PLUS/MINUS SELMER GROUPS 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. In this paper we prove two theorems. The first theorem shows that there is an intimate relationship between the Λ-corank of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$, the Λ-coranks of $\mathrm{Sel}^{\pm}_{p^\infty}(E/K_\infty)$ and the vanishing of $H^2(G_S(K_\infty), E[p^\infty])$. The second theorem proves under suitable conditions that the Pontryagin dual of $\mathrm{Sel}^{\pm}_{p^\infty}(E/K_\infty)$ has Λ-rank one and μ-invariant zero.

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 be an odd prime, 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 an elliptic curve of conductor N defined over $\mathbb{Q}$ with a modular parametrization $\pi : X_0(N) \to E$. Throughout the paper we assume that E has good supersingular reduction at p. Let S be a finite set of primes of K containing all the primes dividing pN. We let K_S be the maximal extension of K unramified outside S. Suppose now that L is a field with $K \subseteq L \subseteq K_S$. We let $G_S(L) = \mathrm{Gal}(K_S/L)$ and S_L be the set of primes of L above those in S. For simplicity, we will denote S_{K_n} by S_n and S_{K_∞} by S_∞.

We now define the Selmer groups we will work with. For any n and m we let $\mathrm{Sel}_{p^m}(E/K_n)$ denote the p^m-Selmer group of E over K_n defined by

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

We also define the p^∞-Selmer group of E over K_n as $\mathrm{Sel}_{p^\infty}(E/K_n) = \varinjlim_m \mathrm{Sel}_{p^m}(E/K_n)$.

Finally we define the p^m-Selmer group and the p^∞-Selmer group of E over K_∞ as $\mathrm{Sel}_{p^m}(E/K_\infty) = \varinjlim_n \mathrm{Sel}_{p^m}(E/K_n)$ and $\mathrm{Sel}_{p^\infty}(E/K_\infty) = \varinjlim_n \mathrm{Sel}_{p^\infty}(E/K_n)$.

Let $\mathfrak{p}$ be a prime of K_n above p. Following Kobayashi [14], we define the following subgroups of $E(K_{n,\mathfrak{p}})$

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

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

Following Kobayashi [14] and Iovita-Pollack [12], we define

$$0 \longrightarrow {\mathrm{Sel}_p}^{\pm}(E/K_n) \longrightarrow \mathrm{Sel}_p(E/K_n) \longrightarrow \prod_{\mathfrak{p}|p} \frac{H^1(K_{n,\mathfrak{p}}, E[p])}{E^{\pm}(K_{n,\mathfrak{p}}) \otimes \mathbb{F}_p}$$

and ${\mathrm{Sel}_p}^{\pm}(E/K_\infty) = \varinjlim_n {\mathrm{Sel}_p}^{\pm}(E/K_n)$

Also we define

$$0 \longrightarrow \mathrm{Sel}^{\pm}_{p^\infty}(E/K_n) \longrightarrow \mathrm{Sel}_{p^\infty}(E/K_n) \longrightarrow \prod_{\mathfrak{p}|p} \frac{H^1(K_{n,\mathfrak{p}}, E[p^\infty])}{E^{\pm}(K_{n,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}$$

and $\mathrm{Sel}^{\pm}_{p^\infty}(E/K_\infty) = \varinjlim_n \mathrm{Sel}^{\pm}_{p^\infty}(E/K_n)$

Finally, we need the definition of the fine p^∞-Selmer group of E/K_∞. This group is defined as

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

Now for any n, let $S_p(E/K_n) := \varprojlim_m \mathrm{Sel}_{p^m}(E/K_n)$ (inverse limit with respect to maps induced by multiplication by p). Let $\mathfrak{p}$ be a prime of K_n above p. We write $E(K_{n,\mathfrak{p}})_p := \varprojlim_m E(K_{n,\mathfrak{p}})/p^m$ for the p-adic completion of $E(K_{n,\mathfrak{p}})$ and define $E(K_{n,p})_p := \oplus_{\mathfrak{p}|p} E(K_{n,\mathfrak{p}})_p$. By the definition of the Selmer group, for any prime $\mathfrak{p}$ of K_n dividing p, there is a natural map $\rho_{n,\mathfrak{p}} : S_p(E/K_n) \to E(K_{n,\mathfrak{p}})_p$. These maps induce a map $\rho_{n,p} : S_p(E/K_n) \to E(K_{n,p})_p$. By abuse of notation, if $\mathfrak{p}$ is a prime of K_∞ above p, we have for any n a map $\rho_{n,\mathfrak{p}}$.

In what follows, if A is a Hausdorff, abelian locally-compact topological group we denote its Pontryagin dual by A^{dual}. Also, as is standard, we will denote a pseudo-isomorphism from Λ-modules A to B by $A \sim B$. Finally, for any rational prime v we will let c_v be the Tamagawa number of E at v.

Theorems A and B below rely on the results of Iovita-Pollack [12]. In order to invoke their results we will need to assume that p splits in $K/\mathbb{Q}$ and that any prime of K above p is totally ramified in K_∞/K. For theorem B we will replace this second condition by the slightly stronger condition that p does not divide the class number of K. This condition that $p \nmid h_K$ is used in [17] prop 3.3 and this proposition is needed for the proof of theorem B.

Theorem A below shows that there is an intimate relationship between the Λ-corank of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$, the Λ-coranks of $\mathrm{Sel}^{\pm}_{p^\infty}(E/K_\infty)$ and the Λ-corank of $R_{p^\infty}(E/K_\infty)$. Another thing the theorem shows is that the growth formula $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/K_n)) = p^n + O(1)$ follows from both $\mathrm{Sel}^{\pm}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ having Λ-rank one. This last statement was proven in [12] prop. 7.1 under the extra condition that $H^2(G_S(K_\infty), E[p^\infty]) = 0$. We remove this condition.

Theorem A. *Assume that $p \ge 5$, all primes dividing pN split in $K/\mathbb{Q}$ and both primes of K above p are totally ramified in K_∞/K. The following are equivalent*

(a) $\mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ *has* Λ*-rank two*
(b) Both $\mathrm{Sel}^{\pm}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ *have* Λ*-rank one*
(c) $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/K_n)) = p^n + O(1)$ *and* $\mathrm{rank}_{\mathbb{Z}_p}(\mathrm{img}\,\rho_{n,p}) = p^n + O(1)$
(d) $H^2(G_S(K_\infty), E[p^\infty]) = 0$
(e) $R_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ *is* Λ*-torsion*

Under some conditions Çiperiani [4] has shown that $\mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ has Λ-rank two and Longo-Vigni [15] have shown that both $\mathrm{Sel}^{\pm}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ have Λ-rank one. If we impose the extra condition in [4] that both primes of K above p are totally ramified in K_∞/K, then the above theorem shows that in this case the results of Çiperiani and Longo-Vigni are equivalent.

By adapting the proof of the ordinary case in [17] to the plus/minus Selmer groups we will show

Theorem B. *Assume the following*

(i) All the primes dividing pN *split in* $K/\mathbb{Q}$
(ii) p *does not divide* $6h_K\varphi(Nd_K)\cdot\prod_{\ell|N} c_v$
(iii) p *does not divide the number of geometrically connected components of the kernel of* $\pi_* : J_0(N) \to E$.

Then both $\mathrm{Sel}^{\pm}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ *have* Λ*-rank one and* μ*-invariant zero*

Under the conditions of theorem B, theorem B gives that both $\mathrm{Sel}^{\pm}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ have Λ-rank one and theorems A and B together imply that $\mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ has Λ-rank two. This gives a different proof to the results of Longo-Vigni [15] and Çiperiani [4]. Both of these cited results are proven under slightly less restrictive conditions. The advantage of imposing our extra conditions is that we also show that both $\mathrm{Sel}^{\pm}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ have μ-invariant zero. This result is analogous to theorem 3.4 of [18] which shows that $\mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ has μ-invariant zero in the case where E has good ordinary reduction at p.

It is an interesting question whether both $\mathrm{Sel}^{\pm}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ have μ-invariant zero implies that $\mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ has μ-invariant zero as well. As proposition 2.2 in the next section shows, we have a map $j : \mathrm{Sel}^{+}_{p^\infty}(E/K_\infty) \oplus \mathrm{Sel}^{-}_{p^\infty}(E/K_\infty) \to \mathrm{Sel}_{p^\infty}(E/K_\infty)$. One can attempt to use this map to relate the μ-invariants, however an understanding of the cokernel of the map j is needed. The author has not been able to get a handle on the μ-invariant of the Pontryagin dual of $\mathrm{coker}\, j$ and hence has been unable to deduce that $\mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ has μ-invariant zero.

In relation to the vanishing of the μ-invariant of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$, we would like to mention the following: in [18] the author conjectured (conjecture B) that $R_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ is cofinitely generated over $\mathbb{Z}_p$. Assuming that $H^2(G_S(K_\infty), E[p^\infty]) = 0$, it is interesting to note that this conjecture is equivalent to $\mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ having μ-invariant zero. This equivalence follows from the main theorem of [19] if one notes that $E(K_\infty)[p^\infty]$ is finite. The finiteness of $E(K_\infty)[p^\infty]$ can be shown by taking a prime $q \nmid pN$ that is inert in $K/\mathbb{Q}$. The prime $\mathfrak{q}$ of K above q splits completely in K_∞/K. Let $\mathfrak{Q}$ be some prime of K_∞ above $\mathfrak{q}$. Since the residue field $\mathbf{K}_{\infty,\mathfrak{Q}}$ of $K_{\infty,\mathfrak{Q}}$ is finite and $E(K_{\infty,\mathfrak{Q}})[p^\infty]$ injects into $E(\mathbf{K}_{\infty,\mathfrak{Q}})[p^\infty]$, the finiteness of $E(K_\infty)[p^\infty]$ follows.

Remark. Let $\mathfrak{p}$ be a prime of K_n above p and let $\hat{E}$ be the formal group of $E/\mathbb{Q}$. Then $\hat{E}(K_{n,\mathfrak{p}})$ is isomorphic to $E_1(K_{n,\mathfrak{p}}) = \ker(E(K_{n,\mathfrak{p}}) \to \bar{E}(\mathbf{K}_\mathfrak{p}))$ where $\mathbf{K}_\mathfrak{p}$ is the residue field of $K_{n,\mathfrak{p}}$. We then define $\hat{E}^{\pm}(K_{n,\mathfrak{p}}) \cong E_1(K_{n,\mathfrak{p}}) \cap E^{\pm}(K_{n,\mathfrak{p}})$. Since E has supersingular reduction at p, therefore $\tilde{E}(\mathbf{K}_{\mathfrak{p}})[p] = 0$. It follows that we have an isomorphism $\hat{E}^{\pm}(K_{n,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong E^{\pm}(K_{n,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. The plus/minus Selmer groups defined in [12] are defined as $\mathrm{Sel}^{\pm}_{p^\infty}(E/K_n)$ but with $E^{\pm}(K_{n,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ replaced with $\hat{E}^{\pm}(K_{n,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. By what we just explained, it follows that $\mathrm{Sel}^{\pm}_{p^\infty}(E/K_n)$ is identical to the Selmer group defined in [12].

