TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 372, Number 1, 1 July 2019, Pages 425–440
https://doi.org/10.1090/tran/7563
Article electronically published on October 1, 2018

2-SELMER NEAR-COMPANION CURVES

MYUNGJUN YU

ABSTRACT. Let E and A be elliptic curves over a number field K. Let χ be a quadratic character of K. We prove the conjecture posed by Mazur and Rubin on n-Selmer near-companion curves in the case $n = 2$. Namely, we show if the difference of the 2-Selmer ranks of E^χ and A^χ is bounded independent of χ, there is a G_K-module isomorphism $E[2] \cong A[2]$.

INTRODUCTION

In [5], Mazur and Rubin introduce the so-called *Selmer companion curves.* By definition, elliptic curves E and A over a number field K are called n-Selmer companion curves over K if for every quadratic character $\chi \in \mathrm{Hom}(G_K, \{\pm 1\})$, where G_K is the absolute Galois group of K, there exists a group isomorphism between $\mathrm{Sel}_n(E^\chi/K)$ and $\mathrm{Sel}_n(A^\chi/K)$, where E^χ and A^χ denote the quadratic twists of E and A by χ, respectively. This definition originates from the question that asks what information about an elliptic curve E/K could be read off from the function

$$\mathrm{Hom}(G_K, \{\pm 1\}) \to \mathbf{N}_{\geq 0}$$

taking χ to $\dim_{\mathbf{F}_p}(\mathrm{Sel}_p(E^\chi/K))$ for a prime p. They also defined a weaker condition on E and A the so-called *n-Selmer near-companion curves* [5, Definition 7.12] over K. To simplify the definition, we define n-Selmer near-companion curves only when n is a prime number, which is sufficient for our purposes.

Definition 1. Let p be a prime number. Let E and A be elliptic curves over a number field K. We say E and A are *p-Selmer near-companion curves* over K if there exists a constant $C := C(E, A, K)$ such that for every $\chi \in \mathrm{Hom}(G_K, \{\pm 1\})$,

$$|\dim_{\mathbf{F}_p}(\mathrm{Sel}_p(E^\chi/K)) - \dim_{\mathbf{F}_p}(\mathrm{Sel}_p(A^\chi/K))| < C.$$

If elliptic curves E and A over a number field K are randomly chosen, there is no reason to expect they are p-Selmer near-companion curves over K. Therefore, it seems natural to expect that if E and A are p-Selmer near-companion curves over K, they should be closely related. In fact, Mazur and Rubin conjectured the following [5, Conjecture 7.15].

Conjecture 1. *Suppose that elliptic curves E and A over a number field K are p-Selmer near-companion curves over K; then there exists a G_K-module isomorphism $E[p] \cong A[p]$.*

They proved the converse (with a stronger assumption if $p = 2$ or 3) of the conjecture as follows [5, Theorem 7.13].

Received by the editors November 8, 2016, and in revised form, February 27, 2018.
2010 *Mathematics Subject Classification.* Primary 11G05.

Theorem 1 (Mazur-Rubin)**.** *Let E and A be elliptic curves over a number field K. Let $m_p = p^2$ if $p = 2$ or 3, and $m_p = p$ if $p > 3$. Suppose that there is a G_K-module isomorphism $E[m_p] \cong A[m_p]$. Then E and A are p-Selmer near-companion curves over K.*

Let us briefly discuss the idea of the proof of Theorem 1. Suppose that there is a G_K-module isomorphism $E[m_p] \cong A[m_p]$. Then one can prove that for every $\chi \in \mathrm{Hom}(G_K, \{\pm 1\})$, the local conditions of $\mathrm{Sel}_p(E^\chi/K)$ and $\mathrm{Sel}_p(A^\chi/K)$ are the same everywhere except possibly at places in some finite set $S_{(E,K,p)}$ of places of K, which is independent of the choice of χ. Applying [3, Theorem 2.3.4], one can prove

$$|\dim_{\mathbf{F}_p}(\mathrm{Sel}_p(E^\chi/K)) - \dim_{\mathbf{F}_p}(\mathrm{Sel}_p(A^\chi/K))| \le \sum_{v \in S_{(E,K,p)}} \dim_{\mathbf{F}_p}(E^\chi(K_v)/pE^\chi(K_v)).$$

Moreover the right-hand side of the inequality is bounded by a certain constant, which is independent of the choice of χ. For example, when v is a prime of K above p, we have

$$\dim_{\mathbf{F}_p}(E^\chi(K_v)/pE^\chi(K_v)) = [K_v : \mathbf{Q}_p] + \dim_{\mathbf{F}_p}(E^\chi(K_v)[p]) \le [K_v : \mathbf{Q}_p] + 2.$$

The main theorem of this article is the following.

Theorem 2. *Suppose that elliptic curves E and A over a number field K are 2-Selmer near-companion curves over K, and then there is a G_K-module isomorphism $E[2] \cong A[2]$.*

We prove its contrapositive. First note that $K(E[2]) = K(A[2])$ if and only if there is a G_K-module isomorphism $E[2] \cong A[2]$, that is, Lemma 1.5. We prove the following theorems by applying Theorem 4.4, Theorem 5.2, Theorem 6.4 inductively (the assumptions on these theorems are only about the extensions $K(E[2])/K$ and $K(A[2])/K$, and they are invariant under quadratic twists by Remark 1.2, so we can use induction).

Theorem 3. *Suppose that $K(E[2]) \ne K(A[2])$ and $[K(E[2]) : K] \le [K(A[2]) : K]$. Then for any integer d, there exist infinitely many $\chi \in \mathrm{Hom}(G_K, \{\pm 1\})$ such that*

$$\dim_{\mathbf{F}_2}(\mathrm{Sel}_2(E^\chi/K)) - \dim_{\mathbf{F}_2}(\mathrm{Sel}_2(A^\chi/K)) > d.$$

Theorem 4. *Suppose that $K(E[2]) \ne K(A[2])$. Suppose that one of the following conditions holds:*

- *$[K(E[2]) : K]$ and $[K(A[2]) : K]$ are divisible by 3, or*
- *$[K(E[2]) : K] = [K(A[2]) : K] = 2$.*

Then for any integer d, there exist infinitely many $\chi_1, \chi_2 \in \mathrm{Hom}(G_K, \{\pm 1\})$ such that

(i) $\dim_{\mathbf{F}_2}(\mathrm{Sel}_2(E^{\chi_1}/K)) - \dim_{\mathbf{F}_2}(\mathrm{Sel}_2(A^{\chi_1}/K)) > d$, *and*
(ii) $\dim_{\mathbf{F}_2}(\mathrm{Sel}_2(A^{\chi_2}/K)) - \dim_{\mathbf{F}_2}(\mathrm{Sel}_2(E^{\chi_2}/K)) > d$.

Let C be an elliptic curve over K, and let $r_{C/K}$ denote the Mordell-Weil rank of C over K. Then the following exact sequence

$$0 \to C(K)/2C(K) \to \mathrm{Sel}_2(C/K) \to Ш_{C/K}[2] \to 0,$$

where $Ш_{C/K}$ denotes the Shafarevich-Tate group of C over K, together with the above theorems imply the following corollaries.

Corollary 1. *Suppose that the hypotheses in Theorem* 3 *hold. Then for any integer* d*, there exist infinitely many* $\chi \in \mathrm{Hom}(G_K, \{\pm 1\})$ *such that*

$$r_{E^\chi/K} - r_{A^\chi/K} > d, \ \textit{or} \ \dim_{\mathbf{F}_2}(\text{Ш}_{E^\chi/K}[2]) - \dim_{\mathbf{F}_2}(\text{Ш}_{A^\chi/K}[2]) > d.$$

Corollary 2. *Suppose that the hypotheses in Theorem* 4 *hold. Then for any integer* d*, there exist infinitely many* $\chi_1, \chi_2 \in \mathrm{Hom}(G_K, \{\pm 1\})$ *such that*

(i) $r_{E^{\chi_1}/K} - r_{A^{\chi_1}/K} > d$, *or* $\dim_{\mathbf{F}_2}(\text{Ш}_{E^{\chi_1}/K}[2]) - \dim_{\mathbf{F}_2}(\text{Ш}_{A^{\chi_1}/K}[2]) > d$,
(ii) $r_{A^{\chi_2}/K} - r_{E^{\chi_2}/K} > d$, *or* $\dim_{\mathbf{F}_2}(\text{Ш}_{A^{\chi_2}/K}[2]) - \dim_{\mathbf{F}_2}(\text{Ш}_{E^{\chi_2}/K}[2]) > d$.

When E and A are elliptic curves over a number field K, and are isogenous over K of degree n, where n is coprime to 2, it is easy to see that E and A are 2-Selmer companion curves over K since the isogeny induces the isomorphism $\mathrm{Sel}_2(E^\chi/K) \cong \mathrm{Sel}_2(A^\chi/K)$ for any $\chi \in \mathrm{Hom}(G_K, \{\pm 1\})$. It is interesting to note that when E and A are isogenous over K of degree 2, it is possible that E and A are not even 2-Selmer near-companion curves over K. A large family of examples of such E and A is given by Theorem 3.

