J. reine angew. Math. **801** (2023), 45–56
DOI 10.1515/crelle-2023-0029

Journal für die reine und angewandte Mathematik

Supersingular elliptic curves over $\mathbb{Z}_p$-extensions

By *Mirela Çiperiani* at Austin

Abstract. Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve and p a prime of supersingular reduction for E. Consider a quadratic extension $L/\mathbb{Q}_p$ and the corresponding anticyclotomic $\mathbb{Z}_p$-extension L_∞/L. We analyze the structure of the points $\mathrm{E}(L_\infty)$ and describe two global implications of our results.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N and p a rational prime such that $p \geq 5$ and E has supersingular reduction at p. Consider a finite extension $L/\mathbb{Q}_p$ and a $\mathbb{Z}_p$-extension L_∞ of L. Denote by L_n the unique subextension of L_∞ of degree p^n over L. Following Kobayashi [13], we define

$$\mathrm{E}^+(L_n) = \{P \in \mathrm{E}(L_n) \mid \mathrm{tr}_{L_n/L_{m+1}} P \in \mathrm{E}(L_m) \text{ for all } m \in 2\mathbb{Z} \text{ such that } 0 \leq m < n\},$$
$$\mathrm{E}^-(L_n) = \{P \in \mathrm{E}(L_n) \mid \mathrm{tr}_{L_n/L_{m+1}} P \in \mathrm{E}(L_m) \text{ for all } m \in 2\mathbb{Z}+1 \text{ such that } 0 \leq m < n\}.$$

Note that in particular $\mathrm{E}^\pm(L_0) = \mathrm{E}(L)$. We now view

$$\varinjlim_n \mathrm{E}^\pm(L_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subseteq \mathrm{H}^1(L_\infty, \mathrm{E}_{p^\infty})$$

as a module over $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(L_\infty/L)]]$.

In the case when $L = \mathbb{Q}_p$ and $L_\infty/\mathbb{Q}_p$ is totally ramified, we know that

$$\mathrm{E}(L_n) = \mathrm{E}^+(L_n) + \mathrm{E}^-(L_n), \quad \mathrm{E}^+(L_n) \cap \mathrm{E}^-(L_n) = \mathrm{E}(L) \quad \text{for all } n \geq 1. \tag{1.1}$$

This was proven by Kobayashi [13] for the cyclotomic $\mathbb{Z}_p$-extension $L_\infty/\mathbb{Q}_p$ and then generalized by Iovita and Pollack [12] to cover all totally ramified extensions $L_\infty/\mathbb{Q}_p$. By Burungale, Kobayashi, and Ota [4, Theorem 2.7], we now know that (1.1) holds also in the case when $L/\mathbb{Q}_p$ is a quadratic unramified extension and L_∞/L is the anticyclotomic $\mathbb{Z}_p$-extension.

Since p is a supersingular prime by work of Rubin [16, Lemma 2.2] and Konovalov [14], we have

$$\mathrm{E}(L_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \simeq \mathrm{H}^1(L_\infty, \mathrm{E}_{p^\infty})$$

The author was partially supported by NSA grant H98230-12-1-0208 and NSF CAREER grant DMS-1352598 during the preparation of this paper.

which together with (1.1) implies that

$$\operatorname{corank}_\Lambda \Big(\varinjlim_n \mathrm{E}^+(L_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cap \varinjlim_n \mathrm{E}^-(L_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p\Big) = 0, \tag{1.2}$$

where

$$\varinjlim_n \mathrm{E}^\pm(L_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

are viewed as submodules of $\mathrm{H}^1(L_\infty, \mathrm{E}_{p^\infty})$. We would like to know that the above statement holds in greater generality. Observe that (1.2) is weaker than

$$\varinjlim_n \mathrm{E}^+(L_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cap \varinjlim_n \mathrm{E}^-(L_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \mathrm{E}(L) \otimes \mathbb{Q}_p/\mathbb{Z}_p, \tag{1.3}$$

which follows from (1.1) and if $L \neq \mathbb{Q}_p$ is only known by work of Burungale, Kobayashi, and Ota [4, Theorem 2.7] in the case when $L/\mathbb{Q}_p$ is an unramified quadratic extension and L_∞/L is the anticyclotomic $\mathbb{Z}_p$-extension. It is our hope that the following theorem can eventually be proven and refined for much more general $L/\mathbb{Q}_p$ even if (1.3) does not hold.

Let $\mathrm{L}/\mathbb{Q}_p$ be a quadratic extension and $\mathrm{L}_\infty/\mathrm{L}$ the anticyclotomic $\mathbb{Z}_p$-extension of L, i.e. the non-trivial element of $\mathrm{Gal}(\mathrm{L}/\mathbb{Q}_p)$ acts on $\mathrm{Gal}(\mathrm{L}_\infty/\mathrm{L})$ by inverting every element. We prove the following theorem.

Theorem 1.1. *Let* $\mathrm{L}/\mathbb{Q}_p$ *be a quadratic extension and* $\mathrm{L}_\infty/\mathrm{L}$ *the anticyclotomic* $\mathbb{Z}_p$*-extension of* L*. Then*

(i) *the intersection of* $\varinjlim_n \mathrm{E}^+(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ *and* $\varinjlim_n \mathrm{E}^-(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ *has trivial* Λ*-corank;*

(ii) *the* Λ*-corank of* $\varinjlim_n \mathrm{E}^\pm(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ *equals* 2*.*

The proof uses Heegner points coming from the anticyclotomic $\mathbb{Z}_p$-extensions of two distinct carefully chosen imaginary quadratic extensions of $\mathbb{Q}$ which both localize to L at the prime p. The existence of these two quadratic extensions follows by work of Friedberg and Hoffstein [9]. However, in the case when $\mathrm{L}/\mathbb{Q}$ is unramified, due to the properties of Heegner points (see (2.1) in the inert case), using our method, we cannot distinguish the contributions of even Heegner points coming from the two quadratic extensions. This is where we use work of Rubin [17] on local units to get an upper bound on the Λ-corank of $\varinjlim_n \mathrm{E}^+(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ which then allows us to complete the argument.

The structure of points of supersingular elliptic curves in local $\mathbb{Z}_p$-extensions of non-trivial extensions of $\mathbb{Q}_p$ is presently opaque. Theorem 1.1 is the our first step towards ellucidating it. The proof is fine enough that it allows us to use our understanding of Heegner points to test conjectures about the further structure of $\mathrm{E}(L_\infty)$. In particular, it can be used to refute the possibility that we could split the local points of $\mathrm{E}(L_n)$ in a modulo $2d$ way with $d = [L : \mathbb{Q}_p]$ analogous to the modulo 2 version which gives rise to the $\mathrm{E}^\pm(L_n)$, in order to break $\mathrm{E}(L_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ into $2d$ Λ-corank 1 submodules. More precisely, if, for $r \in \{0, 2d-1\}$, we consider

$$E^{(r)}(L_n) := \{P \in E(L_n) \mid \mathrm{tr}_{L_n/L_m} P \in E(L_{2[L:\mathbb{Q}_p]k+r}) \text{ for some } k \in \mathbb{Z} \text{ and for all } m \leq n\},$$

then

$$\mathrm{E}^{(r)}(L_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p := \varinjlim_n \mathrm{E}^{(r)}(\mathrm{L}_n)\otimes\mathbb{Q}_p/\mathbb{Z}_p$$

are not necessarily of Λ-corank 1. In fact, if $d = 2$ and $L/\mathbb{Q}_p$ is ramified, using Theorem 1.1, one can see that localizations of Heegner points will give rise to a Λ-corank 2 submodule in $\mathrm{E}^{(r)}(L_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ for each $r \in \{0,1,2,3\}$.