2. Proof of Theorem A

In this section we prove theorem A in the introduction. First we make a few definitions. Let $\Phi_n(X) = \sum_{i=0}^{p-1} X^{ip^{n-1}}$ be the p^n-th cyclotomic polynomial and $\omega_n(X) = (X+1)^{p^n} - 1$. Also set

$$\tilde{\omega}_n^+ = \prod_{\substack{1 \leqq m \leqq n \\ m \text{ even}}} \Phi_m(X+1), \quad \tilde{\omega}_n^- = \prod_{\substack{1 \leqq m \leqq n \\ m \text{ odd}}} \Phi_m(X+1), \quad \tilde{\omega}_0^{\pm} = 1$$

$\omega_n^+ = X \cdot \tilde{\omega}_n^+$ and $\omega_n^- = X \cdot \tilde{\omega}_n^-$. Note that $\omega_n = X \cdot \tilde{\omega}_n^+ \cdot \tilde{\omega}_n^-$

For any $n \geq 0$ we define

$$q_n = \begin{cases} p^n - p^{n-1} + p^{n-2} - p^{n-3} + \cdots + p^2 - p + 1 & \text{if } 2|n \\ p^n - p^{n-1} + p^{n-2} - p^{n-3} + \cdots + p - 1 + 1 & \text{if } 2 \nmid n \end{cases}$$

q_n is the degree of ω_n^+ or ω_n^- depending on whether n is even or odd, respectively. We also define

$$0 \longrightarrow \mathrm{Sel}^1_{p^\infty}(E/K_n) \longrightarrow \mathrm{Sel}_{p^\infty}(E/K_n) \longrightarrow \prod_{\mathfrak{p}|p} \frac{H^1(K_{n,\mathfrak{p}}, E[p^\infty])}{E(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p}$$

Let $\mathrm{Sel}^1_{p^\infty}(E/K_\infty) := \varinjlim_n \mathrm{Sel}^1_{p^\infty}(E/K_n)$

For any n we write $\mathrm{Tr}_{n/n-1}$ for the trace $\mathrm{Tr}_{K_n/K_{n-1}}$ or $\mathrm{Tr}_{K_{n,v}/K_{n-1,v}}$ where v is a prime of K_n. It will be clear to the reader whether we mean the global or local trace.

We now define our Heegner points. 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 [26] and [3]). If we assume that every prime dividing N splits in $K/\mathbb{Q}$, then 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 N 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.

We assume that all primes of K above p are totally ramified in K_∞/K. This implies that K_∞/K and $K[1]/K$ are linearly disjoint ($K[1]$ is the Hilbert class field of K). It follows from this that for any $n \geq 1$ that $K[p^{n+1}]$ is the ring class field of minimal conductor that contains K_n. For any $n \geq 0$, 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 $p \geq 5$ be a prime. Assume that p splits in $K/\mathbb{Q}$. From section 3.3 of [23] it follows that

$$\mathrm{Tr}_{1/0}(\alpha_1) = (a_p - (a_p - 2)^{-1}(p-1))\alpha_0 \tag{1}$$
$$\mathrm{Tr}_{n+1/n}(\alpha_{n+1}) = a_p\alpha_n - \alpha_{n-1} \quad \text{for } n \geq 1 \tag{2}$$

Since E has supersingular reduction at p and $p \geq 5$, $a_p = 0$ so therefore we have

$$\mathrm{Tr}_{1/0}(\alpha_1) = \frac{p-1}{2}\alpha_0 \tag{3}$$
$$\mathrm{Tr}_{n+1/n}(\alpha_{n+1}) = -\alpha_{n-1} \quad \text{for } n \geq 1 \tag{4}$$

Lemma 2.1. *Assume that $p \geq 5$, all primes dividing pN split in $K/\mathbb{Q}$ and all primes of K above p are totally ramified in K_∞/K. For any $n \geq 0$ we have $\omega_{2n}^{+}\alpha_{2n} = 0$ and $\omega_{2n+1}^{-}\alpha_{2n+1} = 0$*

Proof. From equation (4) above we have $\omega_{2n}^{+}\alpha_{2n} = (\gamma-1)\tilde{\omega}_{2n}^{+}\alpha_{2n} = (\gamma-1)\pm\alpha_0 = 0$. A similar proof using also equation (3) shows that $\omega_{2n+1}^{-}\alpha_{2n+1} = 0$ □

We will need the following three intermediate results before proving theorem A

Proposition 2.2. *Assume that $p \geq 5$, p splits in $K/\mathbb{Q}$ and all primes of K above p are totally ramified in K_∞/K. For any $n \geq 0$ we have exact sequences*

$$0 \longrightarrow K \xrightarrow{i} \mathrm{Sel}_{p^\infty}^{+}(E/K_n) \oplus \mathrm{Sel}_{p^\infty}^{-}(E/K_n) \xrightarrow{j} \mathrm{Sel}_{p^\infty}(E/K_n) \longrightarrow C \longrightarrow 0$$

$$0 \longrightarrow K^{\omega_n^{\pm}=0} \xrightarrow{i} \mathrm{Sel}_{p^\infty}^{+}(E/K_n)^{\omega_n^{+}=0} \oplus \mathrm{Sel}_{p^\infty}^{-}(E/K_n)^{\omega_n^{-}=0} \xrightarrow{j} \mathrm{Sel}_{p^\infty}(E/K_n) \longrightarrow C' \longrightarrow 0$$

where i is the diagonal embedding, j is $(x,y) \mapsto x - y$, $K = \mathrm{Sel}_{p^\infty}^{1}(E/K_n)$ and C, C' are finite.

Proof. The description of the kernels of the maps j above follow from [12] prop. 4.11 and lemma 4.13. Clearly, the finiteness of C will follow from the finiteness of C'. The latter is essentially proposition 10.1 of Kobayashi's paper [14]. Given $P \in \mathrm{Sel}_{p^\infty}(E/K_n)_{\mathrm{div}}$ Kobayashi finds $P^+ \in \mathrm{Sel}_{p^\infty}^{+}(E/K_n)$ and $P^- \in \mathrm{Sel}_{p^\infty}^{-}(E/K_n)$ such that $j(P^+, P^-) = P$. We only need to show that $\omega_n^+ P^+ = 0$ and $\omega_n^- P^- = 0$. For a suitably chosen $Q \in \mathrm{Sel}_{p^\infty}(E/K_n), A, B \in \mathbb{Z}_p[X]$ Kobayashi defines $P^+ = A(\gamma-1)\tilde{\omega}_n^- Q$ and $P^- = B(\gamma-1)\omega_n^+ Q$. Since $\omega_n^+\tilde{\omega}_n^- = \gamma^{p^n} - 1$ and $(\gamma^{p^n} - 1)Q = 0$ therefore we see that $\omega_n^+ P^+ = 0$. Similarly one shows that $\omega_n^- P^- = 0$. □

Proposition 2.3. *Assume that $p \geq 5$, all primes dividing pN split in $K/\mathbb{Q}$ and all primes of K above p are totally ramified in K_∞/K. Let $\mathfrak{p}$ be a prime of K_∞ above p. Then we have* $\mathrm{rank}_{\mathbb{Z}_p}(\mathrm{img}\,\rho_{n,\mathfrak{p}}) \geq p^n + O(1)$

Proof. To prove this proposition we adapt Bertolini's strategy ([2] prop. 5.2 and theorem 5.3) from the ordinary case to the supersingular case. We will need to consider the Heegner points α_{2n} and α_{2n+1} separately. For any n, let $E(K_n)_p := E(K_n) \otimes \mathbb{Z}_p$ be the p-adic completion of $E(K_n)$. Denote by $\mathcal{E}(E/K_n)_p$ the submodule $\mathbb{Z}_p[G_n]\alpha_n$ of $E(K_n)_p$ spanned by the group ring $\mathbb{Z}_p[G_n]$ acting on α_n. We claim that for any n the map $\mathrm{res}_n : E(K_n)_p \to E(K_{n+1})_p$ induced by inclusion is injective. To see this, we show that for any m the map induced by inclusion $\mathrm{res}_{n,p^m} : E(K_n)/p^m \to E(K_{n+1})/p^m$ is injective. Suppose that $P \in E(K_n)$ satisfies $p^m Q = P$ for some $Q \in E(K_{n+1})$. Let σ be a generator of $\mathrm{Gal}(K_{n+1}/K_n)$. Then we have $p^m(\sigma(Q) - Q) = \sigma(p^m Q) - p^m Q = \sigma(P) - P = 0$. But by [12] lemma 2.1 we have $E(K_\infty)[p^\infty] = \{0\}$. Therefore $\sigma(Q) - Q = 0$ which implies that $Q \in E(K_n)$. This shows that res_{n,p^m} is injective which, in turn, shows that res_n is injective.

Now consider the restriction of res_n to $\mathcal{E}(E/K_n)$ $\widetilde{\mathrm{res}}_n : \mathcal{E}(E/K_n) \to \mathrm{res}_n(\mathcal{E}(E/K_n))$. As res_n is injective, $\widetilde{\mathrm{res}}_n$ is an isomorphism. We now consider the Heegner points α_{2k}. The norm relation (4) shows that for any $n \geq 1$ we have $\mathrm{Tr}_{2n/2n-1}(\mathcal{E}(E/K_{2n})) = \mathrm{img}\,\widetilde{\mathrm{res}}_{2n-2}$ and so $\widetilde{\mathrm{res}}_{2n-2}^{-1} \circ \mathrm{Tr}_{2n/2n-1}$ defines a surjective map $\mathcal{E}(E/K_{2n}) \to \mathcal{E}(E/K_{2n-2})$. Using these maps, we define $\mathcal{E}^\dagger(E/K_\infty)_p^+ := \varprojlim \mathcal{E}(E/K_{2n})_p$. This is a cyclic Λ-module which is nonzero if and only if for some n α_{2n} has infinite order (note that $E(K_\infty)[p^\infty] = 0$ by [12] lemma 2.1). Using the results of Cornut [6] and Cornut-Vatsal [7] it can be shown as in [17] prop. 4.1 that α_{2n} has infinite order for some n. Hence $\mathcal{E}^\dagger(E/K_\infty)_p^+$ is a nonzero cyclic Λ-module.

We now turn to the local setting. Let $\hat{E}$ be the formal group of $E/\mathbb{Q}$. Combining Mattuck's theorem, [12] lemma 2.1 and [25] IV prop. 2.3, we see that $\hat{E}(K_{n,\mathfrak{p}})$ is a free $\mathbb{Z}_p$-module. Therefore $\varprojlim_m \hat{E}(K_{n,\mathfrak{p}})/p^m = \hat{E}(K_{n,\mathfrak{p}})$. Now $\hat{E}(K_{n,\mathfrak{p}})$ is isomorphic to $E_1(K_{n,\mathfrak{p}}) = \ker(E(K_{n,\mathfrak{p}}) \to \bar{E}(\mathbb{F}_p))$. Since E has supersingular reduction at p, therefore $\bar{E}(\mathbb{F}_p)[p] = \{0\}$. This implies that $\hat{E}(K_{n,\mathfrak{p}}) = \varprojlim_m \hat{E}(K_{n,\mathfrak{p}})/p^m = E(K_{n,\mathfrak{p}})_p$. Define $\hat{E}^\pm(K_{n,\mathfrak{p}}) \cong E_1(K_{n,\mathfrak{p}}) \cap E^\pm(K_{n,\mathfrak{p}})$ where $E^\pm(K_{n,\mathfrak{p}})$ is defined as in the introduction. Since $\hat{E}(K_{n,\mathfrak{p}})$ is a free $\mathbb{Z}_p$-module so are both $\hat{E}^\pm(K_{n,\mathfrak{p}})$.

