FINE SELMER GROUPS, HEEGNER POINTS AND ANTICYCLOTOMIC $\mathbb{Z}_p$-EXTENSIONS

AHMED MATAR

Abstract. Let $E/\mathbb{Q}$ be an elliptic curve, p a prime and K_∞/K the anticyclotomic $\mathbb{Z}_p$-extension of a quadratic imaginary field K satisfying the Heegner hypothesis. In this paper we make a conjecture about the fine Selmer group over K_∞. We also make a conjecture about the structure of the module of Heegner points in $E(K_{\mathfrak{p}_\infty})/p$ where $K_{\mathfrak{p}_\infty}$ is the union of the completions of the fields K_n at a prime of K_∞ above p. We prove that these conjectures are equivalent. When E has supersingular reduction at p we also show that these conjectures are equivalent to the conjecture in our earlier work. Assuming these conjectures when E has supersingular reduction at p, we prove various results about the structure of the Selmer group over K_∞.

1. Introduction

Let K be an imaginary quadratic field with discriminant $d_K \neq -3, -4$ whose class number we will denote by h_K.

Let $p \geq 5$ be a prime and E an elliptic curve of conductor N defined over $\mathbb{Q}$ with a modular parametrization $\pi : X_0(N) \to E$. We shall say that (E, p) satisfies $(*)$ if the following are met:

(i) All the primes dividing N split in $K/\mathbb{Q}$
(ii) p does not divide $N d_K h_K \varphi(N d_K)$
(iii) $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) = GL_2(\mathbb{F}_p)$
(iv) If E has ordinary reduction at p then
    (a) $p \nmid \#E(\mathbb{F}_p)$
    (b) $a_p \not\equiv -1 \pmod{p}$ if p is inert in $K/\mathbb{Q}$
    (c) $a_p \not\equiv 2 \pmod{p}$ if p splits in $K/\mathbb{Q}$

We shall say that (E, π, p) satisfies $(*)$ if (E, p) satisfies $(*)$ and furthermore p does not divide the number of geometrically connected components of the kernel of $\pi_* : J_0(N) \to E$.

Let K_∞/K be the anticyclotomic $\mathbb{Z}_p$-extension of K, $\Gamma = \mathrm{Gal}(K_\infty/K)$ and K_n the unique subfield of K_∞ containing K such that $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$. Denote $\Gamma_n = \Gamma^{p^n}$, $G_n = \Gamma/\Gamma_n$ and $R_n = \mathbb{F}_p[G_n]$.

Let $\Lambda = \mathbb{Z}_p[[\Gamma]]$ be the Iwasawa algebra attached to K_∞/K. Fixing a topological generator $\gamma \in \Gamma$ allows us to identify Λ with the power series ring $\mathbb{Z}_p[[T]]$. Also consider the "mod p" Iwasawa algebra $\overline{\Lambda} = \Lambda/p\Lambda = \mathbb{F}_p[[T]]$.

Now let E' be a strong Weil curve in the isogeny class of E i.e. there exists a modular parametrization $\pi' : X_0(N) \to E'$ which maps the cusp ∞ of $X_0(N)$ to the origin of E' such that the induced map $\pi'_* : J_0(N) \to E'$ has a geometrically connected kernel.

If we assume that all the primes dividing N split in $K/\mathbb{Q}$, then choosing an ideal $\mathcal{N}$ of $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$ allows us to define a family of Heegner points $\alpha_n \in E(K_n)$ using the modular parametrization π and a family of Heegner points $\alpha'_n \in E'(K_n)$ using the modular parametrization π' (see section 2). In [23] we made the following conjecture

Conjecture A*. *Assume that (E, p) satisfies $(*)$, p splits in $K/\mathbb{Q}$ and E has supersingular reduction at p then the $\overline{\Lambda}$-submodule of $E'(K_\infty)/p$ generated by the Heegner points α'_n has $\overline{\Lambda}$-corank greater than or equal to two.*

Assuming this conjecture, we proved in [23] (using the same notation in that paper) that if E has supersingular reduction at p and p splits in $K/\mathbb{Q}$ then the Λ-corank of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ is equal to 2 and that $X_{p^\infty}(E/K_\infty) = \{0\}$.

We now make the slightly stronger conjecture

Conjecture A. *Assume that (E, π, p) satisfies $(*)$, p splits in $K/\mathbb{Q}$ and E has supersingular reduction at p then the Γ-submodule of $E(K_\infty)/p$ generated by the Heegner points α_n has $\overline{\Lambda}$-corank greater than or equal to two.*

It is easy to see that conjecture A implies conjecture A*. We proved theorem B of [23] for a strong Weil curve E' isogenous to E. As theorem B was invariant under isogeny, conjecture A* sufficed for our purposes. The author has not been able to prove that the results in this paper are invariant under isogeny which is the reason we have chosen to work with the slightly stronger conjecture A.

We now define the fine l^∞-Selmer group. Assume that l is an odd prime, F a number field and $\mathcal{E}$ is an elliptic curve defined over F. Let S be a finite set of primes of F containing all the primes dividing l and all the primes where $\mathcal{E}$ has bad reduction. We let F_S be the maximal extension of F unramified outside S. Suppose now that L is a field with $F \subseteq L \subseteq F_S$. We let $G_S(L) = \mathrm{Gal}(F_S/L)$ and S_L be the set of primes of L above those in S. We define the fine l^∞-Selmer group of $\mathcal{E}/L$ as

$$0 \longrightarrow R_{l^\infty}(\mathcal{E}/L) \longrightarrow H^1(G_S(L), \mathcal{E}[l^\infty]) \longrightarrow \prod_{v \in S_L} H^1(L_v, \mathcal{E}[l^\infty])$$

If l is a fixed prime then for any number field F we let F^{cyc} denote the cyclotomic $\mathbb{Z}_l$-extension of F. In [9] Coates and Sujatha make the following conjecture

Conjecture (Coates-Sujatha)**.** *If l is an odd prime, F a number field and $\mathcal{E}$ an elliptic curve defined over F, then $R_{l^\infty}(\mathcal{E}/F^{cyc})$ is a cofinitely generated $\mathbb{Z}_l$-module.*

If l is a fixed prime and F is an imaginary quadratic field we let F^{anti} denote the anticyclotomic $\mathbb{Z}_l$-extension of F (we have denoted this by K_∞ for the imaginary quadratic field K above). In relation to the conjecture of Coates and Sujatha above we propose the following conjecture

Conjecture B. *If l is an odd prime, F an imaginary quadratic field and $\mathcal{E}$ an elliptic curve defined over F, then $R_{l^\infty}(\mathcal{E}/F^{anti})$ is a cofinitely generated $\mathbb{Z}_l$-module.*

Our first result in this paper is the following theorem

Theorem. *Assume that (E, π, p) satisfies $(*)$, p splits in $K/\mathbb{Q}$ and E has supersingular reduction at p, then conjecture A and conjecture B (for $\mathcal{E} = E$, $F = K$ and $l = p$) are equivalent.*

If $\mathfrak{p}_\infty$ is a prime of K_∞ above p, we let $K_{\mathfrak{p}_\infty}$ denote the union of the completions of the fields $K_1 \subset K_2 \subset K_3 \subset \cdots$ at $\mathfrak{p}_\infty$. We now propose a third conjecture

Conjecture C. *Suppose that (E, π, p) satisfies $(*)$*

(i) If E has ordinary reduction at p, then there exists a prime $\mathfrak{p}_\infty$ of K_∞ above p such that the Γ-submodule of $E(K_{\mathfrak{p}_\infty})/p$ generated by the Heegner points α_n has infinite cardinality.

(ii) If E has supersingular reduction at p and p splits in $K/\mathbb{Q}$, then there exists a prime $\mathfrak{p}_\infty$ of K_∞ above p such that the Γ-submodule of $E(K_{\mathfrak{p}_\infty})/p$ generated by the Heegner points α_{2n} and the Γ-submodule of $E(K_{\mathfrak{p}_\infty})/p$ generated by the Heegner points α_{2n+1} are both of infinite cardinalities.

If one replaces $K_{\mathfrak{p}_\infty}$ in the above conjecture with the global field K_∞ then the conjecture becomes true. This can be shown using the results of Cornut [11] and Cornut and Vatsal [12] (see theorems 3.1 and 4.1 of [23]). Therefore, the conjecture is a local analog of this global result.

The relationship between conjectures B and C is given in the following theorem

Theorem. *Assume that (E, π, p) satisfies $(*)$ then we have*

(a) If E has ordinary reduction at p, then conjecture C(i) and conjecture B (for $\mathcal{E} = E$, $F = K$ and $l = p$) are equivalent.

(b) If p splits in $K/\mathbb{Q}$ and E has supersingular reduction at p, then conjecture C(ii) and conjecture B (for $\mathcal{E} = E$, $F = K$ and $l = p$) are equivalent (and hence also equivalent to conjecture A by the previous theorem).

The final result of this paper concerns the μ-invariant of the Pontryagin dual of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ which we denote by $\mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ (see section 2 for a definition of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$). Using the method of proof of [23] we will show

Theorem. *Suppose that (E, π, p) satisfies $(*)$ then we have*

(a) If E has ordinary reduction at p, then $\mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ has Λ-rank equal to 1 and μ-invariant equal to zero.

(b) If p splits in $K/\mathbb{Q}$, E has supersingular reduction at p and conjecture C(ii) is true, then $\mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ has Λ-rank equal to 2 and μ-invariant equal to zero.

Using the results of Wuthrich [32], we end this paper in section 4 by giving examples veryfiying conjecture B.

2. Definitions and Control Theorems

2.1. **Definitions.** In this section we recall the definition of the Heegner points as well as the definition of the Selmer and fine Selmer group.

Let E be an elliptic curve defined over $\mathbb{Q}$. We fix a modular parametrization $\pi : X_0(N) \to E$ which maps the cusp ∞ of $X_0(N)$ to the origin of E (see [30] and [3]). Assume that every prime dividing N splits in $K/\mathbb{Q}$ (condition $(*)$-i). It follows that we can choose an ideal $\mathcal{N}$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. Let m be an integer that is relatively prime to Nd_K and let $\mathcal{O}_m = \mathbb{Z} + m\mathcal{O}_K$ be the order of conductor m in K. The ideal $\mathcal{N}_m = \mathcal{N} \cap \mathcal{O}_m$ satisfies $\mathcal{O}_m/\mathcal{N}_m \cong \mathbb{Z}/N\mathbb{Z}$ and therefore the natural projection of complex tori:

$$\mathbb{C}/\mathcal{O}_m \to \mathbb{C}/\mathcal{N}_m^{-1}$$

is a cyclic N-isogeny, which corresponds to a point of $X_0(N)$. Let $\alpha[m]$ be its image under the modular parametrization π. From the theory of complex multiplication we have that $\alpha[m] \in E(K[m])$ where $K[m]$ is the ring class field of K of conductor m.

If we assume that the class number of K is not divisible by p (condition $(*)$-ii), it follows for any n that $K[p^{n+1}]$ is the ring class field of minimal conductor that contains K_n. We now define $\alpha_n \in E(K_n)$ to be the trace from $K[p^{n+1}]$ to K_n of $\alpha[p^{n+1}]$.

Let $R_n\alpha_n$ denote the R_n-submodule of $H^1(K_n, E[p])$ generated by the image of α_n under the Kummer map

$$E(K_n) \to H^1(K_n, E[p]).$$

If we assume that $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) = GL_2(\mathbb{F}_p)$ (condition $(*)$-iii), then by corollary 2.4 of [23] we have $E(K_\infty)[p^\infty] = \{0\}$. This implies that the restriction map for $m \geq n$

$$H^1(K_n, E[p]) \to H^1(K_m, E[p])$$

is injective and therefore allows us to view $R_n\alpha_n$ as a submodule of $H^1(K_m, E[p])$.

Assume that E has good ordinary reduction at p and condition $(*)$-iv is met. Then we have (see [1] prop 2.1.4) $\mathrm{Tr}_{K_{n+1}/K_n}(\alpha_{n+1}) = u\alpha_n$ for some unit $u \in R_n$. This implies that $R_n\alpha_n \subset R_{n+1}\alpha_{n+1}$ and so we may construct the direct limit $\varinjlim R_n\alpha_n$.

Now assume that E has good supersingular reduction at $p \geq 5$. In this case one can show that $\mathrm{Tr}_{K_{n+1}/K_n}(\alpha_{n+1}) = -\alpha_{n-1}$. This then implies that $R_n\alpha_n \subset R_{n+2}\alpha_{n+2}$ and so we may construct the direct limits $\varinjlim R_{2n}\alpha_{2n}$ and $\varinjlim R_{2n+1}\alpha_{2n+1}$.