Corollary 3. *Let* E *and* A *be elliptic curves over a number field* K*. Suppose that* E *and* A *are isogenous over* K *of degree* 2*. Suppose further* $K(E[2]) \neq K(A[2])$*; then* E *and* A *are not* 2*-Selmer near-companion curves over* K*.*

Due to the lack of the tools to analyze the behavior of the p-Selmer ranks in the family of quadratic twists for prime numbers p other than 2, we focus on the case $p = 2$ in the present article. The point is that when $p = 2$, for any $\chi \in \mathrm{Hom}(G_K, \{\pm 1\})$, there is a canonical G_K-module isomorphism between $E[2]$ and $E^\chi[2]$, so we can compare $\mathrm{Sel}_2(E/K)$ and $\mathrm{Sel}_2(E^\chi/K)$ in the same cohomology group $H^1(K, E[2])$. Moreover, local conditions of $\mathrm{Sel}_2(E/K)$ and $\mathrm{Sel}_2(E^\chi/K)$ at a place v are in the same cohomology group $H^1(K_v, E[2])$, so we can compare the local conditions. In fact, the main idea is to choose χ so that the local conditions of $\mathrm{Sel}_2(E/K)$ and $\mathrm{Sel}_2(E^\chi/K)$ are the same everywhere except one place, whence we get a rank variation in a controllable way.

However, for an odd prime p, there is no canonical G_K-module isomorphism between $E[p]$ and $E^\chi[p]$, so it is rather difficult to compute $\dim_{\mathbf{F}_p}(\mathrm{Sel}_p(E^\chi/K))$ from the information of $\dim_{\mathbf{F}_p}(\mathrm{Sel}_p(E/K))$ (local conditions of $\mathrm{Sel}_p(E/K)$ and $\mathrm{Sel}_p(E^\chi/K)$ are not comparable).

We write M, M' for $K(E[2]), K(A[2])$, respectively. In the rest of the paper, we suppose $M \neq M'$ for our purpose. In Section 3, we define metabolic spaces and Lagrangian subspaces. With these notions, we prove Proposition 3.10, which plays an important role to show our main theorem. We prove the main theorem by case by case. In Section 4, we deal with the case $[M : K], [M' : K]$ are divisible by 3. For the rest of the cases, we assume $[M : K] \leq [M' : K]$ by symmetry. In Section 5, we take care of the case $[M : K] = 1$ or 2, and $[M' : K]$ is divisible by 3. Section 6 will be devoted to the last case: $[M : K] = 1$ or 2, and $[M' : K] = 2$.

1. Preliminaries

We fix a number field K. We write K_v for the completion of K at a place v. In addition, we fix an embedding $\overline{K} \to \overline{K_v}$ for every place v of K, so that $G_{K_v} \subset G_K$, where G_{K_v}, G_K denote the absolute Galois groups of K_v, K, respectively. In this section, let C denote an elliptic curve over K.

Definition 1.1. Let L be a field of characteristic 0. We write

$$\mathcal{C}(L) := \operatorname{Hom}(G_L, \{\pm 1\}).$$

If L is a local field, we often identify $\mathcal{C}(L)$ with $\operatorname{Hom}(L^\times, \{\pm 1\})$ via the local reciprocity map, and let $\mathcal{C}_{\mathrm{ram}}(L) \subset \mathcal{C}(L)$ be the subset of ramified characters in $\mathcal{C}(L)$ (by local class field theory, $\chi \in \mathcal{C}_{\mathrm{ram}}(L)$ if and only if $\chi(\mathcal{O}_L^\times) \neq 1$, where $\mathcal{O}_L^\times$ is the unit group of L).

Remark 1.2. For any $\chi \in \mathcal{C}(K)$, note that there is a canonical G_K-module isomorphism

$$C[2] \cong C^\chi[2],$$

which is the restriction of the canonical isomorphism $\phi : C \to C^\chi$, where $\phi^\sigma(P) = \chi(\sigma)\phi(P)$ for $P \in C(\overline{K})$ and $\sigma \in G_K$. Indeed, if $P \in C[2]$, then for any $\sigma \in G_K$

$$\phi^\sigma(P) = \chi(\sigma)\phi(P) = \pm\phi(P) = \phi(P).$$

The same is true if K is replaced by K_v.

Lemma 1.3. *Let $\mathfrak{q} \nmid 2$ be a prime of K. Then*

$$\dim_{\mathbf{F}_2}(C(K_\mathfrak{q})/2C(K_\mathfrak{q})) = \dim_{\mathbf{F}_2}(C(K_\mathfrak{q})[2]).$$

Proof. For any odd prime p, the pro-p part of $C(K_\mathfrak{q})$ is 2-divisible. Therefore, there is an isomorphism

$$C(K_\mathfrak{q})/2C(K_\mathfrak{q}) \cong C(K_\mathfrak{q})[2^\infty]/2C(K_\mathfrak{q})[2^\infty],$$

so the lemma follows. ☐

Theorem 1.4. *The Tate local duality and the Weil pairing induce a nondegenerate pairing*

$$\langle\ ,\ \rangle_v : H^1(K_v, C[2]) \times H^1(K_v, C[2]) \longrightarrow H^2(K_v, \{\pm 1\}), \tag{1}$$

where $H^2(K_v, \{\pm 1\}) \cong \mathbf{F}_2$ unless v is a complex place.

Proof. For example, see [6, Theorem 7.2.6]. ☐

Lemma 1.5. *Let E, A be elliptic curves over K. Then $K(E[2]) = K(A[2])$ if and only if there exists a G_K-module isomorphism $E[2] \cong A[2]$.*

Proof. If there is a G_K-module isomorphism $E[2] \cong A[2]$, then

$$\{\sigma \in G_K : \sigma P = P \text{ for every } P \in E[2]\} = \{\sigma \in G_K : \sigma P' = P' \text{ for every } P' \in A[2]\},$$

so $K(E[2]) = K(A[2])$ (the fixed field of the group above). Now we prove the converse. Fixing bases of $E[2], A[2]$ over $\mathbf{F}_2$, one can define injective maps $\phi : \operatorname{Gal}(K(E[2])/K) \hookrightarrow \mathrm{GL}_2(\mathbf{F}_2)$ and $\phi' : \operatorname{Gal}(K(A[2])/K) \hookrightarrow \mathrm{GL}_2(\mathbf{F}_2)$. Elementary group theory proves that any (group) isomorphism between two (possibly the same) subgroups of $\mathrm{GL}_2(\mathbf{F}_2)$ is given by the restriction of an inner automorphism of $\mathrm{GL}_2(\mathbf{F}_2)$ ($\cong S_3$). Therefore after an appropriate change of basis, we can identify the maps ϕ and ϕ', whence we derive a G_K-module isomorphism $E[2] \cong A[2]$. ☐

The following lemmas will be used frequently in later sections.

Lemma 1.6. *Let S be a (finite) set of places of K such that $\mathrm{Pic}(\mathcal{O}_{K,S}) = 1$, where $\mathcal{O}_{K,S}$ denotes the ring of S-integers of K. The image of the restriction map*

$$\begin{aligned}\mathcal{C}(K) = \mathrm{Hom}(\mathbf{A}_K^\times/K^\times, \{\pm 1\}) &= \mathrm{Hom}((\textstyle\prod_{\mu \in S} K_\mu^\times \times \prod_{\nu \notin S} \mathcal{O}_\nu^\times)/\mathcal{O}_{K,S}^\times, \{\pm 1\}) \\ &\longrightarrow \textstyle\prod_{\mu \in S} \mathrm{Hom}(K_\mu^\times, \{\pm 1\}) \times \prod_{\nu \notin S} \mathrm{Hom}(\mathcal{O}_\nu^\times, \{\pm 1\})\end{aligned}$$

is the set of all $((f_\mu)_{\mu \in S}, (g_\nu)_{\nu \notin S})$ such that $\prod_{\mu \in S} f_\mu(b) \prod_{\nu \notin S} g_\nu(b) = 1$ for all $b \in \mathcal{O}_{K,S}^\times$, where $f_\mu \in \mathrm{Hom}(K_\mu^\times, \{\pm 1\})$ and $g_\nu \in \mathrm{Hom}(\mathcal{O}_\nu^\times, \{\pm 1\})$.

Proof. The Lemma follows from the class field theory. $\square$

Lemma 1.7. *Let $\mathcal{K}$ be a field of characteristic not equal to 2. Suppose $\mathcal{M}$ is a Galois extension of $\mathcal{K}$. Suppose that $\mathcal{N} \subset \mathcal{M}(\sqrt{\mathcal{M}^\times})$ is an extension of $\mathcal{M}$, i.e., $\mathcal{N}$ is a compositum of quadratic extensions of $\mathcal{M}$. Then the Galois closure of $\mathcal{N}$ over $\mathcal{K}$ is contained in $\mathcal{M}(\sqrt{\mathcal{M}^\times})$.*

Proof. The Galois closure is a compositum of $\sigma\mathcal{N}$, where σ is an embedding from $\mathcal{N}$ to $\overline{\mathcal{K}}$. Since $\sigma(\mathcal{M}) = M$, and $\mathcal{N}$ is a compositum of quadratic extensions of $\mathcal{M}$, it follows that $\sigma\mathcal{N}$ is also a compositum of quadratic extensions of $\mathcal{M}$. $\square$

Lemma 1.8. *The Galois group $\mathrm{Gal}(K(C[4])/K(C[2]))$ is a Boolean group, i.e., an abelian group in which every nontrivial element has order 2. In other words, $K(C[4])$ is a compositum of quadratic extensions of $K(C[2])$.*

Proof. For any $\sigma \in \mathrm{Gal}(K(C[4])/K(C[2]))$ and $P \in C[4]$, since $\sigma(2P) = 2P$, we have $\sigma(P) - P \in C[2]$, so $\sigma(\sigma(P) - P) + (\sigma(P) - P) = 0$, i.e., $\sigma^2(P) = P$. $\square$

2. Selmer groups and local conditions

From now on, fix elliptic curves E and A over K. For the rest of the paper, let $M := K(E[2])$ and $M' := K(A[2])$. For our main purpose, we suppose $M \neq M'$. In this section, we define various 2-Selmer groups and list useful lemmas to be used in later sections. Let S be a (finite) set of places of K containing all primes above 2, all primes where E or A has bad reduction, and all archimedean places. We enlarge S, if necessary so that $\mathrm{Pic}(\mathcal{O}_{K,S}) = 1$, where $\mathcal{O}_{K,S}$ denotes the ring of S-integers of K. We continue to assume that C is an elliptic curve over K. Let $\mathfrak{q}$ denote a place of K.

