KOLYVAGIN'S WORK AND ANTICYCLOTOMIC TOWER FIELDS: THE SUPERSINGULAR CASE

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. Kolyvagin has shown under certain assumptions that if the basic Heegner point $y_K \in E(K)$ is not divisible by p, then $\mathrm{rank}(E(K)) = 1$ and $Ш(E/K)[p^\infty] = 0$. Assuming that E has supersingular reduction at p and other conditions, we show using Kolyvagin's result and Iwasawa theory that for all n we have $\mathrm{rank}(E(K_n)) = p^n$ and $Ш(E/K_n)[p^\infty] = 0$

1. Introduction

Let K be an imaginary quadratic field with discriminant $d_K \neq -3, -4$ and p be a prime. 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 $\Gamma_n = \Gamma^{p^n}$ and $G_n = \Gamma/\Gamma_n$.

Let E an elliptic curve of conductor N defined over $\mathbb{Q}$ with a modular parametrization $\pi : X_0(N) \to E$ which maps the cusp ∞ of $X_0(N)$ to the origin of E (see [17] and [1]).

Assume that every prime dividing N splits in $K/\mathbb{Q}$. It follows that we can choose an ideal $\mathcal{N}$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. Therefore the natural projection of complex tori:

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

is a cyclic N-isogeny, which corresponds to a point of $x_1 \in X_0(N)$. The theory of complex multiplication shows that x_1 is rational over K_1, the Hilbert class field of K. Let $y_1 = \pi(x_1) \in E(K_1)$ and define the point $y_K = \mathrm{Tr}_{K_1/K}(y_1) \in E(K)$. Kolyvagin's celebrated paper [10] proves that when y_K has infinite order, then $E(K)$ has rank 1 and the Tate-Shafarevich group $Ш(E/K)$ is finite.

In this paper, we work with a particular prime p and therefore are interested in the following weaker result of Kolyvagin (see [6] prop. 2.1 and [12] thm. 6.7)

Theorem 1.1 (Kolyvagin)**.** *Let p be an odd prime such that $E[p]$ is an irreducible $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$-module and such that $y_K \notin pE(K)$, then $E(K) \otimes \mathbb{Z}_p = \mathbb{Z}_p(y_K \otimes 1) \cong \mathbb{Z}_p$ and $Ш(E/K)[p^\infty] = \{0\}$.*

The main theorem of this article can be thought of as an extension of the above result of Kolyvagin to the tower fields of the anticyclotomic $\mathbb{Z}_p$-extension of K. Before stating the result let us list the hypotheses we will work under.

Let p be a prime. We shall say that (E, p) satisfies $(\star)$ if the following are met:

(i) p splits in $K/\mathbb{Q}$
(ii) Both primes of K above p are totally ramified in K_∞/K

(iii) p does not divide $6N \cdot \prod_{\ell|N} c_v$

(iv) E has supersingular reduction at p

In the above, c_v is the Tamagawa number of E at the prime v and the product $\prod_{\ell|N} c_v$ runs over all rational primes dividing N. Conditions (i) and (ii) above will be imposed in order to invoke the results of Iovita and Pollack [7]. Note that condition (ii) is satisfied in p does not divide the class number of K.

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

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

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 $\Lambda = \mathbb{Z}_p[[\Gamma]]$ 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 $\mathbb{Z}_p[[T]]$.

For any discrete torsion abelian group A we let $A^{\mathrm{dual}} = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ denote its Pontryagin dual. The main result of this article is the following theorem

Theorem 1.2. *Assume that (E,p) satisfies $(\star)$ and $y_K \notin pE(K)$. Then we have*

(i) $\mathrm{rank}(E(K_n)) = p^n$ *for all* $n \geq 0$

(ii) $\text{Ш}(E/K_n)[p^\infty]$ *is trivial for* $n = 0$ *and finite for all* $n > 0$

If furthermore for some prime $\mathfrak{p}$ of K over p we have $y_K \notin pE(K_{\mathfrak{p}})$, then

(i) $\mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ *is a free Λ-module of rank two*

(ii) $\text{Ш}(E/K_n)[p^\infty] = 0$ *for all* $n \geq 0$.

This theorem may be viewed as the supersingular analog of theorem 4.9 of [12] which was proven in the ordinary case. Unlike the latter theorem, we impose the strong condition that $y_K \notin pE(K_{\mathfrak{p}})$ to get that $\text{Ш}(E/K_n)[p^\infty] = 0$ for all n. It is unclear to the author whether $\text{Ш}(E/K_n)[p^\infty] = 0$ for all n without imposing this condition. This theorem will be proven in section 4.

2. Some definitions and preliminary results

Beginning from this section till the end of the paper we assume that (E,p) satisfies $(\star)$. We now introduce some notation and make some 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.

Let $\mathfrak{p}$ be a prime of K_n above p (note that since we are assuming that p splits in $K/\mathbb{Q}$ and every prime of K above p is totally ramified in K_∞/K, it follows that there are two primes of K_n above p).

Following Kobayashi [9], we define the following subgroups of $E(K_{n,\mathfrak{p}})$

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

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

Following Kobayashi [9] and Iovita-Pollack [7], 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 $\mathrm{Sel}^{\pm}_{p^\infty}(E/K_\infty) = \varinjlim_n \mathrm{Sel}^{\pm}_{p^\infty}(E/K_n)$

Note that the condition defining $E^{\pm}(K_\mathfrak{p})$ is vacuous giving $E^{\pm}(K_\mathfrak{p}) = E(K_\mathfrak{p})$ and hence $\mathrm{Sel}^{\pm}_{p^\infty}(E/K) = \mathrm{Sel}_{p^\infty}(E/K)$

Finally, we define

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

Remark. Let $\hat{E}$ be the formal group of $E/\mathbb{Q}$. Then $\hat{E}(K_{n,\mathfrak{p}})$ is isomorphic to $E_1(K_{n,\mathfrak{p}}) = \ker(E(K_{n,\mathfrak{p}}) \to \bar{E}(\mathbb{F}_p))$. 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 $\bar{E}(\mathbb{F}_p)[p] = \{0\}$. 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 [7] 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 [7].

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 [17] and [1]) We are assuming that every prime dividing N splits in $K/\mathbb{Q}$. 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 are assuming that all the 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 $\alpha[p^{n+1}]$.

