J. Korean Math. Soc. **58** (2021), No. 1, pp. 123–132
https://doi.org/10.4134/JKMS.j190867
pISSN: 0304-9914 / eISSN: 2234-3008

RESTRICTION OF SCALARS AND CUBIC TWISTS OF ELLIPTIC CURVES

Dongho Byeon, Keunyoung Jeong, and Nayoung Kim

Abstract. Let K be a number field and L a finite abelian extension of K. Let E be an elliptic curve defined over K. The restriction of scalars $\mathrm{Res}_K^L E$ decomposes (up to isogeny) into abelian varieties over K

$$\mathrm{Res}_K^L E \sim \bigoplus_{F \in S} A_F,$$

where S is the set of cyclic extensions of K in L. It is known that if L is a quadratic extension, then A_L is the quadratic twist of E. In this paper, we consider the case that K is a number field containing a primitive third root of unity, $L = K(\sqrt[3]{D})$ is the cyclic cubic extension of K for some $D \in K^\times/(K^\times)^3$, $E = E_a : y^2 = x^3 + a$ is an elliptic curve with j-invariant 0 defined over K, and $E_a^D : y^2 = x^3 + aD^2$ is the cubic twist of E_a. In this case, we prove A_L is isogenous over K to $E_a^D \times E_a^{D^2}$ and a property of the Selmer rank of A_L, which is a cubic analogue of a theorem of Mazur and Rubin on quadratic twists.

1. Introduction

Let K be a number field and L a finite abelian extension of K. Let E be an elliptic curve defined over K. The restriction of scalars $\mathrm{Res}_K^L E$ (for the definition, see §2) of E from L to K decomposes (up to isogeny) into abelian varieties over K

$$\mathrm{Res}_K^L E \sim \bigoplus_{F \in S} A_F,$$

where S is the set of cyclic extensions of K in L (for details, see §2 or [1, §3]).

In [1], Mazur and Rubin studied the Selmer rank of E/L by using the Selmer ranks of A_F. In [2], as an application to the simplest case that L is a quadratic extension, they obtained many remarkable results on the Selmer rank of E/L. We note that if L is a quadratic extension, then A_L is the quadratic twist of E (for an example of the proof, see [4, §2.1.2 and §2.2.2]).

In this paper, we consider the next simple case that K is a number field containing a primitive third root of unity, $L = K(\sqrt[3]{D})$ is the cyclic cubic

Received December 26, 2019; Accepted April 24, 2020.
2010 *Mathematics Subject Classification.* 11G05.
Key words and phrases. Elliptic curve, cubic twist, restriction of scalars.

extension of K for some $D \in K^\times/(K^\times)^3$ and $E = E_a : y^2 = x^3 + a$ is an elliptic curve with j-invariant 0 defined over K. In this case, we prove the following theorem.

Theorem 1.1. *Let K be a number field containing a primitive third root of unity and $L = K(\sqrt[3]{D})$ the cyclic cubic extension of K for some $D \in K^\times/(K^\times)^3$. Let $E = E_a : y^2 = x^3 + a$ be an elliptic curve with j-invariant 0 defined over K and $E_a^D : y^2 = x^3 + aD^2$ the cubic twist of E_a. Then A_L is isogenous over K to $E_a^D \times E_a^{D^2}$.*

Let $G := \mathrm{Gal}(L/K)$ be the Galois group L over K. If $F \in S$, let ρ_F be the unique faithful irreducible rational representation of $\mathrm{Gal}(F/K)$. Since the correspondence $F \leftrightarrow \rho_F$ is a bijection between S and the set of irreducible rational representations of G, the semisimple group ring $\mathbb{Q}[G]$ decomposes

$$\mathbb{Q}[G] \cong \bigoplus_{F \in S} \mathbb{Q}[G]_F,$$

where $\mathbb{Q}[G]_F$ is the ρ_F-isotypic component of $\mathbb{Q}[G]$. As a field, $\mathbb{Q}[G]_F$ is isomorphic to the cyclotomic field of $[F : K]$-th roots of unity.

