J. Aust. Math. Soc. **95** (2013), 189–200
doi:10.1017/S1446788713000165

THE PLUS/MINUS SELMER GROUPS FOR SUPERSINGULAR PRIMES

BYOUNG DU KIM

(Received 25 July 2011; accepted 22 September 2011; first published online 7 June 2013)

Communicated by F. Calegari

Abstract

Suppose that an elliptic curve E over $\mathbb{Q}$ has good supersingular reduction at p. We prove that Kobayashi's plus/minus Selmer group of E over a $\mathbb{Z}_p$-extension has no proper Λ-submodule of finite index under some suitable conditions, where Λ is the Iwasawa algebra of the Galois group of the $\mathbb{Z}_p$-extension. This work is analogous to Greenberg's result in the ordinary reduction case.

2010 *Mathematics subject classification*: primary 11G.
Keywords and phrases: elliptic curves, Iwasawa theory.

1. Introduction

Let p be a prime number, and $\mathbb{Z}_p$ be the set of p-adic integers. Let F be a number field in which the prime p is unramified, and F_∞ be a $\mathbb{Z}_p$-extension of F. We suppose that $F_{\infty,q}$ is abelian over $\mathbb{Q}_p$ for any prime q above p. This is obviously true in some cases such as when F_∞ is contained in $F(\mu_{p^\infty})$, or when p splits completely over $F/\mathbb{Q}$. Let Λ be the Iwasawa algebra $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/F)]]$, which may be identified with $\mathbb{Z}_p[[X]]$ by choosing a topological generator γ of $\mathrm{Gal}(F_\infty/F)$ and identifying $\gamma = 1 + X$.

Let E be an elliptic curve over $\mathbb{Q}$, and assume that E has good reduction at p. In other words, assume that its reduced curve $\tilde{E}$ modulo p is smooth. Let a_p denote $1 + p - |\tilde{E}(\mathbb{Z}/p\mathbb{Z})|$.

We recall the definition of the Selmer group of E over a field $L/\mathbb{Q}$ (see [12, Ch. X, Section 4]):

$$\mathrm{Sel}_p(E/L) = \ker\Big(H^1(L, E[p^\infty]) \to \prod_v H^1(L_v, E[p^\infty])/E(L_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p\Big)$$

where v runs over every place of L, $E[p^\infty]$ is the set of every torsion point of $E(\overline{\mathbb{Q}})$ whose order is some power of p, and $E(L_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is regarded as a subgroup of $H^1(L_v, E[p^\infty])$ through the Kummer map.

The author was partially supported by a grant from the Royal Society of New Zealand.
© 2013 Australian Mathematical Publishing Association Inc. 1446-7887/2013 $16.00

https://doi.org/10.1017/S1446788713000165 Published online by Cambridge University Press

Suppose that we want to study the Selmer group $\mathrm{Sel}_p(E/F_\infty)$. When E has good ordinary reduction at p (that is to say, $p \nmid a_p$), $\mathrm{Sel}_p(E/F_\infty)$ has been studied extensively. On the other hand, when E is supersingular at p (in other words, when $p|a_p$), $\mathrm{Sel}_p(E/F_\infty)$ lacks certain crucial properties. For example, there is a missing link between the Selmer group over F_∞ and the Selmer group over F_n for each n, and $\mathrm{Sel}_p(E/F_\infty)$ is never Λ-cotorsion.

In recent years Kobayashi [8] showed that the plus/minus Selmer group theory holds great promise in this regard, and its connection with Pollack's plus/minus p-adic L-function has been widely studied. Many people consider them as a plausible alternative (in the area of supersingular primes) to the conventional Selmer groups and p-adic L-functions. See [8, 11].

Thus, it stands to reason that we should further investigate the properties of the so-called plus/minus Selmer groups. Throughout this paper, we assume that $a_p = 0$ just as in the papers of Kobayashi and Pollack. This is not as restrictive as it seems because if p is supersingular, a_p is divisible by p, and by Hasse, $|a_p| \le 2\sqrt{p}$, thus $a_p = 0$ for all supersingular p with $p > 3$. (It should be noted that the same argument does not work for elliptic curves defined over other fields.)

Theorem 1.1 (See Theorem 3.14). *If* $\mathrm{Sel}_p^+(E/F_\infty)$ *(respectively,* $\mathrm{Sel}_p^-(E/F_\infty)$*) is* Λ*-cotorsion, then* $\mathrm{Sel}_p^+(E/F_\infty)$ *(respectively,* $\mathrm{Sel}_p^-(E/F_\infty)$*) has no proper* Λ*-submodule of finite index. For the statement for* $\mathrm{Sel}_p^+(E/F_\infty)$*, we require an additional condition that* p *splits completely over* $F/\mathbb{Q}$*, and is totally ramified over* F_∞/F*.*

See the discussions before and after Propositions 2.2 and 2.3 where we discuss why we need the additional condition for Sel_p^+, and our current effort to lift this condition.

A similar result for ordinary primes has already been obtained in [2], from which we freely borrow many ideas. To put it simply, [2] is a deep study on various arithmetic dualities in connection with Iwasawa theory.

Theorem 1.1 was already used in the author's other paper [7], published in 2009, to prove that the lambda invariants of the plus/minus Selmer groups can be arbitrarily large. Also, following [2], we prove the following: by the Weierstrass preparation theorem, the Pontryagin dual of the plus/minus Selmer group

$$\mathrm{Sel}_p^\pm(E/F_\infty)^\vee \stackrel{\mathrm{def}}{=} \mathrm{Hom}(\mathrm{Sel}_p^\pm(E/F_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$$

is pseudo-isomorphic to $\prod_{i\in I^\pm} \Lambda/(f_i^\pm)$ for some finite index set $I^\pm$ and some $f_i^\pm \in \Lambda$. (A pseudo-isomorphism is a homomorphism with finite kernel and cokernel.) Let

$$f^\pm(X) \stackrel{\mathrm{def}}{=} \prod_{i\in I^\pm} f_i^\pm \in \Lambda \cong \mathbb{Z}_p[[X]].$$

In other words, $f^\pm(X)$ is a generator of the characteristic ideal of $\mathrm{Sel}_p^\pm(E/F_\infty)^\vee$.