Theorem 4.5 of [12] shows that there exist $d_n \in \hat{E}(K_{n,\mathfrak{p}})$ such that $\mathrm{Tr}_{n+1/n}(d_{n+1}) = -d_{n-1}$ (for $n \geq 1$) and $\mathrm{Tr}_{1/0}(d_1) = u \cdot d_0$ for some $u \in \mathbb{Z}_p^\times$. From (3) and (4) we see that the norm relations for the Heegner points α_n and the points d_n are identical. Lemma 4.13 of [12] shows that for any $n \geq 0$ we have $\hat{E}^+(K_{2n,\mathfrak{p}}) = \mathbb{Z}_p[G_n]d_{2n}$ and $\hat{E}^-(K_{2n+1,\mathfrak{p}}) = \mathbb{Z}_p[G_n]\alpha_{2n+1}$. We shall work with $\hat{E}^+$ now. By what we just mentioned, we see as in the global case, that we may form the inverse limit $\hat{E}^\dagger(K_{\infty,\mathfrak{p}})^+ := \varprojlim \hat{E}^+(K_{2n,\mathfrak{p}})$.

CLAIM: $\hat{E}^\dagger(K_{\infty,\mathfrak{p}})^+$ is a free Λ-module of rank 1 such that for any n the natural map $\pi_{2n}^+ : \hat{E}^\dagger(K_{\infty,\mathfrak{p}})^+/\omega_{2n}^+ \to \hat{E}^+(K_{2n,\mathfrak{p}})$ is an isomorphism (this map exists because of the analog of lemma 2.1 for the points d_{2n}).

To see this, let $n \geq 0$. Since the maps defining the inverse limit $\hat{E}^\dagger(K_{\infty,\mathfrak{p}})^+$ are surjective, therefore π_{2n}^+ is surjective. Prop. 4.15(3) of [12] shows that $\mathrm{rank}_{\mathbb{Z}_p}(\hat{E}^+(K_{2n,\mathfrak{p}})) = \mathrm{rank}_{\mathbb{Z}_p}(\Lambda/\omega_{2n}^+) = q_{2n}$. Therefore from the surjectivity of π_{2n}^+, it follows that $\mathrm{rank}_{\mathbb{Z}_p}(\hat{E}^\dagger(K_{\infty,\mathfrak{p}})^+/\omega_{2n}^+)$ is unbounded and hence $\hat{E}^\dagger(K_{\infty,\mathfrak{p}})^+$ is a free Λ-module of rank 1 since it is cyclic and not torsion. The injectivity of π_{2n}^+ follows from comparing the $\mathbb{Z}_p$-ranks of the domain and codomain of π_{2n}^+.

Consider the localization map $\tilde{\rho}_{2n,\mathfrak{p}} : \mathcal{E}(E/K_{2n})_p \to E(K_{2n,\mathfrak{p}})_p$. Lemma 2.1 implies that img $\tilde{\rho}_{2n,\mathfrak{p}} \subseteq \hat{E}^+(K_{2n,\mathfrak{p}})$. Therefore we get a map $\tilde{\rho}^+_{\infty,\mathfrak{p}} : \mathcal{E}^\dagger(E/K_\infty)^+_p \to \hat{E}^\dagger(K_{\infty,\mathfrak{p}})^+$. Since $\mathcal{E}^\dagger(E/K_\infty)^+_p$ is a cyclic Λ-module and $\hat{E}^\dagger(K_{\infty,\mathfrak{p}})^+$ is torsion-free, therefore $\tilde{\rho}^+_{\infty,\mathfrak{p}}$ is injective if and only if it is nonzero. This is equivalent to saying that $\tilde{\rho}_{2n,\mathfrak{p}}$ is nonzero for some n. As explained before, α_{2n} has infinite order for some n and hence $\tilde{\rho}_{2n,\mathfrak{p}}(\alpha_{2n})$ is nonzero. This shows that $\tilde{\rho}^+_{\infty,\mathfrak{p}}$ is injective.

We now determine $\operatorname{rank}_{\mathbb{Z}_p}(\operatorname{img}\tilde{\rho}_{2n,\mathfrak{p}})$. Fix an isomorphism $\hat{E}^\dagger(K_{\infty,\mathfrak{p}})^+ \cong \Lambda$. As $\tilde{\rho}^+_{\infty,\mathfrak{p}}$ is injective, we may identify $\mathcal{E}^\dagger(E/K_\infty)^+_p$ with $f\Lambda$ for some nonzero $f \in \Lambda$. From the claim above we have

$$\begin{aligned}\operatorname{rank}_{\mathbb{Z}_p}(\operatorname{img}\tilde{\rho}_{2n,\mathfrak{p}}) &= \operatorname{rank}_{\mathbb{Z}_p}(f\Lambda + \omega^+_{2n}\Lambda/\omega^+_{2n}\Lambda)\\ &= \operatorname{rank}_{\mathbb{Z}_p}(f\Lambda/f\Lambda \cap \omega^+_{2n}\Lambda)\\ &= \operatorname{rank}_{\mathbb{Z}_p}(f\Lambda/\omega^+_{2n}f\Lambda) - \operatorname{rank}_{\mathbb{Z}_p}(f\Lambda \cap \omega^+_{2n}\Lambda/\omega^+_{2n}f\Lambda)\end{aligned}$$

Since $\operatorname{rank}_{\mathbb{Z}_p}(f\Lambda/\omega^+_{2n}f\Lambda) = q_{2n}$ and $\operatorname{rank}_{\mathbb{Z}_p}(f\Lambda\cap\omega^+_{2n}\Lambda/\omega^+_{2n}f\Lambda)$ is bounded therefore we get that $\operatorname{rank}_{\mathbb{Z}_p}(\operatorname{img}\tilde{\rho}_{2n,\mathfrak{p}}) = q_{2n} + O(1)$

In an almost identical fashion, one considers the Heegner points α_{2n+1} and the group $\hat{E}^-(K_{2n+1,\mathfrak{p}})$ and constructs the appropriate inverse limits. If one then defines $\tilde{\rho}_{2n+1,\mathfrak{p}}$ analogously as above, one can show that $\operatorname{rank}_{\mathbb{Z}_p}(\operatorname{img}\tilde{\rho}_{2n+1,\mathfrak{p}}) = q_{2n+1} + O(1)$.

We can now finally complete the proof. Let $n \geq 1$. Define $B := \mathbb{Z}_p[G_n]\alpha_n$, $C := \mathbb{Z}_p[G_n]\alpha_{n-1}$ and let $A := B + C \subseteq E(K_n)_p$. Then we have

$$\begin{aligned}\operatorname{rank}_{\mathbb{Z}_p}(\rho_{n,\mathfrak{p}}(A)) &= \operatorname{rank}_{\mathbb{Z}_p}(\operatorname{img}\tilde{\rho}_{n,\mathfrak{p}}) + \operatorname{rank}_{\mathbb{Z}_p}(\operatorname{img}\tilde{\rho}_{n-1,\mathfrak{p}}) - \operatorname{rank}_{\mathbb{Z}_p}(\rho_{n,\mathfrak{p}}(B)\cap\rho_{n,\mathfrak{p}}(C))\\ &= q_n + O(1) + q_{n-1} + O(1) - \operatorname{rank}_{\mathbb{Z}_p}(\rho_{n,\mathfrak{p}}(B)\cap\rho_{n,\mathfrak{p}}(C))\\ &= p^n + 1 - \operatorname{rank}_{\mathbb{Z}_p}(\rho_{n,\mathfrak{p}}(B)\cap\rho_{n,\mathfrak{p}}(C)) + O(1)\end{aligned}$$

Now note that $\rho_{n,\mathfrak{p}}(B) \cap \rho_{n,\mathfrak{p}}(C) \subseteq \hat{E}^+(K_{n,\mathfrak{p}}) \cap \hat{E}^-(K_{n,\mathfrak{p}})$. By [12] prop. 4.11, $\hat{E}^+(K_{n,\mathfrak{p}})\cap\hat{E}^-(K_{n,\mathfrak{p}}) = \hat{E}(\mathbb{Q}_p)$. Since $\operatorname{rank}_{\mathbb{Z}_p}(\hat{E}(\mathbb{Q}_p)) = 1$, it therefore follows from the above that $\operatorname{rank}_{\mathbb{Z}_p}(\rho_{n,\mathfrak{p}}(A)) = p^n + O(1)$. This implies that $\operatorname{rank}_{\mathbb{Z}_p}(\operatorname{img}\rho_{n,\mathfrak{p}}) \geq p^n + O(1)$ which completes the proof of the proposition. □

Lemma 2.4. *Assume that p splits in $K/\mathbb{Q}$. For any $n \geq 0$, the map $\operatorname{Sel}^1_{p^\infty}(E/K) \to \operatorname{Sel}^1_{p^\infty}(E/K_n)^\Gamma$ induced by restriction is an injection with finite cokernel.*

Proof. Define S to be the set of primes of K dividing Np and S_n to be the primes of K_n above those in S. Now define K_S to be the maximal extension of K unramified outside S, $G_S(K) = \operatorname{Gal}(K_S/K)$ and $G_S(K_n) = \operatorname{Gal}(K_S/K_n)$. Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be the primes of K_n above p. We define $\mathcal{P}_p(E/K_n) = \prod_{i=1,2}(H^1(K_{n,\mathfrak{p}_i}, E[p^\infty])/(E(\mathbb{Q}_p)\otimes\mathbb{Q}_p/\mathbb{Z}_p))$ and $\mathcal{P}_*(E/K_n) = \prod_{v\in S_n\setminus\{\mathfrak{p}_1,\mathfrak{p}_2\}} H^1(K_{n,v}, E)[p^\infty]$. Similarly we define $\mathcal{P}_p(E/K)$ and $\mathcal{P}_*(E/K)$.