Under our assumption that p splits in $K/\mathbb{Q}$, it follows from section 3.3 of [15] that we have

$$\mathrm{Tr}_{K_1/K}(\alpha_1) = (a_p - (a_p - 2)^{-1}(p-1))\alpha_0 \tag{1}$$

$$\mathrm{Tr}_{K_{n+1}/K_n}(\alpha_{n+1}) = a_p\alpha_n - \alpha_{n-1} \quad \text{for } n \geq 1 \tag{2}$$

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

$$\mathrm{Tr}_{K_1/K}(\alpha_1) = \frac{p-1}{2}\alpha_0 \tag{3}$$

$$\mathrm{Tr}_{K_{n+1}/K_n}(\alpha_{n+1}) = -\alpha_{n-1} \quad \text{for } n \geq 1 \tag{4}$$

Recall that $y_K = \mathrm{Tr}_{K_1/K}(\alpha[1])$ (in the introduction $\alpha[1]$ was also denoted y_1) and $\alpha_0 = \mathrm{Tr}_{K[p]/K}(\alpha[p])$. From the relations in [15] section 3.3, we see that $\alpha_0 = (a_p - 2)y_K = -2y_K$. From this we see that if p does not divide y_K in $E(K)$, then also p does not divide α_0 in $E(K)$.

Lemma 2.1. *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 have the following important theorem

Theorem 2.2. *For any $n \geq 0$, the natural map*

$$s^\pm_n : \mathrm{Sel}^\pm_{p^\infty}(E/K_n)^{\omega^\pm_n = 0} \to \mathrm{Sel}^\pm_{p^\infty}(E/K_\infty)^{\omega^\pm_n = 0}$$

is an isomorphism.

Proof. Note that we have assumed that p splits in $K/\mathbb{Q}$ and 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 [7].

By theorem 6.8 of [7] $s^\pm_n$ is an injection with finite cokernel. The proof of this result is based on the proof of [9] theorem 9.3. The proof reveals that the cokernel of $s^\pm_n$ 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 [5] lemma 3.3). □

We end this section with the following proposition that will be used to invoke Kolyvagin's theorem (theorem 1.1)

Proposition 2.3. *$E[p]$ is an irreducible $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$-module*

Proof. This is true since E has good supersingular reduction at p. See [8] prop 4.4 or [16] prop 12(c). □

3. Structure theorems for Selmer groups

Theorem 3.1. *If $y_K \notin pE(K)$, then both $\mathrm{Sel}^+_{p^\infty}(E/K_\infty)$ and $\mathrm{Sel}^-_{p^\infty}(E/K_\infty)$ are cofree Λ-modules of rank one*

Proof. Assume that $y_K \notin pE(K)$. First consider the plus Selmer group. Let X be the Pontryagin dual of $\mathrm{Sel}^+_{p^\infty}(E/K_\infty)$. It follows from [11] prop 4.7 that X is not a torsion Λ-module.

Now according to theorem 2.2 the map $s_0^+ : \mathrm{Sel}_{p^\infty}(E/K) \to \mathrm{Sel}^+_{p^\infty}(E/K_\infty)^\Gamma$ is an isomorphism. Taking proposition 2.3 into account, theorem 1.1 gives that $\mathrm{Sel}_{p^\infty}(E/K) \cong \mathbb{Q}_p/\mathbb{Z}_p$, therefore we see that X is a cyclic Λ-module i.e. $X \cong \Lambda/I$ for some ideal I of Λ. But as X is not a torsion Λ-module, therefore $I = 0$ and X is a free Λ-module of rank 1 as claimed. The proof for the minus Selmer group is identical. □

Theorem 3.2. *If for some prime $\mathfrak{p}$ of K $y_K \notin pE(K_\mathfrak{p})$, then $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ is a cofree Λ-module of rank two*

Proof. It is well-known that the analog of Mazur's control theorem in the supersingular case fails. We shall explain this and show that theorem 1.1 together with the analysis of the cokernel of the restriction map between Selmer groups gives our desired result.

Define S to be the set of primes of K dividing Np 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, $G_S(K) = \mathrm{Gal}(K_S/K)$ and $G_S(K_\infty) = \mathrm{Gal}(K_S/K_\infty)$.

It is well-known that the p^∞-Selmer group $\mathrm{Sel}_{p^\infty}(E/K)$ may be defined as

$$0 \longrightarrow \mathrm{Sel}_{p^\infty}(E/K) \longrightarrow H^1(G_S(K), E[p^\infty]) \longrightarrow \prod_{v \in S} H^1(K_v, E)[p^\infty]$$

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

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

Now consider the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}_{p^\infty}(E/K_\infty)^\Gamma \arrow[r] & H^1(G_S(K_\infty), E[p^\infty])^\Gamma \arrow[r, "\psi_\infty"] & (\bigoplus_{v \in S_\infty} H^1(K_{\infty,v}, E)[p^\infty])^\Gamma \\
0 \arrow[r] & \mathrm{Sel}_{p^\infty}(E/K) \arrow[r] \arrow[u, "s"'] & H^1(G_S(K), E[p^\infty]) \arrow[r, "\psi"] \arrow[u, "h"'] & \bigoplus_{v \in S} H^1(K_v, E)[p^\infty] \arrow[u, "g"']
\end{tikzcd} \tag{5}$$

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 [7] 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 $\operatorname{coker} s = \ker g \cap \operatorname{img} \psi$.

We now analyze $\ker g$. Let v be a prime of K that does not divide p and consider the map $g_v : H^1(K_v, E)[p^\infty] \to (\oplus_{w|v} H^1(K_{\infty,w}, E)[p^\infty])^\Gamma$ where the sum is taken over all primes w of K_∞ 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_∞ above v. It follows from [14] proposition I-3.8 that $H^1(\Gamma_w, E)$ is finite of order $c_v^{(p)} = p^{\mathrm{ord}_p(c_v)}$. But by our assumption $p \nmid c_v$ and so therefore $\ker g_v = 0$.

Now let $v \in S_\infty$ above p. Then since E has supersingular reduction at p and K_∞/K is ramified at v, therefore it follows from [2] cor. 3.2 (see [5] pg. 70) that we have $H^1(K_{\infty,v}, E)[p^\infty] = \{0\}$.