Suppose that L is a cyclic extension of K with a prime degree p. Since $\mathbb{Q}[G]_L$ is isomorphic to the p-th cyclotomic field, the maximal order of $\mathbb{Q}[G]_L$ has the unique prime ideal above p, which we denote by $\mathfrak{p}$. Let $\mathrm{Sel}_p(E/K)$ be the p-Selmer group of E/K and $\mathrm{Sel}_{\mathfrak{p}}(A_L/K)$ the $\mathfrak{p}$-Selmer group of A_L/K (see §2 for the definitions). Define the Selmer ranks

$$d_p(E/K) := \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/K),$$
$$d_{\mathfrak{p}}(A_L/K) := \dim_{\mathbb{F}_p} \mathrm{Sel}_{\mathfrak{p}}(A_L/K).$$

In our case, we prove the following theorem on the Selmer rank of A_L, which is a cubic analogue of [2, Theorem 1.4] on quadratic twists.

Theorem 1.2. *Let K be a number field containing a primitive third root of unity, $L = K(\sqrt[3]{D})$ the cyclic cubic extension of K for some $D \in K^\times/(K^\times)^3$ and $\mathfrak{f}(L/K)$ the conductor of L/K. Let $E = E_a : y^2 = x^3 + a$ be an elliptic curve with j-invariant 0 defined over K. If $d_3(E_a/K) = r$ and $E_a(K)[3] = 0$, then*

$$|\{L = K(\sqrt[3]{D}) : d_{\mathfrak{p}}(A_L/K) = r \text{ and } N_{K/\mathbb{Q}}\mathfrak{f}(L/K) < X\}| \gg \frac{X}{(\log X)^{5/6}}.$$

2. Preliminaries

Let L be a finite abelian extension of a number field K with Galois group $G := \mathrm{Gal}(L/K)$. Let $\bar{K}$ be an algebraic closure of K with Galois group $G_K := \mathrm{Gal}(\bar{K}/K)$. Let E be an elliptic curve defined over K. Then the definition of the restriction of scalars ([5, §1.3] or [4, Definition 2.2]) of E from L to K is following.

Definition 2.1. The restriction of scalars of E from L to K, denoted by $\mathrm{Res}_K^L E$, is a commutative algebraic group over K along with a homomorphism

$$\eta_{L/K} : \mathrm{Res}_K^L E \to E$$

defined over L, with the universal property that for every variety X over K, the map

$$\mathrm{Hom}_K(X, \mathrm{Res}_K^L E) \to \mathrm{Hom}_L(X, E) \text{ defined by } f \mapsto \eta_{L/K} \circ f$$

is an isomorphism.

Suppose $\mathcal{I}$ is a free $\mathbb{Z}$-module of finite rank with a continuous right action of G_K and there is a ring homomorphism $\mathbb{Z} \to \mathrm{End}_K(E)$. A twist of a power of E denoted by $\mathcal{I} \otimes_{\mathbb{Z}} E$ is defined in [3, Definition 1.1].

Definition 2.2. Let $s := \mathrm{rank}_{\mathbb{Z}}(\mathcal{I})$ and fix an $\mathbb{Z}$-module isomorphism $j : \mathbb{Z}^s \xrightarrow{\sim} \mathcal{I}$. Let $c_{\mathcal{I}} \in H^1(K, \mathrm{Aut}_{\bar{K}}(E^s))$ be the image of the cocycle $(\gamma \mapsto j^{-1} \circ j^{\gamma})$ under the composition

$$H^1(K, \mathrm{GL}_s(\mathbb{Z})) \to H^1(K, \mathrm{Aut}_K(E^s)) \to H^1(K, \mathrm{Aut}_{\bar{K}}(E^s))$$

induced by the homomorphism $\mathbb{Z} \to \mathrm{End}_K(E)$. Define $\mathcal{I} \otimes_{\mathbb{Z}} E$ to be the twist of E^s by the cocycle $c_{\mathcal{I}}$, i.e., $\mathcal{I} \otimes_{\mathbb{Z}} E$ is the unique commutative algebraic group over K with an isomorphism $\phi : E^s \xrightarrow{\sim} \mathcal{I} \otimes_{\mathbb{Z}} E$ defined over $\bar{K}$ such that for every $\gamma \in G_K$,

$$c_{\mathcal{I}}(\gamma) = \phi^{-1} \circ \phi^{\gamma}.$$

Definition 2.3. For every cyclic extension F of K in L, define

$$\mathcal{I}_F := \mathbb{Q}[G]_F \cap \mathbb{Z}[G] \quad \text{and} \quad A_F := \mathcal{I}_F \otimes_{\mathbb{Z}} E.$$

We note that $A_K = E$ and $\mathrm{Res}_K^L(E)$ is isogenous to $\bigoplus_{F \in S} A_F$ by [1, Theorem 3.5].

