This is a ``preproof'' accepted article for *Canadian Mathematical Bulletin*
This version may be subject to change during the production process.
DOI: 10.4153/S0008439525101446

Canad. Math. Bull. Vol. **00** (0), 2025 pp. 1–15
http://dx.doi.org/10.4153/xxxx

An asymptotic formula for Tate-Shafarevich groups of CM elliptic curves at supersingular primes

Katharina Müller

et K be an imaginary quadratic field and $E/\mathbb{Q}$ an elliptic curve with complex multiplication by $\mathcal{O}_K$. Let K_∞/K be the anticyclotomic $\mathbb{Z}_p$-extension of K and K_n the intermediate layers. Under additional assumptions on Kobayashi's signed Selmer groups we prove an asymptotic formula for $Ш(E/K_n)$.

1 Introduction

Throughout this article $p \geq 5$ is a prime. Let k be a number field and k_∞/k be a $\mathbb{Z}_p$-extension. Let k_n be the unique subextension of degree p^n and h_n the p-class number of k_n. Iwasawa proved in his seminal paper [6] the asymptotic formula

$$v_p(h_n) = \mu p^n + \lambda n + \nu \quad n \gg 0,$$

for invariants $\mu, \lambda \geq 0$ and $\nu \in \mathbb{Z}$.

In light of this key result the analysis of arithmetic objects along $\mathbb{Z}_p$-extensions has become a central topic in modern Iwasawa theory. Mazur [10] generalized Iwasawa's ideas and applied them to elliptic curves with good ordinary reduction at all primes above p. He showed that – if the p-primary Selmer group over k_∞ is cotorsion over the Iwasawa algebra of $\mathrm{Gal}(k_\infty/k)$– there is an asymptotic formula

$$v_p(|Ш(E/k_n)|) = \mu p^n + \lambda n + \nu \quad n \gg 0,$$

where $Ш(E/k_n)$ is the Tate-Shafarevich group of E over k_n (assuming that it is finite) . A crucial step in his argument is a so called control theorem. For supersingular primes this control theorem is no longer valid. Let $E/\mathbb{Q}$ be an elliptic curve supersingular at p and let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. As $p \geq 5$, this implies that $a_p = 0$ by the Hasse bound [11, Chapter V, Theorem 1.1]. Kobayashi [7] constructed plus/minus Selmer groups that satisfy a control theorem. From his control theorem he was able

2020 Mathematics Subject Classification: 11R23, 11G05, 11G15.
Keywords: Iwasawa theory, Tate-Shafarevich groups, plus/minus Selmer groups.

to derive the following asymptotic formula

$$v_p(|\text{Ш}(E/\mathbb{Q}_n)|) = \sum_{k=0}^{\lfloor \frac{n-2}{2} \rfloor} p^{n-1-2k} - \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor \lambda^+ + \left\lfloor \frac{n+1}{2} \right\rfloor \lambda^- \\ -nr + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \phi(p^{2k})\mu^+ + \sum_{k=1}^{\lfloor \frac{n+1}{2} \rfloor} \phi(p^{2k-1})\mu^- + \nu, \quad n \gg 0$$

where $r = \text{rank}(E(\mathbb{Q}_\infty)) < \infty$ and ϕ denotes the Euler ϕ-function. The invariants $\mu^\pm$ and $\lambda^\pm$ are the Iwasawa invariants of the Pontryagin duals of the plus/minus Selmer groups.

Instead of the cyclotomic $\mathbb{Z}_p$-extension we consider the anticyclotomic $\mathbb{Z}_p$-extension for the rest of the paper. We keep the assumption that $E/\mathbb{Q}$ is an elliptic curve and that p is a supersingular prime. Let K be an imaginary quadratic field. Let K_∞/K be the anticyclotomic $\mathbb{Z}_p$-extension, i.e. the $\mathbb{Z}_p$-extension on which $\text{Gal}(K/\mathbb{Q})$ acts as -1, and let K_n be the unique subextension of degree p^n. Assume that K satisfies the generalized Heegner hypothesis: Let $N = N_1N_2$ be the conductor of E, where N_1 and N_2 are coprime and N_2 is square-free. Assume that all primes dividing pN_1 are split in K and that all primes dividing N_2 are inert in K. In particular, we assume that p splits in K. In this setting the rank of $E(K_n)$ is unbounded and the plus/minus Selmer groups are no longer cotorsion. Nevertheless there is– under the assumption that $\text{Ш}(E/K_n)$ is finite and that the representation

$$\rho\colon G_\mathbb{Q} \longrightarrow \text{Aut}(T_p(E))$$

is surjective– an asymptotic formula [8]:

$$v_p(|\text{Ш}(E/K_n)|) = \sum_{k \le n, k \text{ even}} \mu^+\phi(p^k) + \sum_{k\le n, k \text{ odd}} \mu^-\phi(p^k) \\ + \lfloor \frac{n}{2} \rfloor \lambda^+ + \lfloor \frac{n+1}{2} \rfloor \lambda^- + \nu \quad n \gg 0.$$

These Iwasawa invariants are no longer the ones of the plus/minus Selmer groups.

The Heegner hypothesis excludes the case of CM elliptic curves with complex multiplication by $\mathcal{O}_K$ as primes of good supersingular reduction are inert in K. The aim of the present paper is to consider this case. Let $\varepsilon \in \{\pm 1\}$ be the root number of $E/\mathbb{Q}$. Then the $-\varepsilon$-Selmer group is cotorsion while the ε-Selmer group is not. Burungale, Kobayashi and Ota [3, Theorem 1.1] prove that for all n large enough such that $(-1)^n = -\varepsilon$ one has

$$v_p(|\text{Ш}(E/K_n)|) - v_p(|\text{Ш}(E/K_{n-1})|) = \lambda + \mu\phi(p^n) \tag{1.1}$$

for some invariants $\mu, \lambda \geq 0$.