The two observations above imply that $\ker g = H^1(K_{\mathfrak{p}_1}, E)[p^\infty] \times H^1(K_{\mathfrak{p}_2}, E)[p^\infty]$ where $\mathfrak{p}_1, \mathfrak{p}_2$ are the two primes of K above p. Therefore $\operatorname{coker} s = \operatorname{img} \psi \cap H^1(K_{\mathfrak{p}_1}, E)[p^\infty] \times H^1(K_{\mathfrak{p}_2}, E)[p^\infty]$. Let ψ' be the map $\psi' : H^1(G_S(K), E[p^\infty]) \to \bigoplus_{i=1,2} H^1(K_{\mathfrak{p}_i}, E)[p^\infty]$ so that $\operatorname{coker} s = \operatorname{img} \psi'$

We will show below that $\operatorname{coker} s = \operatorname{img} \psi' \cong \mathbb{Q}_p/\mathbb{Z}_p$. Let us explain how this implies the desired result. Since $\mathrm{Sel}_{p^\infty}(E/K) \cong \mathbb{Q}_p/\mathbb{Z}_p$ by Kolyvagin's theorem (theorem 1.1 taking prop 2.3 into account) and $\ker s = 0$ therefore we get an exact sequence

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

Let $X = \mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$. Then taking the dual of the above sequence and noting that $\mathbb{Z}_p$ is a projective $\mathbb{Z}_p$-module we get $X_\Gamma = \mathbb{Z}_p \times \mathbb{Z}_p$. This implies by Nakayama's lemma that X is generated by two elements as a Λ-module and so $X \cong \Lambda^2/I$ for some Λ-submodule I of Λ^2. If $I \neq 0$ then $\mathrm{rank}_\Lambda(X) \leq 1$. This contradicts theorem 1.7 of [5]. Therefore $I = 0$ and we get our desired result.

We study $\operatorname{img} \psi'$ by using the Cassels-Poitou-Tate exact sequence (see [3]):

$$H^1(G_S(K_n), E[p^\infty]) \xrightarrow{\psi'} \bigoplus_{i=1,2} H^1(K_{\mathfrak{p}_i}, E)[p^\infty] \xrightarrow{\theta} S_p(E/K)^{\mathrm{dual}}$$

where $S_p(E/K) = \varprojlim_n \mathrm{Sel}_{p^n}(E/K)$

We want to show that $\ker \theta = \operatorname{img} \psi' \cong \mathbb{Q}_p/\mathbb{Z}_p$ or equivalently $\operatorname{coker} \hat{\theta} \cong \mathbb{Z}_p$ where $\hat{\theta}$ is the dual of θ

$$\hat{\theta} : S_p(E/K) \to \bigoplus_{i=1,2} E(K_{\mathfrak{p}_i}) \otimes \mathbb{Z}_p$$

where $E(K_{\mathfrak{p}_i}) \otimes \mathbb{Z}_p$ is the p-adic completion of $E(K_{\mathfrak{p}_i})$.

By Mattuck's theorem $E(K_{\mathfrak{p}_i}) \cong \mathbb{Z}_p \times T$ where T is a finite group. By [7] lemma 2.1 the order of T is not divisible by p. Therefore $E(K_{\mathfrak{p}_i}) \otimes \mathbb{Z}_p \cong \mathbb{Z}_p$. Also theorem 1.1 implies that $S_p(E/K) = E(K) \otimes \mathbb{Z}_p = \mathbb{Z}_p$

Without loss of generality, we assume that y_K is not divisible by p in $E(K_{\mathfrak{p}_1})$ (it can be shown that this also implies that y_K is not divisible by p in $E(K_{\mathfrak{p}_2})$, but we won't need this). This implies that the restriction map from $S_p(E/K) = \mathbb{Z}_p$ to $E(K_{\mathfrak{p}_1}) \otimes \mathbb{Z}_p = \mathbb{Z}_p$ is an isomorphism. So now we have a map $\hat{\theta} : \mathbb{Z}_p \to \mathbb{Z}_p \times \mathbb{Z}_p$ such that if π_i is the projection of the target group onto its i-th factor then $\pi_1 \circ \hat{\theta}$ is an isomorphism. We want to show that $\operatorname{coker} \hat{\theta} \cong \mathbb{Z}_p$. Since $\hat{\theta}$ is not the zero map, therefore to show this we only need to show that $\mathrm{Tors}_{\mathbb{Z}_p}(\operatorname{coker} \hat{\theta}) = \{0\}$.

Let $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_p$ such that $(ra, rb) \in \operatorname{img} \hat{\theta}$ for some $r \in \mathbb{Z}_p \backslash \{0\}$. We must show that $(a, b) \in \operatorname{img} \hat{\theta}$. Let $x \in \mathbb{Z}_p$ be such that $\hat{\theta}(x) = (ra, rb)$. Since $\pi_1 \circ \hat{\theta}$ is surjective there exists $y \in \mathbb{Z}_p$ such that $\hat{\theta}(y) = (a, c)$ for some $c \in \mathbb{Z}_p$. Then we have $\pi_1(\hat{\theta}(ry)) = r\pi_1(\hat{\theta}(y)) = ra = \pi_1(\hat{\theta}(x))$ which implies that $ry = x$ since $\pi_1 \circ \hat{\theta}$ is injective. Therefore $(ra, rc) = (ra, rb)$ so $b = c$ showing that $(a, b) \in \operatorname{img} \hat{\theta}$ as desired. This completes the proof. □

4. Proof of main theorem

Proposition 4.1. *Let $0 \leq k \leq n$ and $\mathfrak{p}$ be a prime of K_n above p. Let $\mathcal{H}_k$ be the subgroup of $E(K_n)$ generated by all the Galois conjugates of the Heegner point α_k. Consider the following $\mathbb{F}_p[G_n]$-modules*

(i) $\mathcal{H}_k/p\mathcal{H}_k$
(ii) $(\mathcal{H}_k + pE(K_n))/pE(K_n)$
(iii) $(\mathcal{H}_k + pE(K_{n,\mathfrak{p}}))/pE(K_{n,\mathfrak{p}})$

Let $\epsilon = +$ or $-$ depending on whether k is even or odd, respectively and let $\bar{\omega}_k^\epsilon$ be the image of ω_k^ϵ in $\mathbb{F}_p[X]$. We have

(a) If $y_K \notin pE(K)$, then the groups (i) and (ii) are cyclic $\mathbb{F}_p[G_n]$-modules whose annihilator ideal is generated by $\bar{\omega}_k^\epsilon(\gamma - 1)$.
(b) If $y_K \notin pE(K_\mathfrak{p})$, then each of the groups (i), (ii) and (iii) is a cyclic $\mathbb{F}_p[G_n]$-module whose annihilator ideal is generated by $\bar{\omega}_k^\epsilon(\gamma - 1)$.

