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 $\text{Res}_L^K E$ decomposes (up to isogeny) into abelian varieties over $K$
\[ \text{Res}_L^K E \sim \bigoplus_{F \in S} A_F, \]
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 $E^D_a : y^2 = x^3 + aD^2$ is the cubic twist of $E_a$. In this case, we prove $A_L$ is isogenous over $K$ to $E^D_a \times E^{D^2}_a$ 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 $\text{Res}_L^K E$ (for the definition, see §2) of $E$ from $L$ to $K$ decomposes (up to isogeny) into abelian varieties over $K$
\[ \text{Res}_L^K E \sim \bigoplus_{F \in S} A_F, \]
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...
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 $D \in K^\times/(K^\times)^3$ and $E = E_a : y^2 = x^3 + a$ be an elliptic curve with $j$-invariant 0 defined over $K$. In this case, we prove the following theorem.

Let $G := \text{Gal}(L/K)$ be the Galois group $L$ over $K$. If $F \in S$, let $\rho_F$ be the unique faithful irreducible rational representation of $\text{Gal}(F/K)$. 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 $\rho_F$-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 $\text{Sel}_p(E/K)$ be the $p$-Selmer group of $E/K$ and $\text{Sel}_p(A_L/K)$ the $p$-Selmer group of $A_L/K$ (see §2 for the definitions). Define the Selmer ranks

$$d_p(E/K) := \dim_{\mathbb{Q}_p} \text{Sel}_p(E/K),$$
$$d_p(A_L/K) := \dim_{\mathbb{Q}_p} \text{Sel}_p(A_L/K).$$

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

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

2. Preliminaries

Let $L$ be a finite abelian extension of a number field $K$ with Galois group $G := \text{Gal}(L/K)$. Let $K$ be an algebraic closure of $K$ with Galois group $G_K := \text{Gal}(K/K)$. 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 $\text{Res}_L^K E$, is a commutative algebraic group over $K$ along with a homomorphism $\eta_{L/K} : \text{Res}_L^K E \to E$

defined over $L$, with the universal property that for every variety $X$ over $K$, the map $\text{Hom}_K(X, \text{Res}_L^K E) \to \text{Hom}_L(X, E)$ defined by $f \mapsto \eta_{L/K} \circ f$ is an isomorphism.

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

**Definition 2.2.** Let $s := \text{rank}_\mathbb{Z}(I)$ and fix an $\mathbb{Z}$-module isomorphism $j : \mathbb{Z}^s \cong I$. Let $c_I \in H^1(K, \text{Aut}_K(E^s))$ be the image of the cocycle $(\gamma \mapsto j^{-1} \circ j^\gamma)$ under the composition $H^1(K, \text{GL}_s(\mathbb{Z})) \to H^1(K, \text{Aut}_K(E^s))$ induced by the homomorphism $\mathbb{Z} \to \text{End}_K(E)$. Define $I \otimes \mathbb{Z} E$ to be the twist of $E^s$ by the cocycle $c_I$, i.e., $I \otimes \mathbb{Z} E$ is the unique commutative algebraic group over $K$ with an isomorphism $\phi : E^s \cong I \otimes \mathbb{Z} E$ defined over $\bar{K}$ such that for every $\gamma \in G_K$,

$$c_I(\gamma) = \phi^{-1} \circ \phi^\gamma.$$

**Definition 2.3.** For every cyclic extension $F$ of $K$ in $L$, define $I_F := \mathbb{Q}[G]_F \cap \mathbb{Z}[G]$ and $A_F := I_F \otimes \mathbb{Z} E$.

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

From the universal property of $\text{Res}_K^L(E)$, for each $\sigma \in G$, there is $\sigma_{L/K,E} \in \text{Hom}_K(\text{Res}_K^L(E), \text{Res}_K^E)$ such that $\eta_{L/K} \circ \sigma_{L/K,E} = \eta_{L/K}$. So we have the following ring homomorphism $\theta_E : \mathbb{Z}[G] \to \text{End}_K(\text{Res}_K^L(E))$ defined by $a = \sum_{\sigma \in G} a_\sigma \sigma \mapsto a_\sigma \sigma_{L/K,E}$.