The invariants occuring in the asymptotic formula of Burungale-Kobayashi-Ota come from the fine Selmer groups, the $-\varepsilon$ Selmer group, and a finitely generated $\mathbb{Z}_p$-module A independent of n.

https://doi.org/10.4153/S0008439525101446 Published online by Cambridge University Press

Let Λ be the Iwasawa algebra of $\Gamma = \mathrm{Gal}(K_\infty/K)$ over the ring $\mathcal{O}$, the ring of integers of K_p, where K_p denotes the completion of K at p. Define

$$\omega_n^+(T) = \prod_{1\le k\le n, k \text{ even}} \Phi_k(T+1) \quad \omega_n^- = T \prod_{1\le k\le n, k \text{ odd}} \Phi_k(T+1),$$

where Φ_k denotes the p^k-th cyclotomic polynomial. Our main result covers the remaining steps:

Theorem 1 Assume that $Ш(E/K_n)$ and the fine Selmer group $\mathrm{Sel}^0(E/K_n)[\omega_n^{-\varepsilon}]$ are finite for all n. Then for all n large enough and such that $(-1)^n = \varepsilon$ one has

$$v_p(|Ш(E/K_n)|) - v_p(|Ш(E/K_{n-1})|) = \lambda + \mu\phi(p^n).$$

The integers μ and λ are the Iwasawa invariants of the fine Tate-Shafarevich groups.

As an immediate corollary we obtain

Theorem 2 Assume that $Ш(E/K_n)$ and $\mathrm{Sel}^0(E/K_n)[\omega_n^{-\varepsilon}]$ are finite for all n. Then for all n large enough one has

$$v_p(|Ш(E/K_n)|) = \begin{cases} \mu^{-\varepsilon}\sum_{m\le n,(-1)^m=-\varepsilon}\phi(p^m) + \mu^{\varepsilon}\sum_{m\le n,(-1)^m=\varepsilon}\phi(p^m) \\ \quad + \lambda^{\varepsilon}\lfloor \frac{n}{2}\rfloor + \lambda^{-\varepsilon}\lfloor\frac{n+1}{2}\rfloor + \nu & (-1)^n = -\varepsilon \\ \\ \mu^{-\varepsilon}\sum_{m\le n,(-1)^m=-\varepsilon}\phi(p^m) + \mu^{\varepsilon}\sum_{m\le n,(-1)^m=\varepsilon}\phi(p^m) \\ \quad + \lambda^{\varepsilon}\lfloor \frac{n+1}{2}\rfloor + \lambda^{-\varepsilon}\lfloor\frac{n}{2}\rfloor + \nu & (-1)^n = \varepsilon \end{cases}$$

The invariants are the ones from (1.1) and Theorem 1 respectively. Note that one expects $\mu^{\pm} = 0$ in this setting.

Remark 1.1 The condition that $\mathrm{Sel}^0(E/K_n)[\omega_n^{-\varepsilon}]$ is finite is equivalent to the statement that the characteristic ideal of $\mathrm{Sel}^0(E/K_\infty)^\vee$ is corpime to $\omega_n^{-\varepsilon}$.

If one assumes that $Ш(E/K_n)$ is finite, this is equivalent to

$$f_n = \frac{\mathrm{rank}(E(K_n)) - \mathrm{rank}(E(K_{n-1}))}{2\phi(p^n)} \le 1,$$

for all n such that $(-1)^n = -\varepsilon$. It is known that $f_n = 0$ for all such n large enough [5].

The central idea of the proof is to decompose $Ш(E/K_n)$ into plus and minus Tate-Shafarevich groups whose intersection is the fine Tate-Shafarevich group. Using control theorems for the respective Selmer groups we will then derive the above asymptotic formula. This approach differs from the one presented in [2]. In *loc. cit* the authors relate the growth of $Ш(E/K_n)$ to the cokernel of

$$\mathrm{Sel}(E/K_{n-1}) \to \mathrm{Sel}(E/K_n).$$

If $(-1)^n = -\varepsilon$ this cokernel is finite and compuatatable in terms of Iwasawa invariants. In the case $(-1)^n = \varepsilon$, this cokernel is of corank $\phi(p^n)$ for all n. We have thus to apply different methods and need the additional assumption that $\mathrm{Sel}^0(E/K_n)[\omega_n^{-\varepsilon}]$ is finite for all n.

The fine Tate-Shafarevich groups do not only play a central role in our proofs, but are also of independent interest and we are able to derive an asymptotic formula for them.

Theorem 3 Let $\kappa^0(E/K_n)$ be the fine Tate-Shafarevich group of E over K_n. For all $n \gg 0$ we have

$$\nu_p(|\kappa^0(E/K_n)|) = \lambda n + p^n \mu + \nu,$$

for $\mu, \lambda \geq 0$ and $\nu \in \mathbb{Z}$.

Note that Theorem 3 is a generalization of the results in [9]. *Loc. cit.* only conciders the cases of good ordinary reduction (Theorem 1.7) and of $E(K_\infty)$ being of finite rank (Theorem 1.6). Both conditions are not satisfied for supersingular elliptic curves and the anticyclotomic $\mathbb{Z}_p$-extension.

Acknowledgments

The author would like to thank Ben Forrás, Antonio Lei, Meng Fai Lim and Andreas Nickel for helpful comments on an earlier draft of this article. The author would furthermore like to thank the anonymous referee for their helpful suggestions.

2 plus/minus Selmer groups

Let K be an imaginary quadratic field and let p be prime that is inert in K. Let $E/\mathbb{Q}$ be an elliptic curve that has complex multiplication by $\mathcal{O}_K$. Let K_∞/K be the anticyclotomic $\mathbb{Z}_p$-extension and let K_n be the intermediate fields. Let ε be the root number of E. Let τ be a topological generator of $\mathrm{Gal}(K_\infty/K)$, let $T = \tau - 1$ and $\Lambda = \mathcal{O}[\![T]\!]$. Throughout the paper we assume that $\text{Ш}(E/K_n)$ is finite for all n.

Let Ξ denote the set of Dirichlet characters of $\mathrm{Gal}(K_\infty/K)$. Let Ξ^+ be the subset of non-trivial characters whose order is an even power of p and let Ξ^- be the set of characters whose order is an odd power of p and the trivial character. Let $K_{n,p}$ be the localization of K_n at the unique prime above p in K_n. We denote by $\widehat{E}$ the formal group of E at p and by log its formal logarithm. For any character $\chi \in \Xi$ and any $x \in \widehat{E}(K_{n,p})$ we define

$$\lambda_\chi(x) = p^{-m} \sum_{\sigma \in \mathrm{Gal}(K_{m,p}/K_p)} \log(x^\sigma)\chi^{-1}(\sigma),$$

where χ is a character factoring through $\mathrm{Gal}(K_{m,p}/K)$ and $m \geq n$. Let

$$\widehat{E}(K_{n,p})^\pm = \{x \in \widehat{E}(K_{n,p}) \mid \lambda_\chi(x) = 0 \quad \forall \chi \in \Xi^\mp\}.$$

Let Σ the set of primes dividing the conductor of E and p. Let K_Σ be the maximal Galois extension of K unramified outside Σ.

https://doi.org/10.4153/S0008439525101446 Published online by Cambridge University Press