We will now describe two global implications of Theorem 1.1. In [5], we consider an elliptic curve $\mathrm{E}/\mathbb{Q}$ of supersingular reduction at p, an imaginary quadratic extension $K/\mathbb{Q}$ such that every rational prime dividing the conductor of $\mathrm{E}/\mathbb{Q}$ splits, and the anticyclotomic $\mathbb{Z}_p$-extension of K_∞/K. Under the assumption that p splits in $K/\mathbb{Q}$, we prove that the Λ-corank of $\mathrm{E}(K_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ equals 2 and $Ш(\mathrm{E}/K_\infty)_{p^\infty}$ is a cotorsion Λ-module; see [5, Theorem 3.1 and Corollary 3.2]. If p does not split, we can now use Theorem 1.1 to give a proof of [5, Proposition 2.1]. More precisely, by assuming that $K/\mathbb{Q}$ satisfies the Heegner hypothesis, we consider Heegner points $\alpha_n \in \mathrm{E}(K_\infty)$ (see § 2.1 for definitions and relevant properties) which give rise to the following corank 1 Λ-modules:

$$\varinjlim_n \mathbb{Z}_p[\mathrm{Gal}(K_\infty/K)]\alpha_{2n},\ \varinjlim_n \mathbb{Z}_p[\mathrm{Gal}(K_\infty/K)]\alpha_{2n+1} \subseteq \mathrm{E}(K_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p.$$

By localizing each layer $\mathbb{Z}_p[\mathrm{Gal}(K_\infty/K)]\alpha_n$ at the relevant prime above p, we have

$$\mathrm{res}_p\big(\varinjlim_n \mathbb{Z}_p[\mathrm{Gal}(K_\infty/K)]\alpha_{2n}\big)\otimes\mathbb{Q}_p/\mathbb{Z}_p \subseteq \varinjlim_n \mathrm{E}^+(L_n)\otimes\mathbb{Q}_p/\mathbb{Z}_p,$$
$$\mathrm{res}_p\big(\varinjlim_n \mathbb{Z}_p[\mathrm{Gal}(K_\infty/K)]\alpha_{2n+1}\big)\otimes\mathbb{Q}_p/\mathbb{Z}_p \subseteq \varinjlim_n \mathrm{E}^-(L_n)\otimes\mathbb{Q}_p/\mathbb{Z}_p.$$

Then, by Theorem 1.1, it follows that Heegner points give rise to a corank 2 Λ-module within $\mathrm{E}(K_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ as stated in [5, Proposition 2.1]. Since this is the only step of the proof where the splitting of p in $K/\mathbb{Q}$ is used, we now have the following theorem.

Theorem 1.2. *Let* $\mathrm{E}/\mathbb{Q}$ *be an elliptic curve with supersingular reduction at the prime* p *such that* $p \geq 5$, $K/\mathbb{Q}$ *an imaginary quadratic extension satisfying the Heegner hypothesis, and* K_∞ *the anticyclotomic* $\mathbb{Z}_p$*-extension of* K*. Then the* Λ*-corank of* $\mathrm{E}(K_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ *equals* 2 *and* $Ш(\mathrm{E}/K_\infty)_{p^\infty}$ *is a cotorsion* Λ*-module.*

The second global situation is a basic case of the more general set-up that we are aiming to tackle. We consider a real quadratic extension $\mathrm{F}/\mathbb{Q}$ such that p does not split and a totally imaginary quadratic extension K/F such that the prime of $\wp \subseteq \mathrm{F}$ above p splits (see § 3). Then we can consider the $\mathbb{Z}_p$-extension $\mathrm{K}_\infty/\mathrm{K}$ contained in the union of the anticyclotomic extensions of K of conductor $\wp^n$ for all $n \in \mathbb{N}$ such that the completion of K_∞ at $\wp$ equals L_∞, and the CM points $\mathfrak{z}_n \in \mathrm{E}(\mathrm{K}_n)$, where K_n denotes the unique subextension of K_∞ of degree p^n over K. Unlike Heegner points, these CM points do not naturally localize to points in $\mathrm{E}^\pm(\mathrm{L}_n)$; see (3.3). Despite this issue, we use Theorem 1.1 to prove that if[1] $\mathfrak{z}_n \in \mathrm{E}(\mathrm{K}_n)\setminus\mathrm{E}(\mathrm{K}_{n-1})$ for almost all n, then these CM points give rise to a corank 2 submodule in $\mathrm{E}(\mathrm{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ and hence

$$\mathrm{corank}_\Lambda\, \mathrm{E}(\mathrm{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p \geq 2.$$

[1] Cornut and Vatsal [8] have shown that, for almost all anticyclotomic $\mathbb{Z}_p$-extensions of K, we have $\mathfrak{z}_n \in \mathrm{E}(\mathrm{K}_n)\setminus\mathrm{E}(\mathrm{K}_{n-1})$ for almost all n.

2. Local results

Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N, $L/\mathbb{Q}_p$ a quadratic extension, L_∞/L the anticyclotomic $\mathbb{Z}_p$-extension of L, and L_n the unique subextension of L_∞ of degree p^n over L. Denote by $\wp$ the prime of L above p.

2.1. Heegner points. We fix a parametrization $\pi: X_0(N) \to E$ which maps the cusp at ∞ to the origin of E. Let K be an imaginary quadratic extension of $\mathbb{Q}$ such that all primes dividing N split in $K/\mathbb{Q}$, and denote by $\mathcal{O}_K$ the ring of integers of K. We can then choose an ideal $\mathcal{N}$ such that $\mathcal{O}_K/\mathcal{N} \simeq \mathbb{Z}/N\mathbb{Z}$. For any positive integer c prime to N, we can consider $x_c = (\mathbb{C}/\mathcal{O}_c, \mathbb{C}/\mathcal{N}_c) \in X_0(N)$, where $\mathcal{O}_c$ denotes the order of K of conductor c and $\mathcal{N}_c = \mathcal{N} \cap \mathcal{O}_c$. We define the Heegner point $y_c = \pi(x_c)$. The Heegner point y_c is defined over the ring class field of K of conductor c, $K[c]$.

Let

$$K[p^\infty] = \bigcup_{n\geq 1} K[p^n].$$

Then $\mathrm{Gal}(K[p^\infty]/K)$ is isomorphic to $\mathbb{Z}_p \times \Delta$, where Δ is a finite abelian group. The unique $\mathbb{Z}_p$-extension of K contained in $K[p^\infty]$ is the anticyclotomic $\mathbb{Z}_p$-extension K_∞/K. Denote by $K[p^{k(n)}]$ the minimal ring class field of p-power conductor containing K_n, the subextension of K_∞ of degree p^n over K. Then we define $\alpha_n \in E(K_n)$ to be the trace of $y_{p^{k(n)}}$ from $K[p^{k(n)}]$ to K_n. Perrin-Riou [15, Section 3.3, Lemme 2] has shown that

$$\mathrm{tr}_{K[p^{n+2}]/K[p^{n+1}]} y_{p^{n+2}} = a_p y_{p^{n+1}} - y_{p^n} \quad \text{for } n \geq 0,$$

$$\mathrm{tr}_{K[p]/K[1]} y_p = \begin{cases} a_p y_1 & \text{if } p \text{ is inert in } K/\mathbb{Q}, \\ (a_p - \sigma) y_1 & \text{if } p \text{ ramifies in } K/\mathbb{Q}, \end{cases}$$

for some $\sigma \in \mathrm{Gal}(K[1]/K)$.