From the universal property of $\mathrm{Res}_K^L E$, for each $\sigma \in G$, there is

$$\sigma_{L/K,E} \in \mathrm{Hom}_K(\mathrm{Res}_K^L E,\, \mathrm{Res}_K^L E)$$

such that $\eta_{L/K} \circ \sigma_{L/K,E} = \eta_{L/K}^{\sigma}$. So we have the following ring homomorphism

$$\theta_E : \mathbb{Z}[G] \to \mathrm{End}_K(\mathrm{Res}_K^L E) \text{ defined by } \alpha = \sum_{\sigma \in G} a_\sigma\, \sigma \mapsto a_\sigma\, \sigma_{L/K,E}.$$

We denote $\theta_E(\alpha)$ by $\alpha_E \in \mathrm{End}_K(\mathrm{Res}_K^L E)$.

Proposition 2.4 ([3, Proposition 4.2(i)]). *If $\mathbb{Z}[G]/\mathcal{I}$ is a projective $\mathbb{Z}$-module, then*

$$\mathcal{I} \otimes_{\mathbb{Z}} E = \bigcap_{\alpha \in \mathcal{I}^{\perp}} \ker\,(\alpha_E : \mathrm{Res}_K^L E \to \mathrm{Res}_K^L E),$$

where $\mathcal{I}^{\perp}$ is the ideal of $\mathbb{Z}[G]$ defined by $\mathcal{I}^{\perp} := \{\alpha \in \mathbb{Z}[G] : \alpha\mathcal{I} = 0\}$.

Lemma 2.5 ([3, Lemma 5.4(i)]). *Let F/K be cyclic of degree n with a generator σ. Then*

$$\mathcal{I}_F = \Psi_n(\sigma)\,\mathbb{Z}[G] \quad \textit{and} \quad \mathcal{I}_F^{\perp} = \Phi_n(\sigma)\,\mathbb{Z}[G],$$

where $\Phi_n \in \mathbb{Z}[x]$ is the n-th cyclotomic polynomial and $\Psi_n(x) = (x^n - 1)/\Phi_n(x) \in \mathbb{Z}[x]$.

Suppose that L is a cyclic extension of K with a prime degree p and $\mathfrak{p}$ is the unique prime ideal of $\mathbb{Q}[G]_L$ above p.

Definition 2.6. For every prime v of K, let $H^1_{\mathcal{E}}(K_v, E[p])$ denote the image of the Kummer injection

$$E(K_v)/pE(K_v) \hookrightarrow H^1(K_v, E[p])$$

and let $H^1_{\mathcal{A}}(K_v, A_L[\mathfrak{p}])$ denote the image of the Kummer injection

$$A_L(K_v)/\mathfrak{p}A_L(K_v) \hookrightarrow H^1(K_v, A_L[\mathfrak{p}]).$$

Definition 2.7. Define the Selmer groups

$$\mathrm{Sel}_p(E/K) := \ker\big(H^1(K, E[p]) \longrightarrow \bigoplus_v H^1(K_v, E[p])/H^1_{\mathcal{E}}(K_v, E[p])\big) \text{ and}$$

$$\mathrm{Sel}_{\mathfrak{p}}(A_L/K) := \ker\big(H^1(K, A_L[\mathfrak{p}]) \longrightarrow \bigoplus_v H^1(K_v, A_L[\mathfrak{p}])/H^1_{\mathcal{A}}(K_v, A_L[\mathfrak{p}])\big).$$

We note that there is a natural identification of G_K-modules $E[p] = A_L[\mathfrak{p}]$ inside $\mathrm{Res}^L_K E$ (cf. [1, Proposition 4.1 and Remark 4.2]).

Definition 2.8. For every prime v of K, define

$$\delta_v(E, L/K) := \dim_{\mathbb{F}_p}\left(H^1_{\mathcal{E}}(K_v, E[p])/H^1_{\mathcal{E}\cap\mathcal{A}}(K_v, E[p])\right),$$

where $H^1_{\mathcal{E}\cap\mathcal{A}}(K_v, E[p]) := H^1_{\mathcal{E}}(K_v, E[p]) \cap H^1_{\mathcal{A}}(K_v, E[p])$.