Let us now define the Selmer groups we will be working with: If $L/\mathbb{Q}$ is any algebraic extension and E is an elliptic curve defined over L, we let $\mathrm{Sel}_{p^\infty}(E/L)$ denote the p^∞-Selmer group of E over L defined by

$$0 \longrightarrow \mathrm{Sel}_{p^\infty}(E/L) \longrightarrow H^1(L, E[p^\infty]) \longrightarrow \prod_v H^1(L_v, E)[p^\infty].$$

We will also be working with the p-Selmer group $\mathrm{Sel}_p(E/L)$ defined by

$$0 \longrightarrow \mathrm{Sel}_p(E/L) \longrightarrow H^1(L, E[p]) \longrightarrow \prod_v H^1(L_v, E)[p].$$

We now repeat the definition of the fine p^∞-Selmer group from the introduction. Assume that p is an odd prime, F a number field and E is a an elliptic curve defined over F. Let S be a finite set of primes of F containing all the primes dividing p and all the primes where E has bad reduction. We let F_S be the maximal extension of F unramified outside S. Suppose now that L is a field with $F \subseteq L \subseteq F_S$. We let $G_S(L) = \mathrm{Gal}(F_S/L)$ and S_L be the set of primes of L above those in S. We define the fine p^∞-Selmer group of E/L as

$$0 \longrightarrow R_{p^\infty}(E/L) \longrightarrow H^1(G_S(L), E[p^\infty]) \longrightarrow \prod_{v \in S_L} H^1(L_v, E[p^\infty]).$$

The definition of $R_{p^\infty}(E/L)$ does not depend on the set S. In fact, one can show that for any set S as above we have

$$0 \longrightarrow R_{p^\infty}(E/L) \longrightarrow \mathrm{Sel}_{p^\infty}(E/L) \longrightarrow \prod_{v|p} H^1(L_v, E[p^\infty]).$$

We also define the fine p-Selmer group of E/L whose definition may depend on the set S. It is defined as

$$0 \longrightarrow R_p^S(E/L) \longrightarrow H^1(G_S(L), E[p]) \longrightarrow \prod_{v \in S_L} H^1(L_v, E[p]).$$

2.2. **Control Theorems.** In this section we prove two Iwasawa-theoretic control theorems: one for the p-Selmer group and another for the fine p-Selmer group

First we need the following proposition

Proposition 2.1. *Let M be a finitely generated $\overline{\Lambda}$-module. Consider the $\overline{\Lambda}$-module $M^+ = \mathrm{Hom}_{\overline{\Lambda}}(M, \overline{\Lambda})$. Then M^+ is a free $\overline{\Lambda}$-module with the same rank as M and we have an isomorphism $M^+ \cong \varprojlim_n (M^{\text{ dual}})^{\Gamma_n}$ where $M^{\text{ dual}} = \mathrm{Hom}(M, \mathbb{F}_p)$ is the Pontryagin dual of M and the inverse limit is with respect to the norm maps.*

Proof. The proof is basically the same as [27] 2.2 lemma 4. The fact that M^+ is a free $\overline{\Lambda}$-module with the same rank as M is clear. As for the second statement we have the following isomorphisms

$$\begin{aligned} M^+ &= \mathrm{Hom}_{\overline{\Lambda}}(M, \overline{\Lambda}) \\ &\cong \varprojlim_n \mathrm{Hom}_{\overline{\Lambda}}(M, \mathbb{F}_p[G_n]) \\ &\cong \varprojlim_n \mathrm{Hom}_{\mathbb{F}_p[G_n]}(M_{\Gamma_n}, \mathbb{F}_p[G_n]) \\ &\cong \varprojlim_n \mathrm{Hom}_{\mathbb{F}_p}(M_{\Gamma_n}, \mathbb{F}_p) = \varprojlim_n (M^{\text{ dual}})^{\Gamma_n}. \end{aligned}$$

The last isomorphism above is induced by the isomorphism
$\mathrm{Hom}_{\mathbb{F}_p}(M_{\Gamma_n}, \mathbb{F}_p) \cong \mathrm{Hom}_{\mathbb{F}_p[G_n]}(M_{\Gamma_n}, \mathbb{F}_p[G_n])$: $\varphi \mapsto (x \mapsto \sum_{g \in G_n} \varphi(g^{-1}x)g)$. □

We also need the following lemma

Lemma 2.2. *If $X = \varprojlim M_i$ is the inverse limit of finite groups of bounded order, then X is finite.*

Proof. Giving the groups M_i the discrete topology makes X a profinite group. Since the groups M_i have bounded order, therefore it follows from [31] prop 1.1.6(b) that all open subgroups of X have bounded index. Since every nontrivial profinite group contains a proper open subgroup and since open subgroups of profinite groups are themselves a profinite group therefore the indexes of the open subgroups in an infinite profinite group must be unbounded. It follows that X must be finite. □

Assume that (E, π, p) satisfies $(*)$ and S is a finite set of primes of K containing all the primes dividing p and all the primes where E has bad reduction. We now define $X^S_{f,p}(E/K_\infty) := \varprojlim R^S_p(E/K_n)$ where the inverse limit is taken over n with respect to the corestriction maps. Also define $Y^S_{f,p}(E/K_\infty) := \varprojlim R^S_p(E/K_\infty)^{\Gamma_n}$ where the inverse limit is taken over n with respect to the norm maps.

The restriction maps $\mathrm{res} : R^S_p(E/K_n) \to R^S_p(E/K_\infty)^{\Gamma_n}$ induce a map

$$\Xi : X^S_{f,p}(E/K_\infty) \to Y^S_{f,p}(E/K_\infty).$$

We now have the following control theorem

Theorem 2.3. *Assume that (E, π, p) satisfies $(*)$. If S is the set of primes of K dividing Np then the map $\Xi : X^S_{f,p}(E/K_\infty) \to Y^S_{f,p}(E/K_\infty)$ is an injection with finite cokernel.*

Proof. Let S_n be all the primes of K_n dividing S and S_∞ all the primes of K_∞ dividing S and consider the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & R^S_p(E/K_\infty)^{\Gamma_n} \arrow[r] & H^1(K_\infty, E[p])^{\Gamma_n} \arrow[r, "\psi_\infty"] & \bigoplus_{v\in S_\infty} H^1(K_{\infty,v}, E[p])^{\Gamma_n} & (1) \\
0 \arrow[r] & R^S_p(E/K_n) \arrow[r] \arrow[u, "s_n"'] & H^1(K_n, E[p]) \arrow[r, "\psi_n"] \arrow[u, "h_n"'] & \bigoplus_{v\in S_n} H^1(K_{n,v}, E[p]) \arrow[u, "g_n"']
\end{tikzcd}$$

Taking the inverse limit of the groups in the top row with respect to the norm and the groups in the bottom row with respect to corestriction, we obtain the following diagram

$$\begin{tikzcd}
0 \arrow[r] & Y^S_{f,p}(E/K_\infty) \arrow[r] & \varprojlim H^1(K_\infty, E[p])^{\Gamma_n} \arrow[r, "\phi"] & \varprojlim \bigoplus_{v\in S_\infty} H^1(K_{\infty,v}, E[p])^{\Gamma_n} \\
0 \arrow[r] & X^S_{f,p}(E/K_\infty) \arrow[r] \arrow[u, "\Xi"'] & \varprojlim H^1(K_n, E[p]) \arrow[r, "\psi"] \arrow[u, "\Xi'"'] & \varprojlim \bigoplus_{v\in S_n} H^1(K_{n,v}, E[p]) \arrow[u, "\Xi''"']
\end{tikzcd}$$

(2)

By [23] corollary 2.4 we have that $E(K_\infty)[p^\infty] = \{0\}$ and so both $H^1(\Gamma_n, E(K_\infty)[p^\infty])$ and $H^2(\Gamma_n, E(K_\infty)[p^\infty])$ are trivial. This implies that the maps h_n in the diagram (1) above are isomorphisms which in turn implies that the map Ξ' in the diagram (2) is an isomorphism. Therefore by applying the snake lemma to the diagram (2) we see that Ξ is an injection and $\operatorname{coker}\Xi = \operatorname{img}\psi \cap \ker \Xi''$ so the proof will be complete if we can show that $\ker \Xi''$ is finite.

Since we have assumed that all the primes dividing N split in $K/\mathbb{Q}$, therefore it follows from [4] th. 2 that the set S_∞ is finite.

Now choose an M such that $\#S_M = \#S_\infty$ and such that for every $w \in S_\infty$ we have $E(K_{\infty,w})[p] = E(K_{M,v})[p]$ where v is the prime of S_M below w.

Let $m = \#S_M$. For every $n \geq M$ we label the primes in S_n as $v_1, v_2, ..., v_m$ and the primes of S_∞ as $w_1, w_2, ..., w_m$. We choose a labelling such that if $k \geq j \geq M$ then $w_i \in S_\infty$ lies above $v_i \in S_k$ lies above $v_i \in S_j$. With this labelling we have

$$\ker \Xi'' = \bigoplus_{i=1}^{m} \varprojlim_{n\geq M} H^1(\mathrm{Gal}(K_{\infty,w_i}/K_{n,v_i}), E(K_{\infty,w_i})[p])$$

where the inverse limit is taken over n with respect to the corestriction maps.

For any $n \geq M$ and any i we have $\mathrm{Gal}(K_{\infty,w_i}/K_{n,v_i}) = \Gamma_n$, therefore if g is a topological generator of Γ we have $H^1(\mathrm{Gal}(K_{\infty,w_i}/K_{n,v_i}), E(K_{\infty,w_i})[p]) = E(K_{\infty,w_i})[p]/(g^{p^n} - 1)E(K_{\infty,w_i})[p]$ but $E(K_{\infty,w_i})[p] = E(K_{n,v_i})[p]$ so $(g^{p^n} - 1)E(K_{\infty,w_i})[p] = \{0\}$ i.e. $H^1(\mathrm{Gal}(K_{\infty,w_i}/K_{n,v_i}), E(K_{\infty,w_i})[p]) = E(K_{\infty,w_i})[p]$. For $n' \geq n \geq M$ one can check that the corestriction map from $H^1(\mathrm{Gal}(K_{\infty,w_i}/K_{n',v_i}), E(K_{\infty,w_i})[p])$ to $H^1(\mathrm{Gal}(K_{\infty,w_i}/K_{n,v_i}), E(K_{\infty,w_i})[p])$ is the identity map on $E(K_{\infty,w_i})[p]$ hence $\varprojlim_{n\geq M} H^1(\mathrm{Gal}(K_{\infty,w_i}/K_{n,v_i}), E(K_{\infty,w_i})[p]) = E(K_{\infty,w_i})[p]$. This shows that $\ker \Xi''$ is finite which completes the proof. □

Corollary 2.4. *Assume that (E, π, p) satisfies $(*)$. If S is the set of primes of K dividing Np then $R_p^S(E/K_\infty)^{\mathrm{dual}}$ and $X_{f,p}^S(E/K_\infty)$ are both finitely generated $\overline{\Lambda}$-modules and* $\mathrm{corank}_{\overline{\Lambda}}(R_p^S(E/K_\infty)) = \mathrm{rank}_{\overline{\Lambda}}(X_{f,p}^S(E/K_\infty))$.

Proof. By [22] th. 4.5 we know that $\mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ is a finitely generated Λ-module. Since $E(K_\infty)[p^\infty] = \{0\}$ by [23] corollary 2.4, therefore we have an isomorphism $\mathrm{Sel}_p(E/K_\infty) \xrightarrow{\sim} \mathrm{Sel}_{p^\infty}(E/K_\infty)[p]$ and so $\mathrm{Sel}_p(E/K_\infty)^{\mathrm{dual}}$ is a finitely generated $\overline{\Lambda}$-module. The same then holds for $R_p^S(E/K_\infty)^{\mathrm{dual}}$ since $R_p^S(E/K_\infty) \subseteq \mathrm{Sel}_p(E/K_\infty)$ so by proposition 2.1 $Y_{f,p}^S(E/K_\infty)$ is also a finitely generated $\overline{\Lambda}$-module. Since by the control theorem we have an injection $X_{f,p}^S(E/K_\infty) \hookrightarrow Y_{f,p}^S(E/K_\infty)$, therefore we also have that $X_{f,p}^S(E/K_\infty)$ is a finitely generated $\overline{\Lambda}$-module. The corollary now follows from the control theorem and proposition 2.1. □

We now define $X_{s,p}(E/K_\infty) := \varprojlim \mathrm{Sel}_p(E/K_n)$ where the inverse limit is taken over n with repect to the corestriction maps. Note that we have chosen to put an "s" in the subscript so that the reader does not confuse this group with the group $X_p(E/K_\infty)$ in [23] which was defined in a different way.

We also define $Y_{s,p}(E/K_\infty) = \varprojlim \mathrm{Sel}_p(E/K_\infty)^{\Gamma_n}$ where the inverse limit is taken over n with respect to the norm maps.

The restriction maps $\mathrm{res} : \mathrm{Sel}_p(E/K_n) \to \mathrm{Sel}_p(E/K_\infty)^{\Gamma_n}$ induce a map

$$\Xi : X_{s,p}(E/K_\infty) \to Y_{s,p}(E/K_\infty).$$

We will now prove an Iwasawa-theoretic control theorem for the p-Selmer group. The theorem can be thought of as a "mod p" analog of theorem 2.10 in [23].

Theorem 2.5. *Suppose that (E, π, p) satisfies $(*)$. Consider the map Ξ induced by restriction*

$$\Xi : X_{s,p}(E/K_\infty) \to Y_{s,p}(E/K_\infty).$$

(a) If E has ordinary reduction at p, then Ξ is an injection with finite cokernel.