Definition 2.1. We define the restriction map

$$\mathrm{res}_\mathfrak{q} : H^1(K, C[2]) \to H^1(K_\mathfrak{q}, C[2])$$

as the restriction map of group cohomology.

Although the map $\mathrm{res}_\mathfrak{q}$ depends on C, we suppress it from the notation. Which elliptic curve we take for the restriction map will always be clear from the context.

Definition 2.2. For $\chi \in \mathcal{C}(K_v)$, we define

$$\beta_{C,v}(\chi) := \mathrm{Im}\big(C^\chi(K_v)/2C^\chi(K_v) \to H^1(K_v, C^\chi[2]) \cong H^1(K_v, C[2])\big),$$

where the first map is the Kummer map. Define

$$h_{C,v}(\chi) := \dim_{\mathbf{F}_2} \big(\beta_{C,v}(1_v)/(\beta_{C,v}(1_v) \cap \beta_{C,v}(\chi))\big),$$

where $1_v \in \mathcal{C}(K_v)$ denotes the trivial homomorphism.

Definition 2.3. For $i = 0, 1, 2$, define

$$\mathcal{P}_{E,i} := \{\mathfrak{q} : \mathfrak{q} \notin S \text{ and } \dim_{\mathbf{F}_2}(E(K_\mathfrak{q})[2]) = i\} \text{ and}$$
$$\mathcal{P}_{A,i} := \{\mathfrak{q} : \mathfrak{q} \notin S \text{ and } \dim_{\mathbf{F}_2}(A(K_\mathfrak{q})[2]) = i\}.$$

Define $\mathcal{P}_0 := \mathcal{P}_{E,0} \cap \mathcal{P}_{A,0}$.

Remark 2.4. Recall that for any $\chi_\mathfrak{q} \in \mathcal{C}(K_\mathfrak{q})$, there is a canonical isomorphism $E[2] \cong E^{\chi_\mathfrak{q}}[2]$. Hence, Lemma 1.3 shows that if $\mathfrak{q} \in \mathcal{P}_{E,i}$, then

$$\dim_{\mathbf{F}_2}(\beta_{E,\mathfrak{q}}(1_\mathfrak{q})) = \dim_{\mathbf{F}_2}(\beta_{E,\mathfrak{q}}(\chi_\mathfrak{q})) = i.$$

The same is true if E is replaced by A.

Lemma 2.5. *Suppose that $\mathfrak{q} \notin S$. Then*

(i) $\mathfrak{q} \in \mathcal{P}_{E,0}$ *if and only if* $\mathrm{Frob}_\mathfrak{q}|_M \in \mathrm{Gal}(M/K)$ *has order* 3,
(ii) $\mathfrak{q} \in \mathcal{P}_{E,1}$ *if and only if* $\mathrm{Frob}_\mathfrak{q}|_M \in \mathrm{Gal}(M/K)$ *has order* 2,
(iii) $\mathfrak{q} \in \mathcal{P}_{E,2}$ *if and only if* $\mathrm{Frob}_\mathfrak{q}|_M \in \mathrm{Gal}(M/K)$ *is trivial.*

The same is true if E, M are replaced by A, M', respectively.

Proof. Note that for every $\mathfrak{q} \notin S$, the extension M/K is unramified at $\mathfrak{q}$. The lemma follows from Lemma 1.3. ☐

Remark 2.6. Recall that $M \neq M'$. Suppose both $[M : K]$ and $[M' : K]$ are divisible by 3 (so, $\mathrm{Gal}(M/K), \mathrm{Gal}(M'/K)$ are S_3 or $\mathbf{Z}/3\mathbf{Z}$). Then, $[M \cap M' : K]$ is not divisible by 3 since otherwise M and M' would be the Galois closure of $M \cap M'$ over K (S_3 has no normal subgroup of order 2). Hence there exists $\sigma \in \mathrm{Gal}(MM'/K)$ such that

- $\sigma|_{M\cap M'} = 1$,
- $\sigma|_M$ has order 3,
- $\sigma|_{M'}$ has order 3.

By the Chebotarev density theorem there exist infinitely many primes $\mathfrak{q} \notin S$ such that $\mathrm{Frob}_\mathfrak{q}|_{MM'} = \sigma$. Then by Lemma 2.5, $\mathcal{P}_0$ is an infinite set in this case.

Definition 2.7. Let $\chi \in \mathcal{C}(K)$. The 2-Selmer group $\mathrm{Sel}_2(C^\chi) \subset H^1(K, C[2])$ of C^χ (over K) is the (finite dimensional) $\mathbf{F}_2$-vector space defined by the following exact sequence

$$0 \longrightarrow \mathrm{Sel}_2(C^\chi) \longrightarrow H^1(K, C[2]) \longrightarrow \bigoplus_v H^1(K_v, C[2])/\beta_{C,v}(\chi_v),$$

where the rightmost map is the sum of the restriction maps, and χ_v is the restriction of χ to G_{K_v}. In particular, if χ is the trivial character, it is the classical 2-Selmer group of C.

Definition 2.8. Define

$$r_2(C) := \dim_{\mathbf{F}_2}(\mathrm{Sel}_2(C))$$

for the sake of brevity.

The following theorem due to Kramer gives a parity relation between $r_2(C)$ and $r_2(C^\chi)$ for $\chi \in \mathcal{C}(K)$.

Theorem 2.9 (Kramer)**.** *Let $\chi \in \mathcal{C}(K)$. We have*

$$r_2(C) - r_2(C^\chi) \equiv \sum_v h_{C,v}(\chi_v) (\mathit{mod}\ 2),$$

where χ_v is the restriction of χ to G_{K_v}.

Proof. See, for example, [4, Theorem 2.7] and [4, Lemma 2.9]. ☐

Lemma 2.10. *Let $\chi_v \in \mathcal{C}(K_v)$. Suppose that at least one of the following conditions holds:*

- *χ_v is trivial,*
- *$v \nmid \infty$, C/K_v has good reduction, and χ_v is unramified,*
- *$v \nmid 2$ is a prime of K and $C(K_v)[2] = 0$.*

Then $\beta_{C,v}(1_v) = \beta_{C,v}(\chi_v)$, i.e., $h_{C,v}(\chi_v) = 0$.

Proof. The first case is easy to see. The third one follows from Lemma 1.3. Let $L = \overline{K}_v^{\ker(\chi_v)}$. In the second case, [2, Corollary 4.4] shows that $\mathbf{N}_{L/K_v}(C(L)) = C(K_v)$, where $\mathbf{N}_{L/K_v}$ is the norm map from $C(L)$ to $C(K_v)$. Thus, by the lemma [4, Lemma 2.9], the result follows. ☐

Remark 2.11. For a given elliptic curve C over K and $\chi \in \mathcal{C}(K)$, there are only finitely many places where either C has bad reduction or χ is ramified. Thus, by Lemma 2.10, the sum in Theorem 2.9 is indeed a finite sum.

Lemma 2.12. *Let $\mathfrak{q} \nmid 2$ be a prime of K and suppose C has good reduction at $\mathfrak{q}$. Let $\chi_\mathfrak{q} \in \mathcal{C}_{\mathrm{ram}}(K_\mathfrak{q})$. Then*

$$\beta_{C,\mathfrak{q}}(1_\mathfrak{q}) \cap \beta_{C,\mathfrak{q}}(\chi_\mathfrak{q}) = \{0\} \text{ and } h_{C,\mathfrak{q}}(\chi_\mathfrak{q}) = \dim_{\mathbf{F}_2}(C(K_\mathfrak{q})[2]).$$

Proof. This is [4, Lemma 2.11]. ☐

We define strict, relaxed, and locally twisted 2-Selmer groups as follows.