Proposition 2.9 ([1, Corollary 4.6]). *Suppose that $\mathcal{S}$ is a set of primes of K containing all primes above p, all primes ramified in L/K, and all primes where E has bad reduction. Then*

$$d_p(E/K) \equiv d_{\mathfrak{p}}(A_L/K) + \sum_{v\in\mathcal{S}} \delta_v(E, L/K) \pmod 2.$$

3. Proof of Theorem 1.1

For the rest of this paper, let K be a number field containing a primitive third root of unity ω, $L = K(\sqrt[3]{D})$ the cyclic cubic extension of K for some $D \in K^\times/(K^\times)^3$, $E_a : y^2 = x^3 + a$ an elliptic curve with j-invariant 0 defined over K, and $E_a^D : y^2 = x^3 + aD^2$ the cubic twist of E_a.

Proposition 3.1. *If we define isomorphisms over L*

$$\phi_1 : E_a \xrightarrow{\sim} E_a^D \ \textit{ by } (x, y) \mapsto (D^{\frac{2}{3}}x, Dy),$$

$$\phi_2 : E_a \xrightarrow{\sim} E_a^{D^2} \ \textit{ by } (x, y) \mapsto (D^{\frac{4}{3}}x, D^2y),$$

and G_K-invariant subgroup of $E_a \times E_a^D \times E_a^{D^2}$

$$T_a^L := \langle \{ \, (P, \, \phi_1(P), \, \phi_2(P))^{\gamma} \in E_a \times E_a^D \times E_a^{D^2} \, | \, 3P = 0, \ \gamma \in G_K \} \rangle,$$

then

$$\mathrm{Res}_K^L E_a = (E_a \times E_a^D \times E_a^{D^2})/T_a^L$$

with the following homomorphisms

$$\eta_{L/K} : (E_a \times E_a^D \times E_a^{D^2})/T_a^L \to E_a \ \text{ defined by } \ (P, Q, R) \mapsto P + \phi_1^{-1}(Q) + \phi_2^{-1}(R).$$

Proof. We will show that $(E_a \times E_a^D \times E_a^{D^2})/T_a^L$ satisfies the universal property of $\mathrm{Res}_K^L E_a$ with $\eta_{L/K}$ in Definition 2.1. Suppose X is a variety over K and $\varphi \in \mathrm{Hom}_L(X, E_a)$. Let $[3]^{-1} : E_a \to E_a / E_a[3]$ be the inverse map of the induced isomorphism from multiplication by 3, let

$$\lambda : E_a / E_a[3] \to (E_a \times E_a^D \times E_a^{D^2})/T_a^L$$

defined by $P \mapsto \big(P, \phi_1(P), \phi_2(P)\big) \pmod{T_a^L}$, and let σ be the generator of $\mathrm{Gal}(L/K)$ which maps $\sqrt[3]{D}$ to $\sqrt[3]{D}\,\omega$. Define

$$\begin{aligned} \tilde{\varphi} &:= \lambda \circ [3]^{-1} \circ \varphi \, + \, (\lambda \circ [3]^{-1} \circ \varphi)^{\sigma} \, + \, (\lambda \circ [3]^{-1} \circ \varphi)^{\sigma^2} \\ &\in \mathrm{Hom}_K\big(X, \, (E_a \times E_a^D \times E_a^{D^2})/\, T_a^L \,\big). \end{aligned}$$

Then we have

$$\begin{aligned} \eta_{L/K} \circ \ \lambda \circ [3]^{-1} \circ \varphi &= \varphi, \\ \eta_{L/K} \circ (\lambda \circ [3]^{-1} \circ \varphi)^{\sigma} &= 0 \quad (\text{because } \phi_1^{\sigma} = [\omega]\phi_1, \ \phi_2^{\sigma} = [\omega]^2\phi_2 \\ &\qquad\quad \text{and } [1] + [\omega] + [\omega]^2 = [0]), \\ \eta_{L/K} \circ (\lambda \circ [3]^{-1} \circ \varphi)^{\sigma^2} &= 0 \quad (\text{by the same reason}), \end{aligned}$$

where $[\omega] : (x, y) \mapsto (\omega^2 x, y)$ is an endomorphism of E_a, E_a^D, and $E_a^{D^2}$. Thus $\eta_{L/K} \circ \tilde{\varphi} = \varphi$.