(b) If E has supersingular reduction at p and p splits in $K/\mathbb{Q}$ and conjecture C(ii) is true, then Ξ is an injection and $\mathrm{rank}_{\overline{\Lambda}}(\mathrm{coker}\,\Xi) \leq 2$.

Proof. First we prove part (a): Assume that E has ordinary reduction at p. From Mazur's control theorem ([24]; see also [15] and [16]) using the fact that $E(K_\infty)[p^\infty] = \{0\}$ ([23] corollary 2.4) we get that for any n the restriction map

$$\mathrm{res}_n : \mathrm{Sel}_{p^\infty}(E/K_n) \to \mathrm{Sel}_{p^\infty}(E/K_\infty)^{\Gamma_n}$$

is an injection with finite cokernel of bounded order as n varies. Since $E(K_\infty)[p^\infty] = \{0\}$, therefore for any n we have an isomorphism $\mathrm{Sel}_p(E/K_n) \xrightarrow{\sim} \mathrm{Sel}_{p^\infty}(E/K_n)[p]$ and an isomorphism $\mathrm{Sel}_p(E/K_\infty) \xrightarrow{\sim} \mathrm{Sel}_{p^\infty}(E/K_\infty)[p]$. Therefore for any n the restriction map gives an exact sequence

$$\mathrm{res}_n : 0 \longrightarrow \mathrm{Sel}_p(E/K_n) \longrightarrow \mathrm{Sel}_p(E/K_\infty)^{\Gamma_n} \longrightarrow C_n \longrightarrow 0$$

where C_n is finite and of bounded order as n varies. Part (a) then follows from this by taking inverse limits and using lemma 2.2.

Now we prove part (b). The proof of this part is very similar to the proof of theorem 2.10(b) in [23]. Assume that E has supersingular reduction at p, p splits in $K/\mathbb{Q}$ and conjecture C(ii) is true. Define $S = \{p\} \cup \{l \text{ prime} : l|N\}$. For any n, with this set S, we define S_n to be the set of primes of K_n above those in S and S_∞ to be the primes of K_∞ above those in S. Now define K_S to be the maximal extension of K unramified outside S, $G_S(K_n) = \mathrm{Gal}(K_S/K_n)$ and $G_S(K_\infty) = \mathrm{Gal}(K_S/K_\infty)$. Note that since we have assumed all the primes dividing N to split in $K/\mathbb{Q}$, therefore it follows from theorem 2 of [4] that the set S_∞ is finite.

For any K_n it is well-known that the p-Selmer group $\mathrm{Sel}_p(E/K_n)$ may be defined as

$$0 \longrightarrow \mathrm{Sel}_p(E/K_n) \longrightarrow H^1(G_S(K_n), E[p]) \longrightarrow \prod_{v \in S_n} H^1(K_{n,v}E)[p].$$

We may also define $\mathrm{Sel}_p(E/K_\infty)$ as

$$0 \longrightarrow \mathrm{Sel}_p(E/K_\infty) \longrightarrow H^1(G_S(K_\infty), E[p]) \longrightarrow \prod_{v \in S_\infty} H^1(K_{\infty,v}E)[p].$$

For any n consider the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}_p(E/K_\infty)^{\Gamma_n} \arrow[r] & H^1(G_S(K_\infty), E[p])^{\Gamma_n} \arrow[r, "\psi_\infty"] & \bigoplus_{v \in S_\infty} H^1(K_{\infty,v}, E)[p]^{\Gamma_n} \\
0 \arrow[r] & \mathrm{Sel}_p(E/K_n) \arrow[r] \arrow[u, "s_n"] & H^1(G_S(K_n), E[p]) \arrow[r, "\psi_n"] \arrow[u, "h_n"] & \bigoplus_{v \in S_n} H^1(K_{n,v}, E)[p] \arrow[u, "g_n"]
\end{tikzcd} \tag{3}$$

The vertical maps in the above diagram are restriction. Let us note a few things related to this diagram:

(1) The maps h_n are isomorphisms: This follows from the fact that $H^1(\Gamma_n, E(K_\infty)[p^m])$ and $H^2(\Gamma_n, E(K_\infty)[p^m])$ are both trivial because $E(K_\infty)[p^\infty] = \{0\}$ ([23] corollary 2.4).

(2) For any $v \in S_\infty$ above p we have $H^1(K_{\infty,v}, E)[p] = \{0\}$: The result follows from [7] cor. 3.2 as explained in [15] pg. 70. Note that the fact that E has supersingular reduction at p is crucial for this result.

(3) For any $v \in S_n$ not dividing p we have that $H^1(K_{n,v}, E)[p]$ is finite and of bounded order as n varies: This follows from 2 facts. First, by Tate duality for abelian varieties over local fields ([25] cor. 3.4) we have that $H^1(K_{n,v}, E)[p]$ is isomorphic to the dual of $E(K_{n,v})/p$. Secondly, if l is the rational prime lying below v, then by Mattuck's theorems we have that $E(K_{n,v}) \cong \mathbb{Z}_l^d \times T$ where $d = [K_{n,v} : \mathbb{Q}_l]$ and T is a finite group. Therefore it follows from these 2 facts that $\# H^1(K_{n,v}, E)[p] \leq p^2$.

(4) Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be the primes of K above p. Since we have assumed that the class number of K is relatively prime to p, therefore both $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are totally ramified in K_∞/K. So in particular there are only 2 primes $\mathfrak{p}_{n,1}$ and $\mathfrak{p}_{n,2}$ of K_n above p and 2 primes $\mathfrak{p}_{\infty,1}$ and $\mathfrak{p}_{\infty,2}$ of K_∞ above p.

Let $\tilde{S}_\infty = S_\infty \backslash \{\mathfrak{p}_{\infty,1}, \mathfrak{p}_{\infty,2}\}$ (see (4)). Taking the points (2)-(4) into consideration, we take the inverse limit of the objects in the diagram above over n (using the corestriction map for the bottom row and the norm map for the top row) to obtain the following diagram where the group T is finite (using point (3) and lemma 2.2)

$$\begin{tikzcd}
0 \arrow[r] & Y_{s,p}(E/K_\infty) \arrow[r] & \varprojlim H^1(G_S(K_\infty), E[p])^{\Gamma_n} \arrow[r, "\Phi"] & \bigoplus_{v \in \tilde{S}_\infty} \varprojlim H^1(K_{\infty,v}, E)[p]^{\Gamma_n} \\
0 \arrow[r] & X_{s,p}(E/K_\infty) \arrow[r] \arrow[u, "\Xi"'] & \varprojlim H^1(G_S(K_n), E[p]) \arrow[r, "\psi"] \arrow[u, "\Xi'"'] & T \times \bigoplus_{i=1,2} \varprojlim H^1(K_{\mathfrak{p}_{n,i}}, E)[p] \arrow[u, "\Xi''"']
\end{tikzcd} \tag{4}$$

To ease the notation, in the above diagram we have denoted $K_{n,\mathfrak{p}_{n,i}}$ by $K_{\mathfrak{p}_{n,i}}$. Applying the snake lemma to this diagram we get

$$0 \to \ker \Xi \to \ker \Xi' \to \ker \Xi'' \cap \operatorname{img} \psi \to \operatorname{coker} \Xi \to \operatorname{coker} \Xi'$$

From point (1) above, it follows that Ξ' is an isomorphism i.e. $\ker \Xi' = 0$ and $\operatorname{coker} \Xi' = 0$. Therefore from the above sequence we get that $\ker \Xi = 0$ as required. We also get that $\operatorname{coker} \Xi = \ker \Xi'' \cap \operatorname{img} \psi$. Since T is finite and Ξ'' restricted to $H^1(K_{\mathfrak{p}_{n,i}}, E)[p]$ is the zero map, it follows that $\operatorname{rank}_{\overline{\Lambda}}(\operatorname{coker} \Xi) = \operatorname{rank}_{\overline{\Lambda}}(\operatorname{img} \psi)$. Therefore we must show that $\operatorname{rank}_{\overline{\Lambda}}(\operatorname{img} \psi) \leq 2$. To study $\operatorname{img} \psi$ we use the Cassels-Poitou-Tate exact sequence (see [9]) which gives that the following sequence is exact

$$H^1(G_S(K_n), E[p]) \xrightarrow{\psi_n} \bigoplus_{v \in S_n} H^1(K_{n,v}, E)[p] \xrightarrow{\theta_n} \operatorname{Sel}_p(E/K_n)^{\text{dual}}$$

We take the inverse limits of the groups over n using the corestriction map. As all the groups we are dealing with are compact Hausdorff, the resulting sequence is also exact:

$$\varprojlim H^1(G_S(K_n), E[p]) \xrightarrow{\psi} T \times \bigoplus_{i=1,2} \varprojlim H^1(K_{\mathfrak{p}_{n,i}}, E)[p] \xrightarrow{\theta} \mathrm{Sel}_p(E/K_\infty)^{\mathrm{dual}}$$

The fact that this sequence is exact means that $\operatorname{img}\psi = \ker\theta$. So to show that $\mathrm{rank}_{\overline{\Lambda}}(\operatorname{img}\psi) \leq 2$ it suffices to show that $\mathrm{rank}_{\overline{\Lambda}}(\ker\theta) \leq 2$ or equivalently, if $\hat{\theta}$ is the dual map, that $\mathrm{corank}_{\overline{\Lambda}}(\operatorname{coker}\hat{\theta}) \leq 2$.

By Tate local duality the dual of $H^1(K_{\mathfrak{p}_{n,i}}, E)[p]$ may be identified with $E(K_{\mathfrak{p}_{n,i}})/p$. Therefore using this fact, the map $\hat{\theta}$ becomes

$$\hat{\theta} : \mathrm{Sel}_p(E/K_\infty) \to E(K_{\mathfrak{p}_{\infty,1}}) \otimes \mathbb{F}_p \times E(K_{\mathfrak{p}_{\infty,2}}) \otimes \mathbb{F}_p.$$

This map is the usual map induced by restriction

$$H^1(K_\infty, E[p]) \to \bigoplus_{i=1,2} H^1(K_{\mathfrak{p}_{\infty,i}}, E[p]).$$

Note that if $c \in \mathrm{Sel}_p(E/K_\infty) \subset H^1(K_\infty, E[p])$ then its image under this map belongs to $E(K_{\mathfrak{p}_{\infty,1}}) \otimes \mathbb{F}_p \times E(K_{\mathfrak{p}_{\infty,2}}) \otimes \mathbb{F}_p$.

To prove our result we will first calculate $\mathrm{corank}_{\overline{\Lambda}}(E(K_{\mathfrak{p}_{\infty,i}}) \otimes \mathbb{F}_p)$. First we show that $E(K_{\mathfrak{p}_{\infty,i}})[p^\infty] = \{0\}$. Since $\Gamma = \mathrm{Gal}(K_{\mathfrak{p}_{\infty,i}}/\mathbb{Q}_p)$ is pro-p, it suffices to show that $E(\mathbb{Q}_p)[p^\infty] = E(K_{\mathfrak{p}_{\infty,i}})[p^\infty]^\Gamma = \{0\}$. But since E has supersingular reduction at p, we have $E(\mathbb{Q}_p)[p^\infty] = \hat{E}(p\mathbb{Z}_p)[p^\infty]$ where $\hat{E}$ is the formal group of $E/\mathbb{Q}_p$. The result then follows from the fact ([29] ch. 4 th. 6.1) that $\hat{E}(p\mathbb{Z}_p)$ has no p-torsion if $p \geq 3$.

Since $E(K_{\mathfrak{p}_{\infty,i}})[p^\infty] = \{0\}$, therefore, as in point (1) above, the restriction map induces an isomorphism $H^1(K_{\mathfrak{p}_{n,i}}, E[p]) \xrightarrow{\sim} H^1(K_{\mathfrak{p}_{\infty,i}}, E[p])^{\Gamma_n}$. In addition from the local Euler-Poincaré characteristic ([26] VII 7.3.1) and Tate local duality ([26] VII 7.2.6) together with the Weil pairing we have $\dim_{\mathbb{F}_p}(H^1(K_{\mathfrak{p}_{n,i}}, E[p])) = 2p^n + 2\dim_{\mathbb{F}_p}(E(K_{\mathfrak{p}_{n,i}})[p])$. But $E(K_{\mathfrak{p}_{n,i}})[p] = \{0\}$ and so $\dim_{\mathbb{F}_p}(H^1(K_{\mathfrak{p}_{n,i}}, E[p])) = 2p^n$. Therefore we have shown that $\mathrm{corank}_{\overline{\Lambda}}(H^1(K_{\mathfrak{p}_{\infty,i}}, E[p])) = 2$. But by point (2) above $E(K_{\mathfrak{p}_{\infty,i}}) \otimes \mathbb{F}_p$ is isomorphic to $H^1(K_{\mathfrak{p}_{\infty,i}}, E[p])$, so we also have $\mathrm{corank}_{\overline{\Lambda}}(E(K_{\mathfrak{p}_{\infty,i}}) \otimes \mathbb{F}_p) = 2$.