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

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

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

where $\mathcal{I}^+$ is the ideal of $\mathbb{Z}[G]$ defined by $\mathcal{I}^+ := \{\alpha \in \mathbb{Z}[G] : \alpha \mathcal{I} = 0\}$. 
Lemma 2.5 ([3, Lemma 5.4(i)]). Let $F/K$ be cyclic of degree $n$ with a generator $\sigma$. Then
\[ I_F = \Psi_n(\sigma) \mathbb{Z}[G] \quad \text{and} \quad I_F^+ = \Phi_n(\sigma) \mathbb{Z}[G], \]
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 $p$ is the unique prime ideal of $\mathbb{Q}[G]_L$ above $p$.

Definition 2.6. For every prime $v$ of $K$, let $H^1_L(K_v, E[p])$ denote the image of the Kummer injection
\[ E(K_v)/\langle p \rangle E(K_v) \hookrightarrow H^1(K_v, E[p]) \]
and let $H^1_L(K_v, A_L[p])$ denote the image of the Kummer injection
\[ A_L(K_v)/\langle p \rangle A_L(K_v) \hookrightarrow H^1(K_v, A_L[p]). \]

Definition 2.7. Define the Selmer groups
\[ \text{Sel}_p(E/K) := \ker \left( H^1(K, E[p]) \to \bigoplus_v H^1(K_v, E[p])/H^1_L(K_v, E[p]) \right) \quad \text{and} \]
\[ \text{Sel}_p(A_L/K) := \ker \left( H^1(K, A_L[p]) \to \bigoplus_v H^1(K_v, A_L[p])/H^1_L(K_v, A_L[p]) \right). \]

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

Definition 2.8. For every prime $v$ of $K$, define
\[ \delta_v(E, L/K) := \dim_{\mathbb{F}_p} \left( H^1_L(K_v, E[p]) \right), \]
where $H^1_L(K_v, E[p]) := H^1_L(K_v, E[p]) \cap H^1_L(K_v, E[p])$.

Proposition 2.9 ([1, Corollary 4.6]). Suppose that $S$ 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
\[ d_p(E/K) \equiv d_p(A_L/K) + \sum_{v \in S} \delta_v(E, L/K) \pmod{2}. \]

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 $\omega$, $L = K(\sqrt[3]{D})$ the cyclic cubic extension of $K$ for some $D \in K^*/(K^*)^3$, $E_a : y^2 = x^3 + a$ an elliptic curve with $j$-invariant 0 defined over $K$, and $E^D_a : y^2 = x^3 + aD^2$ the cubic twist of $E_a$.

Proposition 3.1. If we define isomorphisms over $L$
\[ \phi_1 : E_a \to E^D_a \text{ by } (x, y) \mapsto (D^{2/3}x, Dy), \]
\[ \phi_2 : E_a \to E^{D^2}_a \text{ by } (x, y) \mapsto (D^{2/3}x, D^2y), \]
and $G_K$-invariant subgroup of $E_a \times E_a^D \times E_a^{D^2}$

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

then

$$\text{Res}_{K} E_a = (E_a \times E_a^D \times E_a^{D^2})/T_a^L$$

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 $\text{Res}_{K} E_a$ with $\eta_{L/K}$ in Definition 2.1. Suppose $X$ is a variety over $K$ and $\varphi \in \text{Hom}_L(X, E_a)$. Let $[3]^{-1} : E_a \to E_a/[E_a[3]]$ be an endomorphism of $E_a/[E_a[3]]$.