Set $k_0 = \max\{n \in \mathbb{N} \mid K_n \subseteq K[1]\}$. Since $p \geq 5$ and E has supersingular reduction at p, it follows[2] that $a_p = 0$ and hence

$$\mathrm{tr}_{K_{n+2}/K_n} \alpha_{n+2} = -\alpha_n \quad \text{for } n > k_0, \tag{2.1}$$

$$\mathrm{tr}_{K_{k_0+2}/K_{k_0+1}} \alpha_{k_0+2} = \begin{cases} 0 & \text{if } p \text{ is inert in } K/\mathbb{Q}, \\ -\alpha_{k_0} & \text{if } p \text{ ramifies in } K/\mathbb{Q}, \end{cases}$$

$$\mathrm{tr}_{K_{k_0+1}/K_{k_0}} \alpha_{k_0+1} = \begin{cases} -(p+1)\alpha_{k_0} & \text{if } p \text{ is inert in } K/\mathbb{Q}, \\ -\sigma\alpha_{k_0} & \text{if } p \text{ ramifies in } K/\mathbb{Q}, \end{cases}$$

for some $\sigma \in \mathrm{Gal}(K_{k_0}/K)$.

Furthermore, complex conjugation $\tau \in \mathrm{Gal}(K_\infty/\mathbb{Q})$ acts on the Heegner points α_n, and by [11, Proposition 5.3], we know that $\alpha_n^\tau \in -\epsilon g^{i_n}(\alpha_n) + E(\mathbb{Q})_{\mathrm{tors}}$, where g denotes a topological generator of $\mathrm{Gal}(K_\infty/K)$, $i_n \in \mathbb{Z}$, and ϵ is the sign of the functional equation of $E/\mathbb{Q}$. In particular,

$$\alpha_0^\tau \in -\epsilon\alpha_0 + E(\mathbb{Q})_{\mathrm{tors}}. \tag{2.2}$$

[2] This is our reason for assuming $p \geq 5$.

2.2. Local points. Following Kobayashi, we have defined

$$\mathrm{E}^+(\mathrm{L}_n) = \{P \in \mathrm{E}(\mathrm{L}_n) \mid \mathrm{tr}_{\mathrm{L}_n/\mathrm{L}_{m+1}} P \in \mathrm{E}(\mathrm{L}_m) \text{ for all } m \in 2\mathbb{Z} \text{ such that } 0 \le m < n\},$$
$$\mathrm{E}^-(\mathrm{L}_n) = \{P \in \mathrm{E}(\mathrm{L}_n) \mid \mathrm{tr}_{\mathrm{L}_n/\mathrm{L}_{m+1}} P \in \mathrm{E}(\mathrm{L}_m) \text{ for all } m \in 2\mathbb{Z}+1 \text{ such that } 0 \le m < n\}.$$

The Galois group $\mathrm{Gal}(\mathrm{L}_n/\mathrm{L})$ acts on $\mathrm{E}^{\pm}(\mathrm{L}_n)$. Hence,

$$\varinjlim_n \mathrm{E}^{\pm}(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

can be viewed as modules over $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(\mathrm{L}_\infty/\mathrm{L})]]$. We will now analyze their Λ-coranks.

Proposition 2.1. *If $\mathrm{L}/\mathbb{Q}_p$ is unramified, then the Λ-corank of $\varinjlim_n \mathrm{E}^+(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is less than or equal to* 2.

Proof. Let $\mathbf{E}/\mathbb{Z}_p$ be the formal group associated to E. We know that, over $\mathcal{O}_\mathrm{L}$, the ring of integers of L, the formal group $\mathbf{E}$ is isomorphic to the Lubin–Tate formal group of height two with uniformizing parameter $-p$; see [13, Proposition 8.6]. Then following Rubin [17], we consider U_n the units of $\mathrm{L}(\mathbf{E}_{p^{n+1}})$ which are congruent to 1 modulo the maximal ideal. Observe that $\mathrm{L}_n \subseteq \mathrm{L}(\mathbf{E}_{p^{n+1}})$ and hence $\mathrm{L}_\infty \subseteq \mathrm{L}(\mathbf{E}_{p^\infty})$. Since

$$\mathrm{Gal}(\mathrm{L}(\mathbf{E}_{p^\infty})/\mathrm{L}) \simeq \mathcal{O}_\mathrm{L}^* \simeq (\mathcal{O}_\mathrm{L}/p\mathcal{O}_\mathrm{L})^* \times \mathcal{O}_\mathrm{L} \simeq \mathrm{Gal}(\mathrm{L}(\mathbf{E}_p)/\mathrm{L}) \times \mathcal{O}_\mathrm{L},$$

we consider the map

$$\kappa\colon \mathrm{Gal}(\mathrm{L}(\mathbf{E}_{p^\infty})/\mathrm{L}) \to \mathcal{O}_\mathrm{L}^*$$

and denote by ω the restriction of κ to $\mathrm{Gal}(\mathrm{L}(\mathbf{E}_p)/\mathrm{L})$. For any $\mathcal{O}_\mathrm{L}[\mathrm{Gal}(\mathrm{L}(\mathbf{E}_p)/\mathrm{L})]$-module M, M^ω denotes the submodule of M on which $\mathrm{Gal}(\mathrm{L}(\mathbf{E}_p)/\mathrm{L})$ acts via ω. We can then define

$$\mathrm{U}_\infty = \big(\varprojlim_n \mathrm{U}_n \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathrm{L}\big)^\omega \quad \text{and} \quad \mathrm{V}_\infty = \mathrm{U}_\infty/(\sigma - \kappa(\sigma))\mathrm{U}_\infty,$$

where the transition maps of the inverse limit are simply the norm maps and σ is a topological generator of $\mathrm{Gal}(\mathrm{L}(\mathbf{E}_{p^\infty})/\mathrm{L}_\infty(\mathbf{E}_p)) \simeq \mathbb{Z}_p$. Then V_∞ is a Λ-module, and by [17, Proposition 1], we know that $\mathrm{rank}_\Lambda \mathrm{V}_\infty = 4$.