It follows that we have

$$\mathrm{corank}_{\overline{\Lambda}}(E(K_{\mathfrak{p}_{\infty,1}}) \otimes \mathbb{F}_p \times E(K_{\mathfrak{p}_{\infty,2}}) \otimes \mathbb{F}_p) = 4.$$

Therefore to show that $\mathrm{corank}_{\overline{\Lambda}}(\operatorname{coker}\hat{\theta}) \leq 2$ we only need to show that $\mathrm{corank}_{\overline{\Lambda}}(\operatorname{img}\hat{\theta}) \geq 2$. This follows from conjecture C(ii) as is explained in the proof of theorem 3.3 in the next section: Consider the subgroup $M := \varinjlim R_{2n}\alpha_{2n} + \varinjlim R_{2n+1}\alpha_{2n+1} \subseteq \mathrm{Sel}_p(E/K_\infty)$. The proof of theorem 3.3 shows that if conjecture C(ii) is true, then for $i = 1$ or $i = 2$ the image of M under the map (induced by restriction)

$$E(K_\infty) \otimes \mathbb{F}_p \to E(K_{\mathfrak{p}_{\infty,i}}) \otimes \mathbb{F}_p$$

has $\overline{\Lambda}$-corank greater than or equal to two. This implies the result.

□

Corollary 2.6. *Assume that (E,π,p) satisfies $(*)$ then both* $\mathrm{Sel}_p(E/K_\infty)^{\mathrm{dual}}$ *and* $X_{s,p}(E/K_\infty)$ *are finitely generated $\overline{\Lambda}$-modules*

(a) If E has ordinary reduction at p, then $\mathrm{corank}_{\overline{\Lambda}}(\mathrm{Sel}_p(E/K_\infty)) = \mathrm{rank}_{\overline{\Lambda}}(X_{s,p}(E/K_\infty))$.

(b) If E has supersingular reduction at p, p splits in $K/\mathbb{Q}$ and conjecture C(ii) is true, then $\mathrm{corank}_{\overline{\Lambda}}(\mathrm{Sel}_p(E/K_\infty)) \leq \mathrm{rank}_{\overline{\Lambda}}(X_{s,p}(E/K_\infty)) + 2$.

Proof. By [22] th. 4.5 we know that $\mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ is a finitely generated Λ-module. Since $E(K_\infty)[p^\infty] = \{0\}$ by [23] corollary 2.4, therefore we have an isomorphism $\mathrm{Sel}_p(E/K_\infty) \xrightarrow{\sim} \mathrm{Sel}_{p^\infty}(E/K_\infty)[p]$ and so $\mathrm{Sel}_p(E/K_\infty)^{\mathrm{dual}}$ is a finitely generated $\overline{\Lambda}$-module. Therefore by proposition 2.1, $Y^S_{f,p}(E/K_\infty)$ is also a finitely generated $\overline{\Lambda}$-module. Since by the control theorem we have an injection $X^S_{f,p}(E/K_\infty) \hookrightarrow Y^S_{f,p}(E/K_\infty)$, therefore we also have that $X^S_{f,p}(E/K_\infty)$ is a finitely generated $\overline{\Lambda}$-module. The corollary now follows from the control theorem and proposition 2.1. □

3. Proofs of Main Theorems

Before proving the theorems listed in the introduction we record the following theorem which is essentially the main result proven in [23]

Theorem 3.1. *Assume that (E,π,p) satisfies $(*)$. Then we have*

1. *If E has ordinary reduction at p, then* $\mathrm{rank}_{\overline{\Lambda}}(X_{s,p}(E/K_\infty)) \leq 1$.
2. *If E has supersingular reduction at p, p splits in $K/\mathbb{Q}$ and conjecture A is true, then* $X_{s,p}(E/K_\infty) = \{0\}$.

Proof. In section 2.3 of [23] (using the notation in that paper) we constructed a map $\psi_\ell : \varinjlim H^1(K_{n,\ell}, E)[p] \to X_p(E/K_\infty)^{\mathrm{dual}}$ as follows: First by Tate local duality we have an isomorphism

$$\varinjlim H^1(K_{n,\ell}, E)[p] \cong (\varprojlim E(K_{n,\ell})/p)^{\mathrm{dual}}.$$

Next for any n we have a restriction map $\mathrm{res}_\ell : \mathrm{Sel}_p(E/K_n) \to E(K_{n,\ell})/p$. Taking inverse limits gives a map

$$\mathrm{res}_\ell : X_{s,p}(E/K_\infty) \to \varprojlim E(K_{n,\ell})/p$$

Dualizing this map and using the Tate duality isomorphism we get a map

$$\psi'_\ell : \varinjlim H^1(K_{n,\ell}, E)[p] \to X_{s,p}(E/K_\infty)^{\mathrm{dual}}.$$

Since $X_p(E/K_\infty)$ injects into $X_{s,p}(E/K_\infty)$, therefore we have a surjection $X_{s,p}(E/K_\infty)^{\mathrm{dual}} \to X_p(E/K_\infty)^{\mathrm{dual}}$ and so composing the map ψ'_ℓ with this surjection we get our desired map

$$\psi_\ell : \varinjlim H^1(K_{n,\ell}, E)[p] \to X_p(E/K_\infty)^{\mathrm{dual}}.$$

If we work with the map ψ'_ℓ rather than ψ_ℓ we obtain results identical those in [23] where the group $X_p(E/K_\infty)$ gets replaced by $X_{s,p}(E/K_\infty)$ so proposition 3.7 in the ordinary case gives that $\mathrm{rank}_{\overline{\Lambda}}(X_{s,p}(E/K_\infty)) \leq 1$ and in the supersingular case the proof of theorem B in section 4 gives that $X_{s,p}(E/K_\infty) = \{0\}$

However the reader should be aware of one important detail. In the beginning of sections 3 and 4 in [23] we noted that the statements of theorems A and B were invariant under isogeny and therefore it would suffice to assume that E is a strong Weil curve with a modular parametrization $\pi : J_0(N) \to E$ having a geometrically connected kernel. This was important to apply the results of Cornut [11] which require that p does not divide the number of geometrically connected components of the kernel of the modular parametrization.

Regarding the theorem that we are proving the author has not been able to prove that it is invariant under isogeny and therefore we cannot pass to a strong Weil curve as we did in [23] but as (E, π, p) was assumed to satisfy $(*)$, therefore p does not divide the number of geometrically connected components of the kernel $\pi : J_0(N) \to E$ and therefore the results of Cornut [11] apply to E without the need to refer to a strong Weil curve. Also we have assumed in the supersingular case that conjecture A is satisfied (rather than conjecture A* in [23]) so we may work with the elliptic curve E directly rather than working with an isogenous strong Weil curve. □

We now prove the theorems in the introduction

Theorem 3.2. *Assume that (E, π, p) satisfies $(*)$, p splits in $K/\mathbb{Q}$ and E has supersingular reduction at p, then conjecture A and conjecture B (for $\mathcal{E} = E$, $F = K$ and $l = p$) are equivalent.*

Proof. Assume that (E, π, p) satisfies $(*)$, p splits in $K/\mathbb{Q}$, E has supersingular reduction at p and conjecture A is true. Let S be the set of primes of K dividing Np. Since for any n we have that $R^S_p(E/K_n)$ is contained in $\mathrm{Sel}_p(E/K_n)$, therefore $X^S_{f,p}(E/K_\infty)$ is contained in $X_{s,p}(E/K_\infty)$. But the latter group is trivial by theorem 3.1 and so $X^S_{f,p}(E/K_\infty)$ is trivial as well. Therefore it follows from corollary 2.4 that $R^S_p(E/K_\infty)$ is finite. Now consider the natural map $R^S_p(E/K_\infty) \to R_{p^\infty}(E/K_\infty)[p]$. We claim this map has a finite cokernel.

This follows from 3 facts. First, by [23] corollary 2.4 we have $E(K_\infty)[p^\infty] = \{0\}$ and therefore it follows that we have an isomorphism $H^1(K_\infty, E[p]) \xrightarrow{\sim} H^1(K_\infty, E[p^\infty])[p]$. Secondly, since we have assumed that all the primes dividing N split in $K/\mathbb{Q}$ it follows from theorem 2 of [4] that the set of primes of K_∞ above S is finite. Finally, it is easy to prove that for any prime v of K_∞ we have the kernel of the natural map $H^1(K_{\infty,v}, E[p]) \to H^1(K_{\infty,v}, E[p^\infty])[p]$ is finite.

The fact that the map $R^S_p(E/K_\infty) \to R_{p^\infty}(E/K_\infty)[p]$ has a finite cokernel follows easily from these 3 facts. Therefore since $R^S_p(E/K_\infty)$ is finite, we have that $R_{p^\infty}(E/K_\infty)[p]$ is finite i.e. $R_{p^\infty}(E/K_\infty)$ is cofinitely generated over $\mathbb{Z}_p$ which proves conjecture B in this case.

Now assume that (E, π, p) satisfies $(*)$, p splits in $K/\mathbb{Q}$, E has supersingular reduction at p and conjecture B is true. Let us first make a few definitions. Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be the 2 primes of K above p. Since we have assumed that the class number of K is prime to p therefore both $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are totally ramified in K_∞/K. So in particular there are 2 primes $\mathfrak{p}_{n,1}$ and $\mathfrak{p}_{n,2}$ of K_n above p and 2 primes $\mathfrak{p}_{\infty,1}$ and $\mathfrak{p}_{\infty,2}$ of K_∞ above p. We will denote the completion of K_n with respect to $\mathfrak{p}_{n,i}$ by $K_{\mathfrak{p}_{n,i}}$ and we let $K_{\mathfrak{p}_{\infty,i}}$ be the union of the completions $K_{\mathfrak{p}_{n,i}}$. Following Kobayashi [20], we define the following subgroups of $E(K_{\mathfrak{p}_{n,i}})$

$$E^+(K_{\mathfrak{p}_{n,i}}) := \{x \in E(K_{\mathfrak{p}_{n,i}}) \mid \mathrm{Tr}_{n/m+1}(x) \in E(K_{\mathfrak{p}_{m,i}}) \text{ for even } m: \ 0 \le m < n\}$$
$$E^-(K_{\mathfrak{p}_{n,i}}) := \{x \in E(K_{\mathfrak{p}_{n,i}}) \mid \mathrm{Tr}_{n/m+1}(x) \in E(K_{\mathfrak{p}_{m,i}}) \text{ for odd } m: \ 0 \le m < n\}.$$

We then define $E^+(K_{\mathfrak{p}_{\infty,i}}) := \bigcup_{n\in\mathbb{N}} E^+(K_{\mathfrak{p}_{n,i}})$ and $E^-(K_{\mathfrak{p}_{\infty,i}}) := \bigcup_{n\in\mathbb{N}} E^-(K_{\mathfrak{p}_{n,i}})$.

We now analyze the intersection of $E^+(K_{\mathfrak{p}_{\infty,i}}) \otimes \mathbb{F}_p$ and $E^-(K_{\mathfrak{p}_{\infty,i}}) \otimes \mathbb{F}_p$ where we view both of these groups as subgroups of $E(K_{\mathfrak{p}_{\infty,i}}) \otimes \mathbb{F}_p$. By a proof which is identical to that of lemma 2.6.5 of [6], using a result of Iovita and Pollack [19], we have

$$E^+(K_{\mathfrak{p}_{\infty,i}}) \otimes \mathbb{F}_p \cap E^-(K_{\mathfrak{p}_{\infty,i}}) \otimes \mathbb{F}_p = E(\mathbb{Q}_p) \otimes \mathbb{F}_p \tag{5}$$

We now define some Selmer groups. First let S be the set of primes of K above p and above all the primes dividing N. We let K_S be the maximal extension of K unramified outside S. For any field F with $K \subseteq F \subseteq K_S$ we let $G_S(F) = \mathrm{Gal}(K_S/F)$ and we let S_F be the set of primes of F that lie over a prime of S.

Let $\tilde{S}_{K_\infty} = S_{K_\infty} \backslash \{\mathfrak{p}_{\infty,1}, \mathfrak{p}_{\infty,2}\}$. Since we have assumed that all the primes dividing N split in $K/\mathbb{Q}$, therefore it follows from theorem 2 of [4] that the set $\tilde{S}_{K_\infty}$ is finite.