Proof. We will prove part (b). The proof of part (a) is almost identical. Assume that $y_K \notin pE(K_\mathfrak{p})$. Lemma 2.1 shows that $\bar{\omega}_k^\epsilon$ annihilates each of the groups (i), (ii) and (iii). Moreover, we have natural surjections

$$\mathcal{H}_k/p\mathcal{H}_k \twoheadrightarrow (\mathcal{H}_k + pE(K_n))/pE(K_n) \twoheadrightarrow (\mathcal{H}_k + pE(K_{n,\mathfrak{p}}))/pE(K_{n,\mathfrak{p}})$$

which proves the containment of the annihilators

$\mathrm{Ann}_{\mathbb{F}_p[G_n]}(\mathcal{H}_k/p\mathcal{H}_k) \subseteq \mathrm{Ann}_{\mathbb{F}_p[G_n]}((\mathcal{H}_k + pE(K_n))/pE(K_n)) \subseteq \mathrm{Ann}_{\mathbb{F}_p[G_n]}((\mathcal{H}_k + pE(K_{n,\mathfrak{p}}))/pE(K_{n,\mathfrak{p}}))$

Therefore we only have to prove that $\mathrm{Ann}_{\mathbb{F}_p[G_n]}((\mathcal{H}_k + pE(K_{n,\mathfrak{p}}))/pE(K_{n,\mathfrak{p}})) = \langle \bar{\omega}_k^\epsilon(\gamma - 1)\rangle$. As explained above, we have the containment $\supseteq$.

Note that for any $m \geq 1$ we have $X^{p^m} - 1 \equiv (X-1)^{p^m} \mod p$. From this it follows that $\bar{\omega}_k^\epsilon = X^{q_k}$. Now $\mathbb{F}_p[X]/\langle X^{p^n}\rangle$ is isomorphic to $\mathbb{F}_p[G_n]$ where the isomorphism is induced by the map taking X to $\gamma - 1$.

Now assume that $\mathrm{Ann}_{\mathbb{F}_p[G_n]}((\mathcal{H}_k + pE(K_{n,\mathfrak{p}}))/pE(K_{n,\mathfrak{p}}))$ is strictly larger than $\langle \bar{\omega}_k^\epsilon(\gamma - 1)\rangle$. As $\mathbb{F}_p[G_n]$ is isomorphic to $\mathbb{F}_p[X]/\langle X^{p^n}\rangle$ and $\mathbb{F}_p[X]$ is a PID, we see this implies that $\mathrm{Ann}_{\mathbb{F}_p[G_n]}((\mathcal{H}_k + pE(K_{n,\mathfrak{p}}))/pE(K_{n,\mathfrak{p}})) = \langle (\gamma - 1)^t\rangle$ where $t < q_k$. Therefore $(\gamma - 1)^{q_k - 1}$ annihilates $\alpha_k + pE(K_{n,\mathfrak{p}})$. But $\bar{\bar{\omega}}_k^\epsilon = X^{q_k - 1}$. So from the trace relations (3) and (4) we see that $(\gamma - 1)^{q_k - 1}(\alpha_k + pE(K_{n,\mathfrak{p}})) = c\alpha_0 + pE(K_{n,\mathfrak{p}}) = -2cy_K + pE(K_{n,\mathfrak{p}})$ for some $c \in \mathbb{F}_p^\times$. So we see that $y_K \in pE(K_{n,\mathfrak{p}})$ i.e. $y_K = pP$ for some $P \in E(K_{n,\mathfrak{p}})$.

Then $0 = (\gamma - 1)y_K = (\gamma - 1)pP = p(\gamma - 1)P$. Since $E(K_{n,\mathfrak{p}})[p^\infty]^\Gamma = E(K_\mathfrak{p})[p^\infty] = \{0\}$ by [7] lemma 2.1, therefore $E(K_{n,\mathfrak{p}})[p^\infty] = \{0\}$. So $(\gamma - 1)P = 0$ i.e. $P \in E(K_\mathfrak{p})$. So $y_K \in pE(K_\mathfrak{p})$ a contradiction. □

We now have the following important result

Theorem 4.2. *If $y_K \notin pE(K)$, then for any $n \geq 0$ the subgroup $\mathcal{H}(K_n)$ of $E(K_n)$ generated by all the Galois conjugates of the Heegner points α_m for $m \leq n$ has rank p^n*

Proof. For $n = 0$ this is theorem 1.1, so assume that $n \geq 1$. Let ϵ be $+$ or $-$ depending on whether n is even or odd, respectively. Let $\mathcal{H}(K_n)^\epsilon$ be the subgroup of $\mathcal{H}(K_n)$ generated by the Galois conjugates of α_n and $\mathcal{H}(K_n)^{-\epsilon}$ be the subgroup generated by the Galois conjugates of α_{n-1}.

By [7] lemma 2.1 $E(K_n)[p^\infty] = \{0\}$ so $\mathrm{rank}_{\mathbb{Z}}(\mathcal{H}(K_n)^\epsilon) = \dim_{\mathbb{F}_p}(\mathcal{H}(K_n)^\epsilon/p\mathcal{H}(K_n)^\epsilon)$ and by proposition 4.1(a)(i) we have

$$\dim_{\mathbb{F}_p}(\mathcal{H}(K_n)^\epsilon/p\mathcal{H}(K_n)^\epsilon) = \dim_{\mathbb{F}_p}(\mathbb{F}_p[G_n]/\langle\bar{\omega}_n^\epsilon(\gamma-1)\rangle) = \dim_{\mathbb{F}_p}(\mathbb{F}_p[X]/\langle\bar{\omega}_n^\epsilon\rangle) = \deg \omega_n^\epsilon = q_n$$

So $\mathrm{rank}_{\mathbb{Z}}(\mathcal{H}(K_n)^\epsilon) = q_n$ and similarly $\mathrm{rank}_{\mathbb{Z}}(\mathcal{H}(K_n)^{-\epsilon}) = q_{n-1}$

When $n = 1$ it is easy to see from the trace relation on the Heegner points (3) that $\mathrm{rank}_{\mathbb{Z}}(\mathcal{H}(K_1)) = \mathrm{rank}_{\mathbb{Z}}(\mathcal{H}(K_1)^\epsilon)$ and by the above the latter is equal to $q_1 = p$. This proves the result for $n = 1$. Now assume that $n > 1$. Then by the trace relation on the Heegner points (4) it is easy to see that $\mathcal{H}(K_n) = \mathcal{H}(K_n)^\epsilon + \mathcal{H}(K_n)^{-\epsilon}$.

