ASIAN J. MATH.
Vol. 13, No. 2, pp. 181–190, June 2009

THE IWASAWA INVARIANTS OF THE PLUS/MINUS SELMER GROUPS[*]

BYOUNG DU KIM[†]

Abstract. We study the Iwasawa μ- and λ-invariants of the non-primitive plus/minus Selmer groups of elliptic curves for supersingular primes. We prove that they are constant for a family of elliptic curves with the same residual representation if the μ-invariant of any of them is 0. As an application we find a family of elliptic curves whose plus/minus Selmer groups have arbitrarily large λ-invariants.

Key words. Elliptic curves, Iwasawa theory.

AMS subject classifications. 11G05

1. Introduction.

Fix a prime p and let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Greenberg and Vatsal found a way to produce elliptic curves with good ordinary reduction at p such that their Selmer groups over $\mathbb{Q}_\infty$ have arbitrarily large λ-invariants. On the other hand, when an elliptic curve E has good supersingular reduction at p, $\mathrm{Sel}_p(E/\mathbb{Q}_\infty)$ does not seem to have any property analogous to the ordinary reduction case. Instead, we should use the plus/minus Selmer group $\mathrm{Sel}_p^\pm(E/\mathbb{Q}_\infty)$ defined by Kobayashi. (To some extent the origin of this group dates back to Perrin-Riou and Rubin. See [8], [13], and [10].) The works of Kobayashi, Pollack, Iovita-Pollack, and the author ([8],[11], [4], [5], [6], and [7]) showed that the plus/minus Selmer group theory of elliptic curves for supersingular primes is analogous to the Selmer group theory of elliptic curves for ordinary primes.

In this paper we study the Iwasawa invariants of the plus/minus Selmer groups. To apply the plus/minus Selmer group theory, we ssume $a_p = 1 + p - |\tilde{E}(\mathbb{F}_p)|$ is 0. Assuming E has good reduction at p, $a_p = 0$ implies E has supersingular reduction at p, and conversely, if E has good supersingular reduction at p, $a_p = 0$ if $p > 3$ or E has complex multiplication. Let $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ and $\Lambda = \mathbb{Z}_p[[\Gamma]]$. Identify $\Lambda = \mathbb{Z}_p[[T]]$ by identifying $\gamma = T + 1$ for a topological generator γ of Γ. The Pontryagin dual $X_E^\pm(\mathbb{Q}_\infty)$ of $\mathrm{Sel}_p^\pm(E/\mathbb{Q}_\infty)$ is a Λ-torsion module ([8] theorem 1.3 for a non-CM elliptic curve, [12] for a CM elliptic curve), and has a pseudo-isomorphism

$$X_E^+(\mathbb{Q}_\infty) \sim (\oplus\Lambda/(f_i(T))^{a_i}) \oplus (\oplus\Lambda/(p^{\mu_j})),$$

$$X_E^-(\mathbb{Q}_\infty) \sim \left(\oplus\Lambda/(g_k(T))^{b_k}\right) \oplus \left(\oplus\Lambda/(p^{\mu_l'})\right),$$

where $f_i(T)$ and $g_k(T)$ are irreducible distinguished polynomials of Λ.

The Iwasawa invariants are defined by

$$\lambda^+ = \sum a_i \mathrm{deg}(f_i(T)), \quad \lambda^- = \sum b_k \mathrm{deg}(g_k(T)),$$

$$\mu^+ = \sum \mu_j, \quad \mu^- = \sum \mu_l'.$$

[*]Received July 31, 2008; accepted for publication November 12, 2008.

[†]Victoria University of Wellington, School of Mathematics, Wellington, 6140 New Zealand (bdkim @mcs.vuw.ac.nz).

Let E and E' be elliptic curves with $E[p] \cong E'[p]$ as $G_{\mathbb{Q}}$-modules. We show that we can relate the μ and λ-invariants of $X_E^{\pm}(\mathbb{Q}_\infty)$ with the μ and λ-invariants of $X_{E'}^{\pm}(\mathbb{Q}_\infty)$. In particular, we show that if the μ-invariant of $X_E^{\pm}(\mathbb{Q}_\infty)$ is 0, we can express the λ-invariant of $X_{E'}^{\pm}(\mathbb{Q}_\infty)$ in terms of the λ-invariant of $X_E^{\pm}(\mathbb{Q}_\infty)$ and the $\mathbb{Z}_p$-coranks of some local cohomology groups. As an application, we find elliptic curves whose plus/minus Selmer groups have arbitrarily large λ-invariants. The readers should also refer to the work of Greenberg and Vatsal for the Selmer group of an elliptic curve for the good ordinary reduction case (see [3]). Greenberg also explained his idea in other papers such as [2].

We explain our results more explicitly. Let Σ be any finite set of places including p, bad reduction primes, and infinite places. Following [8] we define

$$\operatorname{Sel}_p^{\pm}(E/\mathbb{Q}_\infty) := \ker\left(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty]) \to \prod_{w|l, l\in\Sigma} \frac{H^1(\mathbb{Q}_{\infty,w}, E[p^\infty])}{H^1_{\mathcal{F}^\pm}(\mathbb{Q}_{\infty,w}, E[p^\infty])}\right)$$

where

$$H^1_{\mathcal{F}^\pm}(\mathbb{Q}_{\infty,p}, E[p^\infty]) = E^{\pm}(\mathbb{Q}_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

and for $w \nmid p$

$$H^1_{\mathcal{F}^\pm}(\mathbb{Q}_{\infty,w}, E[p^\infty]) = E(\mathbb{Q}_{\infty,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p.$$