Theorem 1.2. *If* $\mathrm{Sel}_p(E/F)$ *is finite, then*

$$|f^\pm(0)| \sim |\mathrm{Sel}_p(E/F)| \prod_l c_l$$

https://doi.org/10.1017/S1446788713000165 Published online by Cambridge University Press

where l runs over every prime, c_l is the Tamagawa number $c_l = [E(\mathbb{Q}_l) : E^0(\mathbb{Q}_l)]$ and $\sim$ means equality up to units of $\mathbb{Z}_p$.

2. Notations and plus/minus universal norms

Let k be a local field of residue characteristic p such that $k/\mathbb{Q}_p$ is unramified, k_∞ be a $\mathbb{Z}_p$-extension of k (in other words, $\mathrm{Gal}(k_\infty/k) \cong \mathbb{Z}_p$), and k_n be its unique subfield such that $\mathrm{Gal}(k_n/k) \cong \mathbb{Z}/p^n\mathbb{Z}$. We assume that k_∞ is totally ramified over k, and k_∞ is abelian over $\mathbb{Q}_p$. Where $\mathcal{F}$ is a formal group (or formal group scheme), the universal norm is the group of points

$$\bigcap_{n=0}^{\infty} N_{k_n/k}\mathcal{F}(k_n)$$

(or rather, the set of inverse limits $\varprojlim_n x_n$, where $x_n \in \mathcal{F}(k_n)$ and $N_{k_{n+1}/k_n} x_{n+1} = x_n$, $n = 0, 1, 2, \ldots$). In this context, $N_{k_n/k}$ means the trace map.

Hazewinkel's computation implies that when $\mathcal{F}$ is a one-parameter formal group of height greater than 1 and k_∞/k is totally ramified, its universal norm is trivial [3, 4]. One implication is as follows. Let E be an elliptic curve over $\mathbb{Q}_p$, and suppose that it is a minimal model over $\mathbb{Z}_p$ and its reduced curve over $\mathbb{Z}/p\mathbb{Z}$ is smooth. If E has supersingular reduction (equivalently, its associated formal group has height 2), its universal norm is trivial. This phenomenon seems to explain why, for example, critical theorems like the control theorem [10, Section 1(a)] are difficult to establish for supersingular primes. (See also Mazur's comment on the matter in [10, Section 1(d)].)

Instead, following Kobayashi, we define the following groups.

Definition 2.1 (Plus/minus norm groups). For notational convenience, let k_{-1} be k. We define

$$E^+(k_n) = \{x \in E(k_n) | \ \mathrm{Tr}_{k_n/k_{m+1}}(x) \in E(k_m) \text{ for every } 0 \le m < n, m \text{ even}\},$$
$$E^-(k_n) = \{x \in E(k_n) | \ \mathrm{Tr}_{k_n/k_{m+1}}(x) \in E(k_m) \text{ for every } -1 \le m < n, m \text{ odd}\}.$$

This definition has to do with the series of points called plus/minus universal norms that we will now explain.

First, consider an infinite extension $L_\infty = k_\infty(\mu_p)$, and let L_n be its unique subfield such that $\mathrm{Gal}(L_n/k) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$ for $n > 0$ (so L_n is simply $k_{n-1}(\mu_p)$), and let L_0 be k.

Suppose that $a_p = 1 + p - \#E(\mathbb{Z}/p\mathbb{Z}) = 0$. As in [6, Section 3.2], we can construct the points $b_n^{(i)} \in E(L_n)$ for $n \ge 0$ and $i = 1, \ldots, d$, where $d = [k : \mathbb{Q}_p]$, which satisfy

$$N_{L_{n+1}/L_n} b_{n+1}^{(i)} = b_{n-1}^{(i)}, \quad n > 0.$$

We can produce points defined over k_n by

$$c_n^{(i)} = N_{L_\infty/k_\infty} b_{n+1}^{(i)}, \quad n \ge -1.$$

https://doi.org/10.1017/S1446788713000165 Published online by Cambridge University Press

It is clear that $c_n^{(i)}$ is contained in $E^+(k_n)$ if n is even, and in $E^-(k_n)$ if n is odd. Accordingly, we define

$$c_n^{(i),+} = \begin{cases} c_n^{(i)} & \text{if } n \text{ is even,} \\ c_{n-1}^{(i)} & \text{if } n \text{ is odd,} \end{cases}$$
$$c_n^{(i),-} = \begin{cases} c_n^{(i)} & \text{if } n \text{ is odd,} \\ c_{n-1}^{(i)} & \text{if } n \text{ is even,} \end{cases}$$

for $n = -1, 0, \ldots$.

When $k = \mathbb{Q}_p$ and $k_\infty \subset \mathbb{Q}_p(\mu_{p^\infty})$, it is known that $\{(c_n^{(i),\pm})^{\sigma_n}\}_{i=1,2,\ldots,d,\sigma_n \in \mathrm{Gal}(k_n/k)}$ generates $E^\pm(k_n)$ for each $n \geq 0$ [8, Proposition 8.12(ii)]. To the best of our knowledge, it is not yet proven for every k and k_∞, but we know enough to prove the following. Let $E^\pm(k_\infty) = \cup E^\pm(k_n)$.

Proposition 2.2 ([8, Proposition 8.23], [6, Propositions 3.17 and 4.9]).

$$(E^-(k_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee \cong \Lambda^d$$

where $d = [k : \mathbb{Q}_p]$.