Recall that the p-Selmer group of E over K_∞ is defined as

$$0 \longrightarrow \mathrm{Sel}_p(E/K_\infty) \longrightarrow H^1(G_S(K_\infty), E[p]) \longrightarrow \prod_{v\in S_{K_\infty}} \frac{H^1(K_{\infty,v}, E[p])}{E(K_{\infty,v}) \otimes \mathbb{F}_p}.$$

Following Kobayashi [20], we define the even (odd) p-Selmer group of E over K_∞ as

$$0 \longrightarrow \mathrm{Sel}_p{}^{\pm}(E/K_\infty) \longrightarrow \mathrm{Sel}_p(E/K_\infty) \longrightarrow \prod_{i=1,2} \frac{H^1(K_{\mathfrak{p}_\infty,i}, E[p])}{E^{\pm}(K_{\mathfrak{p}_\infty,i}) \otimes \mathbb{F}_p}.$$

We also define

$$0 \longrightarrow \mathrm{Sel}^1_p(E/K_\infty) \longrightarrow \mathrm{Sel}_p(E/K_\infty) \longrightarrow \prod_{i=1,2} \frac{H^1(K_{\mathfrak{p}_\infty,i}, E[p])}{E(\mathbb{Q}_p) \otimes \mathbb{F}_p}.$$

We are now ready to show that conjecture A is true in this case. According to theorem 4.1 of [23] neither $\varinjlim R_{2n}\alpha_{2n}$ nor $\varinjlim R_{2n+1}\alpha_{2n+1}$ is $\overline{\Lambda}$-cotorsion. Therefore the conjecture will be proven if we show that $\varinjlim R_{2n}\alpha_{2n} \cap \varinjlim R_{2n+1}\alpha_{2n+1}$ is finite.

Since $\mathrm{Tr}_{K_{n+1}/K_n}(\alpha_{n+1}) = -\alpha_{n-1}$ therefore we have that $\mathrm{res}_{\mathfrak{p}_{2n,i}} \alpha_{2n} \in E^+(K_{\mathfrak{p}_{2n,i}})$ and $\mathrm{res}_{\mathfrak{p}_{2n+1,i}} \alpha_{2n+1} \in E^-(K_{\mathfrak{p}_{2n+1,i}})$. This implies that $\varinjlim R_{2n}\alpha_{2n} \subseteq \mathrm{Sel}_p{}^+(E/K_\infty)$ and $\varinjlim R_{2n+1}\alpha_{2n+1} \subseteq \mathrm{Sel}_p{}^-(E/K_\infty)$ and so it suffices to show that $\mathrm{Sel}_p{}^+(E/K_\infty) \cap \mathrm{Sel}_p{}^-(E/K_\infty)$ is finite. But by (5) above this intersection is $\mathrm{Sel}^1_p(E/K_\infty)$.

Now define

$$\mathcal{L}(K_\infty) = \prod_{i=1,2} E(\mathbb{Q}_p) \otimes \mathbb{F}_p \times \prod_{v \in \tilde{S}_{K_\infty}} E(K_{\infty,v}) \otimes \mathbb{F}_p.$$

We claim that this group is finite. First of all, by Mattuck's theorem we have that $E(\mathbb{Q}_p) \cong \mathbb{Z}_p \times T$ where T is finite group. Therefore $E(\mathbb{Q}_p) \otimes \mathbb{F}_p$ is finite. Now let $v \in \tilde{S}_{K_\infty}$ and let $l \neq p$ be the rational prime below v. For any n we will also let v denote the prime of K_n below v. By Mattuck's theorem we have $E(K_{n,v}) \cong \mathbb{Z}_l^r \times T$ where r is some integer and T is a finite group. Therefore $\#(E(K_{n,v}) \otimes \mathbb{F}_p) \leq p^2$. It follows that $E(K_{\infty,v}) \otimes \mathbb{F}_p$ is finite. Since $\tilde{S}_{K_\infty}$ is finite, we have shown that $\mathcal{L}(K_\infty)$ is in fact finite.

Now consider the following commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[r] \arrow[d] & H^1(G_S(K_\infty), E[p]) \arrow[r] \arrow[d] & H^1(G_S(K_\infty), E[p]) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathcal{L}(K_\infty) \arrow[r] & \prod_{v \in S_{K_\infty}} H^1(K_{\infty,v}, E[p]) \arrow[r] & \prod_{v \in S_{K_\infty}} H^1(K_{\infty,v}, E[p])/\mathcal{L}(K_\infty) \arrow[r] & 0
\end{tikzcd} \tag{6}$$

Applying the snake lemma to this diagram we get an exact sequence

$$0 \longrightarrow R^S_p(E/K_\infty) \longrightarrow \mathrm{Sel}^1_p(E/K_\infty) \longrightarrow \mathcal{L}(K_\infty)$$

Since $\mathcal{L}(K_\infty)$ is finite, the exact sequence shows that $R^S_p(E/K_\infty)$ is finite if and only if $\mathrm{Sel}^1_p(E/K_\infty)$ is finite. Therefore it suffices to show that $R^S_p(E/K_\infty)$ is finite. To show this, we note that by [23] corollary 2.4 we have $E(K_\infty)[p^\infty] = \{0\}$ from which it follows that the natural map $R^S_p(E/K_\infty) \to R_{p^\infty}(E/K_\infty)[p]$ is an injection. Since $R_{p^\infty}(E/K_\infty)$ is cofinitely generated over $\mathbb{Z}_p$, therefore $R_{p^\infty}(E/K_\infty)[p]$ is finite. This in turn implies that $R^S_p(E/K_\infty)$ is finite which completes the proof. □

Theorem 3.3. *Assume that (E, π, p) satisfies $(*)$ then we have*

(a) If E has ordinary reduction at p, then conjecture C(i) and conjecture B (for $\mathcal{E} = E$, $F = K$ and $l = p$) are equivalent.

(b) If p splits in $K/\mathbb{Q}$ and E has supersingular reduction at p, then conjecture C(ii) and conjecture B (for $\mathcal{E} = E$, $F = K$ and $l = p$) are equivalent (and hence also equivalent to conjecture A by the previous theorem).

Proof. First we prove (a): Assume that E has ordinary reduction at p and conjecture C(i) is true. Consider the module $\varinjlim R_n\alpha_n \subseteq \mathrm{Sel}_p(E/K_\infty)$. By [23] theorem 3.1, theorem 3.1 and corollary 2.6 we have that both $\varinjlim R_n\alpha_n$ and $\mathrm{Sel}_p(E/K_\infty)$ are finitely generated $\overline{\Lambda}$-modules and that $\mathrm{corank}_{\overline{\Lambda}}(\varinjlim R_n\alpha_n) \geq 1$ and $\mathrm{corank}_{\overline{\Lambda}}(\mathrm{Sel}_p(E/K_\infty)) \leq 1$. Since $\varinjlim R_n\alpha_n$ is contained in $\mathrm{Sel}_p(E/K_\infty)$, therefore it follows that both their $\overline{\Lambda}$-coranks must be equal to one.

Now let S be the set of primes of K dividing Np. By the same argument in the proof of theorem 3.2, we have that $R^S_p(E/K_\infty) \to R_{p^\infty}(E/K_\infty)[p]$ has a finite cokernel and therefore to prove conjecture B we only have to show that $R_p^S(E/K_\infty)$ is finite. Since $R_p^S(E/K_\infty) \subseteq \mathrm{Sel}_p(E/K_\infty)$ and both $\varinjlim R_n\alpha_n$ and $\mathrm{Sel}_p(E/K_\infty)$ have $\overline{\Lambda}$-coranks equal to one, therefore it is is easy to see that the finiteness of $R_p^S(E/K_\infty)$ will follow if we can show that $M := \varinjlim R_n\alpha_n \cap R_p^S(E/K_\infty)$ is finite.

Assume on the contrary that M is infinite. Since finitely generated torsion $\overline{\Lambda}$-modules are finite and $\mathrm{corank}_{\overline{\Lambda}}(\varinjlim R_n\alpha_n) = 1$, therefore M must also have $\overline{\Lambda}$-corank equal to one. Therefore $\varinjlim R_n\alpha_n/M$ is finite and so is annihilated by $g^{p^m}-1$ for some $m \in \mathbb{N}$ where g is a topological generator of Γ i.e. $(g^{p^m}-1)\varinjlim R_n\alpha_n \subset R_p^S(E/K_\infty)$.

Let $\mathfrak{p}$ be a prime of K above p. Since we have assumed that the class number of K is prime to p, therefore $\mathfrak{p}$ is totally ramified in K_∞/K. For any n let $\mathfrak{p}_n$ be the prime of K_n above $\mathfrak{p}$. Since $(g^{p^m}-1)\varinjlim R_n\alpha_n \subseteq R_p^S(E/K_\infty)$, therefore by the definition of the fine p-Selmer group we have $(g^{p^m}-1)\varinjlim R_n \operatorname{res}_{\mathfrak{p}_n} \alpha_n = 0$ and so $\varinjlim R_n \operatorname{res}_{\mathfrak{p}_n} \alpha_n$ is $\overline{\Lambda}$-cotorsion. This contradicts conjecture C(i) which completes the proof of the forward implication of part (a) of the theorem.

Now assume that E has ordinary reduction at p and conjecture B is true. We must show that conjecture C(i) is true. Arguing by contradiction, assume that conjecture C(i) is false i.e. that for every prime $\mathfrak{p}_\infty$ of K_∞ above p the Γ-submodule of $E(K_{\mathfrak{p}_\infty})/p$ generated by the Heegner points α_n is finite. Let S be the set of primes of K dividing Np and let g be a topological generator of Γ. We claim that there exists a $k \in \mathbb{N}$ such that $(g^{p^k}-1)\varinjlim R_n\alpha_n \subseteq R_p^S(E/K_\infty)$. From the definition of $R_p^S(E/K_\infty)$, to show this, we need to prove that there exists a $k \in \mathbb{N}$ such that for all $s \in \varinjlim R_n\alpha_n$ we have $\operatorname{res}_v((g^{p^k}-1)s) = 0$ for any $v \in S_{K_\infty}$. Note that since we have assumed that all the primes dividing N to split in $K/\mathbb{Q}$ therefore it follows from [4] th. 2 that S_{K_∞} is finite.

Let $v \in S_{K_\infty}$ be a prime not dividing p. Since the set S_{K_∞} is finite, therefore the decomposition group of v in Γ is nontrivial and so is of the form Γ^{p^m} for some m. Now let $s \in \varinjlim R_n\alpha_n$. Then $\operatorname{res}_v(s) \in E(K_{\infty,v})/p$ and we claim that $E(K_{\infty,v})/p$ is finite. To see this, let $l \neq p$ be the rational prime below v. For any n we will also let v denote the prime of K_n below v. By Mattuck's theorem we have $E(K_{n,v}) \cong \mathbb{Z}_l^r \times T$ where r is some integer and T is a finite group. Therefore $\#(E(K_{n,v})/p) \leq p^2$. It follows from this that $E(K_{\infty,v})/p$ is in fact finite as claimed. The decomposition group Γ^{p^m} acts on the finite group $E(K_{\infty,v})/p$ so there exists $k_v \geq m$ such that $(g^{p^{k_v}}-1)E(K_{\infty,v})/p = 0$. It follows that we have $\operatorname{res}_v((g^{p^{k_v}}-1)s) = (g^{p^{k_v}}-1)\operatorname{res}_v(s) = 0$.

Now let $v \in S_{K_\infty}$ be a prime above p. Since we have assumed that the class number of K is relatively prime to p, therefore every prime of K above p is totally ramified in K_∞/K. Let $s \in \varinjlim R_n\alpha_n$. Since conjecture C(i) is false therefore the Γ-submodule of $E(K_{\infty,v})/p$ generated by the points α_n is finite and so there exists $k_v \in N$ such that $g^{p^{k_v}}-1$ that annihilates this submodule. It follows that $\operatorname{res}_v((g^{p^{k_v}}-1)s) = (g^{p^{k_v}}-1)\operatorname{res}_v(s) = 0$.

We have shown that for every $v \in S_{K_\infty}$ there exists $k_v \in \mathbb{N}$ such that $\operatorname{res}_v((g^{p^{k_v}}-1)s) = 0$ for any $s \in \varinjlim R_n\alpha_n$. Then taking k to be the maximum of the integers k_v we get $\operatorname{res}_v((g^{p^k}-1)s) = 0$ for all $s \in \varinjlim R_n\alpha_n$ and any $v \in S_{K_\infty}$. This implies that $(g^{p^m}-1)\varinjlim R_n\alpha_n \subseteq R_p^S(E/K_\infty)$ as desired. By theorem 3.1 of [23], $\varinjlim R_n\alpha_n$

has $\overline{\Lambda}$-corank greater than or equal to one. Therefore $(g^{p^m}-1)\varinjlim R_n\alpha_n$ also has $\overline{\Lambda}$-corank greater than or equal to one and as this group is contained in $R_p^S(E/K_\infty)$ it follows that $R_p^S(E/K_\infty)$ is infinite. Now by corollary 2.4 of [23], $E(K_\infty)[p^\infty]=\{0\}$ so the natural map $R_p^S(E/K_\infty)\to R_{p^\infty}(E/K_\infty)[p]$ is an injection. This proves that $R_{p^\infty}(E/K_\infty)[p]$ is infinite i.e. that $R_{p^\infty}(E/K_\infty)$ is not cofinitely generated over $\mathbb{Z}_p$. This contradicts our assumption that conjecture B is true which thereby proves the backward implication of part (a).