Now let Σ_0 be any subset of Σ that does not include p and ∞. We define the primitive plus/minus Selmer group by

$$\operatorname{Sel}_p^{\Sigma_0,\pm}(E/\mathbb{Q}_\infty) = \ker\left(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty]) \to \prod_{w|l, l\in\Sigma-\Sigma_0} \frac{H^1(\mathbb{Q}_{\infty,w}, E[p^\infty])}{H^1_{\mathcal{F}^\pm}(\mathbb{Q}_{\infty,w}, E[p^\infty])}\right).$$

Suppose $E[p] \cong E'[p]$ as $G_{\mathbb{Q}}$-modules, all the bad reduction primes of E and E' belong to Σ_0, and the μ-invariant of $X_E^{\pm}(\mathbb{Q}_\infty)$ is 0. We show that $\operatorname{Sel}_p^{\Sigma_0,\pm}(E/\mathbb{Q}_\infty)$ and $\operatorname{Sel}_p^{\Sigma_0,\pm}(E'/\mathbb{Q}_\infty)$ have the same $\mathbb{Z}_p$-coranks. Then, we will show that for a certain choice of E' and Σ_0, we can make the $\mathbb{Z}_p$-corank of $\operatorname{Sel}_p^{\Sigma_0,\pm}(E'/\mathbb{Q}_\infty)$ arbitrarily large but the $\mathbb{Z}_p$-corank of $\operatorname{Sel}_p^{\Sigma_0,\pm}(E'/\mathbb{Q}_\infty)/\operatorname{Sel}_p^{\pm}(E'/\mathbb{Q}_\infty)$ comparatively small such that $\operatorname{Sel}_p^{\pm}(E'/\mathbb{Q}_\infty)$ has an arbitrarily large $\mathbb{Z}_p$-corank.

It is our pleasure to thank Karl Rubin for many helpful discussions and Ralph Greenberg for bringing this problem to our attention.

2. Congruences and non-primitive Selmer groups. Throughout this paper we let $M^\vee$ denote the Pontryagin dual $\operatorname{Hom}(M, \mathbb{Q}_p/\mathbb{Z}_p)$.

Let E be an elliptic curve over $\mathbb{Q}$ and fix an odd prime p. We assume E has good supersingular reduction at p and $a_p = 1 + p - |\tilde{E}(\mathbb{F}_p)|$ is 0.

Let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and $\mathbb{Q}_n$ be its subfield such that $\operatorname{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$. Let $\mathbb{Q}_{n,p}$ denote the local field of $\mathbb{Q}_n$ at the unique prime above p. Let $\Gamma = \operatorname{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ and $\Lambda = \mathbb{Z}_p[[\Gamma]]$. Following [8] we define the following.

Definition 2.1 (Plus/Minus norm groups). *Let $\mathbb{Q}_{-1,p}$ be $\mathbb{Q}_p$. We define*

$$\begin{aligned} E^+(\mathbb{Q}_{n,p}) = \{x \in E(\mathbb{Q}_{n,p}) |\, &\operatorname{Tr}_{\mathbb{Q}_{n,p}/\mathbb{Q}_{m+1,p}}(x) \in E(\mathbb{Q}_{m,p}) \\ &\textit{for every } 0 \le m < n, m \textit{ even } \}, \end{aligned}$$

$$E^-(\mathbb{Q}_{n,p}) = \{x \in E(\mathbb{Q}_{n,p}) |\operatorname{Tr}_{\mathbb{Q}_{n,p}/\mathbb{Q}_{m+1,p}}(x) \in E(\mathbb{Q}_{m,p}) \\ \textit{for every } -1 \le m < n, m \textit{ odd } \}.$$

Let Σ be a finite set of places including ∞, p, and bad reduction primes and $\mathbb{Q}_\Sigma$ be the maximal extension of $\mathbb{Q}$ unramified outside Σ. For $l \in \Sigma$ with $l \neq p$, we define a conventional local condition

$$\mathcal{H}_l^\pm(\mathbb{Q}_\infty, E[p^\infty]) := \prod_{\eta|l} \frac{H^1(\mathbb{Q}_{\infty,\eta}, E[p^\infty])}{E(\mathbb{Q}_{\infty,\eta}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}.$$

Note that we have $E(\mathbb{Q}_{\infty,\eta}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$ because η is not above p. We will also let $\mathcal{H}_l(\mathbb{Q}_\infty, E[p^\infty])$ denote $\mathcal{H}_l^\pm(\mathbb{Q}_\infty, E[p^\infty])$ to emphasize $\mathcal{H}_l^+ = \mathcal{H}_l^-$ when $l \neq p$.

For p we let

$$\mathcal{H}_p^\pm(\mathbb{Q}_\infty, E[p^\infty]) := \frac{H^1(\mathbb{Q}_{\infty,p}, E[p^\infty])}{E^\pm(\mathbb{Q}_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}.$$

(Despite the notation, $\mathcal{H}_p^\pm(\mathbb{Q}_\infty, E[p^\infty])$ depends on more than just $E[p^\infty]$.) Also, for every prime l, we let

$$\mathcal{H}_l(\mathbb{Q}, E[p^\infty]) := \frac{H^1(\mathbb{Q}_l, E[p^\infty])}{E(\mathbb{Q}_l) \otimes \mathbb{Q}_p/\mathbb{Z}_p}.$$

Definition 2.2 (Selmer group).

$$\operatorname{Sel}_p(E/\mathbb{Q}) := \ker\left(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, E[p^\infty]) \to \prod_{l\in\Sigma} \mathcal{H}_l(\mathbb{Q}, E[p^\infty])\right).$$

Definition 2.3 (Plus/Minus Selmer group, [8] definition 1.1).

$$\operatorname{Sel}_p^\pm(E/\mathbb{Q}_\infty) := \ker\left(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty]) \to \prod_{l\in\Sigma} \mathcal{H}_l^\pm(\mathbb{Q}_\infty, E[p^\infty])\right).$$

We let $S^\pm_{E[p^\infty]}(\mathbb{Q}_\infty)$ *denote* $\operatorname{Sel}_p^\pm(E/\mathbb{Q}_\infty)$ *as well.*

In [7] we proved the following.