***Definition* 2.1** We define

$$\mathrm{Sel}(E/K_n)$$
$$= \ker\left(H^1(K_\Sigma/K_n, E[p^\infty]) \to \prod_{v\in\Sigma,(v,p)=1} H^1(K_{n,v}, E[p^\infty]) \times \frac{H^1(K_{n,p}, E[p^\infty])}{\widehat{E}(K_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)$$

We define the plus/minus Selmer groups

$$\mathrm{Sel}^\pm(E/K_n)$$
$$= \ker\left(H^1(K_\Sigma/K_n, E[p^\infty]) \to \prod_{v\in\Sigma,(v,p)=1} H^1(K_{n,v}, E[p^\infty]) \times \frac{H^1(K_{n,p}, E[p^\infty])}{\widehat{E}^\pm(K_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)$$

as well as the fine Selmer group

$$\mathrm{Sel}^0(E/K_n) = \ker\left(H^1(K_\Sigma/K_n, E[p^\infty]) \to \prod_{v\in\Sigma} H^1(K_{n,v}, E[p^\infty])\right).$$

For $* \in \{0, +, -\}$ we define

$$\mathcal{M}^*(E/K_n) = \mathrm{Sel}^*(E/K_n) \cap (E(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p).$$

The intersection is taken in $H^1(K_\Sigma/K_n, E[p^\infty])$ and $E(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is a subgroup after applying the Kummer map. We furthemore define

$$\kappa^*(E/K_n) = \frac{\mathrm{Sel}^*(E/K_n)}{\mathcal{M}^*(E/K_n)}.$$

Let $\mathrm{Sel}^*(E/K_\infty) = \varinjlim_n \mathrm{Sel}^*(E/K_n)$.

***Remark* 2.1** By [3, Lemma 2.2] $H^1(K_{n,v}, E[p^\infty]) = 0$ for all v coprime to p. Thus, one can omit the conditions at primes away from p in the definition of Selmer groups.

In the following we will analyze the ε-Selmer groups.

***Lemma* 2.2** $\left(\frac{\mathrm{Sel}^\varepsilon(E/K_\infty)}{\mathrm{Sel}^0(E/K_\infty)}\right)$ *has Λ-corank one.*

Proof By [3, Proposition 3.4] $\mathrm{Sel}^0(E/K_\infty)$ is Λ-cotorsion. By [1, Theorem 3.6] $\mathrm{Sel}^\varepsilon(E/K_\infty)$ has Λ-corank one. Both results together imply the desired result. ■

***Lemma* 2.3** $\left(\frac{\mathrm{Sel}^\varepsilon(E/K_\infty)}{\mathrm{Sel}^0(E/K_\infty)}\right)^\vee \cong \Lambda.$

Proof By [3, Theorem 3.2 and Lemma 3.3] we have

$$(\widehat{E}^\pm(K_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee \cong \omega_n^\mp \Lambda_n,$$

where $\Lambda_n = \mathcal{O}[\mathrm{Gal}(K_n/K)]$. Taking the projective limit, we obtain

$$(\widehat{E}^\pm(K_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee \cong \Lambda.$$

https://doi.org/10.4153/S0008439525101446 Published online by Cambridge University Press

By definition

$$\left(\frac{\mathrm{Sel}^{\varepsilon}(E/K_\infty)}{\mathrm{Sel}^0(E/K_\infty)}\right) \hookrightarrow \widehat{E}^{\varepsilon}(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p.$$

This implies that we have a natural surjection

$$\Lambda \to \left(\frac{\mathrm{Sel}^{\varepsilon}(E/K_\infty)}{\mathrm{Sel}^0(E/K_\infty)}\right)^{\vee}.$$

As the latter module has Λ-rank one by Lemma 2.2, this map is actually an isomorphism. ∎

As an immediate corollary we obtain

Corollary 2.4 The natural map

$$\mathrm{Sel}^{\varepsilon}(E/K_\infty) \to \widehat{E}^{\varepsilon}(K_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

is a surjection.

For all $n \geq 0$ we define

$$e_n = \frac{\mathrm{rank}_{O_K}(E(K_n)) - \mathrm{rank}_{O_K}(E(K_{n-1}))}{\phi(p^n)}.$$

***Lemma* 2.5** *Assume that* $(-1)^n = \varepsilon$*. Then* $e_n \geq 1$.

Proof By [1, Theorem 5.2] there is an injective homomorphism with finite cokernel

$$\mathrm{Sel}^{\varepsilon}(E/K_n)[\omega_n^{\varepsilon}] \to \mathrm{Sel}^{\varepsilon}(E/K_\infty)[\omega_n^{\varepsilon}].$$

By Lemma 2.2 $\mathrm{Sel}^{\varepsilon}(E/K_\infty)$ has a quotient that is isomorphic to $\Lambda^{\vee}$. It follows that $\mathrm{Sel}^{\varepsilon}(E/K_n)^{\vee} \otimes \mathbb{Q}_p$ contains a submodule isomorphic to $\Lambda/(\omega_n^{\varepsilon}/\omega_{n-1}^{\varepsilon}) \otimes \mathbb{Q}_p$. As the Tate-Shafarevich group is assumed to be finite for all n, this implies that $E(K_n) \otimes \mathbb{Q}_p$ contains a submodule isomorphic to $\Lambda/(\omega_n^{\varepsilon}/\omega_{n-1}^{\varepsilon}) \otimes \mathbb{Q}_p$. As $E(K_{n-1})$ is annihilated by ω_{n-1}, we obtain the desired result. ∎

Corollary 2.6 The natural homomorphisms

$$\mathrm{Sel}^{\varepsilon}(E/K_n) \to \widehat{E}^{\varepsilon}(K_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

and

$$\mathcal{M}^{\varepsilon}(E/K_n) \to \widehat{E}^{\varepsilon}(K_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

are surjective. In particular,

$$\frac{\mathrm{Sel}^{\varepsilon}(E/K_n)}{\mathrm{Sel}^{\varepsilon}(E/K_{n-1}) + \mathrm{Sel}^0(E/K_n)} \cong \frac{\widehat{E}^{\varepsilon}(K_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}{\widehat{E}^{\varepsilon}(K_{n-1,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \cong \frac{\mathcal{M}^{\varepsilon}(E/K_n)}{\mathcal{M}^{\varepsilon}(E/K_{n-1}) + \mathcal{M}^0(E/K_n)}$$