Now let H_n be the subgroup of $E(K_n)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ generated by $\mathcal{H}(K_n)$ and $H_n^{\pm\epsilon}$ be the subgroup of $E(K_n)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ generated by $\mathcal{H}(K_n)^{\pm\epsilon}$. Then we have $H_n = H_n^\epsilon + H_n^{-\epsilon}$. Also $\mathrm{rank}_{\mathbb{Z}}(\mathcal{H}(K_n)) = \mathrm{corank}_{\mathbb{Z}_p}(H_n)$ and $\mathrm{rank}_{\mathbb{Z}}(\mathcal{H}(K_n)^{\pm\epsilon}) = \mathrm{corank}_{\mathbb{Z}_p}(H_n^{\pm\epsilon})$

From the above we see that

$$\begin{aligned}\mathrm{rank}_{\mathbb{Z}}(\mathcal{H}(K_n)) &= \mathrm{corank}_{\mathbb{Z}_p}(H_n)\\ &= \mathrm{corank}_{\mathbb{Z}_p}(H_n^\epsilon + H_n^{-\epsilon})\\ &= \mathrm{corank}_{\mathbb{Z}_p}(H_n^\epsilon) + \mathrm{corank}_{\mathbb{Z}_p}(H_n^{-\epsilon}) - \mathrm{corank}_{\mathbb{Z}_p}(H_n^\epsilon \cap H_n^{-\epsilon})\\ &= q_n + q_{n-1} - \mathrm{corank}_{\mathbb{Z}_p}(H_n^\epsilon \cap H_n^{-\epsilon})\\ &= p^n + 1 - \mathrm{corank}_{\mathbb{Z}_p}(H_n^\epsilon \cap H_n^{-\epsilon})\end{aligned}$$

Therefore we see that to prove the theorem we need to show that $\mathrm{corank}_{\mathbb{Z}_p}(H_n^\epsilon \cap H_n^{-\epsilon}) = 1$. We have $\mathbb{Z}\alpha_0 \otimes \mathbb{Q}_p/\mathbb{Z}_p \subseteq H_n^\epsilon \cap H_n^{-\epsilon}$ and α_0 has infinite order by Kolyvagin's theorem. This implies that $\mathrm{corank}(H_n^\epsilon \cap H_n^{-\epsilon}) \geq 1$. Therefore we need to show that $\mathrm{corank}_{\mathbb{Z}_p}(H_n^\epsilon \cap H_n^{-\epsilon}) \leq 1$. To show this, note that the trace relation (4) and lemma 2.1 imply that $H_n^\epsilon \subseteq \mathrm{Sel}^\epsilon_{p^\infty}(E/K_n)^{\omega_n^\epsilon=0}$. Since $\mathrm{Sel}^+_{p^\infty}(E/K_n) \cap \mathrm{Sel}^-_{p^\infty}(E/K_n) = \mathrm{Sel}^1_{p^\infty}(E/K_n)$ by [7] lemma 7.4(3), therefore $H_n^\epsilon \cap H_n^{-\epsilon} \subseteq \mathrm{Sel}^1_{p^\infty}(E/K_n)^{\omega_n^\pm=0}$. So it suffices to show that $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}^1_{p^\infty}(E/K_n)^{\omega_n^\pm=0}) \leq 1$.

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 $\mathrm{Sel}^1_{p^\infty}(E/K_n)^{\omega_n^\pm=0} \subseteq \mathrm{Sel}^1_{p^\infty}(E/K_n)^{p^m(\gamma-1)=0}$ ($\mathrm{Sel}^1_{p^\infty}(E/K_n)^{p^m(\gamma-1)=0}$ means the subgroup of $\mathrm{Sel}^1_{p^\infty}(E/K_n)$ annihilated by $p^m(\gamma-1)$). Therefore it suffices to show that $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}^1_{p^\infty}(E/K_n)^{p^m(\gamma-1)=0}) \leq 1$. As $p^m\,\mathrm{Sel}^1_{p^\infty}(E/K_n)^{p^m(\gamma-1)=0} \subseteq \mathrm{Sel}^1_{p^\infty}(E/K_n)^\Gamma$ and $\mathrm{Sel}^1_{p^\infty}(E/K_n)[p^m] \subseteq \mathrm{Sel}_{p^\infty}(E/K_n)[p^m]$ is finite, $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}^1_{p^\infty}(E/K_n)^{p^m(\gamma-1)=0}) \leq 1$ will follow if we can show that $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}^1_{p^\infty}(E/K_n)^\Gamma) \leq 1$. The next lemma shows that $\mathrm{Sel}^1_{p^\infty}(E/K_n)^\Gamma$ is isomorphic to $\mathrm{Sel}^1_{p^\infty}(E/K)$. Since $\mathrm{Sel}^1_{p^\infty}(E/K) \subseteq \mathrm{Sel}_{p^\infty}(E/K)$ and $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/K)) = 1$ by theorem 1.1 the result follows. □

Lemma 4.3. *For any $n \geq 0$, the restriction map induces an isomorphism* $\mathrm{Sel}^1_{p^\infty}(E/K) \cong \mathrm{Sel}^1_{p^\infty}(E/K_n)^{\Gamma_n}$

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, $G_S(K) = \mathrm{Gal}(K_S/K)$ and $G_S(K_n) = \mathrm{Gal}(K_S/K_n)$. 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

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}^1_{p^\infty}(E/K_n)^{\Gamma_n} \arrow[r] & H^1(G_S(K_n), E[p^\infty])^{\Gamma_n} \arrow[r] & \mathcal{P}_p(E/K_n)^{\Gamma_n} \times \mathcal{P}_*(E/K_n)^{\Gamma_n} \\
0 \arrow[r] & \mathrm{Sel}^1_{p^\infty}(E/K) \arrow[r] \arrow[u, "s"] & H^1(G_S(K), E[p^\infty]) \arrow[r, "\psi"] \arrow[u, "h"] & \mathcal{P}_p(E/K) \times \mathcal{P}_*(E/K) \arrow[u, "g"]
\end{tikzcd} \tag{6}$$

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 [7] 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 $\operatorname{coker} s = \ker g \cap \operatorname{img} \psi$. So to complete the proof of the lemma it will suffice to show that $\ker g = 0$.

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 [14] proposition I-3.8 that $H^1(\Gamma_w, E)$ is finite of order $c_v^{(p)} = p^{\mathrm{ord}_p(c_v)}$. But by our assumption $p \nmid c_v$ and so therefore $\ker g_v = 0$.