For any $(P, Q, R) \in (E_a \times E_a^D \times E_a^{D^2})/T_a^L$, we have

$$\begin{aligned} (P, Q, R) &\overset{\eta_{L/K}}{\longmapsto} && P + \phi_1^{-1}(Q) + \phi_2^{-1}(R) \\ &\overset{[3]^{-1}}{\longmapsto} && P' + \phi_1^{-1}(Q') + \phi_2^{-1}(R') \\ &\overset{\lambda}{\longmapsto} && \big(P' + \phi_1^{-1}(Q') + \phi_2^{-1}(R'), \\ &&& \phi_1(P') + Q' + \phi_1(\phi_2^{-1}(R')), \\ &&& \phi_2(P') + \phi_2(\phi_1^{-1}(Q')) + R'\big) \pmod{T_a^L}, \\ (P, Q, R) &\overset{(\lambda \circ [3]^{-1} \circ \eta_{L/K})^{\sigma}}{\longmapsto} && \big(P' + [\omega]^2\phi_1^{-1}(Q') + [\omega]\phi_2^{-1}(R'), \\ &&& [\omega]\phi_1(P') + Q' + [\omega]^2\phi_1(\phi_2^{-1}(R')), \\ &&& [\omega]^2\phi_2(P') + [\omega]\phi_2(\phi_1^{-1}(Q')) + R'\big) \pmod{T_a^L}, \end{aligned}$$

$$\begin{aligned}(P,Q,R) \overset{(\lambda\circ[3]^{-1}\circ\eta_{L/K})^{\sigma^2}}{\longmapsto} \quad & \big(P'+[\omega]\phi_1^{-1}(Q')+[\omega]^2\phi_2^{-1}(R'),\\ & [\omega]^2\phi_1(P')+Q'+[\omega]\phi_1(\phi_2^{-1}(R')),\\ & [\omega]\phi_2(P')+[\omega]^2\phi_2(\phi_1^{-1}(Q'))+R'\big) \pmod{T_a^L},\end{aligned}$$

where P' (resp. Q', R') is an element satisfying $[3]P' = P$ (resp. $[3]Q' = Q$, $[3]R' = R$). So

$$(\lambda\circ[3]^{-1}\circ\eta_{L/K})+(\lambda\circ[3]^{-1}\circ\eta_{L/K})^{\sigma}+(\lambda\circ[3]^{-1}\circ\eta_{L/K})^{\sigma^2}=\mathrm{id}.$$

Hence for every $f\in\mathrm{Hom}_K(X,(E_a\times E_a^D\times E_a^{D^2})/T_a^L)$, we have

$$\begin{aligned}&\widetilde{(\eta_{L/K}\circ f)}\\ &=(\lambda\circ[3]^{-1}\circ\eta_{L/K}\circ f)+(\lambda\circ[3]^{-1}\circ\eta_{L/K}\circ f)^{\sigma}+(\lambda\circ[3]^{-1}\circ\eta_{L/K}\circ f)^{\sigma^2}\\ &=(\lambda\circ[3]^{-1}\circ\eta_{L/K})\circ f+(\lambda\circ[3]^{-1}\circ\eta_{L/K})^{\sigma}\circ f+(\lambda\circ[3]^{-1}\circ\eta_{L/K})^{\sigma^2}\circ f\\ &=f.\end{aligned}$$

Thus the map

$$\mathrm{Hom}_K\big(X,(E_a\times E_a^D\times E_a^{D^2})/T_a^L\big)\to\mathrm{Hom}_L(X,E_a)$$

defined by $f\mapsto\eta_{L/K}\circ f$ is an isomorphism. □

Proposition 3.2. *Let $A_L=\mathcal{I}_L\otimes_{\mathbb{Z}}E_a$ in Definition 2.3. Then there is a surjective morphism over K with a finite kernel*

$$\theta: E_a^D\times E_a^{D^2}\to A_L.$$

Proof. We continue the notations K, L, σ, E_a, E_a^D, T_a^L, $\eta_{L/K}$, $\widetilde{\cdot}$ in Proposition 3.1 and its proof. Recall that $\mathrm{Res}_K^L E_a$ is $(E_a\times E_a^D\times E_a^{D^2})\,/\,T_a^L$ with the homomorphism $\eta_{L/K}$. Note that for the $\sigma\in\mathrm{Gal}(L/K)$, its induced endomorphism $\sigma_{E_a}\in\mathrm{End}_K(\mathrm{Res}_K^L E_a)$ is precisely

$$\sigma_{E_a}(P,Q,R)=\widetilde{\eta_{L/K}^{\sigma}}(P,Q,R)=(P,\,[\omega]^2Q,\,[\omega]R),$$

and hence $\Phi_3(\sigma)_{E_a}$ is given by

$$\Phi_3(\sigma)_{E_a}(P,Q,R)=(\sigma^2+\sigma+1)_{E_a}(P,Q,R)=(\,3P,\,0\,,\,0\,).$$