We have a commutative diagram

$$\begin{array}{ccccccc} 0 \longrightarrow & \operatorname{Sel}^1_{p^\infty}(E/K_n)^\Gamma & \longrightarrow & H^1(G_S(K_n), E[p^\infty])^\Gamma & \longrightarrow & \mathcal{P}_p(E/K_n)^\Gamma \times \mathcal{P}_*(E/K_n)^\Gamma \\ & \uparrow s & & \uparrow h & & \uparrow g \\ 0 \longrightarrow & \operatorname{Sel}^1_{p^\infty}(E/K) & \longrightarrow & H^1(G_S(K), E[p^\infty]) & \xrightarrow{\psi} & \mathcal{P}_p(E/K) \times \mathcal{P}_*(E/K) \end{array} \tag{5}$$

Applying the snake lemma to the above diagram we get

$$0 \to \ker s \to \ker h \to \ker g \cap \operatorname{img} \psi \to \operatorname{coker} s \to \operatorname{coker} h$$

By [12] lemma 2.1 we have $E(K_\infty)[p^\infty] = \{0\}$ and so the map h is an isomorphism. Therefore from the above exact sequence we get that s is an injection and that $\operatorname{coker} s = \ker g \cap \operatorname{img} \psi$. Therefore to complete the proof of the lemma it will suffice to show that $\ker g$ is finite.

Let v be a prime of K that does not divide p and consider the map $g_v : H^1(K_v, E)[p^\infty] \to (\oplus_{w|v} H^1(K_{n,w}, E)[p^\infty])^\Gamma$ where the sum is taken over all primes w of K_n above v. It can be shown by Shapiro's lemma along with the inflation restriction sequence that $\ker g_v = H^1(\Gamma_w, E)$ where Γ_w is the decomposition group of Γ at a prime w of K_n above v. It follows from [21] proposition I-3.8 that $H^1(\Gamma_w, E)$ is finite of order $c_v^{(p)} = p^{\operatorname{ord}_p(c_v)}$.

To complete the proof it will suffice to show that the restriction map

$$g_\mathfrak{p} : \frac{H^1(K_\mathfrak{p}, E[p^\infty])}{E(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \to \Big(\frac{H^1(K_{n,\mathfrak{p}}, E[p^\infty])}{E(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\Big)^\Gamma$$

is injective where $\mathfrak{p}$ is a prime of K_n above p

To prove this, consider the following commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & (E(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\Gamma & \longrightarrow & H^1(K_{n,\mathfrak{p}}, E[p^\infty])^\Gamma & \longrightarrow & \Big(\frac{H^1(K_{n,\mathfrak{p}}, E[p^\infty])}{E(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\Big)^\Gamma & & \\
 & & \uparrow g'_\mathfrak{p} & & \uparrow g''_\mathfrak{p} & & \uparrow g_\mathfrak{p} & & \\
0 & \longrightarrow & E(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p & \longrightarrow & H^1(K_\mathfrak{p}, E[p^\infty]) & \longrightarrow & \frac{H^1(K_{n,\mathfrak{p}}, E[p^\infty])}{E(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p} & \longrightarrow & 0
\end{array} \tag{6}$$

Applying the snake lemma to the above diagram we see that to show $\ker g_\mathfrak{p} = 0$, we only need to show that $\ker g''_\mathfrak{p} = 0$ and $\operatorname{coker} g'_\mathfrak{p} = 0$. Now $g'_\mathfrak{p}$ is an isomorphism so $\operatorname{coker} g'_\mathfrak{p} = 0$. As for $\ker g''_\mathfrak{p}$ we have $\ker g''_\mathfrak{p} = H^1(\operatorname{Gal}(K_{n,\mathfrak{p}}/K_\mathfrak{p}), E(K_{n,\mathfrak{p}})[p^\infty])$. By [12] lemma 2.1 $E(K_{n,\mathfrak{p}})[p^\infty]^\Gamma = E(K_\mathfrak{p})[p^\infty] = \{0\}$ so $E(K_{n,\mathfrak{p}})[p^\infty] = \{0\}$. This shows that $\ker g''_\mathfrak{p} = 0$ which completes the proof. □

We now prove theorem A

Theorem A. *Assume that $p \geq 5$, all primes dividing pN split in $K/\mathbb{Q}$ and both primes of K above p are totally ramified in K_∞/K. The following are equivalent*

(a) $\operatorname{Sel}_{p^\infty}(E/K_\infty)^{\text{dual}}$ *has Λ-rank two*

(b) Both $\operatorname{Sel}^\pm_{p^\infty}(E/K_\infty)^{\text{dual}}$ *have Λ-rank one*

(c) $\operatorname{corank}_{\mathbb{Z}_p}(\operatorname{Sel}_{p^\infty}(E/K_n)) = p^n + O(1)$ *and* $\operatorname{rank}_{\mathbb{Z}_p}(\operatorname{img} \rho_{n,p}) = p^n + O(1)$

(d) $H^2(G_S(K_\infty), E[p^\infty]) = 0$

(e) $R_{p^\infty}(E/K_\infty)^{\text{dual}}$ *is Λ-torsion*

Proof. We have that (d) and (e) are equivalent by [19] theorem 2.2.

We now show that (a) and (d) are equivalent. Let v be a prime of K above p and w a prime of K_∞ above v. Since v ramifies in K_∞/K, therefore the extension $K_{\infty,w}/K_v$ is deeply ramified in the sense of [5]. So as explained in [9] pg. 70 we have $H^1(K_{\infty,w}, E)[p^\infty] = 0$. Combining this with [10] prop. 2, it follows that $\prod_{v \in S_\infty} H^1(K_{\infty,v}, E)[p^\infty]$ is Λ-cotorsion.

From the definition of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ it follows that $\mathrm{corank}_\Lambda(\mathrm{Sel}_{p^\infty}(E/K_\infty)) = \mathrm{corank}_\Lambda(H^1(G_S(K_\infty), E[p^\infty])$. Also Greenberg [10] prop 3 and 4 has shown that $\mathrm{corank}_\Lambda(H^1(G_S(K_\infty), E[p^\infty])) + \mathrm{corank}_\Lambda(H^2(G_S(K_\infty), E[p^\infty]) = 2$ and that $H^2(G_S(K_\infty), E[p^\infty])$ is a cofree Λ-module. The equivalence of (a) and (d) follows.

Now we show that (a) implies (b). Assume that $\mathrm{corank}_\Lambda(\mathrm{Sel}_{p^\infty}(E/K_\infty)) = 2$. Taking the direct limit (with respect to restriction) of the first exact sequence in proposition 2.2 we get an exact sequence

$$0 \to \mathrm{Sel}^1_{p^\infty}(E/K_\infty) \to \mathrm{Sel}^+_{p^\infty}(E/K_\infty) \oplus \mathrm{Sel}^-_{p^\infty}(E/K_\infty) \to \mathrm{Sel}_{p^\infty}(E/K_\infty) \qquad (7)$$

We now show that $\mathrm{Sel}^1_{p^\infty}(E/K_\infty)$ is Λ-cotorsion. Let $\tilde{S}_\infty := S_\infty \setminus \{\mathfrak{p}_\infty, \bar{\mathfrak{p}}_\infty\}$ where $\mathfrak{p}_\infty, \bar{\mathfrak{p}}_\infty$ are the primes of K_∞ above p.

Now define

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

and consider the commutative diagram

$$\begin{array}{ccccccccc}
 & & 0 & \longrightarrow & H^1(G_S(K_\infty), E[p^\infty]) & \longrightarrow & H^1(G_S(K_\infty), E[p^\infty]) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{L}(K_\infty) & \longrightarrow & \prod_{v \in S_\infty} H^1(K_{\infty,v}, E[p^\infty]) & \longrightarrow & \prod_{v \in S_\infty} H^1(K_{\infty,v}, E[p^\infty])/\mathcal{L}(K_\infty) & \longrightarrow & 0
\end{array} \qquad (8)$$

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

$$0 \longrightarrow R_{p^\infty}(E/K_\infty) \longrightarrow \mathrm{Sel}^1_{p^\infty}(E/K_\infty) \longrightarrow \mathcal{L}(K_\infty) \qquad (9)$$

For any $v \in \tilde{S}_\infty$ we have $E(K_{\infty,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$ this is because for any n by Mattuck's theorem have $E(K_{n,v}) \cong \mathbb{Z}_l^r \times T$ where r is some integer, T is a finite group and $l \neq p$ is the rational prime below v. Therefore it follows that $\mathcal{L}(K_\infty)$ is Λ-cotorsion. Also by the equivalence of (a) and (e) shown above we have that $R_{p^\infty}(E/K_\infty)$ is Λ-cotorsion. The exact sequence (9) then shows that $\mathrm{Sel}^1_{p^\infty}(E/K_\infty)$ is Λ-cotorsion.

Since $\mathrm{Sel}^1_{p^\infty}(E/K_\infty)$ is Λ-cotorsion, therefore from the sequence (7) we get that $\mathrm{corank}_\Lambda(\mathrm{Sel}^+_{p^\infty}(E/K_\infty) \oplus \mathrm{Sel}^-_{p^\infty}(E/K_\infty)) \leq 2$. We see that (b) will follow if we can show that $\mathrm{corank}_\Lambda(\mathrm{Sel}^\pm_{p^\infty}(E/K_\infty)) \geq 1$. So we get (b) from [15] prop 4.7.

We now show that (b) implies (c). Assume that $\mathrm{corank}_\Lambda(\mathrm{Sel}^\pm_{p^\infty}(E/K_\infty)) = 1$. First we show $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/K_n)) = p^n + O(1)$. Since $\mathrm{corank}_\Lambda(\mathrm{Sel}^\pm_{p^\infty}(E/K_\infty)) = 1$, therefore $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}^\pm_{p^\infty}(E/K_\infty)^{\omega_n^\pm = 0}) = \deg \omega_n^\pm + O(1)$. By [12] theorem 6.8 the natural map $\mathrm{Sel}^\pm_{p^\infty}(E/K_n)^{\omega_n^\pm=0} \to \mathrm{Sel}^\pm_{p^\infty}(E/K_\infty)^{\omega_n^\pm=0}$ has finite kernel and cokernel. Therefore $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}^\pm_{p^\infty}(E/K_n)^{\omega_n^\pm=0}) = \deg \omega_n^\pm + O(1)$ Since $\deg \omega_n^+ + \deg \omega_n^- = q_n + q_{n-1} = p^n + 1$, therefore we see by the second exact sequence in prop 2.2 that in order to show $\operatorname{corank}_{\mathbb{Z}_p}(\operatorname{Sel}_{p^\infty}(E/K_n)) = p^n + O(1)$, it will suffice to show that $\operatorname{corank}_{\mathbb{Z}_p}(\operatorname{Sel}^1_{p^\infty}(E/K_n)^{\omega_n^{\pm}=0})$ is bounded with n.