Proof By [3, Theorem 3.2 (1)] $\widehat{E}^{\varepsilon}(K_{n,p}) \otimes \mathbb{Q}_p \cong \mathbb{Q}_p[X]/\omega_n^{\varepsilon}$. As $e_n \geq 1$ for all n with $(-1)^n = \varepsilon$, $E(K_n) \otimes \mathbb{Q}_p$ contains a subrepresentation isomorphic to $\mathbb{Q}_p[X]/\omega_n^{\varepsilon}$.

https://doi.org/10.4153/S0008439525101446 Published online by Cambridge University Press

Thus, $\widehat{E}^{\varepsilon}(K_{n,p}) \otimes \mathbb{Q}_p$ lies in the image of the natural homomorphism

$$E(K_n) \otimes \mathbb{Q}_p \to \widehat{E}(K_{n,p}) \otimes \mathbb{Q}_p.$$

It follows that

$$\mathrm{Sel}^{\varepsilon}(E/K_n) \to \widehat{E}^{\varepsilon}(K_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

and

$$\mathcal{M}^{\varepsilon}(E/K_n) \to \widehat{E}^{\varepsilon}(K_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

have finite cokernels. As the right hand side is divisible, the homomorphism has to be surjective. ∎

The remainder of the section is dedicated to prove the existence of a short exact sequence

$$0 \to \kappa^0(E/K_n) \to \kappa^+(E/K_n) \oplus \kappa^-(E/K_n) \to Ш(E/K_n) \to 0.$$

Proposition 2.7 We have two short exact sequences

$$0 \to \mathrm{Sel}^0(E/K_n) \to \mathrm{Sel}^+(E/K_n) \oplus \mathrm{Sel}^-(E/K_n) \to \mathrm{Sel}(E/K_n) \to 0$$

and

$$0 \to \mathcal{M}^0(E/K_n) \to \mathcal{M}^+(E/K_n) \oplus \mathcal{M}^-(E/K_n) \to E(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to 0$$

Proof For the first claim it suffices to show that

$$\mathrm{Sel}^+(E/K_n) + \mathrm{Sel}^-(E/K_n) = \mathrm{Sel}(E/K_n).$$

As $\widehat{E}(K_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = (\widehat{E}^+(K_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \oplus (\widehat{E}^-(K_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$ (c.f. [3, Theorem 3.2]), Corollary 2.6 implies that indeed

$$\mathrm{im}(\mathrm{Sel}^+(E/K_n) + \mathrm{Sel}^-(E/K_n)) = \mathrm{im}(\mathrm{Sel}(E/K_n)),$$

where $\mathrm{im}(\cdot)$ denotes the image inside $E(K_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. As $\mathrm{Sel}^0(E/K_n) \subset \mathrm{Sel}^{\pm}(E/K_n)$, the first claim follows.

The second claim can be proved similarly. ∎

As an immediate Corollary, we obtain

Corollary 2.8 We have a short exact sequence

$$0 \to \kappa^0(E/K_n) \to \kappa^+(E/K_n) \oplus \kappa^-(E/K_n) \to Ш(E/K_n) \to 0$$

Proof Consider the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \to & \mathcal{M}^0(E/K_n) & \to & \mathcal{M}^+(E/K_n) \oplus \mathcal{M}^-(E/K_n) & \to & E(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \mathrm{Sel}^0(E/K_n) & \to & \mathrm{Sel}^+(E/K_n) \oplus \mathrm{Sel}^-(E/K_n) & \longrightarrow & \mathrm{Sel}(E/K_n) & \longrightarrow & 0 \end{array}$$

The vertical maps are all injective. The claim now follows from the snake lemma. ∎

https://doi.org/10.4153/S0008439525101446 Published online by Cambridge University Press

3 Plus/Minus Tate-Shafarevich groups

In view of Corollary 2.8 it suffices to find asymptotic formulas for $\kappa^*(E/K_n)$ for $* \in \{\pm, 0\}$. In the present section we will concentrate on the comparison of $\kappa^\varepsilon(E/K_n)$ and $\kappa^0(E/K_n)$.

Definition 3.1 Let $* \in \{0, +, -\}$ we denote by

$$\alpha^*_{n,n-1} \colon \kappa^*(E/K_{n-1}) \to \kappa^*(E/K_n)$$

the natural map. We define

$$\kappa^*_{n,n-1} = \frac{\kappa^*(E/K_n)}{\mathrm{im}(\alpha^*_{n,n-1})}.$$

Analogosly we define $Ш_{n,n-1} = \frac{Ш(E/K_n)}{\mathrm{im}(Ш(E/K_{n-1}) \to Ш(E/K_n))}$

Lemma 3.1 *The natural homomorphism*

$$\Phi_n \colon \kappa^0_{n,n-1} \to \kappa^\varepsilon_{n,n-1}$$

is an isomorphism.

Proof By definition,

$$\mathrm{coker}(\Phi_n) \cong \frac{\mathrm{Sel}^\varepsilon(E/K_n)}{\mathrm{Sel}^\varepsilon(E/K_{n-1}) + \mathcal{M}^\varepsilon(E/K_n) + \mathrm{Sel}^0(E/K_n)} = 0$$

by Corollary 2.6. It remains to show that Φ_n is injective.

The kernel of Φ_n is given by the image of $(\mathcal{M}^\varepsilon(E/K_n) + \mathrm{Sel}^\varepsilon(E/K_{n-1})) \cap \mathrm{Sel}^0(E/K_n)$ in $\kappa^0_{n,n-1}$. Note that

$$\begin{aligned}
&(\mathcal{M}^\varepsilon(E/K_n) + \mathrm{Sel}^\varepsilon(E/K_{n-1})) \cap \mathrm{Sel}^0(E/K_n)\\
&\subset (\mathcal{M}^\varepsilon(E/K_{n-1}) + \mathcal{M}^0(E/K_n) + \mathrm{Sel}^\varepsilon(E/K_{n-1})) \cap \mathrm{Sel}^0(E/K_n)\\
&= (\mathcal{M}^0(E/K_n) + \mathrm{Sel}^\varepsilon(E/K_{n-1})) \cap \mathrm{Sel}^0(E/K_n)\\
&= (\mathrm{Sel}^\varepsilon(E/K_{n-1}) \cap \mathrm{Sel}^0(E/K_n)) + \mathcal{M}^0(E/K_n) = \mathrm{Sel}^0(E/K_{n-1}) + \mathcal{M}^0(E/K_n),
\end{aligned}$$

where the first inclusion follows from the following fact. Let $a \in \mathcal{M}^\varepsilon(E/K_n)$, $b \in \mathrm{Sel}^\varepsilon(E/K_{n-1})$ and $a + b \in \mathrm{Sel}^0(E/K_n)$. Then $\mathrm{im}(a) \in \widehat{E}^\varepsilon(K_{n-1,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$, which implies by Corollary 2.6 that $a \in \mathcal{M}^0(E/K_n) + \mathcal{M}^\varepsilon(E/K_{n-1})$.

