Non-triviality of families of Heegner points and ranks of Selmer groups over anticyclotomic towers

Massimo Bertolini*
Henri Darmon**

1 The result

Let $E/\mathbb{Q}$ be a modular elliptic curve of conductor N, and let K be an imaginary quadratic field of discriminant prime to N. Assume that E is semistable at all the prime divisors of N which are inert in K, and that the Hasse-Weil L-function $L(E/K, s)$ vanishes to even order at $s = 1$. Since the sign of the functional equation of $L(E/K, s)$ is $-\epsilon(N)$, where ϵ is the Dirichlet character attached to K (see [GZ], p. 71), it follows that the number of primes dividing N and inert in K is odd. Fix such a prime, say p, throughout the paper.

Let K_∞ be the anticyclotomic $\mathbb{Z}_p$-extension of K, and let $\Gamma \simeq \mathbb{Z}_p$ be its Galois group over K. Write Λ for the Iwasawa algebra $\mathbb{Z}_p[\![\Gamma]\!]$. The field K_∞ is a Galois extension of $\mathbb{Q}$, and the generator τ of $\mathrm{Gal}(K/\mathbb{Q})$ acts on Γ by the rule $\tau\gamma\tau = \gamma^{-1}$ for all $\gamma \in \Gamma$. This property characterizes K_∞ among the $\mathbb{Z}_p$-extensions of K. Denote by $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ the p-primary Selmer group of E over K_∞. It is a cofinitely generated Λ-module (i.e., its Pontryagin dual is a finitely generated Λ-module). It sits in the descent exact sequence

$$0 \to E(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(E/K_\infty) \to \text{Ш}(E/K_\infty)_{p^\infty} \to 0,$$

where $\text{Ш}(E/K_\infty)$ denotes the Shafarevich-Tate group of E over K_∞.

This note combines the results of [BD2] with techniques of Iwasawa theory to prove the following theorem.

Theorem 1.1
If $L(E/K, 1)$ is non-zero, then the Λ-corank of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ is equal to 1. More precisely, $E(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ has Λ-corank equal to 1, and $\text{Ш}(E/K_\infty)_{p^\infty}$ is a cotorsion Λ-module.

Remark 1.2
1. If $\chi : \Gamma \to \mathbb{C}^\times$ is a complex character of finite order which is *ramified* at p, the sign of the functional equation of $L(E/K, \chi, s)$ is $-\epsilon(N/p) = -1$. One expects that $L'(E/K, \chi, s)$ is non-zero for almost all characters χ as above. Assuming this, theorem 1.1 is predicted by the Birch and Swinnerton-Dyer conjecture applied to the finite layers of the extension K_∞.

2. As explained in section 3, the proof of theorem 1.1 is achieved by showing along the way a non-triviality result for the family of Heegner points defined over K_∞. See theorem 3.2 for the precise statement. The proof of theorem 3.2 rests on one of the main results of [BD2].

---

*Partially supported by grants from GNSAGA (CNR), MURST, and the European Community.
**Partially supported by grants from FCAR, NSERC, and by an Alfred P. Sloan research award.

2 An upper bound for the corank of $\mathbf{Sel}_{p^\infty}(\mathbf{E}/\mathbf{K}_\infty)$

This section is devoted to the proof of the following:

Proposition 2.1
If $L(E/K,1)$ is non-zero, then the Λ-corank of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ is ≤ 1.

Proposition 2.1 is a consequence of the next two propositions.

Proposition 2.2
If $L(E/K,1)$ is non-zero, then $\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E/K)=0$.

Proof. If $L(E/K,1)$ is non-zero, a theorem of Kolyvagin (see [K], Theorem A) shows that $E(K)$ and the Shafarevich-Tate group $Ш(E/K)$ of E over K are finite. In particular, the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/K)$ is zero.

The next proposition does not depend on the assumption that $L(E/K,1)$ is non-zero.

Proposition 2.3
$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E/K_\infty)^\Gamma \leq \mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E/K)+1.$

Proof of Proposition 2.1
The structure theory of discrete Λ-modules shows that

$$\mathrm{corank}_\Lambda \mathrm{Sel}_{p^\infty}(E/K_\infty) \leq \mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E/K_\infty)^\Gamma.$$

(See [M], ch. 1, or also [L], ch. 5, sec. 3, for details.) But the propositions 2.2 and 2.3 imply that the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/K_\infty)^\Gamma$ is ≤ 1.