Definition 2.13. Define the strict 2-Selmer group at $\mathfrak{q}$

$$\mathrm{Sel}_{2,\mathfrak{q}}(C) := \{x \in \mathrm{Sel}_2(C) : \mathrm{res}_\mathfrak{q}(x) = 0\}.$$

Define the relaxed 2-Selmer group at $\mathfrak{q}$

$$\mathrm{Sel}_2^\mathfrak{q}(C) := \{x \in H^1(K, C[2]) : \mathrm{res}_v(x) \in \beta_{C,v}(1_v) \text{ if } v \neq \mathfrak{q}\}.$$

For $\psi_\mathfrak{q} \in \mathcal{C}(K_\mathfrak{q})$, define

$$\begin{aligned}\mathrm{Sel}_2(C, \psi_\mathfrak{q}) := \{x \in H^1(K, C[2]) :\ & \mathrm{res}_\mathfrak{q}(x) \in \beta_{C,\mathfrak{q}}(\psi_\mathfrak{q}), \text{ and} \\ & \mathrm{res}_v(x) \in \beta_{C,v}(1_v) \text{ if } v \neq \mathfrak{q}\}.\end{aligned}$$

Theorem 2.14. *The images of right-hand restriction maps of the following exact sequences are orthogonal complements with respect to the pairing given by the pairing* (1) *at $\mathfrak{q}$*

$$0 \longrightarrow \mathrm{Sel}_2(C) \longrightarrow \mathrm{Sel}_2^\mathfrak{q}(C) \longrightarrow H^1(K_\mathfrak{q}, C[2])/\beta_{C,\mathfrak{q}}(1_\mathfrak{q}),$$

$$0 \longrightarrow \mathrm{Sel}_{2,\mathfrak{q}}(C) \longrightarrow \mathrm{Sel}_2(C) \longrightarrow \beta_{C,\mathfrak{q}}(1_\mathfrak{q}).$$

In particular,

$$\dim_{\mathbf{F}_2}(\mathrm{Sel}_2^\mathfrak{q}(C)) - \dim_{\mathbf{F}_2}(\mathrm{Sel}_{2,\mathfrak{q}}(C)) = \dim_{\mathbf{F}_2}(\beta_{C,\mathfrak{q}}(1_\mathfrak{q})) = \frac{1}{2}\dim_{\mathbf{F}_2}(H^1(K_\mathfrak{q}, C[2])).$$

Proof. The theorem follows from the global Poitou-Tate duality. For example, see [3, Theorem 2.3.4]. ☐

3. Metabolic spaces and Lagrangian subspaces

In this section, we define metabolic spaces, Lagrangian (maximal isotropic) subspaces, and canonical quadratic forms induced by the Heisenberg groups. We closely follow [1]. For general theory, we refer the reader to Section 2 and Section 4 of [7]. The main goal of this section is to prove Proposition 3.10, which will play a crucial role to prove Theorem 4.4, Theorem 5.2, and Theorem 6.4. We continue to assume that C is an elliptic curve over K.

Let V be a finite dimensional $\mathbf{F}_2$-vector space.

Definition 3.1. A *quadratic form* on V is a function $q : V \to \mathbf{F}_2$ such that

- $q(av) = a^2 q(v)$ for every $a \in \mathbf{F}_2$ and $v \in V$, and
- the map $(v, w)_q := q(v + w) - q(v) - q(w)$ is a bilinear form.

We call X a *Lagrangian subspace* or *maximal isotropic subspace* of V if

(i) $q(X) = 0$, and
(ii) $X = X^{\perp}$ in the induced bilinear form.

A *metabolic space* (V, q) is a vector space such that $(,)_q$ is nondegenerate and V contains a Lagrangian subspace.

Definition 3.2. Let L be either K or K_v for a place v of K. Define the Heisenberg group of C over L

$$\mathcal{H}_{C,L} := \{(f, P) \in \overline{L}(C) \times C[2] : \text{ the divisor of } f \text{ is } 2[P] - 2[O],$$

where $\overline{L}(C)$ is the function field of C over $\overline{L}$, and O is the trivial element of $C[2]$. The group law is defined by

$$(f, P) \times (g, Q) := (\tau_Q^*(f)g, P + Q),$$

where τ_Q is translation by Q on C.

We have an exact sequence

$$1 \to \overline{L}^{\times} \to \mathcal{H}_{C,L} \to C[2] \to 0, \tag{2}$$

where the middle maps are defined by sending l to (l, O), and by taking (f, P) to P, respectively. Let

$$q_{\mathcal{H}_{C,L}} : H^1(L, C[2]) \to H^2(L, \overline{L}^{\times})$$

be the connecting homomorphism of the long exact sequence of (non-abelian) Galois cohomology groups induced by (2). By the construction, $q_{\mathcal{H}_{C,L}}$ is functorial with respect to the base extension.

Definition 3.3. Define

$$q_{C,v} : H^1(K_v, C[2]) \to H^2(K_v, \overline{K}_v^{\times}) \subset \mathbf{Q}/\mathbf{Z}$$

to be the composition of $q_{\mathcal{H}_{C,K_v}}$ and the invariant map $\mathrm{inv}_v : H^2(K_v, \overline{K}_v^{\times}) \to \mathbf{Q}/\mathbf{Z}$.

Note that since $q_{\mathcal{H}_{C,L}}$ is a quadratic form [7, Corollary 4.7], so is $q_{C,v}$. Recall that for a quadratic form q, we associate a bilinear form $(,)_q$ (Definition 3.1).

Theorem 3.4. *Suppose that $\chi \in \mathcal{C}(K_v)$. We have*

(i) *The bilinear form on $H^1(K_v, C[2])$ associated to $q_{C,v}$ is exactly the pairing* (1) *in Theorem* 1.4.
(ii) *$\beta_{C,v}(1_v)$ is a Lagrangian subspace of $(H^1(K_v, C[2]), q_{C,v})$.*
(iii) *$(H^1(K_v, C[2]), q_{C,v})$ is a metabolic space.*

(iv) *The canonical isomorphism* $C[2] \cong C^\chi[2]$ *identifies* $q_{C,v}$ *and* $q_{C^\chi,v}$.

(v) $\beta_{C,v}(\chi)$ *is a Lagrangian subspace of* $(H^1(K_v, C[2]), q_{C,v})$.

Proof. The assertion (i) is [7, Corollary 4.7]. The assertion (ii) follows from [7, Proposition 4.9]. (iii) is an easy consequence of (i) and (ii). The assertion (iv) is proved in [1, Lemma 5.2], and (v) follows from (ii) and (iv). □

Lemma 3.5. *Suppose that* $x \in H^1(K, C[2])$. *Then*

$$\sum_v q_{C,v}(\mathrm{res}_v(x)) = 0.$$

Proof. We have an exact sequence (see [6, Theorem 8.1.17] for reference)

$$0 \longrightarrow \mathrm{Br}(K) \longrightarrow \bigoplus_v \mathrm{Br}(K_v) \xrightarrow{\oplus \mathrm{inv}_v} \mathbf{Q}/\mathbf{Z} \longrightarrow 0.$$

The lemma follows from the functoriality. □

Lemma 3.6. *Suppose that* (V, q) *is a metabolic space such that* $\dim_{\mathbf{F}_2}(V) = 2n$. *Then for a given Lagrangian subspace* X *of* V, *there are exactly* $2^{n(n-1)/2}$ *Lagrangian subspaces that intersect* X *trivially; i.e.,*

$$|\{Y : Y \text{ is a Lagrangian subspace such that } Y \cap X = \{0\}\}| = 2^{n(n-1)/2}.$$

Proof. This is immediate from Proposition 2.6 (b), (c), and (e) in [7]. □

Proposition 3.7. *Let* $\mathfrak{q}$ *be a prime of* K. *Then* $\mathrm{res}_\mathfrak{q}(\mathrm{Sel}_2^\mathfrak{q}(C)) \subset H^1(K_\mathfrak{q}, C[2])$ *is a Lagrangian subspace of* $(H^1(K_\mathfrak{q}, C[2]), q_{C,\mathfrak{q}})$.

Proof. Theorem 3.4(ii) shows that for $v \neq \mathfrak{q}$, we have $q_{C,v}(\mathrm{res}_v(x)) = 0$. It follows that $q_{C,\mathfrak{q}}(\mathrm{res}_\mathfrak{q}(x)) = 0$ by Lemma 3.5. Therefore, $\mathrm{res}_\mathfrak{q}(\mathrm{Sel}_2^\mathfrak{q}(C))$ is contained in its orthogonal complement in the pairing $(,)_{q_{C,\mathfrak{q}}}$ of Definition 3.1, that is, (1) by Theorem 3.4(i). Since $\dim_{\mathbf{F}_2}(\mathrm{res}_\mathfrak{q}(\mathrm{Sel}_2^\mathfrak{q}(C))) = \frac{1}{2}\dim_{\mathbf{F}_2}(H^1(K_\mathfrak{q}, C[2]))$ by Theorem 2.14, $\mathrm{res}_\mathfrak{q}(\mathrm{Sel}_2^\mathfrak{q}(C))$ is indeed equal to its orthogonal complement. □

Lemma 3.8. *Let* $\mathfrak{q} \nmid 2$ *be a prime of* K, *where* C *has good reduction. Let* $\eta \in \mathcal{C}_{\mathrm{ram}}(K_\mathfrak{q})$. *Then*

$$C^\eta(K_\mathfrak{q})[2^\infty] = C^\eta(K_\mathfrak{q})[2],$$

where C *is naturally regarded as an elliptic curve over* $K_\mathfrak{q}$, *and* C^η *is the quadratic twists of* C *by* η.