Proposition 2.4. *The map*

$$H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty]) \to \prod_{l\in\sum} \mathcal{H}_l^\pm(\mathbb{Q}_\infty, E[p^\infty])$$

is surjective.

Proof. This is [7] proposition 16 and the discussion following it. The proof involves the analogue of the Tate local duality for the local conditions derived from the plus/minus norm groups. Since this is crucial to this paper and [7] is not published yet, we will briefly sketch the proof for the readers.

Fix an isomorphism $\kappa : \Gamma \to 1+p\mathbb{Z}_p$ when we consider $1+p\mathbb{Z}_p$ as a multiplicative group. Let T denote the Tate module $T_p(E)$ and A denote $E[p^\infty]$. Let T_s and A_s denote $T \otimes (\kappa^s)$ and $A \otimes (\kappa^s)$ respectively for any $s \in \mathbb{Z}_p$.

Define

$$\mathbb{H}_{n,p}^{s,\pm} = (E^\pm(\mathbb{Q}_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \otimes \kappa^s)^{\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}_n)},$$

$$H^1_{\mathcal{F}^\pm}(\mathbb{Q}_{n,p}, A_s) = \mathbb{H}_{n,p}^{s,\pm} \subset H^1(\mathbb{Q}_{n,p}, A_s),$$

$$H^1_{\mathcal{F}^\pm}(\mathbb{Q}_{n,p}, T_s) = \varprojlim_k \mathbb{H}_{n,p}^{s,\pm}[p^k] \subset H^1(\mathbb{Q}_{n,p}, T_s).$$

By [7] proposition 14, $H^1_{\mathcal{F}^\pm}(\mathbb{Q}_{n,p}, A_s)$ is the exact annihilator of $H^1_{\mathcal{F}^\pm}(\mathbb{Q}_{n,p}, T_{-s})$ with respect to the Tate local pairing

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

The proof uses the technique similar to [5] proposition 3.15.

For a prime w of $\mathbb{Q}_n$ with $w \nmid p$, we simply let $H^1_{\mathcal{F}^\pm}(\mathbb{Q}_{n,w}, A_s) = 0$ and $H^1_{\mathcal{F}^\pm}(\mathbb{Q}_{n,w}, T_{-s})$ be its exact annihilator with respect to the Tate local pairing.

We let

$$P_n = \prod_{w|l, l\in\Sigma} H^1(\mathbb{Q}_{n,w}, A_s), \quad L_n^\pm = \prod_{w|l, l\in\Sigma} H^1_{\mathcal{F}^\pm}(\mathbb{Q}_{n,w}, A_s),$$

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

We define the following:

$$\gamma_n : H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, A_s) \to P_n,$$

$$\gamma_n^* : H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, T_{-s}) \to P_n^*,$$

$$G_n = \mathrm{im}(\gamma_n),$$

$$G_n^* = \mathrm{im}(\gamma_n^*),$$

$$S^\pm_{A_s}(\mathbb{Q}_n) = \ker(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, A_s) \to P_n/L_n^\pm),$$

$$S^\pm_{T_{-s}}(\mathbb{Q}_n) = \ker(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, T_{-s}) \to P_n^*/U_n^{*,\pm}).$$

Assume that $S^\pm_{A_{-s}}(\mathbb{Q}_n)$ is finite for every n. Since $\mathrm{Sel}_p^\pm(E/\mathbb{Q}_\infty)$ is Λ-cotorsion, there are infinitely many such numbers s. By the duality theorems of Poitou and Tate, G_n and G_n^* are orthogonal complements with respect to the pairing

$$P_n \times P_n^* \to \mathbb{Q}_p/\mathbb{Z}_p$$

given by the Tate local pairing for each prime.

Since $L_n^{\pm}$ and $U_n^{*,\pm}$ are the exact annihilator of each other with respect to the pairing above, $P_n/G_nL_n^{\pm}$ is isomorphic to the Pontryagin dual of $G_n^* \cap U_n^{*,\pm} = \gamma_n^*(S_{T_{-s}}^{\pm}(\mathbb{Q}_n))$.

Since $S_{A_{-s}}^{\pm}(\mathbb{Q}_n)$ is finite, $S_{T_{-s}}^{\pm}(\mathbb{Q}_n)$ is finite, thus $S_{T_{-s}}^{\pm}(\mathbb{Q}_n)$ is contained in $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, T_{-s})_{\text{torsion}}$. We can check the last group is isomorphic to $A_{-s}^{G_{\mathbb{Q}_n}}/(A_{-s}^{G_{\mathbb{Q}_n}})_{div}$ by considering the long exact sequence induced from $0 \to T_{-s} \to T_{-s} \otimes \mathbb{Q}_p \to A_{-s} \to 0$. Since $A_{-s}^{G_{\mathbb{Q}_{n,p}}} = 0$ ([8] proposition 8.7–also it can be proven using more general properties of formal groups), $P_n/G_nL_n^{\pm}$ is trivial.

By taking the direct limit over n, we can see

$$H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, A_s) \to P_\infty/L_\infty^{\pm}$$

is surjective. Since $A_s \cong A$ as $G_{\mathbb{Q}_\infty}$-modules, we have $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, A_s) \cong H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, A)$ and $P_\infty/L_\infty^{\pm} \cong \prod_{l\in\Sigma} \mathcal{H}_l^{\pm}(\mathbb{Q}_\infty, A)$, hence our claim follows. □

Now, let Σ_0 be any subset of Σ not including p and ∞. We define the primitive plus/minus Selmer group by

$$S_{E[p^\infty]}^{\Sigma_0,\pm}(\mathbb{Q}_\infty) = \ker\left(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty]) \to \prod_{l\in\Sigma-\Sigma_0} \mathcal{H}_l^{\pm}(\mathbb{Q}_\infty, E[p^\infty])\right).$$

From proposition 2.4 we obtain the following.