By definition, the last term in the above equation has trivial image in $\kappa^0_{n,n-1}$. Thus Φ_n is indeed injective. ■

The next lemma is a preparation to prove the following exact sequence

$$0 \to \kappa^0_{n,n-1} \to \kappa^+_{n,n-1} \oplus \kappa^-_{n,n-1} \to Ш_{n,n-1} \to 0.$$

Lemma 3.2 *Assume that* $(-1)^n = \varepsilon$. *The natural homomorphism*

$$\kappa^\varepsilon_{n,n-1} \to Ш_{n,n-1}$$

https://doi.org/10.4153/S0008439525101446 Published online by Cambridge University Press

is injective.

Proof Consider the natural homomorphism

$$\Psi_n\colon \operatorname{Sel}^{\varepsilon}(E/K_n) \to Ш_{n,n-1}.$$

The kernel is given by

$$\begin{aligned}&\operatorname{Sel}^{\varepsilon}(E/K_n) \cap (E(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p + \operatorname{Sel}(E/K_{n-1}))\\ &= (E(K_{n-1}) \otimes \mathbb{Q}_p/\mathbb{Z}_p + \mathcal{M}^{\varepsilon}(E/K_n) + \operatorname{Sel}(E/K_{n-1})) \cap \operatorname{Sel}^{\varepsilon}(E/K_n)\\ &= (\operatorname{Sel}(E/K_{n-1}) + \mathcal{M}^{\varepsilon}(E/K_n)) \cap \operatorname{Sel}^{\varepsilon}(E/K_n)\\ &= \operatorname{Sel}^{\varepsilon}(E/K_n) \cap \operatorname{Sel}(E/K_{n-1}) + \mathcal{M}^{\varepsilon}(E/K_n)\\ &= \operatorname{Sel}^{\varepsilon}(E/K_{n-1}) + \mathcal{M}^{\varepsilon}(E/K_n),\end{aligned}$$

which has a trivial image in $\kappa^{\varepsilon}_{n,n-1}$. ■

Proposition 3.3 There is an exact sequence

$$0 \to \kappa^0_{n,n-1} \to \kappa^+_{n,n-1} \oplus \kappa^-_{n,n-1} \to Ш_{n,n-1} \to 0$$

Proof Consider the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & \kappa^0(E/K_{n-1}) & \to & \kappa^+(E/K_{n-1}) \oplus \kappa^-(E/K_{n-1}) & \to & Ш(E/K_{n-1}) & \to & 0\\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \kappa^0(E/K_n) & \to & \kappa^+(E/K_n) \oplus \kappa^-(E/K_n) & \to & Ш(E/K_n) & \to & 0 \end{array},$$

where the rows are exact by Corollary 2.8. Applying the snake lemma we obtain

$$\kappa^0_{n,n-1} \to \kappa^+_{n,n-1} \oplus \kappa^-_{n,n-1} \to Ш_{n,n-1} \to 0.$$

The left most homomorphism is injective by Lemma 3.1, which implies the desired short exact sequence. ■

Corollary 3.4 We have

$$|Ш_{n,n-1}| = |\kappa^{-\varepsilon}_{n,n-1}|.$$

Proof This is an immediate consequence of Lemma 3.1 and Proposition 3.3. ■

3.1 Estimating $\kappa^0_{n,n-1}$

Before we continue to estinmate $Ш_{n,n-1}$ and $\kappa^{-\varepsilon}_{n,n-1}$ we first determine $\kappa^0_{n,n-1}$.

Lemma 3.5 *The natural homomorphism*

$$\kappa^{\varepsilon}(E/K_{n-1}) \to \kappa^{\varepsilon}(E/K_n)$$

is injective.

https://doi.org/10.4153/S0008439525101446 Published online by Cambridge University Press

Proof Consider the natural map

$$\mathrm{Sel}^{\varepsilon}(K_{n-1}/E) \to \kappa^{\varepsilon}(K_n/E).$$

Its kernel is given by

$$\begin{aligned}&\mathcal{M}^{\varepsilon}(E/K_n) \cap \mathrm{Sel}^{\varepsilon}(E/K_{n-1}) = (\mathcal{M}^{\varepsilon}(E/K_{n-1}) + \mathrm{Sel}^{0}(E/K_{n-1})) \cap \mathcal{M}^{\varepsilon}(E/K_n)\\ &= \mathcal{M}^{\varepsilon}(E/K_{n-1}) + \mathcal{M}^{0}(E/K_{n-1}) = \mathcal{M}^{\varepsilon}(E/K_{n-1}),\end{aligned}$$

where the first equality follows from Corollary 2.6. As the image of $\mathcal{M}^{\varepsilon}(E/K_{n-1})$ in $\kappa^{\varepsilon}(E/K_{n-1})$ is trivial, the claim follows. ∎

As an immediate consequence of Lemmas 3.1 and 3.5 we obtain

Corollary 3.6 The homomorphism

$$\kappa^{0}(E/K_{n-1}) \to \kappa^{0}(E/K_n)$$

is injective.

To prove an asymptotic formula for $\kappa^0(E/K_n)$, we need a control theorem for $\mathrm{Sel}^0(E/K_n)$ and $\mathcal{M}(E/K_n)$. We write Γ_n for $\Gamma^{p^n} = \mathrm{Gal}(K_n/K)$.

***Theorem* 3.7** *The natural homomorphisms*

$$\mathrm{Sel}^{0}(E/K_n) \to \mathrm{Sel}^{0}(E/K_\infty)^{\Gamma_n}$$

and

$$\mathcal{M}^{0}(E/K_n) \to \mathcal{M}^{0}(E/K_\infty)^{\Gamma_n}$$

are injective with uniformly bounded cokernels.

