Math. Res. Lett.
Volume 24, Number 5, 1565–1583, 2017

# On 2-Selmer ranks of quadratic twists of elliptic curves

Myungjun Yu

We study the 2-Selmer ranks of elliptic curves. We prove that for an arbitrary elliptic curve $E$ over an arbitrary number field $K$, if the set $A_E$ of 2-Selmer ranks of quadratic twists of $E$ contains an integer $c$, it contains all integers larger than $c$ and having the same parity as $c$. We also find sufficient conditions on $A_E$ such that $A_E$ is equal to $\mathbf{Z}_{\geq t_E}$ for some number $t_E$. When all points in $E[2]$ are rational, we give an upper bound for $t_E$.

## Introduction

Let $E$ be an elliptic curve over a number field $K$ and let $\mathrm{Sel}_2(E)$ denote its 2-Selmer group (Definition 2.2). Let $E^\chi$ be the quadratic twist of $E$ by a quadratic character $\chi : G_K \to \{\pm 1\}$. Let

$$r_2(E^\chi) := \dim_{\mathbf{F}_2}(\mathrm{Sel}_2(E^\chi)).$$

For $E$, one may study the set

$$A_E := \{r_2(E^\chi) : E^\chi \text{ is a quadratic twist of } E\},$$

i.e., the set of (non-negative) integers $r$ that appear as 2-Selmer ranks of some quadratic twists of $E$. Which integers are contained in $A_E$? and how many?

There are many interesting results in this direction. For example, Dokchitser and Dokchitser [1] showed that the elements in $A_E$ have constant parity if and only if $K$ has no real embedding and $E$ acquires everywhere good reduction over an abelian extension of $K$ (which is called "constant 2-Selmer parity condition" from now on). Mazur-Rubin [7] and Klagsbrun-Mazur-Rubin [3] proved that if $E$ does not satisfy the constant 2-Selmer parity condition and $\mathrm{Gal}(K(E[2])/K) \cong S_3$, then $A_E = \mathbf{Z}_{\geq 0}$.

When $\mathrm{Gal}(K(E[2])/K) \cong S_3$ or $\mathbf{Z}/3\mathbf{Z}$, it is known that there are only three possible cases for $A_E$. The following theorem, which exhibits those possible cases, follows from inductively applying [7, Proposition 5.2] and [10, Proposition 6.6].

**Theorem 1 (Mazur-Rubin, Yu).** *Suppose that* $\mathrm{Gal}(K(E[2])/K) \cong S_3$ *or* $\mathbf{Z}/3\mathbf{Z}$ *(equivalently,* $E(K)[2] = 0$*). Then* $A_E = \mathbf{Z}_{\geq 0}$*, or* $A_E = \{a \geq 0 : a \equiv 0 \ (mod\ 2)\}$*, or* $A_E = \{a \geq 0 : a \equiv 1 \ (mod\ 2)\}$*.*

However, in the other cases, the behaviour of $A_E$ was less understood, so we are mainly interested in the case when $\mathrm{Gal}(K(E[2])/K)$ has order 1 or 2. Let $t_E$ denote the smallest integer in $A_E$. In this paper, we derive a result on $A_E$ by proving the following theorem (Theorem 3.2).

**Theorem 2.** *Let* $E$ *be an elliptic curve over a number field* $K$*. Then there exist infinitely many quadratic characters* $\chi$ *such that* $r_2(E^\chi) = r_2(E) + 2$*.*

By applying Theorem 2 inductively, we can see

**Theorem 3.** *Let* $E$ *be an elliptic curve over a number field* $K$*. Then* $A_E \supset \{r \equiv t_E \ (mod\ 2) : r \geq t_E\}$ *(with equality if* $E$ *satisfies the constant* 2*-Selmer parity condition).*

For an elliptic curve $E$, clearly

$$A_E \subset \mathbf{Z}_{\geq t_E}. \tag{1}$$

We find sufficient conditions on $E$ so that equality holds in (1) (See Theorem 4.9, Theorem 4.10 and Theorem 3.2).