Proposition 2.3 ([8, Proposition 8.24], [5, Proposition 4.16]). *If* $k = \mathbb{Q}_p$,

$$E^+(k_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p{}^\vee \cong \Lambda.$$

To prove Proposition 2.2, it is sufficient to know that $\{c_0^{(i),-}\}_{i=1,\ldots,d} = \{c_{-1}^{(i)}\}_{i=1,\ldots,d}$ generates $E(k)$ (the Nakayama lemma and a certain plus/minus p-adic regulator map will take care of the rest).

Similarly, to prove Proposition 2.3, it is enough to know that $\{(c_0^{(i),+})\}_{i=1,\ldots,d} = \{(c_0^{(i)})\}_{i=1,\ldots,d}$ generates $E(k)$, which we do not yet know in general. But, under the given condition, Proposition 2.3 was proven in [5].

We hope that our current project on the case where k is the maximal unramified $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$ will help reach a more conclusive solution.

3. Λ-submodules

Recall that F is a finite extension of $\mathbb{Q}$ in which p is unramified. For convenience we assume that every prime q above p is totally ramified over F_∞/F. Also, we assume that $F_{\infty,q}$ is abelian over $\mathbb{Q}_p$, and additionally, when we work with Sel_p^+, we assume that p splits completely over $F/\mathbb{Q}$.

We let Γ denote $\mathrm{Gal}(F_\infty/F)$ and Λ denote $\mathbb{Z}_p[[\Gamma]]$. Once and for all we fix an isomorphism $\kappa : \Gamma \to 1 + p\mathbb{Z}_p$ where $1 + p\mathbb{Z}_p$ is a multiplicative group.

From this point on, E will be an elliptic curve over $\mathbb{Q}$ with good supersingular reduction at p and $a_p = 0$. We let T denote the Tate module $T_p(E) = \varprojlim_n E[p^n]$, and for every $s \in \mathbb{Z}_p$ we let T_s denote the twisted group $T \otimes (\kappa^s)$. We let V and A

https://doi.org/10.1017/S1446788713000165 Published online by Cambridge University Press

denote $T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and V/T respectively, and V_s and A_s denote $V \otimes \kappa^s$ and $A \otimes \kappa^s$ respectively. We note that $A \cong E[p^\infty]$.

We let Σ be a finite set of places of F containing all primes above p, bad primes of E, and ∞. We let F_Σ denote the maximal extension of F unramified outside Σ.

Definition 3.1 (Plus/minus Selmer groups, [8, Definition 1.1]). We define $\mathrm{Sel}_p^{\pm}(E/F_\infty)$ to be the kernel of

$$\mathbf{f} : H^1(F_\Sigma/F_\infty, A) \to \prod_{w|l, l\in\Sigma, l\nmid p} \frac{H^1(F_{\infty,w}, A)}{E(F_{\infty,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \prod_{v|p} \frac{H^1(F_{\infty,v}, A)}{E^{\pm}(F_{\infty,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}.$$

Our first step is to show that $\mathbf{f}$ is surjective.

Proposition 3.2. *For any n and a prime v of F_n above p, $E(F_{n,v})$ is p-torsion-free.*

Proof. This is [6, Proposition 3.1], which is a slight generalization of [8, Proposition 8.7]. □

In particular, $E(F_{\infty,v})$ is p-torsion-free, which implies that $A^{G_{F_{\infty,v}}} = A_s^{G_{F_{\infty,v}}} = 0$. Hence, the Hochschild–Serre spectral sequence induces the isomorphism

$$H^1(F_{n,v}, A_s) \to H^1(F_{\infty,v}, A_s)^{\mathrm{Gal}(F_{\infty,v}/F_{n,v})}.$$

We use this isomorphism to identify $H^1(F_{n,v}, A_s)$ with $H^1(F_{\infty,v}, A_s)^{\mathrm{Gal}(F_{\infty,v}/F_{n,v})}$.

Similarly, for any integer k the long exact sequence

$$\cdots \to A_s^{F_{n,v}} \to H^1(F_{n,v}, A_s[p^k]) \to H^1(F_{n,v}, A_s) \xrightarrow{p^k} H^1(F_{n,v}, A_s) \to \cdots$$

allows us to identify $H^1(F_{n,v}, A_s[p^k])$ with $H^1(F_{n,v}, A_s)[p^k]$.

Definition 3.3. For any prime w of F_∞ above p, we define

$$\mathbb{H}_w^{\pm} = E^{\pm}(F_{\infty,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subset H^1(F_{\infty,w}, A).$$

For any $s \in \mathbb{Z}_p$ and any prime v of F_n above p, we define

$$\mathbb{H}_{n,v}^{s,\pm} = (\mathbb{H}_w^{\pm} \otimes \kappa^s)^{\mathrm{Gal}(F_\infty/F_n)} \subset H^1(F_{n,v}, A_s)$$

where w denotes the prime of F_∞ above v.

Proposition 3.4. *For every integer k and n, $\mathbb{H}_{n,v}^{s,\pm}[p^k]$ is the exact annihilator of $\mathbb{H}_{n,v}^{-s,\pm}[p^k]$ with respect to the Tate local pairing*

$$H^1(F_{n,v}, A_s[p^k]) \times H^1(F_{n,v}, A_{-s}[p^k]) \to \mathbb{Z}/p^k\mathbb{Z}.$$

Proof. Without loss of generality we can assume that there is only one prime of F_∞ above v. First we choose an integer $N > n$ such that $\kappa(\mathrm{Gal}(F_\infty/F_N)) \equiv 1 \pmod{p^k}$. Then $A_s[p^k]$ and $A_{-s}[p^k]$ are just $A[p^k]$ as G_{F_N}-modules. From [6, Proposition 3.15] it

https://doi.org/10.1017/S1446788713000165 Published online by Cambridge University Press

follows that $\mathbb{H}^{\pm}_{N,v}[p^k] \subset H^1(F_{N,v}, A[p^k])$ is the exact annihilator of itself with respect to the Tate local pairing

$$(\cdot,\cdot)_N : H^1(F_{N,v}, A[p^k]) \times H^1(F_{N,v}, A[p^k]) \to \mathbb{Z}/p^k\mathbb{Z}.$$

(Kim [6, Proposition 3.15] is proven only for $\mathbb{H}^{-}_{N,v}[p^k]$, but under condition (A), the same proof works for $\mathbb{H}^{+}_{N,v}[p^k]$.) Thus $\mathbb{H}^{s,\pm}_{N,v}[p^k]$ is the exact annihilator of $\mathbb{H}^{-s,\pm}_{N,v}[p^k]$.