Set Σ^+ and Σ^- to be the sets of characters $\chi\colon \mathrm{Gal}(\mathrm{L}_\infty/\mathrm{L}) \to \mathbb{Q}_p^*$ of conductor an even and odd, respectively, power of p. For any character $\chi \in \Sigma^\pm$ that factors through $\mathrm{Gal}(\mathrm{L}_n/\mathrm{L})$, we consider the $\mathcal{O}_\mathrm{L}$-linear homomorphism $\delta_\chi\colon \mathrm{U}_\infty \to \mathrm{L}(E_{p^{n+1}})$ defined as follows:

$$\delta_\chi(u) = p^{-n-1} \sum_{\gamma \in \mathrm{Gal}(\mathrm{L}(\mathbf{E}_{p^{n+1}})/\mathrm{L})} \chi(\gamma)\delta_n(u)^\gamma,$$

where $\delta_n\colon \mathrm{U}_\infty \to \mathrm{L}(\mathbf{E}_{p^{n+1}})$ are the Coates–Wiles logarithmic derivatives (they depend on a choice of a generator of the Tate module $T_p(\mathbf{E})$ which we fix); see [17, Section 2]. Since, by [17, Lemma 2.1 (ii)], we have $\delta_\chi((\sigma - \kappa(\sigma))\mathrm{U}_\infty) = 0$ for every $\chi \in \Sigma^\pm$, we can now define

$$\mathrm{V}^+ = \{v \in \mathrm{V}_\infty \mid \delta_\chi(v) = 0 \text{ for every } \chi \in \Sigma^-\}.$$

Using elliptic units Rubin proves that $\mathrm{rank}_\Lambda \mathrm{V}^+ \ge 2$ (see [17, Corollary 3.4]). It then follows that $\mathrm{rank}_\Lambda \mathrm{V}_\infty/\mathrm{V}^+ \le 2$.

Let λ denote the logarithm map of $\mathbf{E}$. For any character $\chi \in \Sigma^+$ and $y \in \mathbf{E}(\mathrm{L}_\infty)$, we define

$$\lambda_\chi(y) = p^{-n} \sum_{\gamma \in \mathrm{Gal}(\mathrm{L}_n/\mathrm{L})} \chi^{-1}(\gamma)\lambda(y)^\gamma,$$

where $n \in \mathbb{N}$ is large enough so that $y \in \mathbf{E}(\mathrm{L}_n)$ and χ factors through $\mathrm{Gal}(\mathrm{L}_n/\mathrm{L})$. Consider the set

$$A^+ = \{y \in \mathbf{E}(\mathrm{L}_\infty) \mid \lambda_\chi(y) = 0 \text{ for all } \chi \in \Sigma^+\}.$$

We will now show that

$$(g-1)\mathbf{E}^+(\mathrm{L}_n) \subseteq A^+ \quad \text{for all } n \in \mathbb{N},$$

where g denotes a topological generator of $\mathrm{Gal}(\mathrm{L}_\infty/\mathrm{L})$ (the argument is identical to the proof of [17, Corollary 6.2]). Let $y \in (g-1)\mathbf{E}^+(\mathrm{L}_n)$ and $\chi \in \Sigma^+$ such that if χ is non-trivial, it factors through $\mathrm{Gal}(\mathrm{L}_m/\mathrm{L})$ and is non-trivial on $\mathrm{Gal}(\mathrm{L}_m/\mathrm{L}_{m-1})$. Observe that, since $\chi \in \Sigma^+$, it follows that m is odd. Moreover, as $\mathbf{E}^+(\mathrm{L}_n) \subseteq \mathbf{E}^+(\mathrm{L}_{2\lfloor n/2 \rfloor})$, we may assume that n is even. We have three cases to consider:

- $n < m$: since χ is non-trivial on $\mathrm{Gal}(\mathrm{L}_m/\mathrm{L}_n)$, we have $\lambda_\chi(y) = 0$;
- $0 < m < n$: $\lambda_\chi(y) = p^{n-m}\lambda_\chi(\mathrm{tr}_{\mathrm{L}_n/\mathrm{L}_m} y) = 0$ since $\mathrm{tr}_{\mathrm{L}_n/\mathrm{L}_m} y \in \mathbf{E}(\mathrm{L}_{m-1})$;
- χ is the trivial character: $\lambda_\chi(y) = \lambda_\chi(\mathrm{tr}_{\mathrm{L}_n/\mathrm{L}} y) = 0$ since $y \in (g-1)\mathbf{E}^+(\mathrm{L}_n)$.

Since $\#\mathrm{E}(\mathbb{F}_{p^2}) = p^2 + 1 - \alpha^2 - \beta^2$, where α, β are the complex roots of $x^2 - a_p x + p = 0$ and in our case $a_p = 0$, we observe that $\#\mathrm{E}(\mathbb{F}_{p^2}) = (p+1)^2$. Then, as $\mathrm{L}_\infty/\mathrm{L}$ is totally ramified, it follows that

$$(p+1)^2\mathrm{E}^+(\mathrm{L}_n) \subseteq \mathbf{E}^+(\mathrm{L}_n),$$

which implies that

$$(g-1)(p+1)^2\mathrm{E}^+(\mathrm{L}_n) \subseteq A^+ \quad \text{for all } n \in \mathbb{N}. \tag{2.3}$$

By [17, Corollary 5.7], we know that

$$A^+ \otimes \mathbb{Q}_p/\mathbb{Z}_p \simeq \mathrm{Hom}_{\mathcal{O}_\mathrm{L}}(V_\infty/V^+, \mathbf{E}_{p^\infty}).$$

Since $\mathrm{rank}_\Lambda \mathrm{V}_\infty/V^+ \leq 2$, it follows that $\mathrm{corank}_\Lambda A^+ \otimes \mathbb{Q}_p/\mathbb{Z}_p \leq 2$ which together with (2.3) allows us to deduce that

$$\mathrm{corank}_\Lambda \varinjlim_n \mathrm{E}^+(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \leq 2. \qquad \square$$

Set $\mathcal{R}_n := \mathbb{Z}_p[\mathrm{Gal}(\mathrm{L}_n/\mathrm{L})]$ and $\mathrm{R}_n := \mathbb{Z}/p\mathbb{Z}[\mathrm{Gal}(\mathrm{L}_n/\mathrm{L})]$. We may now view $\mathrm{E}^\pm(\mathrm{L}_n)$ as $\mathcal{R}_n$-modules and $\mathrm{E}^\pm(\mathrm{L}_n)/p^n$ as R_n-modules. This will be used in the proof of the following theorem.

Theorem 2.2. *The intersection of*

$$\varinjlim_n \mathrm{E}^+(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \quad \textit{and} \quad \varinjlim_n \mathrm{E}^-(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

has trivial Λ-corank.

Proof. Let $\mathrm{L} = \mathbb{Q}_p[\sqrt{d}]$, where $d \in \mathbb{Z}_p$ such that $p^2 \nmid d$. By [9, Theorem B (2)] of Friedberg and Hoffstein, we know that we can find $d_1, d_2 \in \mathbb{Z}$ such that

(i) the quadratic twist $\mathrm{E}^{d_1}/\mathbb{Q}$ has trivial analytic rank and d_1 is a non-trivial quadratic residue modulo p;

(ii) the analytic rank of $\mathrm{E}^{d_2}/\mathbb{Q}$ equals 1 and d_2 is a non-trivial quadratic residue modulo p.

Then the same result of Friedberg and Hoffstein also allows us to choose two negative integers d_3, d_4 such that

(i) $d_3 \equiv d_4 \equiv d$ modulo p;

(ii) the primes dividing the conductor of $\mathrm{E}^{d_1}/\mathbb{Q}$, $\mathrm{E}^{d_2}/\mathbb{Q}$ split in $\mathbb{Q}_p[\sqrt{d_3}]/\mathbb{Q}$, $\mathbb{Q}_p[\sqrt{d_4}]/\mathbb{Q}$, respectively;

(iii) the analytic rank of $\mathrm{E}^{d_3}/\mathbb{Q}$ equals 1, while that of $\mathrm{E}^{d_4}/\mathbb{Q}$ is trivial.