Proof The injectivity follows from the inflation restriction exact sequence and the fact that $E(K_n)[p] = 0$. The fact that the first map has uniformly bounded cokernel follows from [9, Theorem 1.1]. To show the boundedness of the cokernels for the second homomorphism consider the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{M}^{0}(E/K_n) & \longrightarrow & \mathrm{Sel}^{0}(E/K_n) & \longrightarrow & \kappa^{0}(E/K_n) & \longrightarrow & 0 \\ & & \downarrow a_n & & \downarrow b_n & & \downarrow c_n & & \\ 0 & \to & \mathcal{M}^{0}(E/K_\infty)^{\Gamma_n} & \to & \mathrm{Sel}^{0}(E/K_\infty)^{\Gamma_n} & \to & \kappa^{0}(E/K_\infty)^{\Gamma_n} & & \end{array}.$$

By Corollary 3.6 c_n is injective. We therefore obtain an injection $\mathrm{coker}(a_n) \to \mathrm{coker}(b_n)$. As the latter group is uniformly bounded independent of n, the same is true for $\mathrm{coker}(a_n)$. ∎

Recall that $\mathrm{Sel}^0(E/K_\infty)$ is Λ-cotorsion. As $\kappa^0(E/K_\infty)$ is a quotient of $\mathrm{Sel}^0(E/K_\infty)$, $\kappa^0(E/K_\infty)$ is Λ-cotorsion as well. In particular, its Pontryagin dual $\kappa^0(E/K_\infty)^\vee$ is a finitely generated torsion Λ-module.

***Theorem* 3.8** *Let μ and λ be the Iwasawa invariants of $\kappa^0(E/K_\infty)^\vee$. Then for all n large enough we have*

$$v_p(|\kappa^0_{n,n-1}|) = \lambda + \mu\phi(p^n).$$

Proof Using standard arguments in Iwasawa theory Theorem 3.7 implies that there are invariants $\lambda', \lambda'', \mu'$ and μ'' such that

$$v_p(|\operatorname{coker}(\mathrm{Sel}^0(E/K_{n-1}) \to \mathrm{Sel}^0(E/K_n))|) = \lambda' + \mu'\phi(p^n)$$

and

$$v_p(|\operatorname{coker}(\mathcal{M}^0(E/K_{n-1}) \to \mathcal{M}^0(E/K_n))|) = \lambda'' + \mu''\phi(p^n)$$

for $n \gg 0$. By Corollary 3.6 we furthermore have an exact sequence

$$0 \to \operatorname{coker}(\mathcal{M}^0(E/K_{n-1}) \to \mathcal{M}^0(E/K_n)) \to$$
$$\to \operatorname{coker}(\mathrm{Sel}^0(E/K_{n-1}) \to \mathrm{Sel}^0(E/K_n)) \to \kappa^0_{n,n-1} \to 0,$$

which implies

$$v_p(|\kappa^0_{n,n-1}|) = \lambda' - \lambda'' + (\mu' - \mu'')\phi(p^n).$$

Let F' and F'' be the characteristic ideals of $\mathrm{Sel}^0(E/K_\infty)^\vee$ and $\mathcal{M}^0(E/K_\infty)$. Choose n_0 such that $\gcd(F', \omega_n) = \gcd(F', \omega_{n_0})$ and $\gcd(F'', \omega_n) = \gcd(F'', \omega_{n_0})$ for all $n \geq n_0$. Let $G' = \gcd(F', \omega_{n_0})$ and $G'' = \gcd(F'', \omega_{n_0})$. Then we have $\lambda' = \lambda(F') - \lambda(G')$ as well as $\lambda'' = \lambda(F'') - \lambda(G'')$. As we are assuming that $Ш(E/K_n)$ is finite foll all n, $\mathrm{Sel}^0(E/K_n)$ and $\mathcal{M}^0(E/K_n)$ have the same corank for all n. Thus, $G' = G''$. This implies $\lambda' - \lambda'' = \lambda$ and $\mu' - \mu'' = \mu$.

■

3.2 Estimating the kernels

To obtain an asymptotic formula for $Ш(E/K_n)$ we do not only need to understand the cokernels $Ш_{n,n-1}$ but also the kernels of the natural maps $Ш(E/K_{n-1}) \to Ш(E/K_n)$. It turns out that these maps are injetive as we will prove in Proposition 3.10.

***Lemma* 3.9** *Assume that $(-1)^n = \varepsilon$. For all n large enough we have that*

$$\mathcal{M}^{-\varepsilon}(E/K_n) = \mathcal{M}^{-\varepsilon}(E/K_{n-1}) + \mathcal{M}^0(E/K_n).$$

Proof We have a natural isomorphism

$$\frac{E(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p}{E(K_{n-1}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \to \frac{\mathcal{M}^\varepsilon(E/K_n)}{\mathcal{M}^\varepsilon(E/K_{n-1})}.$$

Note that $E(K_{n-1}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \mathcal{M}^\varepsilon(E/K_{n-1}) + \mathcal{M}^{-\varepsilon}(E/K_{n-1})$.

https://doi.org/10.4153/S0008439525101446 Published online by Cambridge University Press

By definition

$$\begin{aligned}\mathcal{M}^{-\varepsilon}(E/K_n) &= \mathcal{M}^{-\varepsilon}(E/K_n) \cap (E(K_{n-1}) \otimes \mathbb{Q}_p/\mathbb{Z}_p + \mathcal{M}^{\varepsilon}(E/K_n)) \\ &= \mathcal{M}^{-\varepsilon}(E/K_n) \cap (\mathcal{M}^{\varepsilon}(E/K_n) + \mathcal{M}^{-\varepsilon}(E/K_{n-1})) \\ &= \mathcal{M}^{-\varepsilon}(E/K_{n-1}) + (\mathcal{M}^{-\varepsilon}(E/K_n) \cap \mathcal{M}^{\varepsilon}(E/K_n)) \\ &= \mathcal{M}^{-\varepsilon}(E/K_{n-1}) + \mathcal{M}^{0}(E/K_n).\end{aligned}$$

■

Proposition 3.10 The natural homomorphism

$$\text{Ш}(E/K_{n-1}) \to \text{Ш}(E/K_n)$$

is injective for all n large enough.