We now let Cor denote the corestriction map $H^1(F_{N,v}, A_{-s}[p^k]) \to H^1(F_{n,v}, A_{-s}[p^k])$ and Res denote the restriction map $H^1(F_{n,v}, A_s[p^k]) \to H^1(F_{N,v}, A_s[p^k])$. From Propositions 2.2 and 2.3, for any m we have the identification

$$(\mathbb{H}^{s,\pm}_{m,v})^\vee \cong \mathbb{Z}_p[\mathrm{Gal}(F_m/F)]^d \cong (\mathbb{Z}_p[X]/((1+X)^{p^m}-1))^d$$

where $d = [F_v : \mathbb{Q}_p]$. Thus we can identify $\mathrm{Cor} : \mathbb{H}^{-s,\pm}_{N,v} \to \mathbb{H}^{-s,\pm}_{n,v}$ with the surjective map

$$\mathrm{Hom}(\mathbb{Z}_p[X]/((1+X)^{p^N}-1), \mathbb{Z}/p^k\mathbb{Z})^d \to \mathrm{Hom}(\mathbb{Z}_p[X]/((1+X)^{p^n}-1), \mathbb{Z}/p^k\mathbb{Z})^d$$

induced from the map $\mathbb{Z}_p[X]/((1+X)^{p^n}-1) \to \mathbb{Z}_p[X]/((1+X)^{p^N}-1)$ given by the multiplication by $(1+X)^{p^N}-1/(1+X)^{p^n}-1$.

By the property of the cup product we have

$$(\mathrm{Res}(x), y)_N = (x, \mathrm{Cor}(y))_n$$

for every $x \in H^1(F_{n,v}, A_s[p^k])$ and $y \in H^1(F_{N,v}, A_{-s}[p^k])$. Since $\mathrm{Res}(\mathbb{H}^{s,\pm}_{n,v}) \subset \mathbb{H}^{s,\pm}_{N,v}$, and $\mathrm{Cor} : \mathbb{H}^{-s,\pm}_{N,v} \to \mathbb{H}^{-s,\pm}_{n,v}$ is surjective, it follows that $(\mathbb{H}^{s,\pm}_{n,v}, \mathbb{H}^{-s,\pm}_{n,v})_n = 0$. On the other hand, by the explicit computation of the local Euler characteristic we find that the order of $H^1(F_{n,v}, A_{-s}[p^k])$ is $p^{2k[F_{n,v}:\mathbb{Q}_p]}$, thus the order of the exact annihilator of $\mathbb{H}^{-s,\pm}_{n,v}$ is equal to the order of $\mathbb{H}^{s,\pm}_{n,v}$, thus the exact annihilator of $\mathbb{H}^{-s,\pm}_{n,v}$ is $\mathbb{H}^{s,\pm}_{n,v}$. □

We fix s. We note that $\mathrm{Hom}(A_s, \mu_{p^\infty}) \cong T_{-s}$.

Definition 3.5. For any integer n and a prime w of F_n, we define the local conditions: $H^1_{\mathcal{F}^\pm}(F_{n,w}, A_s) := \mathbb{H}^{s,\pm}_{n,w}$ for $w|p$; $H^1_{\mathcal{F}^\pm}(F_{n,w}, A_s) := 0$ for $w \nmid p$; $H^1_{\mathcal{F}^\pm}(F_{n,w}, T_{-s}) :=$ the exact annihilator of $H^1_{\mathcal{F}^\pm}(F_{n,w}, A_s)$ with respect to the Tate local pairing

$$H^1(F_{n,w}, A_s) \times H^1(F_{n,w}, T_{-s}) \to \mathbb{Q}_p/\mathbb{Z}_p.$$

We let $U^\pm_{-s}$ be the $\mathbb{Q}_p$-subspace of $H^1(F_{n,w}, V_{-s})$ spanned by $H^1_{\mathcal{F}^\pm}(F_{n,w}, T_{-s})$.

Definition 3.6. Let $H^1_{\mathcal{F}^\pm}(F_{n,w}, A_{-s})$ be the image of $U^\pm_{-s}$ under the map $H^1(F_{n,w}, V_{-s}) \to H^1(F_{n,w}, A_{-s})$ given by $A_{-s} \cong V_{-s}/T_{-s}$.

Note that all the local conditions for A_s and A_{-s} are divisible. Also note that if w is not lying above p, $H^1_{\mathcal{F}^\pm}(F_{n,w}, A_{-s})$ is 0 since $H^1(F_{n,w}, A_{-s})$ is finite. It is critical that $H^1_{\mathcal{F}^\pm}(F_{n,w}, A_{-s})$ is $\mathbb{H}^{-s,\pm}_{n,w}$ for every $w|p$ by Proposition 3.4.

https://doi.org/10.1017/S1446788713000165 Published online by Cambridge University Press

Define the following:

$$P_n = \prod_{w|l,l\in\Sigma} H^1(F_{n,w}, A_s), \quad L_n^{\pm} = \prod_{w|l,l\in\Sigma} H^1_{\mathcal{F}^{\pm}}(F_{n,w}, A_s),$$
$$P_n^* = \prod_{w|l,l\in\Sigma} H^1(F_{n,w}, T_{-s}), \quad U_n^{*,\pm} = \prod_{w|l,l\in\Sigma} H^1_{\mathcal{F}^{\pm}}(F_{n,w}, T_{-s}).$$

In particular, we let P and $L^{\pm}$ denote P_0 and $L_0^{\pm}$, and similarly P^* and $U^{*,\pm}$ denote P_0^* and $U_0^{*,\pm}$.