Corollary 2.5.

$$S_{E[p^\infty]}^{\Sigma_0,\pm}(\mathbb{Q}_\infty)/S_{E[p^\infty]}^{\pm}(\mathbb{Q}_\infty) \cong \prod_{l\in\Sigma_0} \mathcal{H}_l(\mathbb{Q}_\infty, E[p^\infty]).$$

Here we refer to Greenberg's computation of the $\mathbb{Z}_p$-corank of $\mathcal{H}_l(\mathbb{Q}_\infty, E[p^\infty])$.

Proposition 2.6 ([3] proposition 2.4). *Let T_p be the p-adic Tate module of E and V_p be $T_p \otimes \mathbb{Q}_p$. Let $I_l \subset G_{\mathbb{Q}_l}$ denote the inertia group of l. Let $P_l(X) = \det((1 - Frob_l X)|_{(V_p)_{I_l}}) \in \mathbb{Z}_p[X]$ where $(V_p)_{I_l}$ is the maximal quotient of V_p on which I_l acts trivially.*

Then the μ-invariant of $\mathcal{H}_l(\mathbb{Q}_\infty, E[p^\infty])^\vee$ is 0 and its λ-invariant (i.e., $\mathbb{Z}_p$-corank) is $s_l d_l$ where s_l is the maximal power of p satisfying $(l^{p-1}-1)/p \equiv 0 \pmod{s_l}$ and d_l is the multiplicity of $X = \tilde{l}^{-1}$ as a root of $\tilde{P}_l(X) \in \mathbb{Z}/p\mathbb{Z}[X]$.

Let $l (\neq p)$ be a good reduction prime such that $Frob_l$ acts trivially on the residual representation $E[p]$. Then $l^{-1} \equiv 1 \pmod{p}$ is a double root of $\tilde{P}(X) = X^2 - 2X + 1$, and the $\mathbb{Z}_p$-corank of $\mathcal{H}_l(\mathbb{Q}_\infty, E[p^\infty])$ is $2s_l$.

Now, we will define a "plus/minus primitive Selmer" group on $E[p]$. For $l \neq p$ we let

$$\mathcal{H}_l^{\pm}(\mathbb{Q}_\infty, E[p]) = \prod_{\eta|l} H^1(\mathbb{Q}_{\infty,\eta}, E[p])/H_{un}^1(\mathbb{Q}_{\infty,\eta}, E[p]).$$

We also let $\mathcal{H}_l$ denote $\mathcal{H}_l^{\pm}$ when $l \neq p$ to emphasize $\mathcal{H}_l^+ = \mathcal{H}_l^-$. For $l = p$ we let

$$\mathcal{H}_p^{\pm}(\mathbb{Q}_\infty, E[p]) = H^1(\mathbb{Q}_{\infty,p}, E[p])/\left(E^{\pm}(\mathbb{Q}_{\infty,p})/pE^{\pm}(\mathbb{Q}_{\infty,p})\right).$$

Definition 2.7.

$$S^{\Sigma_0,\pm}_{E[p]}(\mathbb{Q}_\infty) = \ker(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p]) \to \prod_{l\in\Sigma-\Sigma_0} \mathcal{H}^\pm_l(\mathbb{Q}_\infty, E[p])).$$

Let $E'/\mathbb{Q}$ be an elliptic curve with $E[p] \cong E'[p]$ as $G_\mathbb{Q}$-modules. Assume Σ contains all the bad reduction primes of E and E'. We will show $S^{\Sigma_0,\pm}_{E[p]}(\mathbb{Q}_\infty) \cong S^{\Sigma_0,\pm}_{E'[p]}(\mathbb{Q}_\infty)$.

An isomorphism $\rho : E[p] \to E'[p]$ naturally induces $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p]) \overset{\sim}{\to} H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E'[p])$ and $\mathcal{H}_l(\mathbb{Q}_\infty, E[p]) \overset{\sim}{\to} \mathcal{H}_l(\mathbb{Q}_\infty, E'[p])$ for $l \neq p$. Thus we need to show the isomorphism $\rho : H^1(\mathbb{Q}_{\infty,p}, E[p]) \to H^1(\mathbb{Q}_{\infty,p}, E'[p])$ induces an isomorphism $E^\pm(\mathbb{Q}_{\infty,p})/pE^\pm(\mathbb{Q}_{\infty,p}) \overset{\sim}{\to} E'^\pm(\mathbb{Q}_{\infty,p})/pE'^\pm(\mathbb{Q}_{\infty,p})$.

Let $\hat{E}$ and $\hat{E}'$ be the formal groups over $\mathbb{Z}$ associated to E and E'. As mentioned in [8] theorem 8.4, $\hat{E}$ and $\hat{E}'$ have the same Honda type $X^2 + p$, thus there is an isomorphism of formal groups $\lambda : \hat{E} \to \hat{E}'$ over $\mathbb{Z}_p$. Since ρ induces an isomorphism $\rho : \hat{E}[p] \to \hat{E}'[p]$, there is an isomorphism $\lambda^{-1} \circ \rho : \hat{E}[p] \to \hat{E}[p]$. We will show this map is given by multiplication by a scalar of $\mathbb{F}_p^\times$.

Proposition 2.8. *The only $G_{\mathbb{Q}_p}$-equivariant maps in* $\mathrm{Aut}(E[p])$ *are the ones given by multiplication by scalars of* $\mathbb{F}_p^\times$.