Thus by Proposition 2.4 and Lemma 2.5, we have

$$\begin{aligned}A_L:=\mathcal{I}_L\otimes_{\mathbb{Z}}E_a &= \ker\big(\Phi_3(\sigma)_{E_a}:\mathrm{Res}_K^L E_a\to\mathrm{Res}_K^L E_a\big)\\ &= \{(P,Q,R)\in(E_a\times E_a^D\times E_a^{D^2})/\,T_a^L\mid(3P,\,0,\,0)\equiv(0,\,0,\,0)\,(\mathrm{mod}\,T_a^L)\}\\ &= \{(P,Q,R)\in(E_a\times E_a^D\times E_a^{D^2})/\,T_a^L\mid P\in E_a[3]\,\}.\end{aligned}$$

Define

$$\theta:E_a^D\times E_a^{D^2}\to A_L\ \text{ by }\ (Q,R)\mapsto(0,Q,R).$$

Then θ is a morphism over K with a finite kernel. For $(P,Q,R)\in A_L$,

$$(P,Q,R)=(P,\,\phi_1(P),\,\phi_2(P))+(0,\,Q-\phi_1(P),\,R-\phi_2(P))$$

$$\equiv (0,\, Q - \phi_1(P),\, R - \phi_2(P)) \pmod{T_a^L}.$$

Thus θ is surjective. □

Proof of Theorem 1.1. It follows from Proposition 3.1. □

4. Proof of Theorem 1.2

To compare $d_3(E_a/K)$ and $d_{\mathfrak{p}}(A_L/K)$, we apply [2, §2 and §3] to our case. By [1, Proposition 5.2], we have the following lemma which is same to [2, Lemma 2.9].

Lemma 4.1. *Let v be a prime of K, w a prime of L above v and N_{L_w/K_v} : $E_a(L_w) \to E_a(K_v)$ the norm map. Under the isomorphism $H^1_{\mathcal{E}}(K_v, E_a[3]) \cong E_a(K_v)/3E_a(K_v)$, we have*

$$H^1_{\mathcal{E}\cap\mathcal{A}}(K_v, E_a[3]) \cong N_{L_w/K_v} E_a(L_w)/3E_a(K_v).$$

Remark. In [2, Definition 2.6], $\delta_v(E, L/K)$ is defined by

$$\dim_{\mathbb{F}_p} E(K_v)/N_{L_w/K_v} E(L_w),$$

where $p = 2$. By Lemma 4.1, [2, Definition 2.6] is same to Definition 2.8 for our case.

By Lemma 4.1, we have the following lemmas which are similar to [2, Lemma 2.10 and Lemma 2.11].

Lemma 4.2. *Let Δ_{E_a} be the discriminant of E_a. If at least one of the following conditions* (i)-(iv) *holds*:

(i) *v splits in L/K,*
(ii) *$v \nmid 3\infty$ and $E_a(K_v)[3] = 0$,*
(iii) *v is real and $(\Delta_{E_a})_v < 0$,*
(iv) *v is a prime where E_a has good reduction and v is unramified in L/K, then $H^1_{\mathcal{E}}(K_v, E_a[3]) = H^1_{\mathcal{A}}(K_v, E_a[3])$ and $\delta_v(E_a, L/K) = 0$.*

Proof. See the proof of [2, Lemma 2.10]. □

Lemma 4.3. *If $v \nmid 3\infty$, E_a has good reduction at v and v is ramified in L/K, then*

$$H^1_{\mathcal{E}\cap\mathcal{A}}(K_v, E_a[3]) = 0 \quad \textit{and} \quad \delta_v(E_a, L/K) = \dim_{\mathbb{F}_3}(E_a(K_v)[3]).$$

Proof. See the proof of [2, Lemma 2.11] □

By Proposition 2.9, Lemma 4.2, and Lemma 4.3, we have the following proposition which is similar to [2, Proposition 3.3].