It remains to prove proposition 2.3. Write K_n for the subfield of K_∞ having degree p^n over K, and G_n for the Galois group $\mathrm{Gal}(K_n/K)$. Let K_{n_0}, with $n_0 \geq 0$ be the maximal unramified extension of K contained in K_∞. Thus, $K_{n_0}=K_\infty \cap H$, where H is the Hilbert class field of K. Note that p is inert in K, totally split in the extension K_{n_0}/K and, for $n>n_0$, all the primes of K_{n_0} above p are totally ramified in K_n/K_{n_0}. Denote by $q \in p\mathbb{Z}_p$ Tate's p-adic period of E, and by Φ_n the group of connected components of E over $K_n \otimes \mathbb{Q}_p$. By Tate's theory of p-adic uniformization, the group Φ_n is a G_{n_0}-module, isomorphic to $(\mathbb{Z}/c_p p^{n-n_0}\mathbb{Z})[G_{n_0}]$, where $c_p := \mathrm{ord}_p(q)$.

Lemma 2.4
The torsion subgroup $E(K_\infty)_{\mathrm{tors}}$ of $E(K_\infty)$ is finite.

Proof. Let q_1 and q_2 be primes of good reduction for E which are inert in K. Then q_1 and q_2 are totally split in K_∞/K, and $E(K_\infty)_{\mathrm{tors}}$ injects in the finite group $E(\mathbb{F}_{q_1^2}) \oplus E(\mathbb{F}_{q_2^2})$.

Proof of Proposition 2.3
The proof is an application of the inflation-restriction sequence. First, note the exact sequence

$$H^1(\Gamma, E_{p^\infty}(K_\infty)) \to H^1(K, E_{p^\infty}) \to H^1(K_\infty, E_{p^\infty})^\Gamma \to H^2(\Gamma, E_{p^\infty}(K_\infty)).$$

The first term is finite, by lemma 2.4, and the fourth one is zero, since Γ has cohomological dimension equal to 1. If ℓ is a rational prime, there are also the local exact sequences

$$H^1(\Gamma, E(K_{\infty,\ell}))_{p^\infty} \to H^1(K_\ell, E)_{p^\infty} \to H^1(K_{\infty,\ell}, E)^\Gamma_{p^\infty},$$

where K_ℓ denotes $K \otimes \mathbb{Q}_\ell$ and $K_{\infty,\ell}$ denotes $\bigcup_n (K_n \otimes \mathbb{Q}_\ell)$. If $\ell \neq p$, the cohomology group $H^1(\Gamma, E(K_{\infty,\ell}))$ is finite, since K_∞ is unramified outside p. Moreover, if $\ell \nmid N$, $H^1(\Gamma, E(K_{\infty,\ell}))$ is zero, since E has good reduction at ℓ. (See [Mi], ch. 1.) The theory of p-adic uniformization can be used to prove that the group $H^1(\Gamma, E(K_{\infty,p}))_{p^\infty}$ has $\mathbb{Z}_p$-corank ≤ 1. One starts from the exact sequence of Γ-modules

$$0 \to Q_E \to K^\times_{\infty,p} \to E(K_{\infty,p}) \to 0,$$

where Q_E denotes the lattice of p-adic periods of E. The action of Γ on Q_E factors through G_{n_0}, and Q_E is isomorphic to $\mathbb{Z}[G_{n_0}]$. Taking cohomology of the above sequence shows that $H^1(\Gamma, E(K_{\infty,p}))$ injects in $H^2(\Gamma, Q_E)$. Combining the exact sequence in cohomology induced by

$$0 \to Q_E \to Q_E \otimes \mathbb{Q} \to Q_E \otimes \mathbb{Q}/\mathbb{Z} \to 0$$

with an inflation-restriction argument identifies $H^2(\Gamma, Q_E)$ with the group of homomorphisms $\mathrm{Hom}(\mathrm{Gal}(K_\infty/K_{n_0}), (Q_E \otimes \mathbb{Q}/\mathbb{Z})^{G_{n_0}})$, which is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$. Proposition 2.3 now follows from the snake lemma applied to the commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}_{p^\infty}(E/K) & \longrightarrow & H^1(K, E_{p^\infty}) & \longrightarrow & \prod_\ell H^1(K_\ell, E)_{p^\infty} \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Sel}_{p^\infty}(E/K_\infty)^\Gamma & \longrightarrow & H^1(K_\infty, E_{p^\infty})^\Gamma & \longrightarrow & \prod_\ell H^1(K_{\infty,\ell}, E)^\Gamma_{p^\infty},
\end{array}$$

where the vertical maps are restriction maps.