We now prove part (b): First we prove the forward implication. Assume that p splits in $K/\mathbb{Q}$, E has supersingular reduction at p and conjecture C(ii) is true. Then there exists a prime $\mathfrak{p}_\infty$ of K_∞ above p such that both $\varinjlim R_{2n}\operatorname{res}_{\mathfrak{p}_{2n}}\alpha_{2n}$ and $\varinjlim R_{2n+1}\operatorname{res}_{\mathfrak{p}_{2n+1}}\alpha_{2n+1}$ are infinite (where $\mathfrak{p}_n$ be the prime of K_n below $\mathfrak{p}_\infty$). In what follows let $K_{\mathfrak{p}_n}$ be the completion of K_n with respect to $\mathfrak{p}_n$.

To prove conjecture B is true, it suffices by theorem 3.2 to prove that conjecture A is true. To prove this, it clearly suffices to show that $\varinjlim R_{2n}\operatorname{res}_{\mathfrak{p}_{2n}}\alpha_{2n}+\varinjlim R_{2n+1}\operatorname{res}_{\mathfrak{p}_{2n+1}}\alpha_{2n+1}$ has $\overline{\Lambda}$-corank greater than or equal to two (note that both $\varinjlim R_{2n}\operatorname{res}_{\mathfrak{p}_{2n}}\alpha_{2n}$ and $\varinjlim R_{2n+1}\operatorname{res}_{\mathfrak{p}_{2n+1}}\alpha_{2n+1}$ are cofinitely generated $\overline{\Lambda}$-modules since both $\varinjlim R_{2n}\alpha_{2n}$ and $\varinjlim R_{2n+1}\alpha_{2n+1}$ are cofinitely generated $\overline{\Lambda}$-modules by the argument in theorem 4.1 of [23]).

Since finitely generated torsion $\overline{\Lambda}$-modules are finite, therefore conjecture C(ii) implies that both $\varinjlim R_{2n}\operatorname{res}_{\mathfrak{p}_{2n}}\alpha_{2n}$ and $\varinjlim R_{2n+1}\operatorname{res}_{\mathfrak{p}_{2n+1}}\alpha_{2n+1}$ have $\overline{\Lambda}$-coranks greater than or equal to one so to prove conjecture A we only have to show that $X:=\varinjlim R_{2n}\operatorname{res}_{\mathfrak{p}_{2n}}\alpha_{2n}\cap\varinjlim R_{2n+1}\operatorname{res}_{\mathfrak{p}_{2n+1}}\alpha_{2n+1}$ is finite. To show this, we use the same argument as in theorem 3.2.

Following Kobayashi [20] we define the following subgroups of $E(K_{\mathfrak{p}_n})$

$$E^+(K_{\mathfrak{p}_n}):=\{x\in E(K_{\mathfrak{p}_n})\mid \operatorname{Tr}_{n/m+1}(x)\in E(K_{\mathfrak{p}_m})\text{ for even }m:\ 0\le m<n\}$$
$$E^-(K_{\mathfrak{p}_n}):=\{x\in E(K_{\mathfrak{p}_n})\mid \operatorname{Tr}_{n/m+1}(x)\in E(K_{\mathfrak{p}_m})\text{ for odd }m:\ 0\le m<n\}.$$

We then define $E^+(K_{\mathfrak{p}_\infty}):=\bigcup_{n\in\mathbb{N}}E^+(K_{\mathfrak{p}_n})$ and $E^-(K_{\mathfrak{p}_\infty}):=\bigcup_{n\in\mathbb{N}}E^-(K_{\mathfrak{p}_n})$.

We now analyze the intersection of $E^+(K_{\mathfrak{p}_\infty})\otimes\mathbb{F}_p$ and $E^-(K_{\mathfrak{p}_\infty})\otimes\mathbb{F}_p$ where we view both of these groups as subgroups of $E(K_{\mathfrak{p}_\infty})\otimes\mathbb{F}_p$. By a proof identical to that of lemma 2.6.5 of [6], using a result of Iovita and Pollack [19], we have

$$E^+(K_{\mathfrak{p}_\infty})\otimes\mathbb{F}_p\cap E^-(K_{\mathfrak{p}_\infty})\otimes\mathbb{F}_p=E(\mathbb{Q}_p)\otimes\mathbb{F}_p.$$

Since $\operatorname{Tr}_{K_{n+1}/K_n}(\alpha_{n+1})=-\alpha_{n-1}$, therefore it follows that $\varinjlim R_{2n}\operatorname{res}_{\mathfrak{p}_{2n}}\alpha_{2n}\subseteq E^+(K_{\mathfrak{p}_\infty})$ and $\varinjlim R_{2n+1}\operatorname{res}_{\mathfrak{p}_{2n+1}}\alpha_{2n+1}\subseteq E^-(K_{\mathfrak{p}_\infty})$ so we have

$$X\subseteq E^+(K_{\mathfrak{p}_\infty})\cap E^-(K_{\mathfrak{p}_\infty})=E(\mathbb{Q}_p)\otimes\mathbb{F}_p.$$

But by Mattuck's theorem, $E(\mathbb{Q}_p)\cong\mathbb{Z}_p\times T$ where T is a finite group. Therefore $E(\mathbb{Q}_p)\otimes\mathbb{F}_p$ is finite which in turn makes X finite. This completes the proof of the forward implication of part (b).

Now assume that p splits in $K/\mathbb{Q}$, E has supersingular reduction at p and conjecture B is true. We will prove that backward implication i.e. that conjecture C(ii) is true. The proof goes along the same lines as the backward implication of part (a), however since we have to deal with the Heegner points α_{2n} and the points α_{2n+1} separately the proof is not as straightforward.

Arguing by contradiction, assume that conjecture C(ii) is false. Since p splits in $K/\mathbb{Q}$ and the class number of K is prime to p therefore there are 2 primes $\mathfrak{p}_\infty$ and $\bar{\mathfrak{p}}_\infty$ of K_∞ above p. Since conjecture C(ii) is false, either the Γ-submodule of $E(K_{\mathfrak{p}_\infty})/p$ generated by the points α_{2n} or the Γ-submodule generated by the points α_{2n+1} is finite. Let us assume that the the former submodule is finite (if the former submodule is infinite and the latter is finite our proof will be very similar). Then there exists an $k \in \mathbb{N}$ such that $(g^{p^k}-1)\varinjlim R_{2n}\operatorname{res}_{\mathfrak{p}_{2n}}\alpha_{2n}=0$ ($\mathfrak{p}_n$ is the prime of K_n below $\mathfrak{p}_\infty$).

Now let S be the set of primes of K dividing Np. We claim that for some $m \in \mathbb{N}$ we have $(g^{p^m}-1)\varinjlim R_{2n}\alpha_{2n} \subseteq R_p^S(E/K_\infty)$. By the proof of the backward implication of part (a), we see that to prove this it suffices to show that $\operatorname{res}_v((g^{p^k}-1)s)=0$ for any $s \in \varinjlim R_{2n}\alpha_{2n}$ any $v \in \{\mathfrak{p}_\infty, \bar{\mathfrak{p}}_\infty\}$. Let τ be a complex conjugation of K_∞ so that $\tau\mathfrak{p}_\infty=\bar{\mathfrak{p}}_\infty$. Since $(g^{p^k}-1)\varinjlim R_{2n}\operatorname{res}_{\mathfrak{p}_{2n}}\alpha_{2n}=0$, therefore for any $s \in \varinjlim R_{2n}\alpha_{2n}$ we have $\operatorname{res}_{\mathfrak{p}_\infty}((g^{p^k}-1)s)=0$ so we only have to show that $\operatorname{res}_{\bar{\mathfrak{p}}_\infty}((g^{p^k}-1)s)=0$.

The automorphism τ induces a "change of group" automorphism τ_* on $H^1(K_\infty, E[p])$ and an isomorphism $\tau_*: H^1(K_{\mathfrak{p}_\infty}, E[p]) \to H^1(K_{\bar{\mathfrak{p}}_\infty}, E[p])$. For any $s \in H^1(K_\infty, E[p])$ we have $\operatorname{res}_{\bar{\mathfrak{p}}_\infty}(\tau_*(s))=\tau_*(\operatorname{res}_{\mathfrak{p}_\infty}(s))$. From this we see that to show that $\operatorname{res}_{\bar{\mathfrak{p}}_\infty}((g^{p^k}-1)s)=0$ for all $s \in \varinjlim R_{2n}\alpha_{2n}$, we only have to show that $(g^{p^k}-1)\varinjlim R_{2n}\alpha_{2n}$ is τ-invariant.

Let $M=\varinjlim R_{2n}\alpha_{2n}$ and denote for any $t \in \mathbb{N}$ the group Γ^{p^t} by Γ_t. Clearly to show that $(g^{p^k}-1)M$ is τ-invariant it suffices to show that $(g-1)^{p^k}M^{\Gamma_t}=(g^{p^k}-1)M^{\Gamma_t}$ is τ-invariant for any t (note that $(g-1)^{p^k}\equiv g^{p^k}-1 \mod p$). Recall that $\tau g\tau=g^{-1}$. Therefore we have $\tau(g-1)^{p^k}M^{\Gamma_t}=(g^{-1}-1)^{p^k}\tau M^{\Gamma_t}$. Again since $\tau g\tau=g^{-1}$, therefore it follows that $\tau M^{\Gamma_t}\subseteq M^{\Gamma_t}$ so our desired result will follow if we can can show that $(g^{-1}-1)^{p^k}M^{\Gamma_t}\subseteq(g-1)^{p^k}M^{\Gamma_t}$. But Γ/Γ_t has order p^t so therefore $(g^{-1}-1)^{p^k}M^{\Gamma_t}=(g^{p^t-1}-1)^{p^k}M^{\Gamma_t}$ and the desired result follows since $g-1$ divides $g^{p^k-1}-1$.

We have shown that $(g^{p^m}-1)\varinjlim R_{2n}\alpha_{2n}\subseteq R_p^S(E/K_\infty)$ for some $m \in \mathbb{N}$. By theorem 4.1 of [23] $\varinjlim R_{2n}\alpha_{2n}$ has $\overline{\Lambda}$-corank greater than or equal to one. Therefore $(g^{p^m}-1)\varinjlim R_{2n}\alpha_{2n}$ also has $\overline{\Lambda}$-corank greater than or equal to one and as this group is contained in $R_p^S(E/K_\infty)$, it follows that $R_p^S(E/K_\infty)$ is infinite. Now by corollary 2.4 of [23] $E(K_\infty)[p^\infty]=\{0\}$ so the natural map $R_p^S(E/K_\infty)\to R_{p^\infty}(E/K_\infty)[p]$ is an injection. This proves that $R_{p^\infty}(E/K_\infty)[p]$ is infinite i.e. that $R_{p^\infty}(E/K_\infty)$ is not cofinitely generated over $\mathbb{Z}_p$. This contradicts our assumption that conjecture B is true which thereby proves the backward implication of part (b).

□

Theorem 3.4. *Suppose that (E,π,p) satisfies $(*)$ then we have*

(a) If E has ordinary reduction at p, then $\operatorname{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ has Λ-rank equal to 1 and μ-invariant equal to zero.

(b) *If p splits in $K/\mathbb{Q}$, E has supersingular reduction at p and conjecture C(ii) is true, then* $\mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ *has Λ-rank equal to 2 and μ-invariant equal to zero.*

Proof. Note that by theorems 3.2 and 3.3, conjecture C(ii) implies conjecture A (also see the comments made in the proof of theorem 3.1 about conjecture A versus conjecture A*). Therefore by theorems A and B in [23], $\mathrm{Sel}_p(E/K_\infty)^{\mathrm{dual}}$ has Λ-rank 1 in the ordinary case (part (a)) and rank 2 in supersingular case (part (b)). By corollary 2.4 in [23] we have that $E(K_\infty)[p^\infty] = \{0\}$ and therefore we have an isomorphism $\mathrm{Sel}_p(E/K_\infty) \xrightarrow{\sim} \mathrm{Sel}_{p^\infty}(E/K_\infty)[p]$. From this and the value of the Λ-corank of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$, we see that to show that $\mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ has μ-invariant equal to zero we need to show that the $\overline{\Lambda}$-corank of $\mathrm{Sel}_p(E/K_\infty)$ is less than or equal to one in the ordinary case (part (a)) and less than or equal to two in the supersingular case (part (b)). This follows from theorem 3.1 and corollary 2.6. □

4. Examples verifying Conjecture B

In the setup for conjecture B let $\Gamma = \mathrm{Gal}(F^{anti}/F)$ and $\Lambda = \mathbb{Z}_l[[\Gamma]]$ the corresponding Iwasawa algebra. Conjecture B predicts that $R_{l^\infty}(\mathcal{E}/F^{anti})$ is cofinitely generated over $\mathbb{Z}_l$. It is easy to see that this is equivalent to both of the following statements
(a) $R_{l^\infty}(\mathcal{E}/F^{anti})^{\mathrm{dual}}$ is a torsion Λ-module
(b) $R_{l^\infty}(\mathcal{E}/F^{anti})^{\mathrm{dual}}$ has μ-invariant equal to zero

Statement (a) is equivalent to $H^2(G_S(F^{anti}), E[p^\infty]) = 0$ (see [9] lemma 3.1) and is usually called the weak Leopoldt conjecture. It has been proven by Bertolini [2] when $\mathcal{E}$ is defined over $\mathbb{Q}$ and l is prime where E has good ordinary reduction (together with some additional conditions listed in that paper). When E has supersingular reduction at l and l splits in $F/\mathbb{Q}$ then the weak Leopoldt conjecture is also true. This follows from [5] theorem 3.1 and [19] theorem 6.1.