Definition 3.7. For maps

$$\gamma_n : H^1(F_\Sigma/F_n, A_s) \to P_n,$$
$$\gamma_n^* : H^1(F_\Sigma/F_n, T_{-s}) \to P_n^*,$$

induced by global-local maps, we let G_n be the image of γ_n, and G_n^* be the image of γ_n^*. Also, for the local conditions $L_n^{\pm}$ and $U_n^{*,\pm}$, we define

$$S^{\pm}_{A_s}(F_n) = \ker(H^1(F_\Sigma/F_n, A_s) \to P_n/L_n^{\pm}),$$
$$S^{\pm}_{T_{-s}}(F_n) = \ker(H^1(F_\Sigma/F_n, T_{-s}) \to P_n^*/U_n^{*,\pm}).$$

Proposition 3.8. *Assume that $S^{\pm}_{A_{-s}}(F_n)$ is finite. Then the map*

$$H^1(F_\Sigma/F_n, A_s) \to P_n/L_n^{\pm}$$

is surjective.

Proof. As in [2], the key technique is the duality of Poitou and Tate (see [2, Section 4], in particular the discussion before Proposition 4.13).

We note that there is a perfect bilinear pairing on $P_n \times P_n^*$ given by the Tate local pairing for each prime. By the duality theorems of Poitou and Tate, G_n and G_n^* are the orthogonal complements with respect to this pairing. On the other hand, $L_n^{\pm}$ and $U_n^{*,\pm}$ are the orthogonal complements by definition. Thus $P_n/G_nL_n^{\pm}$ is isomorphic to the Pontryagin dual of $G_n^* \cap U_n^{*,\pm}$.

For any prime w lying above some prime of Σ, $H^1_{\mathcal{F}^{\pm}}(F_{n,w}, A_s)$ is divisible, thus it follows that $H^1(F_{n,w}, T_{-s})_{\text{tors}}$ is contained in $H^1_{\mathcal{F}^{\pm}}(F_{n,w}, T_{-s})$. It follows in turn that

$$S^{\pm}_{T_{-s}}(F_n)_{\text{tors}} = H^1(F_\Sigma/F_n, T_{-s})_{\text{tors}}.$$

From the long exact sequence induced from $0 \to T_{-s} \to V_{-s} \to A_{-s} \to 0$, we see that $H^1(F_\Sigma/F_n, T_{-s})_{\text{tors}} = A_{-s}^{G_{F_n}}/(A_{-s}^{G_{F_n}})_{\text{div}}$, which is 0 from Proposition 3.2. Thus we obtain $S^{\pm}_{T_{-s}}(F_n)_{\text{tors}} = 0$.

It is easy to check that if $S^{\pm}_{A_{-s}}(F_n)$ is finite, then $S^{\pm}_{T_{-s}}(F_n)$ is finite. Since $S^{\pm}_{T_{-s}}(F_n)_{\text{tors}} = 0$, we obtain $S^{\pm}_{T_{-s}}(F_n) = 0$. Since $G_n^* \cap U_n^{*,\pm}$ is the image of $S^{\pm}_{T_{-s}}(F_n)$, we obtain $G_n^* \cap U_n^{*,\pm} = 0$ and consequently, $P_n/G_nL_n^{\pm} = 0$. □

https://doi.org/10.1017/S1446788713000165 Published online by Cambridge University Press

Recall $\mathbb{H}^{\pm}_w$ for a prime w of F_∞ above p, and $\mathbb{H}^{s,\pm}_{n,v}$ for a prime v of F_n above p in Definition 3.3. First, we prove a lemma analogous to the control theorem.

LEMMA 3.9. *For all but a finite number of integers s, the kernel and cokernel $S^{\pm}_{A_s}(F_n) \to S^{\pm}_{A_s}(F_\infty)^{\mathrm{Gal}(F_\infty/F_n)}$ are finite and bounded as n varies.*

PROOF. We study the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & S^{\pm}_{A_s}(F_n) & \longrightarrow & H^1(F_\Sigma/F_n, A_s) & \longrightarrow & P_n/L^{\pm}_n \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & S^{\pm}_{A_s}(F_\infty)^{\mathrm{Gal}(F_\infty/F_n)} & \longrightarrow & H^1(F_\Sigma/F_\infty, A_s)^{\mathrm{Gal}(F_\infty/F_n)} & \longrightarrow & P_\infty/L^{\pm}_\infty \end{array}$$

where

$$P_\infty = \prod_{w|l, l\in\Sigma} H^1(F_{\infty,w}, A_s),$$
$$L^{\pm}_\infty = \prod_{w|p} \mathbb{H}^{\pm}_w \otimes \kappa^s.$$

By the snake lemma (see [9, pages 157–159]), we only need to show that the kernel and cokernel of the middle vertical arrow and the kernel of the right arrow are finite and bounded.