Remark 2.5

1. The $\mathbb{Z}_p$-corank of the group $H^1(\Gamma, E(K_{\infty,p}))_{p^\infty}$ considered in the proof of proposition 2.3 is in fact equal to 1. To see this, note the exact sequence

$$0 \to H^1(\Gamma, E(K_{\infty,p})) \to H^2(\Gamma, Q_E) \to H^2(\Gamma, K^\times_{\infty,p}) \to H^2(\Gamma, E(K_{\infty,p})) \to 0.$$

The "Brauer group" $H^2(\Gamma, K^\times_{\infty,p})$ has $\mathbb{Z}_p$-corank equal to 1, and it was already observed that $H^2(\Gamma, Q_E)$ has $\mathbb{Z}_p$-corank equal to 1. Let $\hat{E}(K_p)$ be the p-adic completion of $E(K_p)$, and let $\hat{U}E(K_p)$ be the submodule of universal norms along the local extension $K_{\infty,p}/K_p$. The $\mathbb{Z}_p$-corank of $H^2(\Gamma, E(K_{\infty,p}))$ is equal to the $\mathbb{Z}_p$-rank of $\hat{E}(K_p)/\hat{U}E(K_p)$. The theory of p-adic uniformization, combined with class field theory and the fact that the Tate period of E/K_p is a universal norm from $K^\times_{\infty,p}$, shows that $\hat{E}(K_p)/\hat{U}E(K_p)$ has $\mathbb{Z}_p$-rank equal to 1. The claim follows.

2. Recall that proposition 2.2 is a special case of a theorem of Kolyvagin [K]. The condition $L(E/K, 1) \neq 0$ is equivalent to $L(E/\mathbb{Q}, 1) \neq 0$ and $L(E'/\mathbb{Q}, 1) \neq 0$, where E' denotes the quadratic twist of E by K. The opening step in Kolyvagin's

proof consists in choosing auxiliary imaginary quadratic fields F and F' such that the first derivatives $L'(E/F,1)$ and $L'(E/F',1)$ are both non-zero, and such that the primes dividing the conductors of E and E' are split in F and F', respectively. The proof is then achieved by proving the finiteness of the Selmer groups of $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ one at a time, and deducing the finiteness of the Selmer group of E/K. A simpler approach to the proof of proposition 2.2 rests on the methods of [BD2], which allow to bound directly the p-primary Selmer group of E/K.

3 A lower bound for the corank of $\mathbf{Sel}_{p^\infty}(\mathbf{E}/\mathbf{K}_\infty)$

Theorem 1.1 is a consequence of the next proposition, combined with proposition 2.1.

Proposition 3.1
If $L(E/K,1)$ is non-zero, then the Λ-corank of $E(K_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ is ≥ 1. In particular, the Λ-corank of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ is ≥ 1.

Some preliminary results are needed. Recall the integer n_0 defined in the previous section. The field K_∞ is contained in the union of all the ring class fields of K of p-power conductor. More precisely, for $n > n_0$ let H_n be the ring class field of conductor p^{n+1-n_0}. Thus, H_n is an extension of the Hilbert class field H of degree $e_n := p^{n-n_0}(p+1)/u$, where u is one half the order of the group of units of K. The field H_n is the smallest ring class field containing K_n.

For $n > n_0$, a Heegner point construction (which is described in [BD1], sec. 2.5) defines a collection of points $\beta_n \in E(H_n)$, satisfying the compatibility relations

$$\mathrm{Trace}_{H_{n+1}/H_n}\beta_{n+1} = \beta_n, \qquad \mathrm{Trace}_{H_n/H}\beta_n = 0.$$

Set $\alpha_n := \mathrm{Trace}_{H_n/K_n}\beta_n \in E(K_n)$. Thus,

$$\mathrm{Trace}_{K_{n+1}/K_n}\alpha_{n+1} = \alpha_n, \qquad \mathrm{Trace}_{K_n/K_{n_0}}\alpha_n = 0.$$

Theorem 3.2
If $L(E/K,1)$ is non-zero, then there is an integer $n_1 > n_0$ such that α_n has infinite order for all $n \geq n_1$.