In this section we will produce examples verifying conjecture B. The examples will be constructed using the following theorem whose proof relies fundamentally on the work of Wuthrich [32].

Before stating the theorem, consider an elliptic curve E defined over a number field K and let v be a prime of K. If K_v denotes the completion of K at v then, as is standard, we let $E_0(K)$ denote the subgroup of $E(K_v)$ with nonsingular reduction modulo v and $E_1(K_v)$ the subgroup of points in $E_0(K_v)$ that reduce to the identity. Write $c_v = [E_0(K) : E_1(K)]$ and write $\log_{E,v} : E_1(K_v) \to K_v$ for the formal logarithm map. This map depends on our choice of a minimal Weierstrass equation for E over K_v, but its values are well-defined up to multiplication by a unit in O_v, the ring of integers of K_v. Finally, let $i_v : E(K) \to E(K_v)$ be the natural embedding.

Theorem 4.1. *Let E be an elliptic curve of conductor N defined over $\mathbb{Q}$ and let K be an imaginary quadratic field of discriminant d_K such that all the primes dividing N split in $K/\mathbb{Q}$. Let $p \nmid Nd_K$ be an odd rational prime such that* $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) = GL_2(\mathbb{F}_p)$. *For this prime p, let K_∞/K be the anticyclotomic $\mathbb{Z}_p$-extension of K. Now if $K[1]$ is the Hilbert class field of K, then a choice of an ideal $\mathcal{N}$ of $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$ and a modular parametrization $X_0(N) \to E$ allows us* *to define a Heegner point $y_1 \in E(K[1])$. Let y_K be the trace of this point down to K. We make the following assumptions*

(a) The Heegner point $y_K \in E(K)$ has infinite order (equivalent to $L'(E/K,1) \neq 0$ by Zhang's [34] *generalization to the Gross-Zagier theorem* [17] [1]*).*

(b) p does not divide the image of the y_K in $E(K)/E(K)_{tors}$

(c) For every prime v of K dividing p we have $p \nmid \#\tilde{E}(k_v)$ (where k_v is the residue field of K_v and $\tilde{E}$ is the reduced curve)

(d) For every prime v of K we have $p \nmid c_v$

(e) There exists a prime v of K above p and a point $P \in \cap_{w|p} i_w^{-1}(E_1(K_w))$ such that $\mathrm{ord}_v(\log_{E,v}(i_v(P))) = 1$

Under the above assumptions, we have that $R_{p^\infty}(E/K_\infty)$ is cofinitely generated over $\mathbb{Z}_p$.

Proof. The proof of this theorem relies on the work of Wuthrich [32] on the Euler characteristic of the fine Selmer group. First of all, let us consider the compact version of the fine Selmer group. Let S be the finite set of primes of K dividing p and where E has bad reduction. Let K_S be the maximal extension of K unramified outside of S and $G_S(K) = \mathrm{Gal}(K_S/K)$. The compact fine Selmer group $\mathfrak{R}_p(E/K)$ is defined by the following exact sequence

$$0 \longrightarrow \mathfrak{R}_p(E/K) \longrightarrow H^1(G_S(K), T_pE) \longrightarrow \prod_{v|p} H^1(K_v, T_pE).$$

In the above and what follows, if M is an abelian group, then T_pM will denote its p-adic Tate module.

We claim that $\mathfrak{R}_p(E/K)$ is trivial. To see this, first note that by the proof of lemma 3.1 in Wuthrich's paper we have that $\mathfrak{R}_p(E/K)$ injects into $T_pR_{p^\infty}(E/K)$ so we only have to show that $T_pR_{p^\infty}(E/K)$ is trivial. To prove this, note that by [33] we have an exact sequence

$$0 \longrightarrow M_{p^\infty}(E/K) \longrightarrow R_{p^\infty}(E/K) \longrightarrow \text{Ж}_{p^\infty}(E/K) \longrightarrow 0 \tag{7}$$

where $M_{p^\infty}(E/K)$ is defined as

$$0 \longrightarrow M_{p^\infty}(E/K) \longrightarrow E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \prod_{v|p} E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p.$$

and $\text{Ж}_{p^\infty}(E/K)$ is the fine Tate-Shafarevich group defined as simply $\text{Ж}_{p^\infty}(E/K) = R_{p^\infty}(E/K)/M_{p^\infty}(E/K)$. It is shown in [33] that $\text{Ж}_{p^\infty}(E/K)$ is a subgroup of $\text{Ш}(E/K)[p^\infty]$.

From equation (7) above, to show that $T_pR_{p^\infty}(E/K)$ is trivial it suffices to show that both $T_pM_{p^\infty}(E/K)$ and $T_p\text{Ж}_{p^\infty}(E/K)$ are trivial which we now show. Condition (a) of the theorem implies by the work of Kolyvagin [21] that $E(K)$ has rank 1 and that $\text{Ш}(E/K)$ is finite. Since $\text{Ш}(E/K)$ is finite and $\text{Ж}_{p^\infty}(E/K)$ is a subgroup of $\text{Ш}(E/K)[p^\infty]$ therefore $T_p\text{Ж}_{p^\infty}(E/K)$ is trivial. As for $T_pM_{p^\infty}(E/K)$, the fact that it is trivial follows easily from the definition of $M_{p^\infty}(E/K)$, and the fact that the rank of $E(K)$ is 1 and that by Mattuck's theorem for any prime v of K above p we have $E(K_v) \cong {\mathbb{Z}_p}^{[K_v:\mathbb{Q}_p]} \times T$ where T is a finite group. Thus we

[1] Gross and Zagier assume in their paper that the discriminant of K is odd. This assumption is removed by Zhang

have shown that $T_pR_{p^\infty}(E/K)$ is trivial which as we explained above proves that $\mathfrak{R}_p(E/K)$ is trivial.

We now return to Wuthrich's paper [32] and refer to it for the rest of the proof. Attached to the anticyclotomic $\mathbb{Z}_p$-extension K_∞/K Wuthrich defines a p-adic height pairing (he defines a pairing for any $\mathbb{Z}_p$-extension of K):

$$\langle\ ,\ \rangle_{K_\infty} : \mathfrak{R}_p(E/K) \times \mathfrak{R}_p(E/K) \longrightarrow \mathbb{Q}_p.$$

Since $\mathfrak{R}_p(E/K)$ is trivial, therefore the above pairing is non-degenerate. This implies by theorem 6.1 in Wuthrich's paper that $R_{p^\infty}(E/K_\infty)^{\text{dual}}$ is a torsion Λ-module where Λ is the Iwasawa algebra attached to the extension K_∞/K. Let $\Gamma = \text{Gal}(K_\infty/K)$. Choosing a topological generator $\gamma \in \Gamma$ allows us to identify the Iwasawa algebra Λ with $\mathbb{Z}_p[[T]]$ (via an isomorphism mapping $\gamma - 1$ to T) and so with this choice of a topological generator γ we may define the characteristic polynomial $f_R(T)$ of the torsion Λ-module $R_{p^\infty}(E/K_\infty)^{\text{dual}}$. If k is the order of vanishing of $f_R(T)$, then define $f_R^*(0) = T^{-k} f_R(T)|_{T=0}$ (Using part (2) of theorem 6.1 in Wuthrich's paper the value of k is equal to $\text{corank}_{\mathbb{Z}_p}(R_{p^\infty}(E/K))$. It is not hard to show this latter value is 1). $f_R^*(0)$ is called the Euler characteristic of $R_{p^\infty}(E/K_\infty)^{\text{dual}}$ and its valuation is independent of the choice of γ.

To prove that $R_{p^\infty}(E/K_\infty)^{\text{dual}}$ is finitely generated over $\mathbb{Z}_p$ we only need to show that $f_R^*(0)$ is a p-adic unit. We show this using part (4) of theorem 6.1 in Wuthrich. Taking into account that $\mathfrak{R}_p(E/K)$ is trivial, Wuthrich's theorem gives

$$f_R^*(0) \equiv \frac{\# T_{loc} \cdot \#(R_{p^\infty}(E/K)/\operatorname{div})}{\# T_{gl} \cdot \# J \cdot \# I} \pmod{\mathbb{Z}_p^\times} \tag{8}$$

In the above $R_{p^\infty}(E/K)/\operatorname{div}$ means the quoient of $R_{p^\infty}(E/K)$ by its maximal divisible subgroup. I is the cokernel of the injection $\mathfrak{R}_p(E/K) \hookrightarrow T_pR_{p^\infty}(E/K)$ defined in lemma 3.1 of Wuthrich's paper and J is the cokernel of a certain map described in his paper. Now we turn to the description of T_{gl} and T_{loc}. In what follows let S be the primes of K dividing Np

We have $T_{gl} = H^1(\Gamma, E(K_\infty)[p^\infty])$ and $T_{loc} = \prod_{v \in S} H^1(\Gamma_v, E(K_{\infty,v})[p^\infty])$.

In the description of T_{loc} the product runs over all primes v in S where for every such prime v we choose a prime w of K_∞ above v. If K_n is the subfield of K_∞ of degree p^n over K, we denote the union of the completions of the fields K_n at w by $K_{\infty,v}$ and the decomposition group of w by Γ_v.

We now calculate the orders of T_{gl} and T_{loc}. When K_∞ is the cyclotomic $\mathbb{Z}_p$-extension of K, Wuthrich uses a result of Imai [18] which states that if E is an elliptic curve defined over $\mathbb{Q}_p$ with good reduction and $L/\mathbb{Q}_p$ is the cyclotomic $\mathbb{Z}_p$-extension, then $E(L)_{\text{tors}}$ is finite. Using Imai's result allows one to give a nice description of T_{gl} and T_{loc} in the cyclotomic case. But we cannot apply Imai's result in our case so instead we will show that $\# T_{gl} = 1$ and that the order of T_{loc} divides the value stated in Wuthrich's paper. This will suffice for our purpose.

First we show that the fields $\mathbb{Q}(E[p])$ and K are disjoint. To see this, note that the only primes that can ramify in $\mathbb{Q}(E[p])/\mathbb{Q}$ are primes dividing Np, but since N was assumed to split in $K/\mathbb{Q}$ and p not to ramify in $K/\mathbb{Q}$, therefore the intersection of $\mathbb{Q}(E[p])$ and K is an unramified extension of $\mathbb{Q}$ and is therefore $\mathbb{Q}$ itself so $\mathbb{Q}(E[p])$ and K are indeed disjoint from which it follows that $E(K_\infty)[p^\infty]^\Gamma = E(K)[p^\infty] =$

$\{0\}$ which implies that $E(K_\infty)[p^\infty] = \{0\}$ since Γ is a pro-p group. So therefore we have

$$\#T_{gl} = 1 = \#E(K)[p^\infty] \tag{9}$$

We now calculate the order of T_{loc}. To do this, we need to calculate the order of $H^1(\Gamma_v, E(K_{\infty,v})[p^\infty])$ for any $v \in S$. First let $v \nmid p$ i.e. v divides N. Since we have assumed that all the primes dividing N to split in $K/\mathbb{Q}$, therefore by [4] theorem 2, v does not split completely in K_∞/K and so by [9] lemma 3.4 we have $H^1(\Gamma_v, E(K_{\infty,v})[p^\infty]) = c_v^{(p)}$ where $c_v^{(p)}$ indicates the largest power of p dividing c_v. Now let $v|p$ and denote the maximal divisible subgroup of $E(K_{\infty,v})[p^\infty]$ by $\mathcal{D}$. In this case we see from the proof of lemma 4.2 in Wuthrich's paper that we have $\#H^1(\Gamma_v, E(K_\infty)[p^\infty]) = \#E(K_v)[p^\infty]/\#\mathcal{D}^\Gamma$. All together, the above 2 observations imply that

$$t \cdot \#T_{loc} = \prod_{v|p} \#E(K_v)[p^\infty] \cdot \prod_{v \nmid p} c_v^{(p)} \text{ for some } t \in \mathbb{Z} \tag{10}$$

By condition (a) of the theorem and the work of Kolyvagin [21], we have that $\text{Ш}(E/K)$ is finite and since $\text{Ж}(E/K)$ is a subgroup of $\text{Ш}(E/K)[p^\infty]$, it follows that $\text{Ж}(E/K)$ is finite as well. Therefore combining (8), (9) and (10), we see from the proof of corollary 6.2 in Wuthrich's paper that for some $t \in \mathbb{Z}$ we have

$$t \cdot \#J \cdot f_R^*(0) \equiv \#\mathrm{Tors}_{\mathbb{Z}_p}(D) \cdot \prod_{v \nmid p} c_v^{(p)} \cdot \#\text{Ж}_{p^\infty}(E/K) \pmod{\mathbb{Z}_p^\times} \tag{11}$$

where D is the cokernel of the localization map (induced by the maps i_v) from $E(K) \otimes \mathbb{Z}_p$ to the p-adic completion of $\prod_{v|p} E(K_v)$

As we explained above, to prove the theorem we only need to show that $f_R^*(0)$ is a p-adic unit. This will follow if we can show that the right-hand side of the above equivalence (11) is a p-adic unit.