Proposition 4.4. *Suppose that all of the following primes split in L/K*:

- *all primes where E_a has bad reduction,*
- *all primes above* 3,
- *all real places v with $(\Delta_{E_a})_v > 0$.*

Let $\mathcal{T}$ be the set of (finite) primes $\mathfrak{q}$ of K such that L/K is ramified at $\mathfrak{q}$ and $E_a(K_\mathfrak{q})[3] \neq 0$. Let

$$\mathrm{loc}_\mathcal{T} : H^1(K, E_a[3]) \to \bigoplus_{\mathfrak{q}\in\mathcal{T}} H^1(K_\mathfrak{q}, E_a[3])$$

and

$$V_T := \mathrm{loc}_\mathcal{T}(\mathrm{Sel}_3(E_a/K)) \subset \bigoplus_{\mathfrak{q}\in\mathcal{T}} H^1_\mathcal{E}(K_\mathfrak{q}, E_a[3]).$$

Then we have

$$d_\mathfrak{p}(A_L/K) = d_3(E_a/K) - \dim_{\mathbb{F}_3} V_\mathcal{T} + d$$

for some d satisfying

$$0 \leq d \leq \dim_{\mathbb{F}_3}\left(\bigoplus_{\mathfrak{q}\in\mathcal{T}} H^1_\mathcal{E}(K_\mathfrak{q}, E_a[3])/V_\mathcal{T}\right) \quad \textit{and}$$

$$d \equiv \dim_{\mathbb{F}_3}\left(\bigoplus_{\mathfrak{q}\in\mathcal{T}} H^1_\mathcal{E}(K_\mathfrak{q}, E_a[3])/V_\mathcal{T}\right) \pmod 2.$$

Proof. Define strict and relaxed 3-Selmer groups $\mathcal{S}_\mathcal{T} \subset \mathcal{S}^\mathcal{T} \subset H^1(K, E_a[3])$ by the exactness of

$$0 \to \mathcal{S}^\mathcal{T} \to H^1(K, E_a[3]) \to \bigoplus_{\mathfrak{q}\notin\mathcal{T}} H^1(K_\mathfrak{q}, E_a[3])/H^1_\mathcal{E}(K_\mathfrak{q}, E_a[3]) \text{ and}$$

$$0 \to \mathcal{S}_\mathcal{T} \to \mathcal{S}^\mathcal{T} \longrightarrow \bigoplus_{\mathfrak{q}\in\mathcal{T}} H^1(K_\mathfrak{q}, E_a[3]).$$

Then we have $\mathcal{S}_\mathcal{T} \subset \mathrm{Sel}_p(E_a/K) \subset \mathcal{S}^\mathcal{T}$. By Lemma 4.2 we also have $\mathcal{S}_\mathcal{T} \subset \mathrm{Sel}_\mathfrak{p}(A_L/K) \subset \mathcal{S}^\mathcal{T}$ and by Lemma 4.3 we have $\mathrm{Sel}_p(E_a/K) \cap \mathrm{Sel}_\mathfrak{p}(A_L/K) = \mathcal{S}_\mathcal{T}$.

Let $V^L_\mathcal{T} := \mathrm{loc}_\mathcal{T}(\mathrm{Sel}_\mathfrak{p}(A_L/K)) \subset \bigoplus_{\mathfrak{q}\in\mathcal{T}} H^1_\mathcal{A}(K_\mathfrak{q}, E_a[3])$ and $d := \dim_{\mathbb{F}_3} V^L_\mathcal{T}$. Then the theorem follows from the same argument in the proof of [2, Proposition 3.3]. □

By Proposition 4.4, we have the following proposition which is similar to [2, Corollary 3.4].

Proposition 4.5. *Suppose $E_a, L/K$, and $\mathcal{T}$ are as in Proposition 4.4.*

(a) *If $\dim_{\mathbb{F}_p}(\bigoplus_{\mathfrak{q}\in\mathcal{T}} H^1_\mathcal{E}(K_\mathfrak{q}, E_a[3])/V_\mathcal{T}) \leq 1$, then*

$$d_\mathfrak{p}(A_L/K) = d_p(E_a/K) - 2\dim_{\mathbb{F}_p} V_\mathcal{T} + \sum_{\mathfrak{q}\in\mathcal{T}} \dim_{\mathbb{F}_p} H^1_\mathcal{E}(K_\mathfrak{q}, E_a[3]).$$

(b) *If $E(K_\mathfrak{q})[3] = 0$ for every $\mathfrak{q} \in \mathcal{T}$, then $d_\mathfrak{p}(A_L/K) = d_3(E_a/K)$.*

Proof. For (a), see the proof of [2, Corollary 3.4(i)]. (b) follows from (a) because $\mathcal{T}$ is empty in this case. □

Let $M := K(E_a[3])$ and $\mathfrak{S}$ be the set of elements of order 2 in $\mathrm{Gal}(M/K)$.