We therefore see that to show that $\ker g = 0$ we only need to show that the restriction map

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

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

To prove this, consider the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & (E(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma_n} \arrow[r] & H^1(K_{n,\mathfrak{p}}, E[p^\infty])^{\Gamma_n} \arrow[r] & \Big(\frac{H^1(K_{n,\mathfrak{p}}, E[p^\infty])}{E(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\Big)^{\Gamma_n} & \\
0 \arrow[r] & E(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p \arrow[r] \arrow[u, "g'_{\mathfrak{p}}"] & H^1(K_{\mathfrak{p}}, E[p^\infty]) \arrow[r] \arrow[u, "g''_{\mathfrak{p}}"] & \frac{H^1(K_{n,\mathfrak{p}}, E[p^\infty])}{E(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \arrow[r] \arrow[u, "g_{\mathfrak{p}}"] & 0
\end{tikzcd} \tag{7}$$

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 $\ker g''_{\mathfrak{p}} = H^1(\mathrm{Gal}(K_{n,\mathfrak{p}}/K_{\mathfrak{p}}), E(K_{n,\mathfrak{p}})[p^\infty])$. By [7] lemma 2.1 $E(K_{n,\mathfrak{p}})[p^\infty]^{\Gamma_n} = E(K_{\mathfrak{p}})[p^\infty] = \{0\}$ so $E(K_{n,\mathfrak{p}})[p^\infty] = \{0\}$. This shows that $\ker g''_{\mathfrak{p}} = 0$ which completes the proof.

□

Let $j : \mathrm{Sel}^+_{p^\infty}(E/K_n) \oplus \mathrm{Sel}^-_{p^\infty}(E/K_n) \to \mathrm{Sel}_{p^\infty}(E/K_n)$ be the diagonal map $(x, y) \mapsto x - y$

Proposition 4.4. *For any $n \geq 0$ we have an exact sequence*

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

where $K = \mathrm{Sel}^{1}_{p^\infty}(E/K_n)^{\omega_n^\pm=0}$ and C is finite

Proof. This is essentially proposition 10.1 of Kobayashi's paper [9]. 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 $\omega_n^- P^- = 0$. □

Theorem 4.5. *If $y_K \notin pE(K)$, then for any $n \geq 0$ $\mathrm{rank}(E(K_n)) = p^n$ and $\text{Ш}(E/K_n)[p^\infty]$ is finite*

Proof. By theorem 3.1 together with theorem 2.2, we have $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}^{+}_{p^\infty}(E/K_n)^{\omega_n^+=0} \oplus \mathrm{Sel}^{-}_{p^\infty}(E/K_n)^{\omega_n^-=0}) = \mathrm{corank}_{\mathbb{Z}_p}(\Lambda/\omega_n^+\Lambda \oplus \Lambda/\omega_n^-\Lambda) = \deg \omega_n^+ + \deg \omega_n^- = q_n + q_{n-1} = p^n + 1$

The exact sequence in the previous proposition together with this shows that $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/K_n)) = p^n + 1 - \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}^{1}_{p^\infty}(E/K_n)^{\omega_n^\pm=0})$. But $E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subseteq \mathrm{Sel}^{1}_{p^\infty}(E/K_n)^{\omega_n^\pm=0}$ and since $E(K)$ has rank one by theorem 1.1, therefore we see that $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}^{1}_{p^\infty}(E/K_n)^{\omega_n^\pm=0}) \geq 1$. So $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/K_n)) \leq p^n$. Theorem 4.2 implies that $\mathrm{rank}(E(K_n)) \geq p^n$. But $\mathrm{rank}(E(K_n)) = \mathrm{corank}_{\mathbb{Z}_p}(E(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \leq \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/K_n))$. So we get $\mathrm{rank}(E(K_n)) = \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/K_n)) = p^n$. This last equality implies that $\text{Ш}(E/K_n)[p^\infty]$ is finite.

□

In our main theorem we need to show that $\text{Ш}(E/K_n)[p^\infty] = 0$ for all $n \geq 0$ when $y_K \notin pE(K_\mathfrak{p})$ where $\mathfrak{p}$ is some prime of K above p. The first step towards proving this is the following

Proposition 4.6. *If for some prime $\mathfrak{p}$ of K above p $y_K \notin pE(K_\mathfrak{p})$, then $\text{Ш}(E/K_\infty)[p^\infty] = 0$*

Proof. It follows from [4] lemma 2.6.5 that $\mathrm{corank}_\Lambda(E(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \geq 2$. We have an exact sequence

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

Let X be the Pontryagin dual of $\text{Ш}(E/K_\infty)[p^\infty]$. The above exact sequence together with the fact that $\mathrm{corank}_\Lambda(E(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \geq 2$ and $\mathrm{corank}_\Lambda(\mathrm{Sel}_{p^\infty}(E/K_\infty)) = 2$ (theorem 3.2) implies that X is a torsion Λ-module. But X injects into the Pontryagin dual of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ which is a free Λ-module (theorem 3.2). It follows that $X = 0$ i.e. $\text{Ш}(E/K_\infty)[p^\infty] = 0$ as desired. □

We also need the following

Proposition 4.7. *If for some prime $\mathfrak{p}$ of K_∞ above p $y_K \notin pE(K_\mathfrak{p})$, then for any $n \geq 0$ the localization map $\theta_{n,\mathfrak{p}} : E(K_n) \otimes \mathbb{F}_p \to E(K_{n,\mathfrak{p}}) \otimes \mathbb{F}_p$ is an isomorphism*

Proof. For any $n \geq 0$ theorem 4.5 gives $\operatorname{rank}(E(K_n)) = p^n$ so $\dim_{\mathbb{F}_p}(E(K_n) \otimes \mathbb{F}_p) = p^n$. Also by Mattuck's theorem $E(K_{n,\mathfrak{p}}) \cong \mathbb{Z}_p^{p^n} \times T$ where T is a finite group. [7] lemma 2.1 implies that the order of T is prime to p, therefore $\dim_{\mathbb{F}_p}(E(K_{n,\mathfrak{p}}) \otimes \mathbb{F}_p) = p^n$. Thus to show that $\theta_{n,\mathfrak{p}}$ is an isomorphism it suffices to show that $\dim_{\mathbb{F}_p}(\operatorname{img} \theta_{n,\mathfrak{p}}) \geq p^n$ which we now show.