Now X is a greatest common divisor of $\omega_n^+(X)$ and $\omega_n^-(X)$ in $\mathbb{Q}_p[X]$. It follows that there exist polynomials $A(X), B(X) \in \mathbb{Z}_p[X]$ such that $A(X)\omega_n^+(X) + B(X)\omega_n^-(X) = p^m X$ for some integer m. This shows that $\operatorname{Sel}^1_{p^\infty}(E/K_n)^{\omega_n^{\pm}=0} \subseteq \operatorname{Sel}^1_{p^\infty}(E/K_n)^{p^m(\gamma-1)=0}$ ($\operatorname{Sel}^1_{p^\infty}(E/K_n)^{p^m(\gamma-1)=0}$ means the subgroup of $\operatorname{Sel}^1_{p^\infty}(E/K_n)$ annihilated by $p^m(\gamma-1)$). Therefore it suffices to show that $\operatorname{corank}_{\mathbb{Z}_p}(\operatorname{Sel}^1_{p^\infty}(E/K_n)^{p^m(\gamma-1)=0})$ is bounded with n. As $p^m \operatorname{Sel}^1_{p^\infty}(E/K_n)^{p^m(\gamma-1)=0} \subseteq \operatorname{Sel}^1_{p^\infty}(E/K_n)^{\Gamma}$ and $\operatorname{Sel}^1_{p^\infty}(E/K_n)[p^m] \subseteq \operatorname{Sel}_{p^\infty}(E/K_n)[p^m]$ is finite, we only have to show that $\operatorname{corank}_{\mathbb{Z}_p}(\operatorname{Sel}^1_{p^\infty}(E/K_n)^{\Gamma})$ is bounded with n. This follows from lemma 2.4.

If $\mathfrak{p}$ is a prime of K_∞ above p, proposition 2.3 shows that $\operatorname{rank}_{\mathbb{Z}_p}(\operatorname{img}\rho_{n,\mathfrak{p}}) \geq p^n + O(1)$. It follows that $\operatorname{rank}_{\mathbb{Z}_p}(\operatorname{img}\rho_{n,p}) \geq p^n + O(1)$. Since $\operatorname{rank}_{\mathbb{Z}_p}(S_p(E/K_n)) \geq \operatorname{rank}_{\mathbb{Z}_p}(\operatorname{img}\rho_{n,p})$ we get equality. Hence we get (c).

Finally (c) implies (d) follows from [2] theorem 3.1. This completes the proof of theorem A. □

3. Proof of Theorem B

In this section we prove theorem B by a similar technique used in the proof of the ordinary case in [17]. We will prove theorem B for $\operatorname{Sel}^+_{p^\infty}(E/K_\infty)$. The proof for $\operatorname{Sel}^-_{p^\infty}(E/K_\infty)$ will be similar. We use all the notation and definitions from the introduction and the previous section. Throughout this section we assume the following

(i) All the primes dividing pN split in $K/\mathbb{Q}$
(ii) p does not divide $6h_K\varphi(Nd_K) \cdot \prod_{\ell|N} c_v$
(iii) p does not divide the number of geometrically connected components of the kernel of $\pi_* : J_0(N) \to E$.

As we just mentioned, theorem B will be proven by adapting the proof of theorem A in [17]. The first important observation is that since E has good supersingular reduction at p, therefore $E[p]$ is an irreducible $\operatorname{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$-module (see [13] prop 4.4 or [24] prop 12(c)). In [17] we imposed the condition that $\operatorname{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) = GL_2(\mathbb{F}_p)$. In order to adapt the proof of theorem A in [17] to our setting we will need to show that $\operatorname{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) = GL_2(\mathbb{F}_p)$ may be replaced by the condition that $E[p]$ is an irreducible $\operatorname{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$-module in that paper. We now explain this. First we prove lemma 2.3 in [17]

Lemma 3.1. *The extensions $\mathbb{Q}(E[p])/\mathbb{Q}$ and $K_\infty/\mathbb{Q}$ are linearly disjoint*

Proof. $\mathbb{Q}(E[p])/\mathbb{Q}$ and $K/\mathbb{Q}$ are linearly disjoint just as in the proof of lemma 2.3. We now show that $K(E[p])/K$ and K_∞/K are disjoint. If they were not disjoint, then $G := \operatorname{Gal}(K(E[p])/K) = \operatorname{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ would a normal subgroup N of index p and hence in particular the order of G would be divisible by p. This implies by Dickson's classification of subgroups of $GL_2(\mathbb{F}_p)$ ([8] sec 260) that $SL_2(\mathbb{F}_p) \subseteq G$ (the other possibility is that G is contained in a Borel subgroup. This is ruled out by the fact that $E[p]$ is an irreducible $\operatorname{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$-module). Then as in lemma 2.3, we must have that $N \cap SL_2(\mathbb{F}_p)$ has both order and index greater than 2. This contradicts that fact that $PSL_2(\mathbb{F}_p)$ is simple for $p \geq 5$. □

In [17], we defined $L_n := K_n(E[p])$ and $\mathcal{G}_n := \mathrm{Gal}(L_n/K_n)$. We need to prove proposition 2.6 in [17]

Proposition 3.2. *The restriction map induces an isomorphism:*

$$\mathrm{res} : H^1(K_n, E[p]) \xrightarrow{\sim} H^1(L_n, E[p])^{\mathcal{G}_n} = \mathrm{Hom}_{\mathcal{G}_n}(\mathrm{Gal}(\overline{\mathbb{Q}}/L_n), E[p])$$

Proof. To prove this proposition we need to show that $(*)$ $H^i(\mathcal{G}_n, E[p]) = 0$ for $i = 1, 2$. By the above lemma, we have $\mathcal{G}_n = \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$. When $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) = GL_2(\mathbb{F}_p)$, we can use Serre's proof as in [11] prop. 9.1. In general, when $E[p]$ is an irreducible $\mathbb{F}_p[G_{\mathbb{Q}}]$-module we note that $\#\det(\mathcal{G}_n) = \#\chi_{p,\mathbb{Q}}(\mathcal{G}_n) > 2$ (since $p > 3$) where $\chi_{p,\mathbb{Q}} : G_{\mathbb{Q}} \to \mathbb{F}_p^{\times}$ is the mod p cyclotomic character. This implies by [20] prop 5.15 that $\mathcal{G}_n$ contains a nontrivial homothety. Then one gets $(*)$ either by adapting Serre's proof or by Sah's lemma (see [20] 5.5.2). □

Proposition 9.3 in Gross's paper [11] was used in a number of places in [17] (see for example pg. 424). Gross proves this proposition under the assumption that $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) = GL_2(\mathbb{F}_p)$. Proposition 3.2 above shows that [11] prop. 9.3 holds under the weaker assumption that $E[p]$ is an irreducible $\mathbb{F}_p[G_{\mathbb{Q}}]$-module.

The above results show that we may indeed replace $\mathrm{Gal}(\mathbb{Q}(E[p]), \mathbb{Q}) = GL_2(\mathbb{F}_p)$ in [17] by the condition (which holds here) that $E[p]$ is an irreducible $\mathrm{Gal}(\mathbb{Q}(E[p]))/\mathbb{Q})$-module.

Now let A be a discrete Γ-module annihilated by p. For any $n \geq 1$ we have $\mathrm{Tr}_{2n/2n-1}(A^{\omega_{2n}^{+}=0}) \subseteq A^{\omega_{2n-2}^{+}=0}$. Using these maps we can form the inverse limit $\varprojlim A^{\omega_{2n}^{+}=0}$. We now have the following important proposition

Proposition 3.3. *If M is a finitely generated $\overline{\Lambda}$-module, then the module $M^{+} := \varprojlim (M^{\mathrm{dual}})^{\omega_{2n}^{+}=0}$ is a free $\overline{\Lambda}$-module of same rank as M*

Proof. As M is a finitely generated $\overline{\Lambda}$-module and $\overline{\Lambda}$ is a PID, therefore M is isomorphic to $\overline{\Lambda}^r \times T$ for some $r \geq 0$ and some finite group T. From this we see that to prove the proposition, we only need to show that (i) $\varprojlim (T^{\mathrm{dual}})^{\omega_{2n}^{+}=0} = 0$ and that (ii) $\varprojlim (\overline{\Lambda}^{\mathrm{dual}})^{\omega_{2n}^{+}=0} \cong \overline{\Lambda}$

First we show (i). Since T^{dual} is a finite discrete Γ-module, there exists $s \geq 0$ such that Γ_s acts trivially on T^{dual}. Then for all $n \geq s$, $\mathrm{Tr}_{2n/2n-1}$ annihilates T^{dual}. It follows that $\varprojlim (T^{\mathrm{dual}})^{\omega_{2n}^{+}=0} = 0$

We now show (ii). Since $\overline{\Lambda}/\omega_{2n}^{+}$ is a finite group, therefore we have an isomorphism $(\overline{\Lambda}/\omega_{2n}^{+})^{\mathrm{dual}} \cong \overline{\Lambda}/\omega_{2n}^{+}$. If we choose the isomorphisms appropriately, then we get a commutative diagram where π_n is the canonical projection

$$\begin{array}{ccc} (\overline{\Lambda}/\omega_{2n}^{+})^{\mathrm{dual}} & \xrightarrow{\sim} & \overline{\Lambda}/\omega_{2n}^{+} \\ \downarrow{\scriptstyle \mathrm{Tr}_{2n/2n-1}} & & \downarrow{\scriptstyle \pi_n} \\ (\overline{\Lambda}/\omega_{2n-2}^{+})^{\mathrm{dual}} & \xrightarrow{\sim} & \overline{\Lambda}/\omega_{2n-2}^{+} \end{array}$$

The above diagram shows that

$$\varprojlim (\overline{\Lambda}^{\mathrm{dual}})^{\omega_{2n}^{+}=0} \cong \varprojlim (\overline{\Lambda}/\omega_{2n}^{+})^{\mathrm{dual}} \cong \varprojlim \overline{\Lambda}/\omega_{2n}^{+} \cong \overline{\Lambda}$$

This completes the proof. □

Proposition 3.4. *For any $n \geq 0$, the natural map $H^1(K_n, E[p]) \to H^1(K_n, E[p^\infty])$ induces an isomorphism* $\mathrm{Sel}_p^+(E/K_n) \cong \mathrm{Sel}_{p^\infty}^+(E/K_n)[p]$

Proof. Let $\psi_n : \mathrm{Sel}_p(E/K_n) \to \mathrm{Sel}_{p^\infty}(E/K_n)[p]$ and $\psi_n^{'+} : \mathrm{Sel}_p^+(E/K_n) \to \mathrm{Sel}_{p^\infty}^+(E/K_n)[p]$ induced from the map $H^1(K_n, E[p]) \to H^1(K_n, E[p^\infty])$. By [12] lemma 2.1 $E(K_\infty)[p^\infty] = \{0\}$. Therefore ψ_n is an isomorphism. From this an the snake lemma, we get that $\psi_n^{'+}$ is an injection and its cokernel is contained in the kernel of the map

$$\psi_{n,p}^+ : \bigoplus_{\mathfrak{p}|p} \frac{H^1(K_{n,\mathfrak{p}}, E[p])}{E^+(K_{n,\mathfrak{p}}) \otimes \mathbb{F}_p} \to \bigoplus_{\mathfrak{p}|p} \frac{H^1(K_{n,\mathfrak{p}}, E[p^\infty])}{E^+(K_{n,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}$$

We now show that $\psi_{n,p}^+$ is an injection. Let $\mathfrak{p}$ be a prime of K_n above p. We need to show that the map

$$\psi_{n,\mathfrak{p}}^+ : \frac{H^1(K_{n,\mathfrak{p}}, E[p])}{E^+(K_{n,\mathfrak{p}}) \otimes \mathbb{F}_p} \to \frac{H^1(K_{n,\mathfrak{p}}, E[p^\infty])}{E^+(K_{n,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}$$

is an injection.