We will now consider two imaginary quadratic fields $K = \mathbb{Q}(\sqrt{d_3})$ and $K' = \mathbb{Q}(\sqrt{d_4})$. Observe that the completions of K and K' at the prime above p equal L. Moreover,

- if $\mathrm{L}/\mathbb{Q}_p$ is inert, then $\wp$ is principal, and hence it splits completely in $K[1]/K$ and $K'[1]/K'$, respectively,
- if $\mathrm{L}/\mathbb{Q}_p$ is ramified, then $\wp^2$ is principal which implies that $\wp$ splits completely in the p-part of $K[1]/K$ and $K'[1]/K'$, respectively.

This implies that the prime of K and K', respectively, above p splits completely in K_{k_0} and $K'_{k'_0}$, respectively, where $k'_0 = \max\{n \in \mathbb{N} \mid K'_n \subseteq K'[1]\}$.

We will now consider the elliptic curves $\mathrm{E}^{d_1}/\mathbb{Q}$ and $\mathrm{E}^{d_2}/\mathbb{Q}$. Since d_1, d_2 are non-trivial quadratic residues modulo p, we have

$$\mathrm{E}/\mathbb{Q}_p = \mathrm{E}^{d_1}/\mathbb{Q}_p = \mathrm{E}^{d_2}/\mathbb{Q}_p.$$

Then, by the uniqueness of the anticyclotomic $\mathbb{Z}_p$ extension of L which follows from class field theory, we have the following two restriction maps:

$$\mathrm{res}_{\wp_n}\colon \mathrm{E}^{d_1}(K_{n+k_0}) \to \mathrm{E}(\mathrm{L}_n) \quad \text{and} \quad \mathrm{res}_{\wp_n}\colon \mathrm{E}^{d_2}(K'_{n+k'_0}) \to \mathrm{E}(\mathrm{L}_n),$$

where $\wp_n$ denotes the prime of L_n above p, and for simplicity, it also denotes the corresponding prime of K_{n+k_0} and $K'_{n+k'_0}$, respectively, above p. The Heegner points $\alpha_n \in \mathrm{E}^{d_1}(K_n)$ and $\alpha'_n \in \mathrm{E}^{d_2}(K'_n)$ give rise to the local points

$$\beta_n = t\,\mathrm{res}_{\wp_n}(\alpha_{n+k_0}) \quad \text{and} \quad \beta'_n = t'\,\mathrm{res}_{\wp_n}\alpha'_{n+k'_0} \in \mathrm{E}(\mathrm{L}_n),$$

where $t = \#\mathrm{E}^{d_1}(\mathbb{Q})_{\mathrm{tors}}$ and $t' = \#\mathrm{E}^{d_2}(\mathbb{Q})_{\mathrm{tors}}$. Consequently, the Heegner point relations (2.1) imply that

$$\mathrm{tr}_{\mathrm{L}_{n+2}/\mathrm{L}_n}\beta_{n+2} = -\beta_n \quad \text{for } n > 0, \tag{2.4}$$

$$\mathrm{tr}_{\mathrm{L}_2/\mathrm{L}_1}\beta_2 = \begin{cases} 0 & \text{if } p \text{ is inert in } \mathrm{L}/\mathbb{Q}, \\ -\beta_0 = -p^{k_0} t\,\mathrm{res}_{\wp}(\alpha_0) & \text{if } p \text{ ramifies in } \mathrm{L}/\mathbb{Q}, \end{cases}$$

$$\mathrm{tr}_{\mathrm{L}_1/\mathrm{L}}\beta_1 = \begin{cases} -(p+1)\beta_0 = -(p+1)p^{k_0} t\,\mathrm{res}_{\wp}(\alpha_0) & \text{if } p \text{ is inert in } \mathrm{L}/\mathbb{Q}, \\ -\beta_0 = -p^{k_0} t\,\mathrm{res}_{\wp}(\alpha_0) & \text{if } p \text{ ramifies in } \mathrm{L}/\mathbb{Q}, \end{cases}$$

and similarly for $\beta'_n \in \mathrm{E}(\mathrm{L}_n)$.

Observe that, since the analytic ranks of E^{d_1}/K and E^{d_2}/K are equal to 1, the points $\alpha_0 \in \mathrm{E}^{d_1}(K)$ and $\alpha_0' \in \mathrm{E}^{d_2}(K)$ are non-torsion points, and hence $\beta_0, \beta_0' \in \mathrm{E}(\mathrm{L}) \setminus \mathrm{E}(\mathrm{L})_{\mathrm{tors}}$. In addition, since the analytic rank of $\mathrm{E}^{d_1}/\mathbb{Q}$ equals 0, while the analytic rank of $\mathrm{E}^{d_2}/\mathbb{Q}$ is equal to 1, in view of the action of complex conjugation on Heegner points (2.2), it follows that $\tau(t\alpha_0) = -t\alpha_0$, while $t\alpha_0' \in \mathrm{E}^{d_2}(\mathbb{Q})$, and hence

$$\tau\beta_0 = -\beta_0 \quad \text{and} \quad \beta_0' \in \mathrm{E}(\mathbb{Q}_p). \tag{2.5}$$

By (2.4) above, we see that $\beta_{2m}, \beta_{2m}' \in \mathrm{E}^+(\mathrm{L}_{2m})$ and $\beta_{2m+1}, \beta_{2m+1}' \in \mathrm{E}^-(\mathrm{L}_{2m+1})$. We will now use these points in our analysis of $\mathrm{E}^{\pm}(\mathrm{L}_n)$. Observe that

$$\mathrm{E}^+(\mathrm{L}_{2m+1}) \subseteq \mathrm{E}^+(\mathrm{L}_{2m}) \quad \text{and} \quad \mathrm{E}^-(\mathrm{L}_{2m}) \subseteq \mathrm{E}^-(\mathrm{L}_{2m-1}).$$

Moreover, since $\mathrm{E}(\mathrm{L}_n)/(\mathrm{E}^+(\mathrm{L}_n) + \mathrm{E}^-(\mathrm{L}_n))$ is annihilated simultaneously by

$$\prod_{0<2m\leq n} \mathrm{tr}_{\mathrm{L}_{2m}/\mathrm{L}_{2m-1}} \quad \text{and} \quad \prod_{0<2m+1\leq n} \mathrm{tr}_{\mathrm{L}_{2m+1}/\mathrm{L}_{2m}},$$

it follows that

$$p^n\mathrm{E}(\mathrm{L}_n) \subseteq \mathrm{E}^+(\mathrm{L}_n) + \mathrm{E}^-(\mathrm{L}_n). \tag{2.6}$$

Finally, since the $\mathbb{Z}_p$-rank of $\mathrm{E}(\mathrm{L}_n)$ equals that of $\mathcal{O}_n$, the ring of integers of L_n, we deduce that

$$\begin{aligned}
\mathrm{rank}_{\mathbb{Z}_p}\mathrm{E}^+(\mathrm{L}_n) &= \mathrm{rank}_{\mathbb{Z}_p}\mathcal{O}_{\mathrm{L}} + \sum_{0<2m\leq n}(\mathrm{rank}_{\mathbb{Z}_p}\mathcal{O}_{2m} - \mathrm{rank}_{\mathbb{Z}_p}\mathcal{O}_{2m-1}),\\
\mathrm{rank}_{\mathbb{Z}_p}\mathrm{E}^-(\mathrm{L}_n) &= \mathrm{rank}_{\mathbb{Z}_p}\mathcal{O}_{\mathrm{L}} + \sum_{0<2m+1\leq n}(\mathrm{rank}_{\mathbb{Z}_p}\mathcal{O}_{2m+1} - \mathrm{rank}_{\mathbb{Z}_p}\mathcal{O}_{2m}).
\end{aligned}$$