By the Hochschild–Serre spectral sequence, we have an exact sequence

$$0 \to H^1(F_\infty/F_n, A_s^{\mathrm{Gal}(F_\Sigma/F_\infty)}) \to H^1(F_\Sigma/F_n, A_s) \to H^1(F_\Sigma/F_\infty, A_s)^{\mathrm{Gal}(F_\infty/F_n)} \to H^2(F_\infty/F_n, A_s^{\mathrm{Gal}(F_\Sigma/F_\infty)}),$$

and by Proposition 3.2, we have $A_s^{\mathrm{Gal}(F_\Sigma/F_\infty)} \cong A^{\mathrm{Gal}(F_\Sigma/F_\infty)} \otimes \kappa^s = 0$. Thus, the middle arrow has trivial kernel and cokernel for every n.

For a prime v of F_n above p and a prime w of F_∞ above v, the map $H^1(F_{n,v}, A_s)/\mathbb{H}^{s,\pm}_{n,v} \to H^1(F_{\infty,w}, A_s)/(\mathbb{H}^{\pm}_w \otimes \kappa^s)$ is injective by definition.

Lastly, for a prime v of F_n not above p and a prime w of F_∞ above v, the kernel of $H^1(F_{n,v}, A_s) \to H^1(F_{\infty,w}, A_s)$ is $H^1(F_{\infty,w}/F_{n,v}, A_s^{G_{F_{\infty,w}}})$ by the Hochschild–Serre spectral sequence. If v splits completely over F_∞, it is obviously trivial, so we may assume that v does not split completely. Then $\mathrm{Gal}(F_{\infty,w}/F_{n,v})$ is topologically generated by some element $\gamma_{n,v}$, hence $H^1(F_{\infty,w}/F_{n,v}, A_s^{G_{F_{\infty,w}}})$ is isomorphic to $B/(\gamma_{n,v}-1)B$ where $B = A_s^{G_{F_{\infty,w}}}$. Consider the exact sequence

$$0 \to A_s^{G_{F_{n,v}}} \to B \xrightarrow{\gamma_{n,v}-1} B \to B/(\gamma_{n,v}-1)B \to 0.$$

For all but a finite number of integers s, $A_s^{G_{F_{n,v}}}$ is finite for every n, thus $B/(\gamma_{n,v}-1)B$ is finite. In other words, B_{div} is contained in $(\gamma_{n,v}-1)B$. where B_{div} is the maximal divisible subgroup of B, and $B/(\gamma_{n,v}-1)B$ is bounded by B/B_{div}. Thus, our claim follows. □

https://doi.org/10.1017/S1446788713000165 Published online by Cambridge University Press

Then we have the following proposition.

Proposition 3.10. *If* $\mathrm{Sel}_p^{\pm}(E/F_\infty)$ *is* Λ*-cotorsion,*

$$H^1(F_\Sigma/F_\infty, A) \to \prod_{w|l, l\in\Sigma, l\nmid p} H^1(F_{\infty,w}, A) \times \prod_{w|p} \frac{H^1(F_{\infty,w}, A)}{\mathbb{H}_w^{\pm}} \tag{3.1}$$

is surjective.

Proof. If $\mathrm{Sel}_p^{\pm}(E/F_\infty)$ is Λ-cotorsion, for almost all s, $(\mathrm{Sel}_p^{\pm}(E/F_\infty)\otimes\kappa^s)^{\mathrm{Gal}(F_\infty/F_n)} = S_{A_s}^{\pm}(F_\infty)^{\mathrm{Gal}(F_\infty/F_n)}$ is finite for every n. Thus, by Lemma 3.9, for some s, $S_{A_s}^{\pm}(F_n)$ is finite for every n.

Fix s such that $S_{A_{-s}}^{\pm}(F_n)$ is finite for every n. Since we can identify A_s with A as G_{F_∞}-modules, our claim follows from Proposition 3.8. □

Before we proceed to the next step, we wish to mention the following corollary.

Corollary 3.11. *If* $\mathrm{Sel}_p^{-}(E/F_\infty)$ *or* $\mathrm{Sel}_p^{+}(E/F_\infty)$ *is* Λ*-cotorsion, then the* Λ*-corank of* $\mathrm{Sel}_p(E/F_\infty)$ *is* $[F:\mathbb{Q}]$.

Proof. By the local Euler characteristic computation we can check that $\prod_{w|l} H^1(F_{\infty,w}, A)$ for $l\neq p$ is Λ-cotorsion and that the Λ-corank of $\prod_{w|p} H^1(F_{\infty,w}, A)$ is $2[F:\mathbb{Q}]$. From Propositions 2.2 and 2.3, it follows that the Λ-corank of the right-hand side of the map (3.1) in Proposition 3.10 is $[F:\mathbb{Q}]$. Since p is supersingular, we have $E(F_{\infty,w})\otimes\mathbb{Q}_p/\mathbb{Z}_p = H^1(F_{\infty,w}, A)$. This fact has been studied in many papers (for example, [1]), but we will briefly sketch the proof. Let $\hat{E}$ be the formal group over $\mathbb{Z}_p$ associated to E. From [4, Theorem 1.3] and, to a lesser degree, from the main result of [3], it follows that the universal norm $\cap N_{F_{n,w}/F_w}\hat{E}(F_{n,w})$ is trivial, which, by the Tate local duality, implies that $E(F_{\infty,w})\otimes\mathbb{Q}_p/\mathbb{Z}_p = H^1(F_{\infty,w}, A)$ under the Kummer map. Thus from Proposition 3.10, our assertion follows. □

The next simple proposition is another ingredient in the proof of our claim.

Proposition 3.12. *If* $\mathrm{Sel}_p^{+}(E/F_\infty)$ *or* $\mathrm{Sel}_p^{-}(E/F_\infty)$ *is* Λ*-cotorsion, then* $H^2(F_\Sigma/F_\infty, A)$ *is* Λ*-cotorsion, and the* Λ*-corank of* $H^1(F_\Sigma/F_\infty, A)$ *is* $[F:\mathbb{Q}]$.