Proof. Let Ψ_n denote the group of connected components of E over $H_n \otimes \mathbb{Q}_p$. The group Ψ_n is a $\mathrm{Gal}(H/K)$-module, isomorphic to $(\mathbb{Z}/c_p e_n)[\mathrm{Gal}(H/K)]$. Write $\bar{\beta}_n$, resp. $\bar{\alpha}_n$ for the natural image of β_n in Ψ_n, resp. of α_n in Φ_n. Moreover, set

$$\bar{\beta}_n^{\mathbf{1}} := \mathrm{Trace}_{H/K}\bar{\beta}_n, \qquad \bar{\alpha}_n^{\mathbf{1}} := \mathrm{Trace}_{K_{n_0}/K}\bar{\alpha}_n.$$

The operator Trace_{H_n/K_n} induces a surjective map $t_{H_n/K_n} : \Psi_n \to \Phi_n$. Note that

$$t_{H_n/K_n}\bar{\beta}_n^{\mathbf{1}} = \bar{\alpha}_n^{\mathbf{1}}.$$

Theorem A of [BD2] relates the elements $\bar{\beta}_n^{\mathbf{1}}$ to the special value $L(E/K,1)$. In particular, since $L(E/K,1)$ is non-zero, it implies that the order of $\bar{\beta}_n^{\mathbf{1}}$ tends to infinity with n. The same property holds for the order of $\bar{\alpha}_n^{\mathbf{1}}$, since the kernel of

t_{H_n/K_n} is bounded independently of n. This shows that either the points α_n have infinite order for n sufficiently large, or the α_n are a collection of torsion points of unbounded order. But the second possibility is ruled out by lemma 2.4.

Corollary 3.3
The Mordell-Weil group $E(K_\infty)$ has infinite rank over $\mathbb{Z}$.

Proof. Suppose instead that $E(K_\infty)$ has finite rank. Since $E(K_\infty)_{\text{tors}}$ is finite by lemma 2.4, it follows that $E(K_\infty)$ is finitely generated. Thus, there is a positive integer n_2 such that $E(K_\infty) = E(K_{n_2})$, and such that the Heegner point α_n has infinite order for all $n \geq n_2$. By the compatibility of the Heegner points under traces, one obtains that $\alpha_{n_2} = p^{n-n_2}\alpha_n$ for all $n \geq n_2$. But the point α_{n_2} has infinite order, and therefore it cannot be infinitely divisible in $E(K_{n_2})$.

Proof of Proposition 3.1
By corollary 3.3, $E(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ has infinite $\mathbb{Z}_p$-corank. On the other hand, a cotorsion Λ-module has finite $\mathbb{Z}_p$-corank, by the structure theory of discrete Λ-modules ([M], ch. 1). This completes the proof of proposition 3.1, and of theorem 1.1.

The next result gives information on the growth of the Mordell-Weil groups $E(K_n)$.

Proposition 3.4
If $L(E/K, 1)$ is non-zero, then there is a sequence of integers ι_n having absolute value bounded independently of n such that

$$\mathrm{rank}_{\mathbb{Z}} E(K_n) = p^n + \iota_n.$$

Proposition 3.4 follows from theorem 1.1 and theorem 3.2. More precisely, theorem 1.1 implies that $\mathrm{rank}_{\mathbb{Z}} E(K_n) \leq p^n + \iota_n$, for a bounded sequence of integers ι_n. By theorem 3.2, the Heegner points α_n yield a norm-compatible sequence of points of infinite order. The opposite inequality follows from the structure of the modules of universal norms over the layers of K_∞. See [B], ch. 2 and 3. The details of the proof are omitted.

Remark 3.5
1. With the other assumptions on E, K and p as in the rest of the paper, now assume that $L(E/K, s)$ vanishes to even order at $s = 1$ and that $L(E/K, 1) = 0$. The first part of remark 1.2 suggests that in this setting $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ still has Λ-corank equal to 1. Moreover, the Heegner point construction carries over, and for $n > n_0$ provides a norm-compatible collection of points $\alpha_n \in E(K_n)$. A natural generalization (not yet proved) of the Gross-Zagier formula [GZ] to the derivatives $L'(E/K, \chi, 1)$ for ramified characters χ of Γ leads one to expect that again the point α_n has infinite order for n sufficiently large. (However, this cannot be shown by mapping α_n to the group of connected components Φ_n as in the proof of theorem 3.2, since $L(E/K, 1)$ is zero.) In the remainder of this remark, assume that α_n has infinite order for n large enough. The proofs of proposition 3.1 and of corollary 3.3 show that the Λ-corank of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ is ≥ 1. In order to show the opposite