Consider the following submodule of $\mathrm{E}^-(\mathrm{L}_{2m+1})$:

$$\mathcal{R}_{2m+1}\beta_{2m+1} + \mathcal{R}_{2m+1}\beta_{2m+1}' \subseteq \mathrm{E}^-(\mathrm{L}_{2m+1}),$$

and the surjective maps $\mathrm{R}_{2m+1}^2 \to \mathrm{R}_{2m+1}\beta_{2m+1} + \mathrm{R}_{2m+1}\beta_{2m+1}'$. It follows that

$$\widehat{\varinjlim_m(\mathrm{R}_{2m+1}\beta_{2m+1} + \mathrm{R}_{2m+1}\beta_{2m+1}')} \hookrightarrow \Lambda^2,$$

where $\widehat{M} := \mathrm{Hom}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ for any Λ-module M. Observe that, by (2.4) and (2.5), we see that

$$\begin{aligned}
\big(\varinjlim_m(\mathrm{R}_{2m+1}\beta_{2m+1} + \mathrm{R}_{2m+1}\beta_{2m+1}')\big)^{\mathrm{Gal}(\mathrm{L}_\infty/\mathrm{L})} &= (\mathbb{Q}_p/\mathbb{Z}_p)\beta_0 + (\mathbb{Q}_p/\mathbb{Z}_p)\beta_0'\\
&\simeq (\mathbb{Q}_p/\mathbb{Z}_p)^2,
\end{aligned}$$

which implies that

$$\widehat{\varinjlim_m(\mathrm{R}_{2m+1}\beta_{2m+1} + \mathrm{R}_{2m+1}\beta_{2m+1}')} \simeq \Lambda^2.$$

Since

$$\widehat{\varinjlim_m \mathrm{R}_{2m+1}\beta_{2m+1}} \simeq \widehat{\varinjlim_m \mathrm{R}_{2m+1}\beta_{2m+1}'} \simeq \Lambda,$$

it follows that there exists $f \in \Lambda$ such that $f(\mathcal{R}_{2m+1}\beta_{2m+1} \cap \mathcal{R}_{2m+1}\beta'_{2m+1}) = 0$ for all $m \in \mathbb{N}$. Since we also know that

$$(g-1)\prod_{0<r\leq m} \mathrm{tr}_{\mathrm{L}_{2r+1}/\mathrm{L}_{2r}} \in \Lambda$$

is a minimal annihilator of the Λ-modules $\mathcal{R}_{2m+1}\beta_{2m+1}$ and $\mathcal{R}_{2m+1}\beta'_{2m+1}$, it follows that the difference between the $\mathbb{Z}_p$-rank of $\mathrm{E}^-(\mathrm{L}_{2m+1})$ and the $\mathbb{Z}_p$-rank of its submodule

$$\mathcal{R}_{2m+1}\beta_{2m+1} + \mathcal{R}_{2m+1}\beta'_{2m+1}$$

is bounded independently of m. It then follows that

$$\mathrm{corank}_\Lambda \varinjlim_m (\mathrm{R}_{2m+1}\beta_{2m+1} + \mathrm{R}_{2m+1}\beta'_{2m+1}) = \mathrm{corank}_\Lambda \varinjlim_n \mathrm{E}^-(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 2.$$

If p ramifies in $\mathrm{L}/\mathbb{Q}$, then by (2.4) and (2.5), we also have that

$$\begin{aligned} \Big(\varinjlim_m (\mathrm{R}_{2m}\beta_{2m} + \mathrm{R}_{2m}\beta'_{2m})\Big)^{\mathrm{Gal}(\mathrm{L}_\infty/\mathrm{L})} &= (\mathbb{Q}_p/\mathbb{Z}_p)\beta_0 + (\mathbb{Q}_p/\mathbb{Z}_p)\beta'_0 \\ &\simeq (\mathbb{Q}_p/\mathbb{Z}_p)^2, \end{aligned} \tag{2.7}$$

and as above, we deduce that

$$\mathrm{corank}_\Lambda \varinjlim_m (\mathrm{R}_{2m}\beta_{2m} + \mathrm{R}_{2m}\beta'_{2m}) = \mathrm{corank}_\Lambda \varinjlim_n \mathrm{E}^+(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 2.$$

Observe that if p is inert in $\mathrm{L}/\mathbb{Q}$, then relations (2.4) do not imply (2.7). However, in this case, by Proposition 2.1, we know that

$$\mathrm{corank}_\Lambda \varinjlim_n \mathrm{E}^+(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \leq 2.$$

We now view $\varinjlim_n \mathrm{E}^\pm(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ as submodules of $\mathrm{H}^1(\mathrm{L}_\infty, \mathrm{E}_{p^\infty})$. Notice that (2.6) implies that

$$\big(\mathrm{E}^+(\mathrm{L}_n) + \mathrm{E}^-(\mathrm{L}_n)\big) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \mathrm{E}(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p.$$

Since $\mathrm{L}_\infty/\mathrm{L}$ is ramified, we have

$$\varinjlim_n \mathrm{E}(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \mathrm{H}^1(\mathrm{L}_\infty, \mathrm{E}_{p^\infty}).$$

Then, since $\mathrm{E}_p(\mathrm{L}_\infty)$ is bounded by the Corank Lemma [10, Chapter 2], we know that

$$\mathrm{corank}_{\mathbb{Z}_p} \mathrm{H}^1(\mathrm{L}_n, E_{p^\infty}) - 2[\mathrm{L}_n : \mathbb{Q}_p]$$

is bounded independently of n, and hence $\mathrm{corank}_\Lambda \mathrm{H}^1(\mathrm{L}_\infty, E_{p^\infty}) = 4$. Consequently, we have

$$\mathrm{corank}_\Lambda \Big(\varinjlim_n \mathrm{E}^+(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p + \varinjlim_n \mathrm{E}^-(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p\Big) = 4. \tag{2.8}$$

Finally, since we have shown that

$$\mathrm{corank}_\Lambda \varinjlim_n \mathrm{E}^\pm(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \leq 2,$$

it follows that

$$\mathrm{corank}_\Lambda \Big(\varinjlim_n \mathrm{E}^+(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cap \varinjlim_n \mathrm{E}^-(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p\Big) = 0. \qquad \square$$

Corollary 2.3. *The Λ-corank of $\varinjlim_n \mathrm{E}^{\pm}(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ equals 2.*

Proof. Observe that, by the proof of the above theorem, we know that

$$\mathrm{corank}_\Lambda \varinjlim_n \mathrm{E}^{-}(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 2.$$

This together with (2.8) and the above theorem imply that

$$\mathrm{corank}_\Lambda \varinjlim_n \mathrm{E}^{+}(\mathrm{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 2. \qquad \square$$

3. Complex multiplication points

Let F be a real quadratic extension of $\mathbb{Q}$, $\wp$ the unique[3)] prime of F above p, K/F a totally imaginary quadratic extension such that

(i) the prime $\wp$ of F above p splits in K,

(ii) the discriminant of K/F is coprime to $\mathrm{N}_{\mathrm{E/F}}$, the conductor of E over F, and

(iii) the number of prime divisors of the squarefree part of the ideal $\mathrm{N}_{\mathrm{E/F}}$ that are inert in K/F is odd.