Define

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

where $[\lambda] : (x, y) \mapsto (\omega x, y)$ is an endomorphism of $E_a$, $E_a^D$, and $E_a^{D^2}$. Thus $\eta_{L/K} \circ \lambda \varphi = \varphi$. For any $(P, Q, R) \in (E_a \times E_a^D \times E_a^{D^2})/T_a^L$, we have

$$(P, Q, R) \mapsto (P + \phi_1^{-1}(Q) + \phi_2^{-1}(R)),$$

$$(\lambda \circ [3]^{-1} \circ \eta_{L/K}) (P, Q, R) \mapsto (P' + \phi_1^{-1}(Q') + \phi_2^{-1}(R')).$$

Then we have

$$\eta_{L/K} \circ \lambda \circ [3]^{-1} \circ \varphi = \varphi,$$

$$\eta_{L/K} \circ (\lambda \circ [3]^{-1} \circ \varphi) = 0 \quad \text{because } \phi_1^\sigma = [\omega] \phi_1, \phi_2^\sigma = [\omega]^2 \phi_2$$

and $[1] + [\omega] + [\omega]^2 = [0])$,

$$\eta_{L/K} \circ (\lambda \circ [3]^{-1} \circ \varphi) = 0 \quad \text{by the same reason},$$

where $[\omega] : (x, y) \mapsto (\omega x, y)$ is an endomorphism of $E_a$, $E_a^D$, and $E_a^{D^2}$.
Define $f$ where

$$\theta = \frac{\eta_{L/K}^{\circ}}{\sigma_{L/K}}.$$ 

Thus the map $\theta$ is surjective over $K$.

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 $K$, $L$, $\sigma$, $E_a$, $E_a^D$, $T_a^L$, $\eta_{L/K}$, $\tilde{\gamma}$ in Proposition 3.1 and its proof. Recall that $\text{Res}_{K}^{L} E_a = (E_a \times E_a^D \times E_a^{D^2}) / T_a^L$ with the homomorphism $\eta_{L/K}$. Note that for the $\sigma$ in $\text{Gal}(L/K)$, its induced endomorphism $\sigma_{E_a} \in \text{End}_{K}(\text{Res}_{K}^{L} E_a)$ is precisely

$$\eta_{L/K}^{\circ} \circ \sigma = \sigma_{E_a} \circ \eta_{L/K}^{\circ}.$$ 

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

$$A_L := \mathcal{I}_L \otimes_{\mathbb{Z}} E_a = \ker(\Phi_{3}(\sigma)_{E_a} : \text{Res}_{K}^{L} E_a \to \text{Res}_{K}^{L} E_a)$$

$$= \{(P, Q, R) \in (E_a \times E_a^D \times E_a^{D^2}) / T_a^L \mid (3P, 0, 0) \equiv (0, 0, 0) \pmod{T_a^L} \}$$

$$= \{(P, Q, R) \in (E_a \times E_a^D \times E_a^{D^2}) / T_a^L \mid P \in E_a[3] \}.$$ 

Define

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

by $(Q, R) \mapsto (0, Q, R)$.

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

$$(P, Q, R) = (P, \phi_1(P), \phi_2(P)) + (0, Q - \phi_1(P), R - \phi_2(P)).$$
Thus \( \theta \) is surjective.

Proof of Theorem 1.1. It follows from Proposition 3.1.

4. Proof of Theorem 1.2

To compare \( d_E(E_a/K) \) and \( d_p(A_L/K) \), 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 \( N_{L_w/K_v} : E_a(L_w) \rightarrow E_a(K_v) \) the norm map. Under the isomorphism \( H^1_2(K_v, E_a[3]) \cong E_a(K_v)/3E_a(K_v) \), we have

\[
H^1_2(K_v, E_a[3]) \cong N_{L_w/K_v}E_a(L_w)/3E_a(K_v).
\]

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

\[
\dim_{F_p} E(K_v)/N_{L_w/K_v}E(L_w),
\]

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 \( \Delta_{E_a} \) 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 \( H^1_2(K_v, E_a[3]) = H^1_3(K_v, E_a[3]) \) 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

\[
H^1_2(K_v, E_a[3]) = 0 \quad \text{and} \quad \delta_v(E_a, L/K) = \dim_{F_p}(E_a(K_v)[3]).
\]