Since y_K is not divisible by p in $E(K_\mathfrak{p})$ this implies that $\dim_{\mathbb{F}_p}(\operatorname{img} \theta_{0,\mathfrak{p}}) \geq 1$ which proves the result for $n = 0$. Now assume $n \geq 1$. Now let ϵ be $+$ or $-$ depending on whether n is even or odd, respectively. Let $\mathcal{H}(K_n)^\epsilon$ be the subgroup of $E(K_n)$ generated by the Galois conjugates of α_n and $\mathcal{H}(K_n)^{-\epsilon}$ be the subgroup generated by the Galois conjugates of α_{n-1}. To simplify notation we denote $(\mathcal{H}(K_n)^{\pm\epsilon} + pE(K_n))/pE(K_n)$ by $\overline{\mathcal{H}}(K_n)^{\pm\epsilon}$ and in turn denote $\theta_{n,\mathfrak{p}}(\overline{\mathcal{H}}(K_n)^{\pm\epsilon})$ by $\overline{\mathcal{H}}(K_{n,\mathfrak{p}})^{\pm\epsilon}$

By proposition 4.1(b)(iii) we have

$$\dim_{\mathbb{F}_p}(\overline{\mathcal{H}}(K_{n,\mathfrak{p}})^\epsilon) = \dim_{\mathbb{F}_p}(\mathbb{F}_p[G_n]/\langle\bar{\omega}_n^\epsilon(\gamma-1)\rangle) = \dim_{\mathbb{F}_p}(\mathbb{F}_p[X]/\langle\bar{\omega}_n^\epsilon\rangle) = \deg \omega_n^\epsilon = q_n$$

and similarly $\dim_{\mathbb{F}_p}(\overline{\mathcal{H}}(K_{n,\mathfrak{p}})^{-\epsilon}) = q_{n-1}$

Since $q_1 = p$ the above implies that $\dim_{\mathbb{F}_p}(\operatorname{img} \theta_{1,\mathfrak{p}}) \geq p$ as desired. So now assume that $n > 1$. Then we have

$$\begin{aligned}\dim_{\mathbb{F}_p}(\overline{\mathcal{H}}(K_{n,\mathfrak{p}})^\epsilon + \overline{\mathcal{H}}(K_{n,\mathfrak{p}})^{-\epsilon}) &= \dim_{\mathbb{F}_p}(\overline{\mathcal{H}}(K_{n,\mathfrak{p}})^\epsilon) + \dim_{\mathbb{F}_p}(\overline{\mathcal{H}}(K_{n,\mathfrak{p}})^{-\epsilon}) - \dim_{\mathbb{F}_p}(\overline{\mathcal{H}}(K_{n,\mathfrak{p}})^\epsilon \cap \overline{\mathcal{H}}(K_{n,\mathfrak{p}})^{-\epsilon})\\ &= q_n + q_{n-1} - \dim_{\mathbb{F}_p}(\overline{\mathcal{H}}(K_{n,\mathfrak{p}})^\epsilon \cap \overline{\mathcal{H}}(K_{n,\mathfrak{p}})^{-\epsilon})\\ &= p^n + 1 - \dim_{\mathbb{F}_p}(\overline{\mathcal{H}}(K_{n,\mathfrak{p}})^\epsilon \cap \overline{\mathcal{H}}(K_{n,\mathfrak{p}})^{-\epsilon})\end{aligned}$$

From this we see that to show that $\dim_{\mathbb{F}_p}(\operatorname{img} \theta_{n,\mathfrak{p}}) \geq p^n$ we only have to show that $\dim_{\mathbb{F}_p}(\overline{\mathcal{H}}(K_{n,\mathfrak{p}})^\epsilon \cap \overline{\mathcal{H}}(K_{n,\mathfrak{p}})^{-\epsilon}) \leq 1$

The trace relation (4) implies that

$$\overline{\mathcal{H}}(K_{n,\mathfrak{p}})^{\pm\epsilon} \subseteq (E(K_{n,\mathfrak{p}})^{\pm\epsilon} + pE(K_{n,\mathfrak{p}}))/pE(K_{n,\mathfrak{p}})$$

. Therefore we only have to show that

$$\dim_{\mathbb{F}_p}((E(K_{n,\mathfrak{p}})^+ + pE(K_{n,\mathfrak{p}}))/pE(K_{n,\mathfrak{p}}) \cap (E(K_{n,\mathfrak{p}})^- + pE(K_{n,\mathfrak{p}}))/pE(K_{n,\mathfrak{p}})) \leq 1$$

By a proof identical to [4] lemma 2.6.5 using the results of Iovita and Pollack [7] we have

$$(E(K_{n,\mathfrak{p}})^+ + pE(K_{n,\mathfrak{p}}))/pE(K_{n,\mathfrak{p}}) \cap (E(K_{n,\mathfrak{p}})^- + pE(K_{n,\mathfrak{p}}))/pE(K_{n,\mathfrak{p}}) = (E(\mathbb{Q}_p) + pE(K_{n,\mathfrak{p}}))/pE(K_{n,\mathfrak{p}})$$

By Mattuck's theorem $E(\mathbb{Q}_p) \cong \mathbb{Z}_p \times T$ where T is a finite group. [7] lemma 2.1 implies that the order of T is prime to p. It follows from this that

$$\dim_{\mathbb{F}_p}((E(\mathbb{Q}_p) + pE(K_{n,\mathfrak{p}}))/pE(K_{n,\mathfrak{p}})) \leq 1$$

This completes the proof. □

Theorem 4.8. *If for some prime $\mathfrak{p}$ of K above p $y_K \notin pE(K_\mathfrak{p})$, then $\text{Ш}(E/K_n)[p^\infty] = 0$ for all $n \geq 0$*

Proof. Let $n \geq 0$. By proposition 4.6 $\text{Ш}(E/K_\infty)[p] = 0$ so we need to show that the restriction map $\operatorname{res}_n : \text{Ш}(E/K_n)[p] \to (\text{Ш}(E/K_\infty)[p])^{\Gamma_n}$ is an injection. Consider the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & (E(K_\infty)\otimes\mathbb{F}_p)^{\Gamma_n} \arrow[r, "\kappa_\infty"] & \mathrm{Sel}_p(E/K_\infty)^{\Gamma_n} \arrow[r] & (Ш(E/K_\infty)[p])^{\Gamma_n} & \\
0 \arrow[r] & E(K_n)\otimes\mathbb{F}_p \arrow[r, "\kappa_n"] \arrow[u, "\mathrm{res}''_n"'] & \mathrm{Sel}_p(E/K_n) \arrow[r] \arrow[u, "\mathrm{res}'_n"'] & Ш(E/K_n)[p] \arrow[r] \arrow[u, "\mathrm{res}_n"'] & 0
\end{tikzcd} \tag{8}$$