Since E is defined over $\mathbb{Q}$ and hence modular by [2, 21], condition (iii) together with the fact that F/$\mathbb{Q}$ is cyclic imply that there exists a Shimura curve X that parametrizes the elliptic curve E over F; see [1]. By work of Shimura, we know that X is equipped with complex multiplication (CM) points which are defined over number fields. We then use the parametrization to view the CM points of X as points on E. For each ideal $\mathfrak{f}$ prime to the conductor $\mathrm{N}_{\mathrm{E/F}}$, we consider the CM point $y_\mathfrak{f} \in \mathrm{E}(\mathrm{K}[\mathfrak{f}])$, where $\mathrm{K}[\mathfrak{f}]/\mathrm{K}$ is the ring class field of conductor $\mathfrak{f}$ (see [19, Section 7.2]).

We now focus on the case when $\mathfrak{f} = \wp^n$, where $\wp$ is the prime of F above p and $n \in \mathbb{N}$. For every abelian group G, we set $\widehat{G} = G \otimes \prod_p \mathbb{Z}_p$. Let $\mathrm{K}[\wp^\infty] = \bigcup_n \mathrm{K}[\wp^n]$. The Galois group $\mathrm{Gal}(\mathrm{K}[\wp^n]/\mathrm{K}) \simeq \mathrm{K}^\times \setminus \widehat{\mathrm{K}}^\times/\mathrm{F}^\times\widehat{\mathcal{O}}_{\wp^n}^\times$, where $\mathcal{O}_\mathrm{F}$ and $\mathcal{O}_\mathrm{K}$ denote the ring of integers of F and K, respectively, and $\mathcal{O}_{\wp^n} = \mathcal{O}_\mathrm{F} + \wp^n\mathcal{O}_\mathrm{K}$. Hence, the Galois group of $\mathrm{K}[\wp^\infty]/\mathrm{K}$ contains a subgroup of finite index isomorphic to $\mathbb{Z}_p^{[\mathrm{F}_\wp:\mathbb{Q}_p]}$.

By [19, Proposition 7.5], we have

$$\mathrm{tr}_{\mathrm{K}[\wp^{n+1}]/\mathrm{K}[\wp^n]} y_{\wp^{n+1}} = \frac{u_{n+1}}{u_n} a_\wp y_{\wp^n} - y_{\wp^{n-1}}, \tag{3.1}$$

where u_n denotes the cardinality of $(\widehat{\mathcal{O}}_{\wp^n}^\times \cap \mathrm{K}^\times\widehat{\mathrm{F}}^\times)/\widehat{\mathcal{O}}_\mathrm{F}^\times$. Since $\mathcal{O}_{\wp^n} \subset \mathcal{O}_{\wp^{n+1}}$, it follows that $u_n \le u_{n+1}$. By [19, Lemma 7.3], we know that u_n divides $2[\mathcal{O}_\mathrm{K}^\times : \mathcal{O}_\mathrm{F}^\times]$, which immediately implies that $\frac{u_{n+1}}{u_n} = 1$ for almost all $n \in \mathbb{N}$. Moreover, if E has supersingular reduction at p and $p \ge 5$, we find that

$$a_\wp = \begin{cases} 0 & \text{if } p \text{ ramifies in } \mathrm{F}/\mathbb{Q}, \\ 2p & \text{if } p \text{ is inert in } \mathrm{F}/\mathbb{Q}. \end{cases} \tag{3.2}$$

[3)] The case where p splits in F/$\mathbb{Q}$ is treated in earlier work; see [5].

Let $\mathrm{K}_\infty \subseteq \mathrm{K}[\wp^\infty]$ be a $\mathbb{Z}_p$-extension of K and let K_n be the subextension of K_∞ of degree p^n over K. Denote by $\wp^{k(n)}$ the minimal power of $\wp$ such that $\mathrm{K}_n \subseteq \mathrm{K}[\wp^{k(n)}]$. Observe that, for n sufficiently large, we have

$$k(n+1) = \begin{cases} k(n)+2 & \text{if } p \text{ ramifies in } \mathrm{F}/\mathbb{Q}, \\ k(n)+1 & \text{if } p \text{ is inert in } \mathrm{F}/\mathbb{Q}. \end{cases}$$

We now define

$$z_n = \mathrm{tr}_{\mathrm{K}[\wp^{k(n)}]/\mathrm{K}_n} y_{\wp^{k(n)}} \in \mathrm{E}(\mathrm{K}_n).$$

By (3.1) and (3.2), we find that there exists $c \in \mathbb{N}$ such that, for $n \geq c$, we have

$$\mathrm{tr}_{\mathrm{K}_{n+1}/\mathrm{K}_n} z_{n+1} = \begin{cases} -p z_n & \text{if } p \text{ ramifies in } \mathrm{F}/\mathbb{Q}, \\ 2p z_n - p z_{n-1} & \text{if } p \text{ is inert in } \mathrm{F}/\mathbb{Q}. \end{cases} \tag{3.3}$$

Let $\mathcal{H}_{\mathrm{K}_\infty}$ denote the $\mathbb{Z}[\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K})]$-submodule of $\mathrm{E}(\mathrm{K}_\infty)$ generated by the CM points $\{z_n \in \mathrm{E}(\mathrm{K}_n) \mid n \in \mathbb{N},\ n \geq c\}$. By [8, Theorem 1.10] of Cornut and Vatsal, we know that there exists a $\mathbb{Z}_p$-extension of $\mathrm{K}_\infty \subseteq \mathrm{K}[\wp^\infty]$ such that the CM points $z_n \in \mathrm{E}(\mathrm{K}_n) \setminus \mathrm{E}(\mathrm{K}_{n-1})$, and in particular are non-trivial, for sufficiently large n.

Observe that relations (3.3) imply that if the prime p ramifies in $\mathrm{F}/\mathbb{Q}$, then

$$\mathrm{tr}_{\mathrm{K}_{n+1}/\mathrm{K}_n}(z_{n+1} + z_n) = 0 \quad \text{for all } n \geq c,$$

and when the prime p is inert in $\mathrm{F}/\mathbb{Q}$, we have

$$\mathrm{tr}_{\mathrm{K}_{n+1}/\mathrm{K}_n}(z_{n+1} - 2z_n + z_{n-1}) = 0 \quad \text{for all } n \geq c.$$

Theorem 3.1. *Let* $\mathrm{K}_\infty \subseteq \mathrm{K}[\wp^\infty]$ *be a* $\mathbb{Z}_p$*-extension of* K *such that the completion of* K_∞ *at a prime above* p *is the anticyclotomic* $\mathbb{Z}_p$*-extension of* $\mathrm{K}_\wp$*. If* $z_n \in \mathrm{E}(\mathrm{K}_n) \setminus \mathrm{E}(\mathrm{K}_{n-1})$ *for almost all* n*, then*

$$\mathrm{corank}_\Lambda\, \mathcal{H}_{\mathrm{K}_\infty} \otimes \mathbb{Q}_p/\mathbb{Z}_p \geq 2.$$