Proof. Since $\hat{E}$ is a Lubin-Tate group of height 2 over O_p where O_p is the ring of integers of the unramified quadratic extension K_p of $\mathbb{Q}_p$ ([8] proposition 8.6), we can identify $E[p]$ with O_p/pO_p such that the Artin map $[\alpha, K_p]$ for any $\alpha \in O_p^\times$ acts on $E[p]$ as multiplication by α^{-1}. Thus the image of $[O_p^\times, K_p]$ in $\mathrm{Aut}(E[p])$ is a non-split Cartan group of $GL_2(\mathbb{F}_p)$ when we identify $\mathrm{Aut}(E[p]) \cong GL_2(\mathbb{F}_p)$ ([9] Chapter XVIII section 12, p. 712, lemma 12.2). We let B denote the image of $[O_p^\times, K_p]$ in $\mathrm{Aut}(E[p])$.

Let $\tau \in G_{\mathbb{Q}_p}$ be a lifting of the non-trivial element of $\mathrm{Gal}(K_p/\mathbb{Q}_p)$. Since $\tau[\alpha, K_p]\tau^{-1} = [\alpha^\tau, K_p]$ for $\alpha \in O_p^\times$, the image of τ in $\mathrm{Aut}(E[p])$ is not commutative with B. Since a non-split Cartan group has index 2 in its normalizer ([9] Chap.XVIII sec.12, p. 713, proposition 12.1), the image of $G_{\mathbb{Q}_p}$ in $\mathrm{Aut}(E[p])$ is the normalizer of B. We let C denote the image of $G_{\mathbb{Q}_p}$ in $\mathrm{Aut}(E[p])$.

It is easy to see that an element of $GL_2(\mathbb{F}_p)$ commutes with C if and only if it is given by multiplication by a scalar of $\mathbb{F}_p^\times$. Thus our claim follows. □

Thus it follows that ρ is equal to $\lambda \circ \mu$ for some scalar multiplication μ (*i.e.*, $\mu(x) = \alpha \cdot x$ for some $\alpha \in \mathbb{F}_p^\times$). Hence $\rho : H^1(\mathbb{Q}_{\infty,p}, E[p]) \to H^1(\mathbb{Q}_{\infty,p}, E'[p])$ induces an isomorphism

$$E^\pm(\mathbb{Q}_{\infty,p})/pE^\pm(\mathbb{Q}_{\infty,p}) \xrightarrow{\mu} E^\pm(\mathbb{Q}_{\infty,p})/pE^\pm(\mathbb{Q}_{\infty,p}) \xrightarrow{\lambda} E'^\pm(\mathbb{Q}_{\infty,p})/pE'^\pm(\mathbb{Q}_{\infty,p}).$$

Thus we have the following.

Proposition 2.9.

$$S^{\Sigma_0,\pm}_{E[p]}(\mathbb{Q}_\infty) \cong S^{\Sigma_0,\pm}_{E'[p]}(\mathbb{Q}_\infty).$$

From now on, assume Σ_0 includes all the bad reduction primes of E and E'.

Proposition 2.10. *We have*

$$S^{\Sigma_0,\pm}_{E[p]}(\mathbb{Q}_\infty) \cong S^{\Sigma_0,\pm}_{E[p^\infty]}(\mathbb{Q}_\infty)[p]$$

Proof. We consider the following diagram.

$$\begin{tikzcd}
0 \arrow[r] & S^{\Sigma_0,\pm}_{E[p]}(\mathbb{Q}_\infty) \arrow[r] \arrow[d] & H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p]) \arrow[r] \arrow[d] & \prod_{\Sigma-\Sigma_0} \mathcal{H}^\pm_l(\mathbb{Q}_\infty, E[p]) \arrow[d] \\
0 \arrow[r] & S^{\Sigma_0,\pm}_{E[p^\infty]}(\mathbb{Q}_\infty)[p] \arrow[r] & H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty])[p] \arrow[r] & \prod_{\Sigma-\Sigma_0} \mathcal{H}^\pm_l(\mathbb{Q}_\infty, E[p^\infty]).
\end{tikzcd}$$

The short exact sequence $0 \to E[p] \to E[p^\infty] \to E[p^\infty] \to 0$ induces

$$\begin{aligned}
&E[p^\infty]^{\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)}/pE[p^\infty]^{\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)} \\
&\to H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p]) \to H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty])[p] \to 0.
\end{aligned}$$

Since $E[p^\infty]^{G_{\mathbb{Q}_{\infty,p}}} = 0$ ([8] proposition 8.7), $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p]) \to H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty])[p]$ is an isomorphism.

Similarly it follows that $H^1(\mathbb{Q}_{\infty,p}, E[p]) \to H^1(\mathbb{Q}_{\infty,p}, E[p^\infty])[p]$ is an isomorphism. Since $E^\pm(\mathbb{Q}_{\infty,p})$ is torsion-free, we have $(E^\pm(\mathbb{Q}_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)[p] = E^\pm(\mathbb{Q}_{\infty,p})/pE^\pm(\mathbb{Q}_{\infty,p})$. Note that $E^\pm(\mathbb{Q}_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(\mathbb{Q}_{\infty,p}, E[p^\infty])$ is injective ([8] lemma 8.17). Combining them it follows that

$$\mathcal{H}^\pm_p(\mathbb{Q}_{\infty,p}, E[p]) \to \mathcal{H}^\pm_p(\mathbb{Q}_{\infty,p}, E[p^\infty])[p]$$

is an isomorphism.