Lemma 4.6. *Suppose that* $E_a(K)[3] = 0$. *Then* $\mathrm{Gal}(M/K) \cong \mathbb{Z}/2\mathbb{Z}$ *or* $\mathbb{Z}/6\mathbb{Z}$, *depending on whether* $K \ni \sqrt[3]{-4a}$ *or not, so* $|\mathfrak{S}| = 1$.

Proof. The lemma follows from

$$E_a[3] = \{O, (0, \pm\sqrt{a}), (\sqrt[3]{-4a}, \pm\sqrt{-3a}), (\sqrt[3]{-4a}\omega, \pm\sqrt{-3a}), (\sqrt[3]{-4a}\omega^2, \pm\sqrt{-3a})\}.$$

□

Let $N := K(27\Delta_{E_a}\infty)$ be the ray class field of K modulo $27\Delta_{E_a}$ and all infinite primes. Define a set of primes of K

$$\mathcal{P} := \{v : v \text{ is unramified in } NM/K \text{ and } \mathrm{Frob}_v(M/K) \subset \mathfrak{S}\},$$

where $\mathrm{Frob}_v(M/K)$ denotes the Frobenius conjugacy class of v in $\mathrm{Gal}(M/K)$, and two sets of ideals $\mathcal{N}_1 \subset \mathcal{N}$ of K

$$\mathcal{N} := \{\mathfrak{a} : \mathfrak{a} \text{ is a cubefree product of primes in } \mathcal{P}\},$$
$$\mathcal{N}_1 := \{\mathfrak{a} \in \mathcal{N} : [\mathfrak{a}, N/K] = 1\},$$

where $[\,\cdot\,, N/K]$ denotes the global Artin symbol.

Lemma 4.7 ([2, Lemma 4.1])**.** *There is a constant* c *such that*

$$|\{\mathfrak{a} \in \mathcal{N}_1 : N_{K/\mathbb{Q}}\mathfrak{a} < X\}| = (c + o(1))\frac{X}{(\log X)^{1-|\mathfrak{S}|/[M:K]}}.$$

Proposition 4.8. *Suppose that* $E_a(K)[3] = 0$. *For* $\mathfrak{a} \in \mathcal{N}_1$, *there is a cyclic cubic extension* L/K *of conductor* $\mathfrak{a}$ *such that* $d_{\mathfrak{p}}(A_L/K) = d_3(E_a/K)$.

Proof. Fix $\mathfrak{a} \in \mathcal{N}_1$. Then $\mathfrak{a}$ is principal, with a totally positive generator $\alpha \equiv 1 \pmod{27\Delta_{E_a}}$. Let $L := K(\sqrt[3]{\alpha})$. Then all primes above 3, all primes of bad reduction, and all infinite primes split in L/K. If v ramifies in L/K, then $v|\mathfrak{a}$, so $v \in \mathcal{P}$. Thus the Frobenius of v in $\mathrm{Gal}(M/K)$ has order 2, which shows that $E_a(K_v)[3] = 0$. Now the proposition follows from Proposition 4.5(b). □

Proof of Theorem 1.2. It follows from Lemma 4.6, Lemma 4.7 and Proposition 4.8. □

References

[1] B. Mazur and K. Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. (2) **166** (2007), no. 2, 579–612. `https://doi.org/10.4007/annals.2007.166.579`

[2] ———, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), no. 3, 541–575. `https://doi.org/10.1007/s00222-010-0252-0`

[3] B. Mazur, K. Rubin, and A. Silverberg, *Twisting commutative algebraic groups*, J. Algebra **314** (2007), no. 1, 419–438. `https://doi.org/10.1016/j.jalgebra.2007.02.052`

[4] A. Silverberg, *Applications to cryptography of twisting commutative algebraic groups*, Discrete Appl. Math. **156** (2008), no. 16, 3122–3138. `https://doi.org/10.1016/j.dam.2008.01.024`

[5] A. Weil, *Adeles and Algebraic Groups*, Progress in Mathematics, **23**, Birkhäuser, Boston, MA, 1982.

Dongho Byeon
Department of Mathematical Sciences
Seoul National University
Seoul 08826, Korea
Email address: dhbyeon@snu.ac.kr

Keunyoung Jeong
Department of Mathematical Sciences
Ulsan National Institute of Science and Technology
Ulsan 44919, Korea
Email address: kyjeong@unist.ac.kr

Nayoung Kim
Department of Mathematical Sciences
Seoul National University
Seoul 08826, Korea
Email address: na0@snu.ac.kr