Consider the map

$$\psi_{n,\mathfrak{p}} : \frac{H^1(K_{n,\mathfrak{p}}, E[p])}{E(K_{n,\mathfrak{p}}) \otimes \mathbb{F}_p} \to \frac{H^1(K_{n,\mathfrak{p}}, E[p^\infty])}{E(K_{n,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}$$

Since $H^1(K_{n,\mathfrak{p}}, E)[p] \cong H^1(K_{n,\mathfrak{p}}, E[p])/(E(K_{n,\mathfrak{p}}) \otimes \mathbb{F}_p)$, $H^1(K_{n,\mathfrak{p}}, E)[p^\infty] \cong H^1(K_{n,\mathfrak{p}}, E[p^\infty])/(E(K_{n,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$ and the inclusion map $H^1(K_{n,\mathfrak{p}}, E)[p] \to H^1(K_{n,\mathfrak{p}}, E)[p^\infty]$ is an injection, therefore $\psi_{n,\mathfrak{p}}$ is an injection. Now consider the following commutative diagram

$$\begin{array}{ccccc}
\frac{E(K_{n,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}{E^+(K_{n,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} & \longrightarrow & \frac{H^1(K_{n,\mathfrak{p}}, E[p^\infty])}{E^+(K_{n,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} & \longrightarrow & \frac{H^1(K_{n,\mathfrak{p}}, E[p^\infty])}{E(K_{n,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \\
\uparrow \psi_{n,\mathfrak{p}}^{'+} & & \uparrow \psi_{n,\mathfrak{p}}^{+} & & \uparrow \psi_{n,\mathfrak{p}} \\
\frac{E(K_{n,\mathfrak{p}}) \otimes \mathbb{F}_p}{E^+(K_{n,\mathfrak{p}}) \otimes \mathbb{F}_p} & \longrightarrow & \frac{H^1(K_{n,\mathfrak{p}}, E[p])}{E^+(K_{n,\mathfrak{p}}) \otimes \mathbb{F}_p} & \longrightarrow & \frac{H^1(K_{n,\mathfrak{p}}, E[p])}{E(K_{n,\mathfrak{p}}) \otimes \mathbb{F}_p}
\end{array}$$

Since $\psi_{n,\mathfrak{p}}$ is an injection, the above commutative diagram shows that to prove that $\psi_{n,\mathfrak{p}}^+$ is an injection, we only need to show that $\psi_{n,\mathfrak{p}}^{'+}$ is an injection. We have $E(K_{n,\mathfrak{p}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \varinjlim E(K_{n,\mathfrak{p}})/p^m$ where the transition maps in the direct limit are induced by the multiplication-by-p map.

Suppose that $P + pE(K_{n,\mathfrak{p}}) \in E(K_{n,\mathfrak{p}})/p$ considered as an element of $\varinjlim E(K_{n,\mathfrak{p}})/p^m$ is contained in $\varinjlim E^+(K_{n,\mathfrak{p}})/p^m$. This implies that there exists $Q \in E^+(K_{n,\mathfrak{p}})$ and an $t \geq 1$ such that $p^t P - Q \in p^{t+1}E(K_{n,\mathfrak{p}})$ i.e. $p^t P - Q = p^{t+1}P'$ for some $P' \in E(K_{n,\mathfrak{p}})$. This gives $p^t(P - pP') = Q$. Let $S = P - pP'$. We want to show that $S \in E(K_{n,\mathfrak{p}})^+$. To this end, let m be an odd integer with $1 \leq m \leq n$. Since $Q \in E^+(K_{n,\mathfrak{p}})$ we have $p^t \,\mathrm{Tr}_{n/m}(S) = \mathrm{Tr}_{n/m}(Q) \in E(K_{m-1,\mathfrak{p}})$.

Now let $T = \mathrm{Tr}_{n/m}(S)$. We need to show that $T \in E(K_{m-1,\mathfrak{p}})$. Let σ be a generator of $\mathrm{Gal}(K_{m,\mathfrak{p}}/K_{m-1,\mathfrak{p}})$. Then we have $p^t(\sigma(T) - T) = \sigma(p^t T) - p^t T = 0$ because $p^t T \in E(K_{m-1,\mathfrak{p}})$. But by [12] lemma 2.1 we have $E(K_{\infty,\mathfrak{p}})[p^\infty]^\Gamma = E(K_\mathfrak{p})[p^\infty] = \{0\}$ so $E(K_{\infty,\mathfrak{p}})[p^\infty] = \{0\}$. Therefore $\sigma(T) - T = 0$ which implies that $T \in E(K_{m-1,\mathfrak{p}})$ as desired. This proves that $\psi_{n,\mathfrak{p}}^{'+}$ is an injection which as mentioned above proves that $\psi_{n,\mathfrak{p}}^+$ is also an injection. This completes the proof. $\square$

Theorem 3.5. *For any $n \geq 0$, the natural map*

$$\mathrm{Sel}_p^+(E/K_n)^{\omega_n^+=0} \to \mathrm{Sel}_p^+(E/K_\infty)^{\omega_n^+=0}$$

is an isomorphism.

Proof. For any $n \geq 0$, let $s_n : \mathrm{Sel}_{p^\infty}^+(E/K_n)^{\omega_n^+=0} \to \mathrm{Sel}_{p^\infty}^+(E/K_\infty)^{\omega_n^+=0}$ be the natural map induced by restriction. Note that we have assumed that p splits in $K/\mathbb{Q}$ and that p does not divide the class number of K (which implies that K_∞/K is totally ramified at any prime of K above p). These two assumptions allow us to use the results of Iovita and Pollack [12].

By theorem 6.8 of [12] s_n is an injection with finite cokernel. The proof of this result is based on the proof of [14] theorem 9.3. The proof reveals that the cokernel of s_n will be trivial if for any prime v of K_n not dividing p the kernel of the restriction map $g_{n,v} : H^1(K_{n,v}, E)[p^\infty] \to \oplus_{w|v} H^1(K_{\infty,w}, E)[p^\infty]$ is trivial and this is the case since p was assumed not to divide $\prod_{v|N} c_v$ (see the remark following [9] lemma 3.3). Therefore s_n is an isomorphism. The result now follows from proposition 3.4. $\square$

Now for any n, we let $\mathrm{res}_n : H^1(K_n, E[p]) \to H^1(K_{n+1}, E[p])$ be the restriction map and $\mathrm{cor}_n : H^1(K_n, E[p]) \to H^1(K_{n-1}, E[p])$ be the corestriction map. Using the above theorem, we show

Proposition 3.6. *For any $n \geq 1$ and any $s \in \mathrm{Sel}_p^+(E/K_{2n})^{\omega_{2n}^+=0}$, there exists $s' \in \mathrm{Sel}_p^+(E/K_{2n-2})^{\omega_{2n-2}^+=0}$ such that $\mathrm{cor}_{2n}(s) = \mathrm{res}_{2n-2}(s')$*

Proof. Consider the following diagram

$$\begin{array}{ccc}
\mathrm{Sel}_p^+(E/K_{2n})^{\omega_{2n}^+=0} & \xrightarrow{\sim} & \mathrm{Sel}_p^+(E/K_\infty)^{\omega_{2n}^+=0} \\
\downarrow{\scriptstyle \mathrm{cor}_{2n}} & & \downarrow{\scriptstyle \mathrm{Tr}_{2n/2n-1}} \\
\mathrm{Sel}_p^+(E/K_{2n-1}) & \longrightarrow & \mathrm{Sel}_p^+(E/K_\infty) \\
\uparrow{\scriptstyle \mathrm{res}_{2n-2}} & & \uparrow{\scriptstyle \iota_{2n-2}} \\
\mathrm{Sel}_p^+(E/K_{2n-2})^{\omega_{2n-2}^+=0} & \xrightarrow{\sim} & \mathrm{Sel}_p^+(E/K_\infty)^{\omega_{2n-2}^+=0}
\end{array}$$

In the diagram above the horizontal maps are restriction and the map ι_{2n-2} is just the inclusion map. By theorem 3.5 the top and bottom horizontal maps are isomorphisms. This diagram commutes.

For any $t \in \mathrm{Sel}_p^+(E/K_\infty)^{\omega_{2n}^+=0}$ there exists $t' \in \mathrm{Sel}_p^+(E/K_\infty)^{\omega_{2n-2}^+=0}$ such that $\mathrm{Tr}_{2n/2n-2}(t) = \iota_{2n-2}(t')$. Also by [12] lemma 2.1 $E(K_\infty)[p^\infty] = 0$ so the middle horizontal map is an injection. The proposition follows easily from these two facts using a diagram chase. $\square$

For any $n \geq 1$, consider the restriction map $\mathrm{res}_{2n-2} : \mathrm{Sel}_p^+(E/K_{2n-2})^{\omega_{2n-2}^+=0} \to \mathrm{Sel}_p^+(E/K_{2n-1})$. By [12] lemma 2.1, $E(K_\infty)[p^\infty] = 0$ so res_{2n-2} is injective. The above proposition shows that $\mathrm{cor}_{2n}(\mathrm{Sel}_p^+(E/K_{2n})^{\omega_{2n}^+=0}) \subseteq \mathrm{img}\,\mathrm{res}_{2n-2}$ and so if we consider res_{2n-2} to be an isomorphism onto it's image, therefore we see that $\mathrm{res}_{2n-2}^{-1} \circ \mathrm{cor}_{2n}$ defines a map from $\mathrm{Sel}_p^+(E/K_{2n})^{\omega_{2n}^+=0}$ to $\mathrm{Sel}_p^+(E/K_{2n-2})^{\omega_{2n-2}^+=0}$. Using these maps, we construct the inverse limit. We now define $X_p^\dagger(E/K_\infty) :=$

$\varprojlim \mathrm{Sel}_p^+(E/K_{2n})^{\omega_{2n}^+=0}$. Note that we have chosen to put an "†" in the superscript so that the reader does not confuse this group with the group $X_p(E/K_\infty)$ in [17] and the groups $X_{s,p}(E/K_\infty)$ and $X_{f,p}(E/K_\infty)$ in [18] which were defined in a different way.

We now have the following key theorem

Theorem 3.7. *The group $X_p^\dagger(E/K_\infty)$ is a finitely generated $\overline{\Lambda}$-module with* $\mathrm{rank}_{\overline{\Lambda}}(X_p^\dagger(E/K_\infty)) = \mathrm{rank}_{\overline{\Lambda}}(\mathrm{Sel}_p^+(E/K_\infty)^{\mathrm{dual}})$

Proof. By [16] 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 [12] lemma 2.1, 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. Then same is true for $\mathrm{Sel}_p^+(E/K_\infty)^{\mathrm{dual}}$ since $\mathrm{Sel}_p^+(E/K_\infty) \subseteq \mathrm{Sel}_p(E/K_\infty)$.