Proof. From the global Euler characteristic formula,

$$\mathrm{corank}_\Lambda\, H^1(F_\Sigma/F_\infty, A) = \mathrm{corank}_\Lambda\, H^2(F_\Sigma/F_\infty, A) + [F:\mathbb{Q}].$$

The Λ-corank of the right-hand side of the map (3.1) in Proposition 3.10 is $[F:\mathbb{Q}]$ for the reason mentioned in the proof of Corollary 3.11, thus by Proposition 3.10, the Λ-corank of $H^1(F_\Sigma/F_\infty, A)$ is $[F:\mathbb{Q}]$. Hence, our claim follows. □

We can say a little more.

Proposition 3.13 [2, Proposition 4.9]. *If* $H^2(F_\Sigma/F_\infty, A)$ *is* Λ*-cotorsion, then* $H^1(F_\Sigma/F_\infty, A)^\vee$ *has no nontrivial finite* Λ*-submodule and* $H^2(F_\Sigma/F_\infty, A) = 0$.

https://doi.org/10.1017/S1446788713000165 Published online by Cambridge University Press

PROOF. Although [2] assumes that the ordinary reduction throughout, the proof for this particular proposition can be carried out quite generally, and does not require the ordinary reduction assumption. □

We now prove our main result.

THEOREM 3.14. *Assume that* $\mathrm{Sel}_p^{\pm}(E/F_\infty)$ *is* Λ*-cotorsion. Then* $\mathrm{Sel}_p^{\pm}(E/F_\infty)$ *has no proper* Λ*-submodule of finite index.*

PROOF. As we saw in Lemma 3.9, we can choose s such that $H^1(F_\Sigma/F, A_s) \to P/L^{\pm}$ is surjective. Since Γ has cohomological dimension one, from the Hochschild–Serre spectral sequence it follows that

$$H^1(F_\Sigma/F, A_s) \to H^1(F_\Sigma/F_\infty, A_s)^\Gamma \tag{3.2}$$

is surjective. When $w \nmid p$, it similarly follows that

$$H^1(F_v, A_s) \to \Big(\prod_{w|v} H^1(F_{\infty,w}, A_s)\Big)^\Gamma$$

is surjective.

If a prime v of F lies above p, $(\prod_{w|v} \mathbb{H}_w^{s,\pm})^\vee \cong \Lambda^{[F_v:\mathbb{Q}_p]}$, thus $(\prod_{w|v} \mathbb{H}_w^{s,\pm})_\Gamma = 0$. Thus we have an exact sequence

$$0 \to \Big(\prod_{w|v} \mathbb{H}_w^{s,\pm}\Big)^\Gamma \to \Big(\prod_{w|v} H^1(F_{\infty,w}, A_s)\Big)^\Gamma \to \Big(\prod_{w|v} \frac{H^1(F_{\infty,w}, A_s)}{\mathbb{H}_w^{s,\pm}}\Big)^\Gamma \to 0. \tag{3.3}$$

Since $A_s^{G_{F_\infty}} = 0$, it easily follows from the Hochschild–Serre sequence that $H^1(F_v, A_s) \xrightarrow{\sim} (\prod_{w|v} H^1(F_{\infty,w}, A_s))^\Gamma$. Since $H^1_{\mathcal{F}^\pm}(F_v, A_s) = (\prod_{w|v} \mathbb{H}_w^{s,\pm})^\Gamma$ by definition, the surjectivity of

$$\frac{H^1(F_v, A_s)}{H^1_{\mathcal{F}^\pm}(F_v, A_s)} \to \Big(\prod_{w|v} \frac{H^1(F_{\infty,w}, A_s)}{\mathbb{H}_w^{s,\pm}}\Big)^\Gamma$$

follows from the sequence (3.3).

Thus it follows that

$$P/L^{\pm} \to (P_\infty/L_\infty^{\pm})^\Gamma$$

is surjective. Since $H^1(F_\Sigma/F, A_s) \to P/L^{\pm}$ and the map in (3.2) are surjective,

$$H^1(F_\Sigma/F_\infty, A_s)^\Gamma \to (P_\infty/L_\infty^{\pm})^\Gamma$$

is surjective.

The exact sequence from Proposition 3.10,

$$0 \to S_{A_s}^{\pm}(F_\infty) \to H^1(F_\Sigma/F_\infty, A_s) \to P_\infty/L_\infty^{\pm} \to 0,$$

induces the sequence

$$H^1(F_\Sigma/F_\infty, A_s)^\Gamma \to (P_\infty/L_\infty^{\pm})^\Gamma \to S_{A_s}^{\pm}(F_\infty)_\Gamma \to H^1(F_\Sigma/F_\infty, A_s)_\Gamma.$$

https://doi.org/10.1017/S1446788713000165 Published online by Cambridge University Press

Since the first map is surjective, $S^{\pm}_{A_s}(F_\infty)_\Gamma \to H^1(F_\Sigma/F_\infty, A_s)_\Gamma$ is injective. From Proposition 3.13 it follows that $H^1(F_\Sigma/F_\infty, A_s)_\Gamma = 0$. Thus $S^{\pm}_{A_s}(F_\infty)_\Gamma = 0$, and in turn, $\mathrm{Sel}^{\pm}_p(E/F_\infty)_\Gamma = 0$, which implies our claim. □

Now as an application, we will study the precise connection of the order of $\mathrm{Sel}_p(E/F)$ with the characteristic ideal of the Pontryagin dual of $\mathrm{Sel}^{\pm}_p(E/F_\infty)$.

Let c_v be the Tamagawa number for E at v, in other words, $c_v = [E(F_v) : E_0(F_v)]$ where $E_0(F_v)$ is the subgroup of local points which have nonsingular reduction at v. We have the following corollary.