Proof. Let $K_\mathfrak{q}^{\mathrm{ur}}$ denote the maximal unramified extension of $K_\mathfrak{q}$. We show

$$C^\eta(K_\mathfrak{q}^{\mathrm{ur}})[2^\infty] = C^\eta(K_\mathfrak{q}^{\mathrm{ur}})[2],$$

and then the result follows by taking the submodules of $\mathrm{Gal}(K_\mathfrak{q}^{\mathrm{ur}}/K_\mathfrak{q})$-invariant elements on both sides. Under our assumption that C has good reduction at $\mathfrak{q} \nmid 2$, it is well known that $C(K_\mathfrak{q}^{\mathrm{ur}})[2^\infty] = C[2^\infty]$. Thus, if $P \in C^\eta(K_\mathfrak{q}^{\mathrm{ur}})[2^\infty]$, then $\eta(\sigma)(P) = P$ for any $\sigma \in G_{K_\mathfrak{q}^{\mathrm{ur}}}$ by the definition of quadratic twists. Since η is ramified, it follows that $2P = 0$, so $P \in C^\eta(K_\mathfrak{q}^{\mathrm{ur}})[2]$, whence the assertion follows. □

Lemma 3.9. *Let* $\mathfrak{q} \nmid 2$ *be a prime of* K, *where* C *has good reduction. Suppose that* $C(K_\mathfrak{q})[2] = C[2]$. *Let* $\mathcal{C}_{\mathrm{ram}}(K_\mathfrak{q}) = \{\eta_1, \eta_2\}$. *Then* $\beta_{C,\mathfrak{q}}(1_\mathfrak{q}), \beta_{C,\mathfrak{q}}(\eta_1)$, *and* $\beta_{C,\mathfrak{q}}(\eta_2)$

are Lagrangian subspaces of the metabolic space $(H^1(K_{\mathfrak{q}}, C[2]), q_{C,\mathfrak{q}})$*, whose pairwise intersections are trivial, i.e.,*

$$\beta_{C,\mathfrak{q}}(1_{\mathfrak{q}}) \cap \beta_{C,\mathfrak{q}}(\eta_1) = \beta_{C,\mathfrak{q}}(1_{\mathfrak{q}}) \cap \beta_{C,\mathfrak{q}}(\eta_2) = \beta_{C,\mathfrak{q}}(\eta_1) \cap \beta_{C,\mathfrak{q}}(\eta_2) = \{0\}.$$

Proof. By Theorem 3.4(v), we have that $\beta_{C,\mathfrak{q}}(1_{\mathfrak{q}}), \beta_{C,\mathfrak{q}}(\eta_1)$, and $\beta_{C,\mathfrak{q}}(\eta_2)$ are Lagrangian subspaces. By Lemma 2.12, it only remains to prove that

$$\beta_{C,\mathfrak{q}}(\eta_1) \cap \beta_{C,\mathfrak{q}}(\eta_2) = \{0\}.$$

Let $F_{\mathfrak{q}}$ be the unramified quadratic extension of $K_{\mathfrak{q}}$. Then by [9, Lemma 2.16], it is enough to show that the natural injection $C^{\eta_1}(K_{\mathfrak{q}}) \hookrightarrow C^{\eta_1}(F_{\mathfrak{q}})$ induces

$$C^{\eta_1}(K_{\mathfrak{q}})/2C^{\eta_1}(K_{\mathfrak{q}}) \cong C^{\eta_1}(F_{\mathfrak{q}})/2C^{\eta_1}(F_{\mathfrak{q}}). \tag{3}$$

By the isomorphism in the proof of Lemma 1.3 and Lemma 3.8, it follows that

$$C^{\eta_1}(K_{\mathfrak{q}})/2C^{\eta_1}(K_{\mathfrak{q}}) \cong C^{\eta_1}(K_{\mathfrak{q}})[2^\infty]/2C^{\eta_1}(K_{\mathfrak{q}})[2^\infty] \cong C^{\eta_1}(K_{\mathfrak{q}})[2] \cong C^{\eta_1}[2],$$

where we get the last isomorphism by the assumption $C(K_{\mathfrak{q}})[2] = C[2]$ and the canonical isomorphism $C[2] \cong C^{\eta_1}[2]$. Similarly,

$$C^{\eta_1}(F_{\mathfrak{q}})/2C^{\eta_1}(F_{\mathfrak{q}}) \cong C^{\eta_1}[2],$$

whence (3). □

Proposition 3.10. *Suppose that* $\mathfrak{q} \nmid 2$. *Suppose that* C *has good reduction at* $\mathfrak{q}$ *and* $C(K_{\mathfrak{q}})[2] = C[2]$. *Then*

(i) *If* $\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_2(C)) = 0$*, then there exists* $\psi_{\mathfrak{q}} \in \mathcal{C}_{\mathrm{ram}}(K_{\mathfrak{q}})$ *so that* $\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_2^{\mathfrak{q}}(C)) = \beta_{C,\mathfrak{q}}(\psi_{\mathfrak{q}})$*;*

(ii) *If* $\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_2(C)) = 0$ *and* $\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_2(C, \psi_{\mathfrak{q}})) \neq 0$ *for some* $\psi_{\mathfrak{q}} \in \mathcal{C}_{\mathrm{ram}}(K_{\mathfrak{q}})$*, then* $\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_2^{\mathfrak{q}}(C)) = \beta_{C,\mathfrak{q}}(\psi_{\mathfrak{q}})$*, so* $\mathrm{Sel}_2^{\mathfrak{q}}(C) = \mathrm{Sel}_2(C, \psi_{\mathfrak{q}})$*;*

(iii) *If there is* $s \in \mathrm{Sel}_2(C)$ *such that* $\mathrm{res}_{\mathfrak{q}}(s) \neq 0$*, then for any* $\eta_{\mathfrak{q}} \in \mathcal{C}_{\mathrm{ram}}(K_{\mathfrak{q}})$*, we have* $\dim_{\mathbf{F}_2}(\mathrm{Sel}_2(C, \eta_{\mathfrak{q}})) \leq r_2(C)$*.*

Proof. Lemma 1.3 and Theorem 2.14 show

$$\dim_{\mathbf{F}_2}(\mathrm{Sel}_2^{\mathfrak{q}}(C)) - \dim_{\mathbf{F}_2}(\mathrm{Sel}_{2,\mathfrak{q}}(C)) = 2 \text{ and } \dim_{\mathbf{F}_2}(\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_2^{\mathfrak{q}}(C))) = 2.$$

For (iii), we first note that

$$\mathrm{Sel}_{2,\mathfrak{q}}(C) \subset \mathrm{Sel}_2(C), \mathrm{Sel}_2(C, \eta_{\mathfrak{q}}) \subset \mathrm{Sel}_2^{\mathfrak{q}}(C).$$

Let

$$X := \mathrm{Sel}_2(C)/\mathrm{Sel}_{2,\mathfrak{q}}(C), \text{ and}$$
$$Y := \mathrm{Sel}_2(C, \eta_{\mathfrak{q}})/\mathrm{Sel}_{2,\mathfrak{q}}(C),$$

for convenience. Clearly $\dim_{\mathbf{F}_2}(X+Y) \leq 2$ and Lemma 2.12 implies $X \cap Y = \{0\}$. The assumption of (iii) shows $\dim_{\mathbf{F}_2}(X) \geq 1$, so $\dim_{\mathbf{F}_2}(Y) \leq 1$, whence (iii) follows. We now show (i) and (ii). Let $\mathcal{C}_{\mathrm{ram}}(K_{\mathfrak{q}}) = \{\eta_1, \eta_2\}$. Since $\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_2(C)) = 0$, we have

$$\beta_{C,\mathfrak{q}}(1_{\mathfrak{q}}) \cap \mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_2^{\mathfrak{q}}(C)) = \{0\}.$$

Thus, $\beta_{C,\mathfrak{q}}(\eta_1), \beta_{C,\mathfrak{q}}(\eta_2)$, and $\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_2^{\mathfrak{q}}(C))$ are Lagrangian subspaces of $(H^1(K_{\mathfrak{q}}, C[2]), q_{C,\mathfrak{q}})$, whose intersections with $\beta_{C,\mathfrak{q}}(1_{\mathfrak{q}})$ are trivial. However, Lemma 3.6 asserts that there are only two such Lagrangian subspaces. Hence by Lemma 3.9, we conclude that

$$\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_2^{\mathfrak{q}}(C)) = \beta_{C,\mathfrak{q}}(\eta_1) \text{ or } \mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_2^{\mathfrak{q}}(C)) = \beta_{C,\mathfrak{q}}(\eta_2).$$

Now it is easy to see (i) and (ii) by Lemma 3.9 again. □

4. Case 1: $[M : K], [M' : K]$ are divisible by 3

In this section, we assume that $\mathrm{Gal}(M/K) \cong S_3$ or $\mathbf{Z}/3\mathbf{Z}$, and $\mathrm{Gal}(M'/K) \cong S_3$ or $\mathbf{Z}/3\mathbf{Z}$. Recall that we suppose $M \neq M'$ in this paper. Let Δ_E, Δ_A denote the discriminants of models of E, A, respectively. Let S be a set of places of K defined as in the beginning of Section 2. Enlarge S if necessary, so that $\Delta_E, \Delta_A \in \mathcal{O}_{K,S}^\times$.