Now consider the group $Y_p^\dagger(E/K_\infty) := \varprojlim \mathrm{Sel}_p^+(E/K_\infty)^{\omega_{2n}^+=0}$ defined as in the paragraph proceeding proposition 3.3. Proposition 3.3 shows that $Y_p^\dagger(E/K_\infty)$ is a finitely generated free $\overline{\Lambda}$-module with $\mathrm{rank}_{\overline{\Lambda}}(Y_p^\dagger(E/K_\infty)) = \mathrm{rank}_{\overline{\Lambda}}(\mathrm{Sel}_p^+(E/K_\infty)^{\mathrm{dual}})$. Therefore to complete the proof, we only have to show that $X_p^\dagger(E/K_\infty)$ and $Y_p^\dagger(E/K_\infty)$ are isomorphic.

Let $n \geq 1$. The transition map from $\mathrm{Sel}_p^+(E/K_\infty)^{\omega_{2n}^+=0}$ to $\mathrm{Sel}_p^+(E/K_\infty)^{\omega_{2n-2}^+=0}$ in $Y_p^\dagger(E/K_\infty)$ is $\mathrm{Tr}_{2n/2n-1}$. Let $\iota_{2n-2} : \mathrm{Sel}_p^+(E/K_\infty)^{\omega_{2n-2}^+=0} \hookrightarrow \mathrm{Sel}_p^+(E/K_\infty)$ be the inclusion map. One sees that $\mathrm{Tr}_{2n/2n-1}(\mathrm{Sel}_p^+(E/K_\infty)^{\omega_{2n}^+=0}) \subseteq \mathrm{img}\, \iota_{2n-2}$ and so by considering ι_{2n-2} to be an isomorphism onto it's image, we may write the transition maps defining the inverse limit $Y_p^\dagger(E/K_\infty)$ as $\iota_{2n-2}^{-1} \circ \mathrm{Tr}_{2n/2n-1}$. This shows that the restriction maps induce a map $\Xi : X_p^\dagger(E/K_\infty) \to Y_p^\dagger(E/K_\infty)$ and it follows from theorem 3.5 that this map is an isomorphism. This completes the proof. □

As in [17], we call a rational prime ℓ is called a *Kolyvagin prime* if ℓ is relatively prime to Nd and $\mathrm{Frob}_\ell(K(E[p])/\mathbb{Q}) = [\tau]$ where τ is a fixed complex conjugation on $\overline{\mathbb{Q}}$ (the algebraic closure of $\mathbb{Q}$).

If ℓ is a rational prime and F is a number field we define

$$E(F_\ell)/p := \oplus_{\lambda|\ell} E(F_\lambda)/p$$

$$H^1(F_\ell, E[p]) := \oplus_{\lambda|\ell} H^1(F_\lambda, E[p])$$

$$H^1(F_\ell, E)[p] := \oplus_{\lambda|\ell} H^1(F_\lambda, E)[p]$$

where the sum is taken over all primes of F dividing ℓ.

With this notation we let res_ℓ be the localization map:

$$\mathrm{res}_\ell : E(F)/p \to E(F_\ell)/p$$

$$\mathrm{res}_\ell : H^1(F, E[p]) \to H^1(F_\ell, E[p])$$

$$\mathrm{res}_\ell : H^1(F, E)[p] \to H^1(F_\ell, E)[p]$$

Now let ℓ be a Kolyvagin prime. For any n, local Tate duality gives a non-degenerate pairing (see [11] prop. 7.5)

$$\langle\ ,\ \rangle'_\ell : E(K_{2n,\ell})/p \times H^1(K_{2n,\ell}, E)[p] \to \mathbb{F}_p \tag{10}$$

This induces a non-degenerate pairing

$$\langle\ ,\ \rangle'_\ell : (E(K_{2n,\ell})/p)/\omega^+_{2n} \times H^1(K_{2n,\ell}, E)[p]^{\omega^+_{2n}=0} \to \mathbb{F}_p \tag{11}$$

Now as ℓ is inert in $K/\mathbb{Q}$ and $\ell \neq p$, it follows that ℓ splits completely in the anticyclotomic $\mathbb{Z}_p$-extension K_∞/K. We have $E(K_{n,\ell})/p = \oplus_{\lambda_n|\ell} E(K_{n,\lambda_n})/p$. For any $\lambda_n|\ell$ we have by Mattuck's theorem that $E(K_{n,\lambda_n}) \cong \mathbb{Z}_\ell^2 \times T$ where T is a finite group. This together with the fact that ℓ splits in $K(E[p])/K$ implies that $E(K_{n,\lambda_n})/p = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Thus we have an isomorphism

$$E(K_{n,\ell})/p \cong R_n \times R_n \tag{12}$$

The above isomorphism shows that multiplication by $\tilde{\omega}^-_{2n}$ induces an isomorphism $\theta : (E(K_{2n,\ell})/p)/\omega^+_{2n} \xrightarrow{\sim} \tilde{\omega}^-_{2n} E(K_{2n,\ell})/p = (E(K_{2n,\ell})/p)^{\omega^+_{2n}=0}$. Thus we have a non-degenerate pairing

$$\langle\ ,\ \rangle_\ell : (E(K_{2n,\ell})/p)^{\omega^+_{2n}=0} \times H^1(K_{2n,\ell}, E)[p]^{\omega^+_{2n}=0} \to \mathbb{F}_p \tag{13}$$

defined by the relation $\langle a, b\rangle'_\ell = \langle \theta(a), b\rangle_\ell$.

Now let $\mathrm{res}_n : H^1(K_{n,\ell}, E[p]) \to H^1(K_{n+1,\ell}, E[p])$ and $\mathrm{cor}_n : H^1(K_{n,\ell}, E[p]) \to H^1(K_{n-1,\ell}, E[p])$ be the restriction and corestriction maps, respectively. We will also let res_n and cor_n denote these maps on $E(K_{n,\ell})/p$ and $H^1(K_{n,\ell}, E)[p]$. Noting that $\tilde{\omega}^+_m = \tilde{\omega}^+_{m-1}$ and $\omega^+_m = \omega^+_{m-1}$ when m is odd and $\tilde{\omega}^-_m = \tilde{\omega}^-_{m-1}$ and $\omega^-_m = \omega^-_{m-1}$ when m is even, we get a commutative diagram

$$\begin{array}{ccc}
(E(K_{2n,\ell})/p)/\omega^+_{2n} & \xrightarrow{\times\tilde{\omega}^-_{2n}} & (E(K_{2n,\ell})/p)^{\omega^+_{2n}=0} \\
\downarrow{\scriptstyle \mathrm{cor}_{2n}} & & \downarrow{\scriptstyle \mathrm{cor}_{2n}} \\
(E(K_{2n-1,\ell})/p)/\omega^+_{2n-2} & \xrightarrow{\times\tilde{\omega}^-_{2n-1}} & (E(K_{2n-1,\ell})/p)^{\omega^+_{2n-2}=0} \\
\downarrow{\scriptstyle \mathrm{cor}_{2n-1}} & & \downarrow{\scriptstyle \mathrm{res}^{-1}_{2n-2}} \\
(E(K_{2n-2,\ell})/p)/\omega^+_{2n-2} & \xrightarrow{\times\tilde{\omega}^-_{2n-2}} & (E(K_{2n-2,\ell})/p)^{\omega^+_{2n-2}=0}
\end{array} \tag{14}$$

Let $\varinjlim H^1(K_{2n,\ell}, E)[p]^{\omega^+_{2n}=0}$ be the direct limit with transition maps being restriction and $\varprojlim (E(K_{2n,\ell})/p)^{\omega^+_{2n}=0}$ be the inverse limit with transition maps $\mathrm{res}^{-1}_{2n-2} \circ \mathrm{cor}_{2n} : (E(K_{2n,\ell})/p)^{\omega^+_{2n}=0} \to (E(K_{2n-2,\ell})/p)^{\omega^+_{2n-2}=0}$.

A property of Tate local duality gives that $\langle \mathrm{res}_n(a), b\rangle'_\ell = \langle a, \mathrm{cor}_{n+1}(b)\rangle'_\ell$. Taking this and the above commutative diagram into account, we see that the pairing $\langle\ ,\ \rangle_\ell$ induces an isomorphism

$$\varinjlim H^1(K_{2n,\ell}, E)[p]^{\omega^+_{2n}=0} \cong (\varprojlim (E(K_{2n,\ell})/p)^{\omega^+_{2n}=0})^{\mathrm{dual}} \tag{15}$$

Let $n \geq 0$ be an integer and ℓ a Kolyvagin prime. By the definition of $\mathrm{Sel}_p^+(E/K_{2n})$, we have $\mathrm{res}_\ell(\mathrm{Sel}_p^+(E/K_{2n})) \subseteq E(K_{2n,\ell})/p$ and so $\mathrm{res}_\ell(\mathrm{Sel}_p^+(E/K_{2n})^{\omega_{2n}^+=0}) \subseteq (E(K_{2n,\ell})/p)^{\omega_{2n}+=0}$.

The definitions of $X_p^\dagger(E/K_\infty)$ and $\varprojlim(E(K_{2n,\ell})/p)^{\omega_{2n}^+=0}$ show that the transition maps of these groups are compatible with the maps res_ℓ and therefore the maps res_ℓ induce a map

$$\mathrm{res}_\ell : X_p^\dagger(E/K_\infty) \to \varprojlim(E(K_{2n,\ell})/p)^{\omega_{2n}^+=0} \tag{16}$$

Dualizing this map and using the isomorphism (15) above we get a map

$$\psi_\ell : \varinjlim H^1(K_{2n,\ell}, E)[p]^{\omega_{2n}^+=0} \to X_p^\dagger(E/K_\infty)^{\mathrm{dual}}$$

We now follow the proof of the ordinary case in [17] carefully making the necessary adjustments to suit our setting. First we prove the analog of [17] prop. 2.5. We remark that there is a mistake in the proof of [17]: In the last line of the proof the $\mathbb{F}_p$-dimension should be $2+c$ rather that $2p+c$.

Proposition 3.8. *If ℓ is a Kolyvagin prime, then $\varinjlim H^1(K_{2n,\ell}, E)[p]^{\omega_{2n}^+=0}$ is a cofree $\overline{\Lambda}$-module of rank two*

Proof. Let $Z := \varinjlim H^1(K_{2n,\ell}, E)[p]^{\omega_{2n}^+=0}$. As in the proof of [17] prop. 2.5, we have $Z^{\omega_{2n}^+=0} = H^1(K_{2n,\ell}, E)[p]^{\omega_{2n}^+=0}$ and for any $\lambda_{2n}|\ell$ we have $H^1(K_{2n,\lambda_{2n}}, E)[p] = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Therefore it follows that $H^1(K_{2n,\ell}, E[p]) \cong R_{2n} \times R_{2n}$. Just as we observed after (12), we have $R_{2n}^{\omega_{2n}^+=0} \cong R_{2n}/\omega_{2n}^+$. Summing up, we get $Z^{\omega_{2n}^+=0} \cong R_{2n}/\omega_{2n}^+ \times R_{2n}/\omega_{2n}^+ \cong \overline{\Lambda}/\omega_{2n}^+ \times \overline{\Lambda}/\omega_{2n}^+$. The proposition follows from this. □

Let g be a topological generator of Γ. Since $X^{p^{n-1}(p-1)}\Phi_n(X^{-1}) = \Phi_n(X)$ and $\tau g \tau = g^{-1}$, therefore it easily follows from this and the fact that τ acts on $\mathrm{Sel}_p^+(E/K_{2n})$ that τ acts on $\mathrm{Sel}_p^+(E/K_{2n})^{\omega_{2n}^+=0}$ and hence also on $X_p^\dagger(E/K_\infty)$.