Proof If $(-1)^n = -\varepsilon$ this follows from [3, Lemma 4.5 and Remark 4.6]. Assume now that $(-1)^n = \varepsilon$. By Corollary 2.8 it suffices to show that $\kappa^{\pm}(E/K_{n-1}) \to \kappa^{\pm}(E/K_n)$ is injective. For the ε part this is Lemma 3.5. It remains to consider the kernel of $\kappa^{-\varepsilon}(E/K_{n-1}) \to \kappa^{-\varepsilon}(E/K_n)$. Consider the natural map

$$\psi_n^{-\varepsilon}\colon \operatorname{Sel}^{-\varepsilon}(E/K_{n-1}) \to \kappa^{-\varepsilon}(E/K_n).$$

The kernel is given by $\operatorname{Sel}^{-\varepsilon}(E/K_{n-1}) \cap \mathcal{M}^{-\varepsilon}(E/K_n)$. By Lemma 3.9 we know

$$\mathcal{M}^{-\varepsilon}(E/K_n) = \mathcal{M}^{-\varepsilon}(E/K_{n-1}) + \mathcal{M}^{0}(E/K_n).$$

Thus,

$$\begin{aligned}\operatorname{Sel}^{-\varepsilon}(E/K_{n-1}) \cap \mathcal{M}^{-\varepsilon}(E/K_n) &= \operatorname{Sel}^{-\varepsilon}(E/K_{n-1}) \cap (\mathcal{M}^{-\varepsilon}(E/K_{n-1}) + \mathcal{M}^{0}(E/K_n)) \\ &= \mathcal{M}^{-\varepsilon}(E/K_{n-1}) + (\operatorname{Sel}^{-\varepsilon}(E/K_{n-1}) \cap \mathcal{M}^{0}(E/K_n)) \\ &= \mathcal{M}^{-\varepsilon}(E/K_{n-1}) + (\operatorname{Sel}^{0}(E/K_{n-1}) \cap \mathcal{M}^{0}(E/K_n)).\end{aligned}$$

Corollary 3.6 implies that $\operatorname{Sel}^0(E/K_{n-1}) \cap \mathcal{M}^0(E/K_n) = \mathcal{M}^0(E/K_{n-1})$. Thus,

$$\mathcal{M}^{-\varepsilon}(E/K_{n-1}) + (\operatorname{Sel}^{0}(E/K_{n-1}) \cap \mathcal{M}^{0}(E/K_n)) = \mathcal{M}^{-\varepsilon}(E/K_{n-1}).$$

Therefore $\ker(\psi_n^{-\varepsilon}) = \mathcal{M}^{-\varepsilon}(E/K_{n-1})$, which implies that

$$\kappa^{-\varepsilon}(E/K_{n-1}) \to \kappa^{-\varepsilon}(E/K_n)$$

is indeed injective. ■

Corollary 3.11 For $n \gg 0$ we have

$$\operatorname{Sel}(E/K_{n-1}) \cap (E(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p) = E(K_{n-1}) \otimes \mathbb{Q}_p/\mathbb{Z}_p.$$

3.3 Estimating $\kappa_{n,n-1}^{-\varepsilon}$

In this section we always assume that $(-1)^n = \varepsilon$. Before we can analyze $\kappa_{n,n-1}^{-\varepsilon}$, we first need the following result on signed Selmer groups.

https://doi.org/10.4153/S0008439525101446 Published online by Cambridge University Press

***Lemma* 3.12** *Assume that the* $\mathrm{Sel}^0(E/K_n)[\omega_n^{-\varepsilon}]$ *is finite for all n. The natural maps*

$$\frac{\mathrm{Sel}^{-\varepsilon}(E/K_n)}{\mathrm{Sel}^0(E/K_n)}[\omega_n^{-\varepsilon}] \to \frac{\mathrm{Sel}^{-\varepsilon}(E/K_\infty)}{\mathrm{Sel}^0(E/K_\infty)}[\omega_n^{-\varepsilon}]$$

are injective with uniformly bounded cokernel.

Proof Consider the exact sequence

$$H^1(K_\Sigma/K_\infty, E[p^\infty])[\omega_n^{-\varepsilon}] \to \left(\frac{H^1(K_\Sigma/K_\infty, E[p^\infty])}{\mathrm{Sel}^0(E/K_\infty)}\right)[\omega_n^{-\varepsilon}] \to \mathrm{Sel}^0(E/K_\infty)/\omega_n^{-\varepsilon}\,\mathrm{Sel}^0(E/K_\infty).$$

If $\mathrm{Sel}^0(E/K_n)[\omega_n^{-\varepsilon}]$ is finite for all n, the characteristic ideal of $\mathrm{Sel}^0(E/K_\infty)$ is coprime to $\omega_n^{-\varepsilon}$ for all n. In particular, $\mathrm{Sel}^0(E/K_\infty)/\omega_n^{-\varepsilon}\,\mathrm{Sel}^0(E/K_n)$ is uniformly bounded. It follows that the natural homomorphism

$$H^1(K_\Sigma/K_\infty, E[p^\infty])[\omega_n^{-\varepsilon}] \to \frac{H^1(K_\Sigma/K_\infty, E[p^\infty])}{\mathrm{Sel}^0(E/K_\infty)}[\omega_n^{-\varepsilon}]$$

is injective with uniformly bounded cokernel. In particular,

$$\frac{H^1(K_\Sigma/K_n, E[p^\infty])}{\mathrm{Sel}^0(E/K_n)}[\omega_n^{-\varepsilon}] \to \frac{H^1(K_\Sigma/K_\infty, E[p^\infty])}{\mathrm{Sel}^0(E/K_\infty)}[\omega_n^{-\varepsilon}]$$

is injective with uniformly bounded cokernel. Consider the following commutative diagram

$$\begin{array}{ccccccc}
0 \longrightarrow & \frac{\mathrm{Sel}^{-\varepsilon}(E/K_n)}{\mathrm{Sel}^0(E/K_n)} & \longrightarrow & \frac{H^1(K_\Sigma/K_n, E[p^\infty])}{\mathrm{Sel}^0(E/K_n)}[\omega_n^{-\varepsilon}] & \to & \frac{H^1(K_{n,p}, E[p^\infty])}{\widehat{E}^{-\varepsilon}(K_{n,p})\otimes\mathbb{Q}_p/\mathbb{Z}_p}[\omega_n^{-\varepsilon}] \\
& \downarrow & & \downarrow & & \downarrow \\
0 \to & \frac{\mathrm{Sel}^{-\varepsilon}(E/K_\infty)}{\mathrm{Sel}^0(E/K_\infty)}[\omega_n^{-\varepsilon}] & \to & \frac{H^1(K_\Sigma/K_\infty, E[p^\infty])}{\mathrm{Sel}^0(E/K_\infty)}[\omega_n^{-\varepsilon}] & \to & \frac{H^1(K_{\infty,p}, E[p^\infty])}{\widehat{E}^{-\varepsilon}(K_{\infty,p})\otimes\mathbb{Q}_p/\mathbb{Z}_p}[\omega_n^{-\varepsilon}]
\end{array}$$

The right vertical map is injective (this can be proved as in [7, Theorem 9.2] using the Coleman maps defined by [4]). The middle vertical map is injective with uniformly bounded cokernel. Thus, the left vertical map is injective with uniformly bounded cokernel. ∎