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

$$\text{loc}_T : H^1(K, E_a[3]) \to \bigoplus_{q \in T} H^1(K_q, E_a[3])$$

and

$$V_T := \text{loc}_T(\text{Sel}_3(E_a/K)) \subset \bigoplus_{q \in T} H^2_2(K_q, E_a[3]).$$

Then we have

$$d_p(A_L/K) = d_3(E_a/K) - \dim_{F_3} V_T + d$$

for some $d$ satisfying

$$0 \leq d \leq \dim_{F_3} \left( \bigoplus_{q \in T} \frac{H^2_2(K_q, E_a[3])}{V_T} \right)$$

and

$$d \equiv \dim_{F_3} \left( \bigoplus_{q \in T} \frac{H^2_2(K_q, E_a[3])}{V_T} \right) \pmod{2}.$$

**Proof.** Define strict and relaxed 3-Selmer groups $S_T \subset S_T \subset H^1(K, E_a[3])$ by the exactness of

$$0 \to S_T \to H^1(K, E_a[3]) \to \bigoplus_{q \notin T} H^1(K_q, E_a[3]) / H^2_2(K_q, E_a[3])$$

and

$$0 \to S_T \to S_T \to \bigoplus_{q \in T} H^1(K_q, E_a[3]).$$

Then we have $S_T \subset \text{Sel}_p(E_a/K) \subset S_T$. By Lemma 4.2 we also have $S_T \subset \text{Sel}_p(A_L/K) \subset S_T$ and by Lemma 4.3 we have $\text{Sel}_p(E_a/K) \cap \text{Sel}_p(A_L/K) = S_T$.

Let $V_T := \text{loc}_T(\text{Sel}_p(A_L/K)) \subset \bigoplus_{q \in T} H^2_2(K_q, E_a[3])$ and $d := \dim_{F_3} V_T$.

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 $T$ are as in Proposition 4.4.

(a) If $\dim_{F_3} \left( \bigoplus_{q \in T} \frac{H^2_2(K_q, E_a[3])}{V_T} \right) \leq 1$, then

$$d_p(A_L/K) = d_p(E_a/K) - 2 \dim_{F_3} V_T + \sum_{q \in T} \dim_{F_3} H^2_2(K_q, E_a[3]).$$

(b) If $E(K_q)[3] = 0$ for every $q \in T$, then $d_p(A_L/K) = d_3(E_a/K)$.

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

Let $M := K(E_a[3])$ and $S$ be the set of elements of order 2 in $\text{Gal}(M/K)$. 
Lemma 4.6. Suppose that $E_a(K)[3] = 0$. Then $\text{Gal}(M/K) \cong \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z}$, depending on whether $K \ni \sqrt[3]{-4a}$ or not, so $|\mathcal{D}| = 1$.

Proof. The lemma follows from

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

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 $K$

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

where $\text{Frob}_v(M/K)$ denotes the Frobenius conjugacy class of $v$ in $\text{Gal}(M/K)$, and two sets of ideals $N_1 \subset N$ of $K$

$$N := \{a : a \text{ is a cubefree product of primes in } P\},$$

$$N_1 := \{a \in N : [a, N/K] = 1\},$$

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

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

$$|\{a \in N_1 : N_K/Q a < X\}| = (c + o(1))\frac{X}{(\log X)^{1-\frac{1}{|\mathcal{D}|}}/|M/K|}.$$ 

Proposition 4.8. Suppose that $E_a(K)[3] = 0$. For $a \in N_1$, there is a cyclic cubic extension $L/K$ of conductor $a$ such that $d_p(A_L/K) = d_3(E_a/K)$.

Proof. Fix $a \in N_1$. Then $a$ 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 $v|a$, so $v \in P$. Thus the Frobenius of $v$ in $\text{Gal}(M/K)$ 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


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