By [7] lemma 2.1 $E(K_\infty)[p^\infty] = 0$. This implies that that the restriction map $\mathrm{res}'_n : \mathrm{Sel}_p(E/K_n) \to \mathrm{Sel}_p(E/K_\infty)^{\Gamma_n}$ is an injection. Therefore applying the snake lemma to the above diagram we see that to show that res_n is an injection we need to show that

$$\bar{\kappa}_\infty : \frac{(E(K_\infty)\otimes\mathbb{F}_p)^{\Gamma_n}}{\mathrm{res}''_n(E(K_n)\otimes\mathbb{F}_p)} \to \frac{\mathrm{Sel}_p(E/K_\infty)^{\Gamma_n}}{\mathrm{res}'_n(\mathrm{Sel}_p(E/K_n))}$$

is an injection

Let $x \in (E(K_\infty)\otimes\mathbb{F}_p)^{\Gamma_n}$ and assume that $\kappa_\infty(x) = \mathrm{res}'_n(s)$ for some $s \in \mathrm{Sel}_p(E/K_n)$. We must show that $x \in \mathrm{img}\,\mathrm{res}''_n$

We will also denote the prime of K_∞ above $\mathfrak{p}$ by $\mathfrak{p}$. Let $\phi_{n,\mathfrak{p}} : H^1(K_n, E[p]) \to H^1(K_{n,\mathfrak{p}}, E[p])$ and $\phi_{\infty,\mathfrak{p}} : H^1(K_\infty, E[p]) \to H^1(K_{\infty,\mathfrak{p}}, E[p])$ be the restriction maps. Also let $\kappa_{n,\mathfrak{p}} : E(K_{n,\mathfrak{p}})\otimes\mathbb{F}_p \to H^1(K_{n,\mathfrak{p}}, E[p])$ and $\kappa_{\infty,\mathfrak{p}} : E(K_{\infty,\mathfrak{p}})\otimes\mathbb{F}_p \to H^1(K_{\infty,\mathfrak{p}}, E[p])$ be the Kummer maps. By definition, if $s \in \mathrm{Sel}_p(E/K_n)$ then $\phi_{n,\mathfrak{p}}(s) \in \mathrm{img}\,\kappa_{n,\mathfrak{p}}$ and if $s \in \mathrm{Sel}_p(E/K_\infty)$ then $\phi_{\infty,\mathfrak{p}}(s) \in \mathrm{img}\,\kappa_{\infty,\mathfrak{p}}$

Now let $\mathrm{res}_{n,\mathfrak{p}} : H^1(K_{n,\mathfrak{p}}, E[p]) \to H^1(K_{\infty,\mathfrak{p}}, E[p])^{\Gamma_n}$ and $\mathrm{res}_{n,\mathfrak{p}} : E(K_{n,\mathfrak{p}})\otimes\mathbb{F}_p \to (E(K_{\infty,\mathfrak{p}})\otimes\mathbb{F}_p)^{\Gamma_n}$ be the local restriction maps. Also let $\theta_{n,\mathfrak{p}} : E(K_n)\otimes\mathbb{F}_p \to E(K_{n,\mathfrak{p}})\otimes\mathbb{F}_p$ and $\theta_{\infty,\mathfrak{p}} : E(K_\infty)\otimes\mathbb{F}_p \to E(K_{\infty,\mathfrak{p}})\otimes\mathbb{F}_p$ be the localization maps. Both maps are isomorphisms by proposition 4.7.

Now we have

$$\kappa_{\infty,\mathfrak{p}}(\theta_{\infty,\mathfrak{p}}(x)) = \phi_{\infty,\mathfrak{p}}(\kappa_\infty(x)) = \phi_{\infty,\mathfrak{p}}(\mathrm{res}'_n(s)) = \mathrm{res}_{n,\mathfrak{p}}(\phi_{n,\mathfrak{p}}(s)) \tag{9}$$

As mentioned above, we have $\phi_{n,\mathfrak{p}}(s) = \kappa_{n,\mathfrak{p}}(y_\mathfrak{p})$ for some $y_\mathfrak{p} \in E(K_{n,\mathfrak{p}})\otimes\mathbb{F}_p$. Therefore from (9) we get

$$\kappa_{\infty,\mathfrak{p}}(\theta_{\infty,\mathfrak{p}}(x)) = \mathrm{res}_{n,\mathfrak{p}}(\phi_{n,\mathfrak{p}}(s)) = \mathrm{res}_{n,\mathfrak{p}}(\kappa_{n,\mathfrak{p}}(y_\mathfrak{p})) = \kappa_{\infty,\mathfrak{p}}(\mathrm{res}_{n,\mathfrak{p}}(y_\mathfrak{p})) \tag{10}$$

But $\theta_{n,\mathfrak{p}}$ is an isomorphism so $y_\mathfrak{p} = \theta_{n,\mathfrak{p}}(y)$ for some $y \in E(K_n)\otimes\mathbb{F}_p$. So from equation (10) we get

$$\kappa_{\infty,\mathfrak{p}}(\theta_{\infty,\mathfrak{p}}(x)) = \kappa_{\infty,\mathfrak{p}}(\mathrm{res}_{n,\mathfrak{p}}(y_\mathfrak{p})) = \kappa_{\infty,\mathfrak{p}}(\mathrm{res}_{n,\mathfrak{p}}(\theta_{n,\mathfrak{p}}(y))) = \kappa_{\infty,\mathfrak{p}}(\theta_{\infty,\mathfrak{p}}(\mathrm{res}''_n(y)))$$

But $\kappa_{\infty,\mathfrak{p}}$ and $\theta_{\infty,\mathfrak{p}}$ are both injections so the above equation gives $x = \mathrm{res}''_n(y)$. This proves the theorem. □

Our main theorem is now proven

Theorem 4.9. *Assume that (E, p) satisfies $(\star)$ and $y_K \notin pE(K)$. Then we have*

(i) $\mathrm{rank}(E(K_n)) = p^n$ *for all* $n \geq 0$
(ii) $Ш(E/K_n)[p^\infty]$ *is trivial for* $n = 0$ *and finite for all* $n > 0$

If furthermore for some prime $\mathfrak{p}$ of K over p we have $y_K \notin pE(K_\mathfrak{p})$, then

(i) $\mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$ *is a free Λ-module of rank two*
(ii) $Ш(E/K_n)[p^\infty] = 0$ *for all* $n \geq 0$.

Proof. This follows from theorems 1.1, 3.2, 4.5 and 4.8. □

Acknowledgments The author would like to thank Jan Nekovář for his comments on an earlier draft of this paper.

References

[1] 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.

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

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

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

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

[6] B. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic, 235-256, London Math. Soc. Lecture Series, **153**, 1989.

[7] 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

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

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

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

[11] 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.

[12] 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

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

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

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

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

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

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

Email address: amatar@uob.edu.bh