We define the sets and define the sets, U, V and $\mathcal{L}(U)$ in the same way as in section 2 of [17]. Then as in [17] prop. 2.8 we get

Proposition 3.9. *If U^+ generates V^+, then $\operatorname{img}\psi_\ell$ with ℓ ranging over $\mathscr{L}(U)$ generate $X_p^\dagger(E/K_\infty)^{\mathrm{dual}}$*

Also, using our modified pairing $\langle\ ,\ \rangle_\ell$ we get as in [17] prop. 2.9 that

Proposition 3.10. *For any n, if $s \in \mathrm{Sel}_p(E/K_{2n})^{\omega_{2n}^+=0}$ and $\gamma \in H^1(K_n, E)[p]^{\omega_{2n}^+=0}$, then*

$$\sum_\ell \langle \mathrm{res}_\ell\, s,\ \mathrm{res}_\ell\, \gamma\rangle_\ell = 0$$

where the sum is taken over all the rational primes

Let r be a squrefree product of Kolyvagin primes. We define Kolyvagin classes $c_n(r) \in H^1(K_n, E[p])$ and $d_n(r) \in H^1(K_n, E)[p]$ as in section 2.2 of [17]. We need

Proposition 3.11. *Let $n \geq 0$ and r a squarefree product of Kolyvagin prime. Let $\mathrm{res}_n : H^1(K_n, E[p]) \to H^1(K_{n+1}, E[p])$ be the restriction map. Then we have*

(a) $\mathrm{Tr}_{1/0}(c_1(r)) = \mathrm{res}_0(\frac{p-1}{2} c_0(r))$

$\mathrm{Tr}_{n+1/n}(c_{n+1}(r)) = -\mathrm{res}_{n-1}(c_{n-1}(r))$ *for $n \geq 1$*

(b) $\omega_{2n}^{+} c_{2n}(r) = 0$
(c) $\omega_{2n+1}^{+} c_{2n+1}(r) = 0$

Proof. If $K[r]$ is the ring class field of K of conductor r, we defined in [17] section 2.2 $K_n[r]$ to be $K_n K[r]$ and defined a Heegner point $\alpha_n(r) \in K_n(r)$. From section 3 of [23] one sees that the points $\alpha_n(r)$ satisfy identical norm relations to (3) and (4) which were shown for the points α_n. Therefore (a) follows from the definition of $c_n(r)$ and diagram (3) in [17] section 2.2. (b) and (c) follow from (a) as in lemma 2.1. □

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

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

By [12] lemma 2.1 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 $H^1(K_m, E[p])$.

The norm relation (4) in section 2 shows that $R_{2n}\alpha_{2n} \subseteq R_{2n+2}\alpha_{2n+2}$ and so we may form the direct limit $\varinjlim R_{2n}\alpha_{2n}$. From [17] theorem 4.1 we get

Theorem 3.12. *The $\overline{\Lambda}$-module $(\varinjlim R_{2n}\alpha_{2n})^{\mathrm{dual}}$ is finitely generated and not torsion*

Then as in [17] section 3, the above theorem implies that there exists a nonzero map

$$\phi : \overline{\Lambda}^{\ \mathrm{dual}} \to \varinjlim R_n\alpha_n$$

and one chooses an auxiliary prime ℓ_1 and this map to show

Proposition 3.13. *As a $\overline{\Lambda}$-module $(\varinjlim R_{2n}c_{2n}(\ell_1))^{\mathrm{dual}}$ is finitely generated and not torsion*

Note that $R_{2n}c_{2n}(\ell_1) \subseteq R_{2n+2}c_{2n+2}(\ell_1)$ by proposition 3.11. As in [17] section 3, one chooses $s \in \varinjlim R_{2n}\alpha_{2n}$ and $s' \in \varinjlim R_{2n}c_{2n}(\ell_1)$ and proves as in [17] prop. 3.3 that s and s' viewed as elements of $H^1(K_\infty, E[p])$ are linearly independent over $\mathbb{F}_p$. Then one defines the set $S_{n_0} \subset H^1(K_{n_0}, E[p])$ and the set U in the same way as in [17]. If $\ell \neq \ell_1$ is a Kolyvagin prime, then it follows from lemma 2.1 and proposition 3.11 that $\mathrm{res}_\ell(R_{2n}\alpha_{2n}) \subseteq (E(K_{2n,\ell})/p)^{\omega_{2n}^{+}=0}$ and $\mathrm{res}_\ell(R_{2n}c_{2n}(\ell_1)) \subseteq (E(K_{2n,\ell})/p)^{\omega_{2n}^{+}=0}$. Then by the same proof of [17] prop. 3.4, we get

Proposition 3.14. *For any $\ell \in \mathscr{L}(U)$ the submodules $\varinjlim \mathrm{res}_\ell R_{2n}\alpha_{2n}$ and $\varinjlim \mathrm{res}_\ell R_{2n}c_{2n}(\ell_1)$ of $\varinjlim (E(K_{2n,\ell})/p)^{\omega_{2n}=0}$ each have $\overline{\Lambda}$-corank greater or equal to one and together they generate a submodule of $\overline{\Lambda}$-corank equal to two*

Using property (3) of the Kolyvagin classes in section 2.2 of [17], the same proof of [17] corollary 3.5 gives

Corollary 3.15. *For any* $\ell \in \mathscr{L}(U)$ *the submodules* $\varinjlim \operatorname{res}_\ell R_{2n} d_{2n}(\ell)$ *and* $\varinjlim \operatorname{res}_\ell R_{2n} d_{2n}(\ell\ell_1)$ *of* $\varinjlim H^1(K_{2n,\ell}, E)[p]^{\omega_{2n}^+=0}$ *each have* $\overline{\Lambda}$*-corank greater or equal to one and together they generate* $\varinjlim H^1(K_{2n,\ell}, E)[p]^{\omega_{2n}^+=0}$

Using proposition 3.10 together with property (2) of the Kolyvagin classes in section 2.2 of [17], one proves the analog of [17] prop. 3.6 by the same way

Proposition 3.16. *For any* $\ell \in \mathscr{L}(U)$, $\operatorname{img} \psi_\ell$ *is a cofree* $\overline{\Lambda}$*-module and* $\operatorname{img} \psi_\ell = \psi_\ell(\varinjlim \operatorname{res}_\ell R_{2n} d_{2n}(\ell\ell_1))$

Then in an identical way to [17] prop. 3.7, one proves

Proposition 3.17. *We have* $\operatorname{rank}_{\overline{\Lambda}}(X_p^\dagger(E/K_\infty)) \leq 1$

We can now finally prove theorem B

Theorem B. *Assume the following*

(i) All the primes dividing pN *split in* $K/\mathbb{Q}$
(ii) p *does not divide* $6h_K\varphi(Nd_K) \cdot \prod_{\ell|N} c_v$
(iii) p *does not divide the number of geometrically connected components of the kernel of* $\pi_* : J_0(N) \to E$.

Then both $\operatorname{Sel}^{\pm}_{p^\infty}(E/K_\infty)^{\text{dual}}$ *have* Λ*-rank one and* μ*-invariant zero*

Proof. By proposition 3.4 it follows that $\operatorname{Sel}^+_{p^\infty}(E/K_\infty)[p] \cong \operatorname{Sel}^+_p(E/K_\infty)$. Therefore if $X := \operatorname{Sel}^+_{p^\infty}(E/K_\infty)^{\text{dual}}$, then $X/p \cong \operatorname{Sel}^+_p(E/K_\infty)^{\text{dual}}$. We see from this that to prove the theorem we only have to show that (i) $\operatorname{rank}_\Lambda(\operatorname{Sel}^+_{p^\infty}(E/K_\infty)^{\text{dual}}) \geq 1$ and that (ii) $\operatorname{rank}_{\overline{\Lambda}}(\operatorname{Sel}^+_p(E/K_\infty)^{\text{dual}}) \leq 1$. (i) follows from [15] prop. 4.7 and (ii) follows from the previous proposition together with theorem 3.7. This proves theorem B for $\operatorname{Sel}^+_{p^\infty}(E/K_\infty)$. The proof for $\operatorname{Sel}^-_{p^\infty}(E/K_\infty)$ is similar. □

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 théorie 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] M. Çiperiani, *Tate-Shafarevich groups in anticyclotomic* $\mathbb{Z}_p$*-extensions at supersingular primes*, Compositio Math. **145** (2009), 293-308
[5] J. Coates, R. Greenberg, *Kummer Theory for Abelian Varieties over Local Fields*, Invent. Math., **124** (1996), 129-174.
[6] C. Cornut, *Mazur's conjecture on higher Heegner points*, Invent. Math. **148** (2002), 495-523
[7] C. Cornut, V. Vatsal, *CM points and quarternion algebras*, Doc. Math **10** (2005), 263-309
[8] L. Dickson, *Linear groups: With an exposition of the Galois field theory*, Dover, New York, 1958.
[9] R. Greenberg, *Iwasawa theory for elliptic curves.* Lecture Notes in Math. 1716, Springer, New York 1999, pp.51-144.
[10] R. Greenberg, *Iwasawa theory for p-adic representations*, in Algebraic number theory, 97-137, Adv. Stud. Pure Math., 17, Academic Press, Boston, MA, 1989.
[11] B. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic, 235-256, London Math. Soc. Lecture Series, **153**, 1989.
[12] 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

[13] B.D. Kim, *The parity conjecture for elliptic curves at supersingular reduction primes*, Compositio Math. 143 (2007) 47–72.

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

[15] M. Longo, S. Vigni, *Plus/Minus Heegner points and Iwasawa theory of elliptic curves at supersingular primes*, Bollettino dell'Unione Matematica Italiana, Vol 12, No. 3 (2019), 315-347.

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

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

[18] A. Matar, *Fine Selmer Groups, Heegner points and Anticyclotomic $\mathbb{Z}_p$-extensions*, International Journal of Number Theory, Vol 14, No. 5 (2018), 1279-1304.

[19] A. Matar, *On the Λ-cotorsion subgroup of the Selmer group*, https://arxiv.org/abs/1812.00207 to appear in Asian Journal of Mathematics

[20] A. Matar, J. Nekovář, *Kolyvagin's result on the vanishing of $Ш(E/K)[p^\infty]$ and its consequences for anticyclotmic Iwasawa theory*, J. Théorie des Nombres de Bordeaux **31**(2) 2019, 455-501

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

[22] J. Nekovář, *Selmer complexes*, Astérisque 310 (2006), Soc. Math. de France, Paris.

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

[24] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331

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

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