Corollary 3.15. *Assume that* $\mathrm{Sel}_p(E/F)$ *is finite. Let* $(f^{\pm}) \subset \Lambda$ *be the characteristic ideal of* $\mathrm{Sel}^{\pm}_p(E/F_\infty)^\vee$. *Then*

$$|f^{\pm}(0)| \sim |\mathrm{Sel}_p(E/F)| \prod_{v:\ \textit{every prime}} c_v$$

where $\sim$ *means equality up to units.*

Proof. First, we note that our assumption implies that $\mathrm{Sel}^{\pm}_p(E/F_\infty)$ is Λ-cotorsion because the control theorem holds true for the plus/minus Selmer groups (see [8, Theorem 9.3] or [6, Proposition 4.28]). Let

$$\prod_{v\in\Sigma} \mathcal{P}_v = \prod_{v\in\Sigma} \frac{H^1(F_v, A)}{E(F_v)\otimes \mathbb{Q}_p/\mathbb{Z}_p},$$

$$\prod_{w|v, v\in\Sigma} \mathcal{P}^{\pm}_w = \prod_{w|v, v\in\Sigma, v\nmid p} \frac{H^1(F_{\infty,w}, A)}{E(F_{\infty,w})\otimes \mathbb{Q}_p/\mathbb{Z}_p} \prod_{w|p} \frac{H^1(F_{\infty,w}, A)}{\mathbb{H}^{\pm}_w}$$

(note that $E(K)\otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$ if K is a local field with residue characteristic prime to p).

From the definition of $\mathrm{Sel}^{\pm}_p(E/F_\infty)$ we have the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Sel}_p(E/F) & \longrightarrow & H^1(F_\Sigma/F, A) & \xrightarrow{a} & \prod \mathcal{P}_v \\ & & \downarrow & & \downarrow & & \downarrow \prod g_v \\ 0 & \longrightarrow & \mathrm{Sel}^{\pm}_p(E/F_\infty)^\Gamma & \longrightarrow & H^1(F_\Sigma/F_\infty, A)^\Gamma & \longrightarrow & (\prod \mathcal{P}^{\pm}_w)^\Gamma \end{array}$$

From the Hochschild–Serre spectral sequence, it follows that the middle vertical map is an isomorphism. If $v|p$, g_v is injective because $E(F_v)\otimes \mathbb{Q}_p/\mathbb{Z}_p = (\prod_{w|v} \mathbb{H}^{\pm}_w)^\Gamma$ (see the proof of [6, Proposition 4.28]). Since $\mathrm{Sel}_p(E/F)$ is finite, the map a in the diagram above is surjective by Proposition 3.8.

Thus we have

$$|\mathrm{Sel}^{\pm}_p(E/F_\infty)^\Gamma| \sim |\mathrm{Sel}_p(E/F)| \prod_{v\in\Sigma} |\ker(g_v)|.$$

https://doi.org/10.1017/S1446788713000165 Published online by Cambridge University Press

If $v|p$, g_v is injective as we mentioned, thus $|\ker(g_v)| = 1 = c_v$ (the last equality is because E has good reduction at v). For other primes $v \nmid p$, by [2, Lemma 3.3] and the discussion following it,

$$|\ker(g_v)| \sim c_v.$$

From [2, Lemma 4.2] we have

$$\begin{aligned} f^{\pm}(0) &\sim |\mathrm{Sel}_p^{\pm}(E/F_\infty)^{\Gamma}|/|\mathrm{Sel}_p^{\pm}(E/F_\infty)_{\Gamma}| \\ &= |\mathrm{Sel}_p^{\pm}(E/F_\infty)^{\Gamma}|. \end{aligned}$$

(The last equality is from Theorem 3.14.) Since $c_v = 1$ for $v \notin \Sigma$, our claim follows. □

Acknowledgements

This work was part of the author's PhD thesis at Stanford University. The author is grateful to Professor Karl Rubin and Professor Ralph Greenberg for suggesting this problem.

References

[1] J. Coates and R. Greenberg, 'Kummer theory for abelian varieties over local fields', *Invent. Math.* **124** (1996), 129–174.
[2] R. Greenberg, 'Iwasawa theory for elliptic curves', in: *Arithmetic Theory of Elliptic Curves (Cetraro, 1997)*, Lecture Notes in Mathematics, 1716 (Springer, Berlin, 1999), 51–144.
[3] M. Hazewinkel, 'On norm maps for one dimensional formal groups. I. The cyclotomic Γ-extension', *J. Algebra* **32** (1974), 89–108.
[4] M. Hazewinkel, 'On norm maps for one dimensional formal groups III', *Duke Math. J.* **44**(2) (1977), 305–314.
[5] A. Iovita and R. Pollack, 'Iwasawa theory of elliptic curves at supersingular primes over towers of extensions of number fields', *J. reine angew. Math.* **598** (2006), 71–103.
[6] B. D. Kim, 'The parity conjecture for elliptic curves at supersingular reduction primes', *Compositio Math.* **143** (2007), 47–72.
[7] B. D. Kim, 'The Iwasawa invariants of the plus/minus Selmer groups', *Asian J. Math.* **13**(2) (2009), 181–190.
[8] S. Kobayashi, 'Iwasawa theory for elliptic curves at supersingular primes', *Invent. Math.* **152**(1) (2003), 1–36.
[9] S. Lang, *Algebra*, 3rd edn (Springer, New York, 2002).
[10] B. Mazur, 'Rational points of abelian varieties with values in towers of number fields', *Invent. Math.* **18** (1972), 183–266.
[11] R. Pollack, 'On the p-adic L-function of a modular form at a supersingular prime', *Duke Math. J.* **118**(3) (2003), 523–558.
[12] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd edn. Graduate Texts in Mathematics, 106 (Springer, New York, 2009).

BYOUNG DU KIM, Victoria University of Wellington,
Wellington 6140, New Zealand
e-mail: bdkim@msor.vuw.ac.nz

https://doi.org/10.1017/S1446788713000165 Published online by Cambridge University Press