From condition (b) and since we have assumed that p is odd and $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) = GL_2(\mathbb{F}_p)$, therefore by the work of Kolyvagin [21] $\text{Ш}(E/K)[p^\infty] = \{0\}$. So we have $\text{Ж}_{p^\infty}(E/K) = \{0\}$ as well since $\text{Ж}_{p^\infty}(E/K)$ is a subgroup of $\text{Ш}(E/K)[p^\infty]$. Also condition (d) gives $\prod_{v \nmid p} c_v^{(p)} = 1$ and so the right-hand side of the equivalence (11) is $\#\mathrm{Tors}_{\mathbb{Z}_p}(D)$. So we see that the theorem follows from the following proposition. □

Proposition 4.2. *If D is the cokernel of the localization map (induced from the maps i_v) from $E(K) \otimes \mathbb{Z}_p$ to the p-adic completion of $\prod_{v|p} E(K_v)$, then under conditions (a), (c) and (e) of theorem 4.1 $\#\mathit{Tors}_{\mathbb{Z}_p}(D) = 1$.*

Proof. If M is an abelian group we write $M^* = \varprojlim M/p^n M$ for its p-adic completion (p is the prime in the proposition). Also will denote $\cap_{w|p} i_w^{-1}(E_1(K_w))$ by $E_1(K)$.

Let $\psi_p : E(K)^* \to \prod_{v|p} E(K_v)^*$ be the map in the proposition. We need to prove that $\mathrm{Tors}_{\mathbb{Z}_p}(\mathrm{coker}(\psi_p)) = \{0\}$. We proceed as in [8] lemma 9. Since $\prod_{v|p} E(K_v)/E_1(K_v)$ is finite, therefore by [8] lemma 6 we have an exact sequence

$$0 \longrightarrow \prod_{v|p} E_1(K_v)^* \longrightarrow \prod_{v|p} E(K_v)^* \longrightarrow \prod_{v|p} (E(K_v)/E_1(K_v))^* \longrightarrow 0.$$

$E(K)/E_1(K)$ injects into $\prod_{v|p} E(K_v)/E_1(K_v)$ so is finite. Therefore, we also get an exact sequence

$$0 \longrightarrow E_1(K)^* \longrightarrow E(K)^* \longrightarrow (E(K)/E_1(K))^* \longrightarrow 0.$$

Condition (c) of theorem 4.1 implies that $\prod_{v|p}(E(K_v)/E_1(K_v))^*$ is trivial. This also in turn proves that $(E(K)/E_1(K))^*$ is also trivial. So we see from the above exact sequences that we have isomorphisms $E_1(K)^* \cong E(K)^*$ and $\prod_{v|p} E_1(K_v)^* \cong \prod_{v|p} E(K_v)^*$. Therefore we see that if $\psi'_p : E_1(K)^* \to \prod_{v|p} E_1(K_v)^*$ is the map induced by ψ_p, then to prove the proposition we only need to show that $\mathrm{Tors}_{\mathbb{Z}_p}(\mathrm{coker}(\psi'_p)) = \{0\}$.

Since p is odd and unramified in $K/\mathbb{Q}$, therefore from [29] ch. 4 th. 6.4 we have that for any v above p the map $\log_{E,v} : E_1(K_v) \to pO_v$ is an isomorphism (O_v is the ring of integers in K_v). Composing this isomorphism with multiplication by p^{-1} we get an isomorphism $E_1(K_v) \cong O_v$. Noting that $O_v^* = O_v$, this isomorphism induces an isomorphism $E_1(K_v)^* \cong O_v$. Finally composing the map ψ'_p with this last isomorphism, we get a map $\phi_p : E_1(K)^* \to \prod_{v|p} O_v$ and we will show that $\mathrm{Tors}_{\mathbb{Z}_p}(\mathrm{coker}(\phi_p)) = \{0\}$. Note that the map ϕ_p is a $\mathbb{Z}_p$-module homomorphism. Let $\theta : E(K) \to E(K)^*$ be the natural map. Then condition (e) of theorem 4.1 translates to: there exists $P \in E_1(K)$ such that for some i we have $\pi_i(\phi_p(\theta(P)))$ is a unit in O_v (π_i is the projection from $\prod_{v|p} O_v$ onto its i-th component).

Now consider 2 cases. First assume that p splits in $K/\mathbb{Q}$. Let v_1 and v_2 be the primes of K above p. In this case we have a map $\phi_p : E_1(K)^* \to O_{v_1} \times O_{v_2} = \mathbb{Z}_p \times \mathbb{Z}_p$. Condition (e) of theorem 4.1 implies that $\pi_i \circ \phi_p : E_1(K)^* \to \mathbb{Z}_p$ is surjective for $i = 1$ or $i = 2$. Without loss of generality assume that it is surjective for $i = 1$. Let $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_p$ such that $(ra, rb) \in \mathrm{img}(\phi_p)$ for some $r \in \mathbb{Z}_p\backslash\{0\}$. We must show that $(a, b) \in \mathrm{img}(\phi_p)$. Let $Q \in E_1(K)^*$ be such that $\phi_p(Q) = (ra, rb)$. Also since $\pi_1(\phi_p)$ is surjective there exists $P \in E_1(K)^*$ such that $\phi_p(P) = (a, c)$ for some $c \in \mathbb{Z}_p$. We now note that $\pi_1 \circ \phi_p$ is injective. This follows from the work of Kolyvagin [21] which shows that under condtion (a) of theorem 4.1 $E(K)$ has rank 1. This in turn also implies that $E_1(K)$ has rank 1 since $E(K)/E_1(K)$ is finite. Then we have $\pi_1(\phi_p(rP)) = r\pi_1(\phi(P)) = ra = \pi_1(\phi_p(Q))$ which implies that $rP = Q$ since $\pi_1 \circ \phi_p$ is injective. Therefore $(ra, rc) = (ra, rb)$ so $b = c$ showing that $(a, b) \in \mathrm{img}(\phi_p)$ as desired.

Now consider the case when p is inert in $K/\mathbb{Q}$. In this case we have a map $\phi_p : E_1(K)^* \to O_v$ where v is the prime of K above p. Note that O_v is free of rank 2 over $\mathbb{Z}_p$. Condition (e) of theorem 4.1 implies that there exists a $P \in E_1(K)^*$ such that $Q = \phi_p(P) \in O_v^\times$. Then by [14] ch. 2 prop 2.4 there exists $Q' \in O_v$ such that Q and Q' form a basis for the free $\mathbb{Z}_p$-module O_v. Since $\mathrm{img}(\phi_p) = \mathbb{Z}_pQ$, therefore we easily see from this that $\mathrm{Tors}_{\mathbb{Z}_p}(\mathrm{coker}(\phi_p)) = \{0\}$ as desired. This completes the proof of the proposition. □

The table below lists examples chosen to satisfy the conditions of theorem 4.1. The columns of the table are as follows: E is an elliptic curve defined over $\mathbb{Q}$ with the given Cremona labeling [13], D is a fundamental discriminant such that $K = \sqrt{D}$, p is a prime, (D/p) is the Legendre symbol which tells us whether our unramified prime p splits in $K/\mathbb{Q}$ ($(D/p) = 1$) or is inert in $K/\mathbb{Q}$ ($(D/p) = -1$) and the last column is the integer $a_p = p + 1 - \tilde{E}(\mathbb{F}_p)$. Since all the entries in the table have $p \geq 5$, therefore the elliptic curves E in the table with $a_p = 0$ are precisely the ones with supersingular reduction at p. In addition to satisfying the conditions of theorem 4.1, the entries in the table were chosen such that (E,p) satisfies $(*)$. All of the computations for the table were performed in SAGE [28].

E	D	p	(D/p)	a_p
11a1	-7	13	-1	4
11a1	-7	29	1	0
17a1	-8	11	1	0
17a1	-8	41	1	-6
43a1	-7	17	-1	-3
43a1	-7	37	1	0
53a1	-11	19	-1	-5
53a1	-11	751	1	0
57a1	-8	13	-1	2
57a1	-8	17	1	-1
57a1	-8	37	-1	0
58a1	-7	11	1	-1
58a1	-7	23	1	0
58a1	-23	13	1	3
58a1	-23	139	1	0
75a1	-11	17	-1	2
75a1	-11	79	-1	0
99a1	-35	17	1	2
99a1	-35	71	1	0

References

[1] M. Bertolini, *Selmer groups and Heegner points in anticyclotomic $\mathbb{Z}_p$-extensions*, Compositio Math. **99** (1995), 153-182

[2] M. Bertolini *Iwasawa theory for elliptic curves over imaginary quadratic fields*, Journal de thorie des nombres de Bordeaux **13**(1) (2001), 1-25

[3] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843-939.

[4] D. Brink, *Prime decomposition in the anti-cyclotomic extensions*, Mathematics of Computation, **76** (2007), no. 260, 2127-2138.

[5] M. Ciperiani, *Tate-Shafarevich groups in anticyclotomic $\mathbb{Z}_p$-extensions at supersingular primes*, Compositio Math. **145** (2009), 293-308

[6] M. Ciperiani, A. Wiles, *Solvable points on genus one cuves*, Duke Math. J. **142** (2008), 381-464

[7] J. Coates, R. Greenberg, *Kummer Theory for Abelian Varieties over Local Fields*, Invent. Math., **124** (1996), 129-174.

[8] J. Coates, G. McConnell, *Iwasawa theory of modular elliptic curves of analytic rank at most 1*, Jour. London Math. Soc. **2** (1994), 243-264

[9] J. Coates and R. Sujatha, *Fine Selmer groups of elliptic curves over p-adic Lie extensions*, Math. Ann. **331**, 2005, 809-839.

[10] J. Coates, R. Sujatha, *Galois Cohomology of Elliptic Curves* Tata Inst. Fund. Res. Lecture Notes, Narosa Publishing House, 2000.

[11] C. Cornut, *Mazur's conjecture on higher Heegner points*, Invent. Math. **148** (2002), 495-523

[12] C. Cornut, V. Vatsal, *CM points and quarternion algebras*, Doc. Math **10** (2005), 263-309

[13] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[14] I.B. Fesenko, S.V. Vostokov, *Local Fields and Their Extensions*, Second edition, American Mathematical Society, 2002, Translations of Mathematical Monographs no. 121.

[15] R. Greenberg, *Iwasawa theory for elliptic curves.* Lecture Notes in Math. 1716, Springer, New York 1999, pp.51-144.

[16] R. Greenberg, *Introduction to Iwasawa theory for elliptic curves*, IAS/Park City Math. Ser. 9, Amer. Math Soc. Providence, 2001, pp. 407-464.

[17] B. Gross, D. Zagier, *Heegner points and derivatives of L-series* Invent. Math. **84** (1986), no. 2, 225-320.

[18] , H. Imai, *A remark on the rational points of Abelian varieties with values in cyclotomic $\mathbb{Z}_p$-extensions*, Proc. Japan Acad. **51** (1975), 12-16.

[19] A. Iovita, R. Pollack, *Iwasawa theory of elliptic curves at supersingular primes over $\mathbb{Z}_p$-extensions of number fields*, J. Reine Angew. Math. **598** (2006), 71-103

[20] S. Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), 1-36

[21] V. Kolyvagin, *Euler Systems*, The Grothendieck Festschrift, Progr. in Math. 87, Birkhäuser Boston, Boston, MA (1990).

[22] Y.I. Manin, *Cyclotomic fields and modular curves.* Russian Math. Surveys **26**(6) 1971, 7-78.

[23] A. Matar, *Selmer groups and anticyclotomic $\mathbb{Z}_p$-extensions*, Math. Proc. Camb. Phil. Soc. **161**(3) (2016), 409-433

[24] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math **18** (1972), 183-266.

[25] J.S. Milne, *Arithmetic Duality Theorems*, second ed., BookSurge, LLC, Charleston, SC, 2006.

[26] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields*, second edition, Grundlehren der Mathematischen Wissenschaften **323**, Springer, 2008, xvi+825.

[27] B. Perrin-Riou, *Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner*, Bull. Soc. Math. France **115** (1987), 399-456

[28] *SageMath, the Sage Mathematics Software System (Version 7.4)*, The Sage Developers, 2016, http://www.sagemath.org.

[29] J. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. **106**, Springer-Verlag (1986)

[30] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (2) (1995), 443-551.

[31] J.S. Wilson, *Profinite Groups*, Oxford University Press, Oxford, UK, 1998.

[32] C. Wuthrich, *Iwasawa theory of the fine Selmer group*, J. Algebraic Geom. **16** (1) (2007) 83-108.

[33] C. Wuthrich, *The fine Tate-Shafarevich group*, Math. Proc. Camb. Phil. Soc. **142**(1) (2007) 1-12

[34] S.-W. Zhang, *Gross-Zagier formula for GL_2*, Asian J. Math. **5** (2001), 183-290.

Department of Mathematics, University of Bahrain, P.O. Box 32038, Sukhair, Bahrain

E-mail address: amatar@uob.edu.bh