For $l \in \Sigma - \Sigma_0$ with $l \neq p$, since l is a good reduction prime, $\mathcal{H}^\pm_l(\mathbb{Q}_\infty, E[p]) \to \mathcal{H}^\pm_l(\mathbb{Q}_\infty, E[p^\infty])$ is injective. (See [3] proposition 2.8.) By the Snake Lemma our claim follows. □

Proposition 2.11. *$S^{\Sigma_0,\pm}_{E[p^\infty]}(\mathbb{Q}_\infty)$ has no proper Λ-submodule of finite index.*

Proof. Without loss of generality we assume $\Sigma = \Sigma_0 \cup \{p, \infty\}$. By proposition 2.4 we have

$$H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty])/S^{\Sigma_0,\pm}_{E[p^\infty]}(\mathbb{Q}_\infty) \cong \mathcal{H}^\pm_p(\mathbb{Q}_\infty, E[p^\infty]).$$

Since $H^1(\mathbb{Q}_{\infty,p}, E[p^\infty])^\vee \cong \Lambda^2$ and $(E^\pm(\mathbb{Q}_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee \cong \Lambda$ ([8] propositions 8.23 and 24), $\mathcal{H}^\pm_p(\mathbb{Q}_\infty, E[p^\infty])^\vee$ is projective, thus free because Λ is a local ring. Its Λ-rank is obviously 1, thus $\mathcal{H}^\pm_p(\mathbb{Q}_\infty, E[p^\infty])^\vee \cong \Lambda$.

From [7] proposition 20 (which easily follows from proposition 2.4) and proposition 23 (which is just a restatement of [2] proposition 4.9) it follows that $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty])$ has no proper Λ-submodule of finite index. Thus our claim follows from the following lemma of Greenberg. □

Lemma 2.12 ([1], p. 123, also [3] lemma 2.6). *Let Y be a finitely generated Λ-module and Z a free Λ-submodule. If Y contains no nonzero finite Λ-submodule, then the same is true for Y/Z.*

Corollary 2.13. *The μ-invariant of $\mathrm{Sel}^\pm_p(E/\mathbb{Q}_\infty)^\vee$ is 0 if and only if that of $\mathrm{Sel}^\pm_p(E'/\mathbb{Q}_\infty)^\vee$ is 0. Assuming either, the λ-invariants of $S^{\Sigma_0,\pm}_{E[p^\infty]}(\mathbb{Q}_\infty)^\vee$ and $S^{\Sigma_0,\pm}_{E'[p^\infty]}(\mathbb{Q}_\infty)^\vee$ are equal.*

Proof. We make the following observation: Let M be a finitely generated Λ module which is a free $\mathbb{Z}_p$-module. Then the λ-invariant of M is equal to the $\mathbb{Z}_p$-rank of M, which is also equal to the length of M/pM.

The first claim follows from propositions 2.9 and 2.10. The second claim follows from propositions 2.9, 2.10, and 2.11 combined with our observation. □

3. Arbitrarily large λ-invariants. Finally we will discuss how to find an elliptic curve $E'/\mathbb{Q}$ with a large λ-invariant for its plus/minus Selmer group.

Lemma 3.1. *Assume E and E' are elliptic curves defined over $\mathbb{Q}$ with $E[p] \cong E'[p]$. Let l be a prime not equal to p.*

1. *If E and E' both have good reduction at l, $\mathrm{corank}_{\mathbb{Z}_p} \mathcal{H}_l(\mathbb{Q}_\infty, E[p^\infty]) = \mathrm{corank}_{\mathbb{Z}_p} \mathcal{H}_l(\mathbb{Q}_\infty, E'[p^\infty])$.*
2. *If E has good reduction at l and E' has bad reduction at l, $\mathrm{corank}_{\mathbb{Z}_p} \mathcal{H}_l(\mathbb{Q}_\infty, E[p^\infty]) \geq \mathrm{corank}_{\mathbb{Z}_p} \mathcal{H}_l(\mathbb{Q}_\infty, E'[p^\infty])$.*
3. *If E has good reduction at l and $Frob_l$ acts trivially on $E[p]$ and E' has bad reduction at l, $\mathrm{corank}_{\mathbb{Z}_p} \mathcal{H}_l(\mathbb{Q}_\infty, E[p^\infty]) - \mathrm{corank}_{\mathbb{Z}_p} \mathcal{H}_l(\mathbb{Q}_\infty, E'[p^\infty]) \geq s_l$ for s_l mentioned in proposition 2.6.*

Proof. Case 1) Proposition 2.6 implies that $\mathrm{corank}_{\mathbb{Z}_p} \mathcal{H}_l(\mathbb{Q}_\infty, E[p^\infty])$ depends only on the action of $Frob_l$ on $E[p]$. Thus $\mathrm{corank}_{\mathbb{Z}_p} \mathcal{H}_l(\mathbb{Q}_\infty, E[p^\infty]) = \mathrm{corank}_{\mathbb{Z}_p} \mathcal{H}_l(\mathbb{Q}_\infty, E'[p^\infty])$.

