K, D))$.

Case I: Suppose $m\sigma = 0$.

Then $q|m$. But $Q = (B\cap C)/D = B/D\cap C/D$. Now B is the abelian subvariety of $J_0(N)$ generated by $A_g^\vee$ as g ranges over all the eigenforms of of weight 2 on $\Gamma_0(N)$ except f. Thus as in [Aga07, §5], the fact that q divides the order of $B/D\cap C/D$ implies that there is a normalized eigenform $g\in S_2(\Gamma_0(N), \mathbf{C})$ such that g has analytic rank not equal to one 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 (this is analogous to the fact that the modular exponent divides the congruence exponent [ARS07]). By the hypothesis f is not congruent modulo a prime over q to a newform of lower level, we see that g is a newform. Since q is odd, considering that the eigenvalue of the Atkin-Lehner involution W_N on g is the same as that of f, we see that g has odd analytic rank, and hence its analytic rank is at least 3. Since we are assuming the first part of the Birch and Swinnerton-Dyer conjecture, this implies that A_g has Mordell-Weil rank at least $3\cdot\dim(A_f) = 3$.

It follows now from Theorem 6.1 of [DSW03] that q^2 divides the order of $Ш(E^\vee/K)$, as we now indicate. In the notation of loc. cit., r is at least the analytic rank of g (since we are assuming the first part of the Birch and Swinnerton-Dyer conjecture for $A_g^\vee$). The conclusion of Theorem 6.1 of loc. cit. then tells us that the Selmer group $H^1_f(K, A_{\mathfrak{q}}(1))$ of $E^\vee$ has $\mathbf{F}_{\mathfrak{q}}$-rank at least r. Since we are assuming that $E^\vee(K)[q] = 0$, and $E^\vee$ has Mordell-Weil rank one, the image of $H^1_f(K, V_{\mathfrak{q}}(1))$ in the Selmer group of $E^\vee$ has $\mathbf{F}_{\mathfrak{q}}$-rank at most one. So the q-primary part of $Ш(E^\vee/K)$ has $\mathbf{F}_q$-rank at least $r-1$, i.e., at least the analytic rank of g minus one, i.e., at least 2.

By the perfectness of the Cassels-Tate pairing, we see that q^2 divides the order of $Ш(E/K)$ as well.

Case II: Suppose $m\sigma \neq 0$.

For some multiple n of m, $n\sigma$ has order q. Now $m\sigma \in H^1(K, B \cap C)$ maps to zero in $H^1(K, Q)$ under the last map in (6), and hence so does $n\sigma$. Thus there is a nontrivial element σ' of $H^1(K, D)$ of order divisible by q that maps to $n\sigma \in H^1(K, B \cap C)$ under the map induced by the inclusion $D \hookrightarrow B \cap C$. Now $m\sigma$ is in the kernel of the map $H^1(K, B \cap C) \to H^1(K, B \oplus C)$, hence so is $n\sigma$. Thus σ' maps to zero under the map $H^1(K, D) \to H^1(K, C)$ induced by the inclusion $D \hookrightarrow C$. Now consider the short exact sequence

$$0 \to E^\vee \cap D \to E^\vee \oplus D \to C \to 0.$$

Part of the associated long exact sequence is

$$\cdots \to H^1(K, E^\vee \cap D) \to H^1(K, E^\vee) \oplus H^1(K, D) \to H^1(K, C) \to \cdots.$$

The element $(0, \sigma') \in H^1(K, E^\vee) \oplus H^1(K, D)$ maps to zero in $H^1(K, C)$, and thus there is a $\sigma'' \in H^1(K, E^\vee \cap D)$ of order divisible by q that maps to $(0, \sigma') \in H^1(K, E^\vee) \oplus H^1(K, D)$. But then q divides the order of $E^\vee \cap D$, which not possible by our hypothesis. Thus Case II does not happen.

The theorem now follows from our discussion in Case I.

References

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

[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.

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

[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] Neil Dummigan, William Stein, and Mark 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. MR MR2053457

[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

[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.