***Lemma* 3.13** *Assume that* $(-1)^n = \varepsilon$ *and that* $\mathrm{Sel}^0(E/K_n)[\omega_n^{-\varepsilon}]$ *is finite for all n. Then we have*

$$\mathrm{Sel}^{-\varepsilon}(E/K_n) = \mathrm{Sel}^{-\varepsilon}(E/K_{n-1}) + \mathrm{Sel}^0(E/K_n).$$

Proof As $\omega_n^{-\varepsilon} = \omega_{n-1}^{-\varepsilon}$ Lemma 3.12 implies that

$$\frac{\mathrm{Sel}^{-\varepsilon}(E/K_n)}{\mathrm{Sel}^0(E/K_n)}[\omega_n^{-\varepsilon}] = \frac{\mathrm{Sel}^{-\varepsilon}(E/K_{n-1})}{\mathrm{Sel}^0(E/K_{n-1})}[\omega_{n-1}^{-\varepsilon}].$$

https://doi.org/10.4153/S0008439525101446 Published online by Cambridge University Press

As $\frac{\mathrm{Sel}^{-\varepsilon}(E/K_m)}{\mathrm{Sel}^0(E/K_m)}$ is annihilated by $\omega_m^{-\varepsilon}$ for all m, we obtain that

$$\frac{\mathrm{Sel}^{-\varepsilon}(E/K_n)}{\mathrm{Sel}^0(E/K_n)} = \frac{\mathrm{Sel}^{-\varepsilon}(E/K_{n-1})}{\mathrm{Sel}^0(E/K_{n-1})}$$

In particular $\mathrm{Sel}^{-\varepsilon}(E/K_n) = \mathrm{Sel}^{-\varepsilon}(E/K_{n-1}) + \mathrm{Sel}^0(E/K_n)$. ∎

As an immediate corollary we obtain

Corollary 3.14 Assume that $(-1)^n = \varepsilon$ and that $\mathrm{Sel}^0(E/K_n)[\omega_n^{-\varepsilon}]$ is finite for all n. The natural homomorphism

$$\kappa^0_{n,n-1} \to \kappa^{-\varepsilon}_{n,n-1}$$

is surjective.

3.4 Estimating $Ш_{n,n-1}$

In this section we put the results from previous sections together to obtain an estimate for $Ш_{n,n-1}$ and to derive an asymptotic formula for $Ш(E/K_n)$.

***Theorem* 3.15** *Assume that* $(-1)^n = \varepsilon$ *and that* $\mathrm{Sel}^0(E/K_n)[\omega_n^{-\varepsilon}]$ *is finite for all n. Then we have*

$$|Ш_{n,n-1}| = |\kappa^0_{n,n-1}|.$$

Proof By Corollaries 3.4 and 3.14 we obtain

$$|Ш_{n,n-1}| \le |\kappa^0_{n,n-1}|.$$

On the other hand Lemmas 3.1 and 3.2 imply that there is a chain of injective homomorphisms

$$\kappa^0_{n,n-1} \to \kappa^{\varepsilon}_{n,n-1} \to Ш_{n,n-1},$$

which implies

$$|\kappa^0_{n,n-1}| \le |Ш_{n,n-1}|.$$

∎

As a direct consequence of the above analysis we obtain

***Theorem* 3.16** *Assume that* $\mathrm{Sel}^0(E/K_n)[\omega_n^{-\varepsilon}]$ *is finite for all n. For all n large enough we have*

$$v_p(|Ш(E/K_n)|) = \begin{cases} \mu^{-\varepsilon}\sum_{m\le n,(-1)^m=-\varepsilon}\phi(p^m) + \mu^{\varepsilon}\sum_{m\le n,(-1)^m=\varepsilon}\phi(p^m) \\ \quad + \lambda^{\varepsilon}\lfloor\frac{n}{2}\rfloor + \lambda^{-\varepsilon}\lfloor\frac{n+1}{2}\rfloor + \nu & (-1)^n = -\varepsilon \\ \\ \mu^{-\varepsilon}\sum_{m\le n,(-1)^m=-\varepsilon}\phi(p^m) + \mu^{\varepsilon}\sum_{m\le n,(-1)^m=\varepsilon}\phi(p^m) \\ \quad + \lambda^{\varepsilon}\lfloor\frac{n+1}{2}\rfloor + \lambda^{-\varepsilon}\lfloor\frac{n}{2}\rfloor + \nu & (-1)^n = \varepsilon \end{cases}$$

https://doi.org/10.4153/S0008439525101446 Published online by Cambridge University Press

Proof This is a direct consequence of [3, Theorem 1.1], Theorem 3.15, Proposition 3.10 and Theorem 3.8. ■

References

[1] Agboola, A. and Howard, B. (2005). Anticyclotomic Iwasawa theory of CM elliptic curves. II. *Math. Res. Lett.*, 12(5-6):611–621.

[2] Burungale, A., Kobayashi, S., and Ota, K. (2021). Rubin's conjecture on local units in the anticyclotomic tower at inert primes. *Ann. of Math. (2)*, 194(3):943–966.

[3] Burungale, A., Kobayashi, S., and Ota, K. (2024a). On the tate-shafarevich groups of cm elliptic curves over anticyclotmoic $\mathbb{Z}_p$ extensions at inert primes.

[4] Burungale, A., Kobayashi, S., and Ota, K. ((2024)b). p-adic L-functions and rational points on CM elliptic curves at inert primes. *J. Inst. Math. Jussieu*, 23(no. 3):1417–1460.

[5] Greenberg, R. (1999). Introduction to Iwasawa theory for elliptic curves. *Arithmetic algebraic geometry. IAS/Park City Math. Ser*, 9:407–464.

[6] Iwasawa, K. (1973). On $\mathbf{Z}_l$-extensions of algebraic number fields. *Ann. of Math. (2)*, 98:246–326.

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

[8] Lei, A., Lim, M. F., and Müller, K. (2023). Asymptotic formula for Tate-Shafarevich groups of p-supersingular elliptic curves over anticyclotomic extensions. *Adv. Math.*, 434:Paper No. 109320, 28.

[9] Lim, M. F. (2020). On the control theorem for fine Selmer groups and the growth of fine Tate–Shafarevich groups in $\mathbb{Z}_p$-extensions. *Doc. Math.*, 25:2445–2471.

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

[11] Silverman, J. H. (2009). *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition.

Institut für Theoretische Informatik, Mathematik und Operations Research,Universität der Bundeswehr München, Werner-Heisenberg-Weg 39, , 85577
e-mail: katharina-mueller@unibw.de.