Case 2) We note that $V_p(E')_{I_l} \cong \mathrm{Hom}(V_p(E')^{I_l}, \mathbb{Q}_p(1))$ by Weil pairing. Let $\bar{T}_1 = \mathrm{Hom}(T_p(E')/pT_p(E'), \mu_p) \cong E'[p]$ and $\bar{T}_2 = \mathrm{Hom}(T_p(E')^{I_l}/pT_p(E')^{I_l}, \mu_p)$. Then there is a short exact sequence $0 \to \bar{T}_3 \to \bar{T}_1 \to \bar{T}_2 \to 0$ for some $\mathbb{F}_p$-module $\bar{T}_3$. Then

$$det((1 - Frob_l X)|_{\bar{T}_1}) = det((1 - Frob_l X)|_{\bar{T}_2}) \cdot det((1 - Frob_l X)|_{\bar{T}_3}).$$

(We note that although E' has bad reduction at l, the $Frob_l$-action on $\bar{T}_1$ makes sense because $E'[p] \cong E[p]$.) Thus we can see the multiplicity of $X = \tilde{l}^{-1}$ as a root of $det((1 - Frob_l X)|_{V_p(E)}) \in \mathbb{F}_p[X]$ (when we consider it as a polynomial of $\mathbb{F}_p[X]$) is greater than or equal to the multiplicity of $X = \tilde{l}^{-1}$ as a root of $det((1 - Frob_l X)|_{V_p(E')_{I_l}}) \in \mathbb{F}_p[X]$. Combined with corollary 2.5 it implies

$$\mathrm{corank}_{\mathbb{Z}_p} \mathcal{H}_l(\mathbb{Q}_\infty, E[p^\infty]) \geq \mathrm{corank}_{\mathbb{Z}_p} \mathcal{H}_l(\mathbb{Q}_\infty, E'[p^\infty]).$$

Case 3) As discussed after proposition 2.6, $\mathrm{corank}_{\mathbb{Z}_p} \mathcal{H}_l(\mathbb{Q}_\infty, E[p^\infty]) = 2s_l$. Since the dimension of $V_p(E')_{I_l}$ is less than or equal to 1, $\mathrm{corank}_{\mathbb{Z}_p} \mathcal{H}_l(\mathbb{Q}_\infty, E'[p^\infty]) \leq s_l$. □

We will fix an elliptic curve $E/\mathbb{Q}$ such that the μ-invariant of $\mathrm{Sel}_p^{\pm}(E/\mathbb{Q}_\infty)^\vee$ is 0 with a given family of elliptic curves $E_t/\mathbb{Q}$ parametrized by $t \in \mathbb{Q}$ such that $E[p] \cong E_t[p]$. Note that from corollary 2.5 we have

$$\mathrm{corank}_{\mathbb{Z}_p} S^{\Sigma_0, \pm}_{E_t[p^\infty]}(\mathbb{Q}_\infty) = \mathrm{corank}_{\mathbb{Z}_p} S^{\pm}_{E_t[p^\infty]}(\mathbb{Q}_\infty) + \sum_{l \in \Sigma_0} \mathrm{corank}_{\mathbb{Z}_p} \mathcal{H}_l(\mathbb{Q}_\infty, E_t[p^\infty]).$$

Choose t such that E_t has bad reduction at many primes whose Frobenius maps act trivially on $E[p]$. Then by corollary 2.13 and lemma 3.1 the λ-invariant of $\mathrm{Sel}_p^{\pm}(E_t/\mathbb{Q}_\infty)$ will be large.

Let $E : Y^2 = X^3 - X$ and fix $p = 3$. The method should work quite generally, but this elliptic curve and $p = 3$ are particularly easy to deal with.

Proposition 3.2. $\mathrm{Sel}_p^{\pm}(E/\mathbb{Q}_\infty) = 0$.

Proof. First, $\mathrm{Sel}_p(E/\mathbb{Q}) = 0$ by [15] section 12.3, which uses the main conjecture of Iwasawa theory for imaginary quadratic fields proven in [14]. (In fact, Rubin proved $\mathrm{Sel}_q(E/\mathbb{Q}) = 0$ for every prime q, and also proved the full version of the Birch and Swinnerton-Dyer conjecture for this E.)

We will show $\iota^{\pm} : \mathrm{Sel}_p(E/\mathbb{Q}) \to \mathrm{Sel}_p^{\pm}(E/\mathbb{Q}_\infty)^{\Gamma}$ has trivial kernel and cokernel similar to [7] corollary 26.

We consider the following diagram.

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}_p(E/\mathbb{Q}) \arrow[r] \arrow[d] & H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, E[p^\infty]) \arrow[r] \arrow[d] & \prod_{l\in\Sigma} \mathcal{H}_l(\mathbb{Q}, E[p^\infty]) \arrow[d, "\prod g_l^{\pm}"] \\
0 \arrow[r] & \mathrm{Sel}_p^{\pm}(E/\mathbb{Q}_\infty)^{\Gamma} \arrow[r] & H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty])^{\Gamma} \arrow[r] & \prod_{l\in\Sigma} \mathcal{H}_l^{\pm}(\mathbb{Q}_\infty, E[p^\infty]).
\end{tikzcd}$$

Since $E[p^\infty]^{\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)} = 0$ as mentioned before, by Hochschild-Serre spectral sequence the middle vertical map is an isomorphism. Thus the kernel of $\iota^{\pm}$ is trivial, and the cokernel of $\iota^{\pm}$ is also trivial if the kernel of $\prod_{l\in\Sigma} g_l^{\pm}$ is trivial. It is proven in the proof of [5] proposition 4.28 that $g_p^{\pm}$ is injective. If $l \neq p$, by [2] lemma 3.3 and the discussion following that we have

$$|\ker(g_l^{\pm})| = c_l^{(p)}$$

where $c_l^{(p)}$ is the biggest p-power divisor of the Tamagawa number c_l. The Tamagawa number c_l is 1 for all primes except $l = 2$, for which the Tamagawa number is 4. Hence, $\iota^{\pm}$ is an isomorphism.