Proof. Consider the following $\mathbb{Z}[\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K})]$-submodules of $\mathrm{E}(\mathrm{K}_\infty)$:

$$\mathcal{H}^+_{\mathrm{K}_\infty} = \begin{cases} \langle \mathbb{Z}[\mathrm{Gal}(\mathrm{K}_n/\mathrm{K})](z_n + z_{n-1}) \mid n \in 2\mathbb{N},\ n \geq c \rangle & \text{if } p \text{ ramifies in } \mathrm{F}/\mathbb{Q}, \\ \langle \mathbb{Z}[\mathrm{Gal}(\mathrm{K}_n/\mathrm{K})](z_n - 2z_{n-1} + z_{n-2}) \mid n \in 2\mathbb{N},\ n \geq c \rangle & \text{if } p \text{ is inert in } \mathrm{F}/\mathbb{Q}; \end{cases}$$

$$\mathcal{H}^-_{\mathrm{K}_\infty} = \begin{cases} \langle \mathbb{Z}[\mathrm{Gal}(\mathrm{K}_n/\mathrm{K})](z_n + z_{n-1}) \mid n \in 2\mathbb{N}+1,\ n \geq c \rangle & \text{if } p \text{ ramifies in } \mathrm{F}/\mathbb{Q}, \\ \langle \mathbb{Z}[\mathrm{Gal}(\mathrm{K}_n/\mathrm{K})](z_n - 2z_{n-1} + z_{n-2}) \mid n \in 2\mathbb{N}+1,\ n \geq c \rangle & \text{if } p \text{ is inert in } \mathrm{F}/\mathbb{Q}. \end{cases}$$

Observe that $\mathrm{res}_\wp\, \mathcal{H}^\pm_{\mathrm{K}_\infty} \subseteq \varinjlim_n \mathrm{E}^\pm(\mathrm{L}_n)$, and hence Theorem 2.2 implies that

$$\mathrm{corank}_\Lambda(\mathrm{res}_\wp\, \mathcal{H}^+_{\mathrm{K}_\infty} \otimes \mathbb{Q}_p/\mathbb{Z}_p \cap \mathrm{res}_\wp\, \mathcal{H}^-_{\mathrm{K}_\infty} \otimes \mathbb{Q}_p/\mathbb{Z}_p) = 0. \tag{3.4}$$

Our assumption that $z_n \in \mathrm{E}(\mathrm{K}_n) \setminus \mathrm{E}(\mathrm{K}_{n-1})$ for almost all $n \in \mathbb{N}$ implies that

$$z_n + z_{n-1}, z_n - 2z_{n-1} + z_{n-2} \in \mathrm{E}(\mathrm{K}_n) \setminus \mathrm{E}(\mathrm{K}_{n-1}) \quad \text{for almost all } n \in \mathbb{N}.$$

It then follows that

$$\mathrm{corank}_\Lambda\, \mathcal{H}^\pm_{\mathrm{K}_\infty} \otimes \mathbb{Q}_p/\mathbb{Z}_p \geq 1.$$

Then, by (3.4), we deduce that the Λ-corank of $\mathcal{H}_{\mathrm{K}_\infty} \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is at least 2. □

Remark 3.2. Note that, by Corollary 2.3, we know that $\mathrm{corank}_\Lambda\, \mathcal{H}^\pm_{\mathrm{K}_\infty} \otimes \mathbb{Q}_p/\mathbb{Z}_p \leq 2$, and by ongoing joint work extending [6], we expect/hope that equality holds.

Acknowledgement. The author would like to thank Jennifer Balakrishnan, Brian Conrad, and Dorian Goldfeld for useful discussions.

References

[1] *J. Arthur* and *L. Clozel*, Simple algebras, base change, and the advanced theory of the trace formula, Ann. of Math. Stud. **120**, Princeton University, Princeton 1989.
[2] *C. Breuil*, *B. Conrad*, *F. Diamond* and *R. Taylor*, On the modularity of elliptic curves over **Q**: Wild 3-adic exercises, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.
[3] *A. Burungale*, *S. Kobayashi* and *K. Ota*, Rubin's conjecture on local units in the anticyclotomic tower at inert primes, Ann. of Math. (2) **194** (2021), no. 3, 943–966.
[4] *A. Burungale*, *S. Kobayashi* and *K. Ota*, p-adic L-functions and rational points on CM elliptic curves at inert primes, preprint; to appear in J. Inst. Math. Jussieu.
[5] *M. Çiperiani*, Tate–Shafarevich groups in anticyclotomic $\mathbb{Z}_p$-extensions at supersingular primes, Compos. Math. **145** (2009), no. 2, 293–308.
[6] *M. Çiperiani* and *A. Wiles*, Solvable points on genus one curves, Duke Math. J. **142** (2008), no. 3, 381–464.
[7] *C. Cornut*, Mazur's conjecture on higher Heegner points, Invent. Math. **148** (2002), no. 3, 495–523.
[8] *C. Cornut* and *V. Vatsal*, Nontriviality of Rankin-Selberg L-functions and CM points, in: L-functions and Galois representations, London Math. Soc. Lecture Note Ser. **320**, Cambridge University, Cambridge (2007), 121–186.
[9] *S. Friedberg* and *J. Hoffstein*, Nonvanishing theorems for automorphic L-functions on GL(2), Ann. of Math. (2) **142** (1995), no. 2, 385–423.
[10] *R. Greenberg*, Introduction to Iwasawa theory for elliptic curves, in: Arithmetic algebraic geometry (Park City 1999), IAS/Park City Math. Ser. **9**, American Mathematical Society, Providence (2001), 407–464.
[11] *B. H. Gross*, Kolyvagin's work on modular elliptic curves, in: L-functions and arithmetic (Durham 1989), London Math. Soc. Lecture Note Ser. **153**, Cambridge University, Cambridge (1991), 235–256.
[12] *A. Iovita* and *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] *S. Kobayashi*, Iwasawa theory for elliptic curves at supersingular primes, Invent. Math. **152** (2003), no. 1, 1–36.
[14] *G. T. Konovalov*, The universal G-norms of formal groups over a local field, Ukrainian Math. J. **28** (1976), no. 3, 310–311.
[15] *B. Perrin-Riou*, Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner, Bull. Soc. Math. France **115** (1987), no. 4, 399–456.
[16] *K. Rubin*, Elliptic curves and $\mathbf{Z}_p$-extensions, Compos. Math. **56** (1985), no. 2, 237–250.
[17] *K. Rubin*, Local units, elliptic units, Heegner points and elliptic curves, Invent. Math. **88** (1987), no. 2, 405–422.
[18] *J.-P. Serre*, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972), no. 4, 259–331.
[19] *Y. Tian*, Euler systems of CM points on Shimura curves, Ph.D. Thesis, Columbia University, 2003.
[20] *V. Vatsal*, Special values of anticyclotomic L-functions, Duke Math. J. **116** (2003), no. 2, 219–261.
[21] *A. Wiles*, Modular elliptic curves and Fermat's last theorem, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

Mirela Çiperiani, Department of Mathematics, The University of Texas at Austin, Austin, TX 78712, USA
e-mail: mirela@math.utexas.edu

Eingegangen 30. Januar 2021, in revidierter Fassung 8. April 2023