Lemma 4.1. *If $i = 0$ or 2, then for every $\mathfrak{q} \in \mathcal{P}_{E,i}$, we have $\Delta_E \in (\mathcal{O}_\mathfrak{q}^\times)^2$.*

Proof. It is easy to see $K(\sqrt{\Delta_E})$ is the only (possibly trivial) quadratic extension over K in M. Then Lemma 2.5 shows that $\mathrm{Frob}_\mathfrak{q}|_M \in \mathrm{Gal}(M/K)$ fixes $\sqrt{\Delta_E}$, and hence $\sqrt{\Delta_E} \in K_\mathfrak{q}^\times$. Since $\Delta_E \in \mathcal{O}_{K,S}^\times$, the result follows immediately. □

We recall $\mathcal{P}_0 = \mathcal{P}_{E,0} \cap \mathcal{P}_{A,0}$.

Lemma 4.2. *Define $\mathcal{A} \subset K^\times/(K^\times)^2$ by*

$$\mathcal{A} := \ker(\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^2 \to \prod_{\mathfrak{q} \in \mathcal{P}_0} \mathcal{O}_\mathfrak{q}^\times/(\mathcal{O}_\mathfrak{q}^\times)^2).$$

Then $\mathcal{A}$ is generated by Δ_E and Δ_A (they are possibly the same or even trivial).

Proof. By Lemma 4.1, clearly $\Delta_E, \Delta_A \in \mathcal{A}$. Suppose $\alpha \in \mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^2$ is not generated by Δ_E, Δ_A. Then MM' and $K(\sqrt{\alpha})$ are linearly disjoint over K, i.e., $MM' \cap K(\sqrt{\alpha}) = K$. By Remark 2.6, there exists $\sigma \in \mathrm{Gal}(MM'K(\sqrt{\alpha})/K)$ such that

- $\sigma|_M \in \mathrm{Gal}(M/K)$ has order 3,
- $\sigma|_{M'} \in \mathrm{Gal}(M'/K)$ has order 3, and
- $\sigma(\sqrt{\alpha}) = -\sqrt{\alpha}$.

Then by the Chebotarev density theorem, there exist infinitely many primes v of K satisfying $\mathrm{Frob}_v|_{MM'K(\sqrt{\alpha})} = \sigma$. By Lemma 2.5, $v \in \mathcal{P}_0$, and the image of α in the natural map

$$\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^2 \to \mathcal{O}_v^\times/(\mathcal{O}_v^\times)^2$$

is not trivial. Hence the lemma follows. □

Proposition 4.3. *For even integers $0 \le i, j \le 2$, the set $\mathcal{P}_{E,i} \cap \mathcal{P}_{A,j}$ is an infinite set. Suppose that $\ell \in \mathcal{P}_{E,i} \cap \mathcal{P}_{A,j}$ and $\psi_\ell \in \mathcal{C}(K_\ell)$. Then, there exists $\chi \in \mathcal{C}(K)$ such that*

$$\mathrm{Sel}_2(E^\chi) = \mathrm{Sel}_2(E, \psi_\ell) \quad \textit{and} \quad \mathrm{Sel}_2(A^\chi) = \mathrm{Sel}_2(A, \psi_\ell).$$

Proof. One can see that $\mathcal{P}_{E,i} \cap \mathcal{P}_{A,j}$ is an infinite set when i, j are even by a similar argument to Remark 2.6 using Lemma 2.5 suitably. The condition that i, j are even numbers implies that $\sqrt{\Delta_E}, \sqrt{\Delta_A} \in K_\ell^\times$ by Lemma 4.1. Therefore, $\psi_\ell(\Delta_E) = \psi_\ell(\Delta_A) = 1$. Let $S(\ell) := S \cup \{\ell\}$. Recall that $\mathrm{Pic}(\mathcal{O}_{K,S}) = 0$, so $\mathrm{Pic}(\mathcal{O}_{K,S(\ell)}) = 0$. Thus global class field theory shows that

$$\mathcal{C}(K) = \mathrm{Hom}(\mathbf{A}_K^\times/K^\times, \{\pm 1\}) = \mathrm{Hom}((\textstyle\prod_{v \in S(\ell)} K_v^\times \times \prod_{\mathfrak{q} \notin S(\ell)} \mathcal{O}_\mathfrak{q}^\times)/\mathcal{O}_{K,S(\ell)}^\times, \{\pm 1\}).$$

Let $\mathcal{P}^K$ denote the set of all places of K. Let

$$\begin{aligned} Q &:= \mathcal{P}^K - \{\mathcal{P}_0 \cup S(\ell)\}, \\ J &:= \mathcal{O}^{\times}_{K,S(\ell)}, \\ G &:= \prod_{\mathfrak{q}\in\mathcal{P}_0} \mathcal{O}^{\times}_{\mathfrak{q}}, \text{ and} \\ H &:= \prod_{\mathfrak{q}\in Q} \mathcal{O}^{\times}_{\mathfrak{q}} \times \prod_{v\in S(\ell)} K_v^{\times}. \end{aligned}$$

Suppose the map

$$\begin{aligned} \Phi : \mathcal{C}(K) = \mathrm{Hom}((G\times H)/J, \{\pm1\}) \longrightarrow & \mathrm{Hom}(H, \{\pm 1\}) \\ & \cong \prod_{\mathfrak{q}\in Q} \mathrm{Hom}(\mathcal{O}^{\times}_{\mathfrak{q}}, \{\pm1\}) \\ & \quad \times \prod_{v\in S(\ell)} \mathrm{Hom}(K_v^{\times}, \{\pm1\}) \end{aligned}$$

is induced by the natural map $H \to (G\times H)/J$. Then [1, Lemma 6.6(i)] and Lemma 4.2 show that $\mathrm{Im}(\Phi)$ is exactly

$$\{h \in \mathrm{Hom}(H, \{\pm1\}) : h(\Delta_E) = h(\Delta_A) = 1\}.$$

Put $f_\mu \in \mathrm{Hom}(K_\mu^{\times}, \{\pm1\})$ for $\mu \in S(\ell)$ and $g_\nu \in \mathrm{Hom}(\mathcal{O}_\nu^{\times}, \{\pm1\})$ for $\nu \in Q$ such that

- $f_\ell = \psi_\ell$,
- $g_{\mathfrak{q}}$ is trivial for $\mathfrak{q} \in Q$,
- $f_v = 1_v$ for $v \in S$.

Note that

$$\begin{aligned} f_\ell(\Delta_E) \cdot \prod_{\mathfrak{q}\in Q} g_{\mathfrak{q}}(\Delta_E) \cdot \prod_{v\in S} f_v(\Delta_E) = 1, \\ f_\ell(\Delta_A) \cdot \prod_{\mathfrak{q}\in Q} g_{\mathfrak{q}}(\Delta_A) \cdot \prod_{v\in S} f_v(\Delta_A) = 1. \end{aligned}$$

Therefore there is a global character $\chi \in \mathcal{C}(K)$ such that

- $\chi_\ell = \psi_\ell$,
- $\chi_{\mathfrak{q}}|_{\mathcal{O}^{\times}_{\mathfrak{q}}} = 1_{\mathfrak{q}}$ for $\mathfrak{q} \in Q$,
- $\chi_v = 1_v$ for $v \in S$,

where $\chi_\ell, \chi_{\mathfrak{q}}, \chi_v$ are the restrictions of χ to $K_\ell^{\times}, K_{\mathfrak{q}}^{\times}, K_v^{\times}$ via the local reciprocity maps, respectively. In particular, if $\mathfrak{q} \in Q$, then $\chi_{\mathfrak{q}}$ is an unramified character of $G_{K_{\mathfrak{q}}}$. Then by Lemma 2.10,

$$\beta_{E,\mathfrak{p}}(1_{\mathfrak{p}}) = \beta_{E,\mathfrak{p}}(\chi_{\mathfrak{p}}) \text{ and } \beta_{A,\mathfrak{p}}(1_{\mathfrak{p}}) = \beta_{A,\mathfrak{p}}(\chi_{\mathfrak{p}})$$

for all places $\mathfrak{p}$ but ℓ, where $\chi_{\mathfrak{p}}$ denotes the restriction of χ to $G_{K_{\mathfrak{p}}}$. Therefore the result follows. □

Theorem 4.4. *Suppose that $[M : K], [M' : K]$ are divisible by 3 and $M \neq M'$. Then there exist infinitely many $\chi_1, \chi_2 \in \mathcal{C}(K)$ such that*

(i) *$r_2(E^{\chi_1}) = r_2(E) + 2$ and $r_2(A^{\chi_1}) = r_2(A)$,*
(ii) *$r_2(A^{\chi_2}) = r_2(A) + 2$ and $r_2(E^{\chi_2}) = r_2(E)$.*

Proof. We prove (i), and (ii) follows similarly. Let $\tilde{s}$ denote the image of $s \in \mathrm{Sel}_2(E)$ in the restriction map

$$\mathrm{Sel}_2(E) \subset H^1(K, E[2]) \to \mathrm{Hom}(G_M, E[2]).$$

Let L be the fixed field of $\bigcap_{s\in\mathrm{Sel}_2(E)} \ker(\tilde{s})$, so $[L : M]$ is a 2-power. Let N denote the Galois closure of L over K. Then $[N : K] = 2^a \cdot 3$ for some a by Lemma 1.7. Then it follows that $[N \cap M' : K]$ is not divisible by 3 since otherwise it would mean $9|[N : K]$ by Remark 2.6. Therefore by the Chebotarev density theorem, there are infinitely many primes $\mathfrak{q} \notin S$ such that

- $\mathrm{Frob}_\mathfrak{q}|_N = 1$,
- $\mathfrak{q} \in \mathcal{P}_{A,0}$, i.e., $\mathrm{Frob}_\mathfrak{q}|_{M'}$ has order 3.