By Nakayama lemma, $\mathrm{Sel}_p^{\pm}(E/\mathbb{Q}_\infty) = 0$. □

In [16] Rubin and Silverberg discuss a general method to generate a family of elliptic curves $E_t/\mathbb{Q}$ parametrized by rational numbers t such that $E_t[p] \cong E[p]$ as $G_{\mathbb{Q}}$-modules. For $E : Y^2 = X^3 - DX$ for a nonzero integer D, they explicitly described this family in [16] theorem 4.4:

$$Y^2 = X^3 + D(27D^2t^4 - 18Dt^2 - 1)X + 4D^2t(27D^2t^4 + 1).$$

In particular, if D is prime to 3 and $t \in \mathbb{Q}$ is integral at 3, then E_t has good reduction at 3. The curve E has CM by $\mathbb{Q}(\sqrt{-1})$ thus $p = 3$ is a good supersingular prime and $a_p = 1 + p - |\tilde{E}(\mathbb{F}_p)| = 0$. If $3|t$, $E_t = E$ modulo $p = 3$, thus $a_p(E_t) = 1 + p - |\tilde{E}_t(\mathbb{F}_p)| = 0$ as well.

Let $D = 1$. The discriminant of E_t is

$$\Delta(E_t) = -2^6(27t^4 + 18t^2 - 1)^3.$$

Let $f(t) = 27t^4 + 18t^2 - 1$. We can directly verify $f(t)$ is prime to $f'(t)$. Thus $f(t)$ is prime to $f'(t)$ modulo l for all but finitely many primes l. Let $\mathcal{A}$ be the set of primes l $(l \neq 2, 3)$ such that $f(t)$ and $f'(t)$ are prime to each other modulo l.

Let k be any positive integer. Let L be a field of $\mathbb{Q}$ adjoined by the coordinates of $E[p]$ and the roots of $f(t)$. By Chebotarev theorem there are primes $l_1, \ldots, l_k \in \mathcal{A}$ that split completely over $L/\mathbb{Q}$. Then $Frob_{l_i}$ acts trivially on $E[p]$ for each l_i and there is an integer t_0 such that $f(t_0) \equiv 0 \pmod{l_i}$, and $f'(t_0) \not\equiv 0 \pmod{l_i}$ for each l_i. Thus we can write

$$f(t_0 + X) = \cdots + a_1X + a_0$$

with $a_0 \equiv 0 \pmod{l_1 \cdot \cdots \cdot l_k}$ and $a_1 \not\equiv 0 \pmod{l_i}$ for each l_i.

If $v_{l_i}(a_0) = 1$, let $b_i = l_i^2$. If $v_{l_i}(a_0) > 1$, let $b_i = l_i$. Let $t = t_0 + \alpha \prod b_i$ where $\alpha = 1, 2$, or 3 such that $t \equiv 0 \pmod 3$. Then we have $v_{l_i}(f(t)) = 1$ for each i, thus $v_{l_i}(\Delta(E_t)) = 3$. Thus the minimal model of E_t has bad reduction at each l_i.

By lemma 3.1 the λ-invariant of $\mathrm{Sel}_p^{\pm}(E_t/\mathbb{Q}_\infty)^\vee$ is greater than or equal to k. By taking an arbitrarily large k we can find E_t such that the λ-invariant of its plus/minus Selmer group is also arbitrarily large.

Remark 3.3. *We might note the following as well: Let E_1 and E_2 be elliptic curves over $\mathbb{Q}$ with supersingular reduction at the prime p with $a_p(E_i) = 0$ for $i = 1, 2$. Assume $E_1[p] \cong E_2[p]$. Let $\lambda_i^{\pm}$ be the λ-invariant of $\mathrm{Sel}_p^{\pm}(E_i/\mathbb{Q}_\infty)^\vee$ for $i = 1, 2$. Then $\lambda_1^+ - \lambda_1^- = \lambda_2^+ - \lambda_2^-$. In particular, $\lambda^+(E_t) - \lambda^-(E_t)$ for E_t above is constant for varying t.*

REFERENCES

[1] R. Greenberg, *Iwasawa theory for p-adic representations,* Advanced Studies in Pure Math., 17 (1989), pp. 97–137.

[2] R. Greenberg, *Iwasawa theory for elliptic curves.* Arithmetic theory of elliptic curves (Cetraro, 1997), pp. 51–144, Lecture Notes in Math., 1716, Springer, Berlin, 1999.

[3] R. Greenberg and V. Vatsal, *On the Iwasawa invariants of elliptic curves*, Invent. Math., 142:1 (2000), pp. 17–63.

[4] A. Iovita and R. Pollack, *Iwasawa theory of elliptic curves at supersingular primes over Z_p-extensions of number fields,* Journal fur die Reine und Angewandte Mathematik, 598 (2006), pp. 71–103.

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

[6] B. Kim, *The algebraic functional equation of an elliptic curve at supersingular primes,* Mathematical Research Letter, 15:1 (2008).

[7] B. Kim, *The plus/minus Selmer groups for supersingular primes and the Selmer groups,* submitted.

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

[9] S. Lang, *Algebra, Second edition,* Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1984.

[10] B. Perrin-Riou, *Théorie d'Iwasawa p-adique locale et globale,* Invent. Math., 99:2 (1990), pp. 247–292.

[11] R. Pollack, *On the p-adic L-function of a modular form at a supersingular prime,* Duke Mathematical Journal, 118:3 (2003) pp. 523–558.

[12] R. Pollack and K. Rubin, *The main conjecture for CM elliptic curves at supersingular primes,* Ann. of Math. (2), 159:1 (2004), pp. 447–464.

[13] K. Rubin, *Local units, elliptic units, Heegner points and elliptic curves,* Invent. Math., 88:2 (1987), pp. 405–422.

[14] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields,* Invent. Math., 103 (1991), pp. 25–68.

[15] K. Rubin, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, pp. 167–234, Arithmetic theory of elliptic curves. Edited by C. Viola. Lecture Notes in Mathematics, 1716. Springer-Verlag, Berlin.

[16] K. Rubin and A. Silverberg, *Families of elliptic curves with constant mod p representations,* Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), pp. 148–161, Int. Press, Cambridge, MA, 1995.