In particular, since $\mathrm{Frob}_\mathfrak{q}|_M = 1$, we have $\mathfrak{q} \in \mathcal{P}_{E,2}$ (Lemma 2.5). By our construction, $\mathrm{res}_\mathfrak{q}(\mathrm{Sel}_2(E)) = 0$, so $\mathrm{Sel}_2(E) = \mathrm{Sel}_{2,\mathfrak{q}}(E)$. By Proposition 3.10(i), there exists $\psi_\mathfrak{q} \in \mathcal{C}_{\mathrm{ram}}(K_\mathfrak{q})$ such that $\beta_{E,\mathfrak{q}}(\psi_\mathfrak{q}) = \mathrm{res}_\mathfrak{q}(\mathrm{Sel}_2^\mathfrak{q}(E))$. Then Proposition 4.3 shows the existence of $\chi_1 \in \mathcal{C}(K)$ such that $\mathrm{Sel}_2(E^{\chi_1}) = \mathrm{Sel}_2^\mathfrak{q}(E)$ and $\mathrm{Sel}_2(A^{\chi_1}) = \mathrm{Sel}_2(A)$, whence the latter can be proved by Lemma 2.10 (the third condition). Hence (i) follows from Lemma 1.3 and Theorem 2.14. ☐

5. Case 2: $[M : K] = 1$ or 2, and $[M' : K] = 3$ or 6

In this section, we assume that $[M : K] = 1$ or 2, and $[M' : K] = 3$ or 6. Let S be the set of places of K as defined in Section 4.

Lemma 5.1. *Suppose $\mathfrak{q} \nmid 2$ and $E[4] \subset E(K_\mathfrak{q})$. Then for any nontrivial $\chi_\mathfrak{q} \in \mathcal{C}(K_\mathfrak{q})$, we have $E^{\chi_\mathfrak{q}}(K_\mathfrak{q})[2^\infty] = E^{\chi_\mathfrak{q}}[2]$. Moreover, there exists a natural isomorphism*

$$E^{\chi_\mathfrak{q}}[2] \cong E^{\chi_\mathfrak{q}}(K_\mathfrak{q})/2E^{\chi_\mathfrak{q}}(K_\mathfrak{q}).$$

Proof. The first assertion follows from the definition of quadratic twist. Then the isomorphism in the proof of Lemma 1.3 shows the second assertion. ☐

Theorem 5.2. *Suppose that $[M : K] = 1$ or 2, and $[M' : K] = 3$ or 6. Then there exist infinitely many $\chi \in \mathcal{C}(K)$ such that $r_2(E^\chi) = r_2(E) + 2$ and $r_2(A^\chi) = r_2(A)$.*

Proof. Let $\tilde{s}$ denote the image of $s \in \mathrm{Sel}_2(E/K)$ in the restriction map

$$\mathrm{Sel}_2(E) \subset H^1(K, E[2]) \to \mathrm{Hom}(G_M, E[2]).$$

Let L be the fixed field of $\bigcap_{s\in\mathrm{Sel}_2(E)} \ker(\tilde{s})$, so $[L : K]$ is a 2-power. Define N to be the Galois closure of $LK(E[4])K(\sqrt{\mathcal{O}_{K,S}^\times})$ over K, where $\mathcal{O}_{K,S}^\times$ is the group of S-units (N is a finite extension of K by Dirichlet's unit theorem; see [8, Lemma 4.1] for example). Then $[N : K]$ is a 2-power as well by Lemma 1.7 and Lemma 1.8. Therefore there exists $\sigma \in \mathrm{Gal}(NM'/K)$ such that

- $\sigma|_N \in \mathrm{Gal}(N/K)$ is trivial,
- $\sigma|_{M'} \in \mathrm{Gal}(M'/K)$ has order 3.

By the Chebotarev density theorem, there exist infinitely many $\mathfrak{q} \notin S$ such that $\mathrm{Frob}_\mathfrak{q}|_{NM'} = \sigma$. Then Lemma 2.5 shows that

$$\mathfrak{q} \in \mathcal{P}_{E,2} \cap \mathcal{P}_{A,0}.$$

Put $f_\mu \in \mathrm{Hom}(K_\mu^\times, \{\pm 1\})$ for $\mu \in S$ and $g_\nu \in \mathrm{Hom}(\mathcal{O}_\nu^\times, \{\pm 1\})$ for $\nu \notin S$ such that

- $f_v = 1_v$ for $v \in S$,

- $g_{\mathfrak{q}}$ is not trivial, and
- $g_{\mathfrak{p}}$ is trivial for $\mathfrak{p} \notin S \cup \{\mathfrak{q}\}$.

Since $K(\sqrt{O_{K,S}^{\times}}) \subset N$ and $\mathrm{Frob}_{\mathfrak{q}}|_N = 1$, we have $g_{\mathfrak{q}}(O_{K,S}^{\times}) = 1$. Therefore Lemma 1.6 shows that there exists $\chi \in \mathcal{C}(K)$ satisfying

- $\chi_v = 1_v$ for $v \in S$,
- $\chi_{\mathfrak{q}}$ is ramified,
- $\chi_{\mathfrak{p}}$ is unramified for $\mathfrak{p} \notin S \cup \{\mathfrak{q}\}$,

where $\chi_v, \chi_{\mathfrak{q}}, \chi_{\mathfrak{p}}$ are restrictions of χ to $K_v^{\times}, K_{\mathfrak{q}}^{\times}, K_{\mathfrak{p}}^{\times}$ via the local reciprocity maps, respectively. Note that $\mathrm{Sel}_2(E) = \mathrm{Sel}_{2,\mathfrak{q}}(E)$ and $\mathrm{Sel}_2(E^{\chi}) = \mathrm{Sel}_2(E, \chi_{\mathfrak{q}})$ by the choice of χ and Lemma 2.10. Hence Theorem 2.14 proves that

$$0 \leq r_2(E^{\chi}) - r_2(E) \leq 2.$$

By our choice of $\mathfrak{q}$, we have $E[4] \subset E(K_{\mathfrak{q}})$. By Lemma 5.1, there is an isomorphism

$$E^{\chi_{\mathfrak{q}}}[2] \cong E^{\chi_{\mathfrak{q}}}(K_{\mathfrak{q}})/2E^{\chi_{\mathfrak{q}}}(K_{\mathfrak{q}}) \cong \beta_{E,\mathfrak{q}}(\chi_{\mathfrak{q}}). \tag{4}$$

Let P be a nontrivial K-rational 2-torsion point of E^{χ}. Define a composition

$$\phi : E^{\chi}(K) \to E^{\chi}(K)/2E^{\chi}(K) \to H^1(K, E^{\chi}[2]),$$

where the first map is the projection and the second map is given by the Kummer map. We have $0 \neq \phi(P) \in \mathrm{Sel}_2(E^{\chi})$ because P is not trivial in $E^{\chi}(K)/2E^{\chi}(K)$ (note that $E^{\chi}(K)[2^{\infty}] \subset E^{\chi}(K_{\mathfrak{q}})[2^{\infty}] = E^{\chi}(K_{\mathfrak{q}})[2]$ by Lemma 5.1). The isomorphism (4) implies that $\mathrm{res}_{\mathfrak{q}}(\phi(P)) \neq 0$. Therefore Theorem 2.14 and Proposition 3.10(ii) show $r_2(E^{\chi}) = r_2(E) + 2$. Since $\mathfrak{q} \in \mathcal{P}_{A,0}$ and $\mathrm{Sel}_2(A^{\chi}) = \mathrm{Sel}_2(A, \chi_{\mathfrak{q}})$, Lemma 2.10 proves that

$$\mathrm{Sel}_2(A) = \mathrm{Sel}_2(A^{\chi}), \text{ and } r_2(A^{\chi}) = r_2(A).$$

□

6. Case 3: $[M : K] = 1$ or 2, and $[M' : K] = 2$

In this section, we assume that $[M : K] = 1$ or 2. We assume further that $[M' : K] = 2$ and $M \neq M'$. Let S be the finite set of places of K as defined in previous sections. For $t \in \mathrm{Sel}_2(A)$, we denote the image in the natural restriction map

$$\mathrm{Sel}_2(A) \subset H^1(K, A[2]) \to \mathrm{Hom}(G_{M'}, A[2])$$

by $\tilde{t}$ and let $\underline{t}$ denote the image of t in the restriction map

$$\mathrm{Sel}_2(A) \subset H^1(K, A[2]) \to H^1(M, A[2]).$$

Let T be a (finite) set of places of M containing all primes above 2, all primes where E has bad reduction, and all archimedean places. In addition, we assume that $\mathrm{Pic}(\mathcal{O}_{M,T}) = 1$, where $\mathcal{O}_{M,T}$ is the ring of T-integers of M. In the following Lemma, we use notations $\mathrm{Sel}_2(E/K), \mathrm{Sel}_2(E/M)$ to specify the base fields K, M on which the Selmer groups are defined.

Lemma 6.1. *There is a composition of injective group homomorphisms*

$$\mathrm{Sel}_2(E/K) \hookrightarrow \mathrm{Sel}_2(E/M) \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(M(\sqrt{\mathcal{O}_{M,T}^{\times}})/M), E[2]).$$

Proof. The first map is given by the restriction map. The injectivity can be checked by [8, Lemma 4.8]. The second injection is given in the proof of [8, Proposition 5.5]. □

Proposition 6.2. *Suppose that there exists an element $t \in \mathrm{Sel}_2(A)$ such that the fixed field of $\ker(\tilde{t})$ is not contained in $M(\sqrt{M^\times})$. Then there exist infinitely many quadratic characters $\chi \in \mathcal{C}(K)$ such that $r_2(E^\chi) = r_2(E) + 2$ and $r_2(A^\chi) \leq r_2(A)$.*

Proof. Let F be the fixed field of $\ker(\tilde{t})$. We denote the Galois closure of F over K by R. Choose N as in the proof of Theorem 5.2. Then Lemma 6.1, Lemma 1.8, and Lemma 1.7 show that $N \subset M(\sqrt{M^\times})$. The assumption on $\ker(\tilde{t})$ shows that there exists $\sigma \in \mathrm{Gal}(NR/K)$ satisfying

- $\sigma|_{NM'} = 1$,
- $\sigma|_F \neq 1$.

By Chebotarev's density theorem, there exist infinitely many primes $\mathfrak{q} \notin S$ of K such that $\mathrm{Frob}_\mathfrak{q}|_{NR} = \sigma$. As in the proof of Theorem 5.2, there exists $\chi \in \mathcal{C}(K)$ satisfying

- $\chi_v = 1_v$ for $v \in S$,
- $\chi_\mathfrak{q}$ is ramified,
- $\chi_\mathfrak{p}$ is unramified for $\mathfrak{p} \notin S \cup \{\mathfrak{q}\}$,

where $\chi_v, \chi_\mathfrak{q}, \chi_\mathfrak{p}$ are restrictions of χ to $K_v^\times, K_\mathfrak{q}^\times, K_\mathfrak{p}^\times$ via the local reciprocity maps, respectively. Then

$$\mathrm{Sel}_2(E^\chi) = \mathrm{Sel}_2(E, \chi_\mathfrak{q}) \text{ and } \mathrm{Sel}_2(A^\chi) = \mathrm{Sel}_2(A, \chi_\mathfrak{q})$$

by Lemma 2.10. By our assumption on t, we have $\mathrm{res}_\mathfrak{q}(t) \neq 0$, so by Proposition 3.10(iii), $r_2(A^\chi) \leq r_2(A)$. The equality $r_2(E^\chi) = r_2(E) + 2$ follows from the proof of Theorem 5.2. ☐

Proposition 6.3. *There exist infinitely many $\chi \in \mathcal{C}(K)$ satisfying*

(i) $r_2(A^\chi) = r_2(A) + 2$,
(ii) $r_2(E^\chi) = r_2(E) + 2$,
(iii) *there exists $s \in \mathrm{Sel}_2(A^\chi)$ so that (the fixed field of $\ker(\tilde{s})$) $\not\subset M(\sqrt{M^\times})$.*

Proof. Choose N as in the proof of Theorem 5.2. Choose N' for A as we construct N by replacing the role of E with that of A. By the Chebotarev density theorem, there exist infinitely many $\mathfrak{q} \notin S$ such that $\mathrm{Frob}_\mathfrak{q}|_{NN'} = 1$. As in the proof of Theorem 5.2, there exists $\chi \in \mathcal{C}(K)$ such that

- $\chi_v = 1_v$ for $v \in S$,
- $\chi_\mathfrak{q}$ is ramified,
- $\chi_\mathfrak{p}$ is unramified for $\mathfrak{p} \notin S \cup \{\mathfrak{q}\}$,

where $\chi_v, \chi_\mathfrak{q}, \chi_\mathfrak{p}$ are restrictions of χ to $K_v^\times, K_\mathfrak{q}^\times, K_\mathfrak{p}^\times$ via the local reciprocity maps, respectively. Again by the proof of Theorem 5.2, one can check (i) and (ii). By Lemma 5.1, there is an isomorphism $A^\chi[2] \cong A^\chi(K_\mathfrak{q})/2A^\chi(K_\mathfrak{q})$. By Proposition 3.10(ii) and the proof of Theorem 5.2, we see

$$\mathrm{res}_\mathfrak{q}(\mathrm{Sel}_2(A^\chi)) = A^\chi(K_\mathfrak{q})/2A^\chi(K_\mathfrak{q}), \tag{5}$$

where the latter is identified with its Kummer image in $H^1(K_\mathfrak{q}, A^\chi[2]) = \mathrm{Hom}(G_{K_\mathfrak{q}}, A^\chi[2])$. We choose $d \in K^\times$ so that the fixed field of $\ker(\chi)$ is $K(\sqrt{d})$. We define the composition of the maps as

$$\Phi : A[2] \cong A^\chi[2] \cong A^\chi(K_\mathfrak{q})/2A^\chi(K_\mathfrak{q}) \to \mathrm{Hom}(G_{K_\mathfrak{q}}, A^\chi[2]) \cong \mathrm{Hom}(G_{K_\mathfrak{q}}, A[2]).$$

By using the fact that $A[4] \subset A(K_\mathfrak{q})$, one can check that the map Φ takes $P \in A[2]$ to the homomorphism that sends $\sigma \in G_{K_\mathfrak{q}}$ to $(\chi(\sigma) - 1)Q$, where $P = 2Q$. Let

$s \in \mathrm{Sel}_2(A^\chi)$ be such that $\mathrm{res}_{\mathfrak{q}}(s) = \Phi(P_2)$ (the existence of s is guaranteed by (5)), where $P_2 \in A[2] - A(K)[2]$. Let P_1 denote the nontrivial 2-torsion point of $A(K)$. Suppose that (iii) does not hold (so in particular $\tilde{s}(\tau^2) = 0$ for $\tau \in G_M$). Then for any $\tau \in G_M$ with $\tau|_{MM'} \neq 1$ (so $\tau(P_1) = P_1$ and $\tau(P_2) = P_1 + P_2$), we have

$$0 = \tilde{s}(\tau^2) = \underline{s}(\tau^2) = \underline{s}(\tau) + \tau\underline{s}(\tau),$$

so $\underline{s}(\tau) = P_1$ or 0. Choose $\xi \in G_{K_{\mathfrak{q}}} \subset G_{MM'} \subset G_M$ such that $\xi(\sqrt{d}) = -\sqrt{d}$, so $\tilde{s}(\xi) = P_2$ by our choice of $s \in \mathrm{Sel}_2(A^\chi)$. However, we have

$$\tilde{s}(\xi) = \underline{s}(\xi) = \underline{s}(\tau \cdot \tau^{-1}\xi) = \underline{s}(\tau) + \tau\underline{s}(\tau^{-1}\xi) = P_1 \text{ or } 0,$$

where $\tau \in G_M$ is chosen so that $\tau|_{MM'} \neq 1$ (so $\tau^{-1}\xi$ also satisfies the same property). We get a contradiction, and therefore (iii) also holds. $\square$

By applying Proposition 6.3 and Proposition 6.2, we finally prove the following.

Theorem 6.4. *Suppose that $[M : K] = 1$ or 2, $[M' : K] = 2$, and $M \neq M'$. Then there exist infinitely many $\chi \in \mathcal{C}(K)$ such that $r_2(E^\chi) - r_2(A^\chi) \geq r_2(E) - r_2(A) + 2$.*

Remark 6.5. In the proof of Theorem 6.4, using Proposition 6.3 is crucial in order to apply Proposition 6.2. Without this step, it could be possible that the fixed field of $\ker(\tilde{t})$ is contained in $M(\sqrt{M^\times})$ for every $t \in \mathrm{Sel}_2(A)$.

Acknowledgment

The author is very grateful to Professor Karl Rubin for directing him to [5] and discussions.

References

[1] Zev Klagsbrun, Barry Mazur, and Karl Rubin, *Disparity in Selmer ranks of quadratic twists of elliptic curves*, Ann. of Math. (2) **178** (2013), no. 1, 287–320, DOI 10.4007/annals.2013.178.1.5. MR3043582

[2] Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266, DOI 10.1007/BF01389815. MR0444670

[3] Barry Mazur and Karl Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799, viii+96, DOI 10.1090/memo/0799. MR2031496

[4] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), no. 3, 541–575, DOI 10.1007/s00222-010-0252-0. MR2660452

[5] Barry Mazur and Karl Rubin, *Selmer companion curves*, Trans. Amer. Math. Soc. **367** (2015), no. 1, 401–421, DOI 10.1090/S0002-9947-2014-06114-X. MR3271266

[6] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. MR2392026

[7] Bjorn Poonen and Eric Rains, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25** (2012), no. 1, 245–269, DOI 10.1090/S0894-0347-2011-00710-8. MR2833483

[8] Myungjun Yu, *On 2-Selmer ranks of quadratic twists of elliptic curves*, Math. Res. Lett. **24** (2017), no. 5, 1565–1583, DOI 10.4310/MRL.2017.v24.n5.a11. MR3747176

[9] Myungjun Yu, *Selmer ranks of twists of hyperelliptic curves and superelliptic curves*, J. Number Theory **160** (2016), 148–185, DOI 10.1016/j.jnt.2015.08.009. MR3425203

Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48109-1043

Email address: `myungjuy@umich.edu`