**Theorem 4.** *Suppose that* $\mathrm{Gal}(K(E[2])/K)$ *has order* 1 *or* 2*. Suppose that either*

(i) *$K$ has a real embedding, or*

(ii) $\mathrm{Gal}(K(E[2])/K)$ *has order* 2 *and* $E$ *has multiplicative reduction at a place* $\mathfrak{q}$ *such that* $\mathfrak{q} \nmid 2$ *and* $v_\mathfrak{q}(\Delta_E)$ *is odd, where* $\Delta_E$ *is the discriminant of a model of* $E$ *and* $v_\mathfrak{q}$ *is the normalized (additive) valuation of* $K_\mathfrak{q}$*.*

*Then* $A_E = \mathbf{Z}_{\geq t_E}$*.*

Let $\Sigma$ be a finite set of places of $K$ containing all primes above 2, all primes where $E$ has bad reduction, and all infinite places. We suppose the elements (finite places) of $\Sigma$ generate the ideal class group of $K$. For $t_E$, we have a trivial lower bound $\dim_{\mathbf{F}_2}(E(K)[2])$. However, this lower bound turns out not to be sharp in some cases. Klagsbrun [2] found examples of elliptic curves $E$ such that $t_E$ is at least $s_2+1$, where $s_2$ denotes the number of complex places of $K$ (see Example 5.1 and Remark 5.2 for a discussion of this). In Section 5, when $E[2] \subset E(K)$, we give an upper bound for $t_E$ as follows (see Theorem 5.6 and Theorem 5.8).

**Theorem 5.** *Suppose that $E[2] \subset E(K)$. We have $t_E \leq |\Sigma| + 1$. If moreover, $E$ does not satisfy the constant 2-Selmer parity condition, then $t_E \leq |\Sigma|$.*

## 1. Preliminaries

Let $K$ be a number field and $v$ be a place of $K$. We denote the completion of $K$ at $v$ by $K_v$. Let $E$ be an elliptic curve defined over $K$. We write $E^\chi$ for the quadratic twist of $E$ by a quadratic character $\chi$. For $d \in K^\times/(K^\times)^2$, we sometimes write $E^d$ for $E^\chi$ when $K(\sqrt{d})$ is the corresponding quadratic extension to $\chi$. For any quadratic twists $E^\chi$ of $E$, note that there is a canonical ($G_K$-module) isomorphism $E[2] \cong E^\chi[2]$. Throughout the paper, for (topological) groups A and B, we denote the group of continuous homomorphisms from $A$ to $B$ simply by $\mathrm{Hom}(A, B)$.

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

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

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

**Definition 1.2.** For $\chi \in \mathcal{C}(K_v)$, define

$$\alpha_v(\chi) := \mathrm{Im}(E^\chi(K_v)/2E^\chi(K_v) \to H^1(K_v, E^\chi[2]) \cong H^1(K_v, E[2])),$$

where the first map is given by the Kummer map. Define

$$h_v(\chi) := \dim_{\mathbf{F}_2}(\alpha_v(1_v)/(\alpha_v(1_v) \cap \alpha_v(\chi))).$$

**Lemma 1.3.** *For $\chi \in \mathcal{C}(K_v)$, let $L = \overline{K_v}^{\ker(\chi)}$. Then*

$$h_v(\chi) = \dim_{\mathbf{F}_2}(E(K_v)/\mathbf{N}E(L)),$$

*where $\mathbf{N}E(L)$ is the image of the norm map $\mathbf{N} : E(L) \to E(K_v)$.*

*Proof.* This is [4, Proposition 7]. □

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

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

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

*Proof.* For example, see [9, Theorem 7.2.6]. □

## 2. Selmer groups and comparing local conditions

Let $K$ be a number field and $E$ be an elliptic curve defined over $K$. We fix embeddings $\overline{K} \hookrightarrow \overline{K_v}$ for all places $v$ so that $G_{K_v} \subset G_K$.

**Definition 2.1.** For every place $v$ of $K$, we let

$$\mathrm{res}_v : H^1(K, E[2]) \to H^1(K_v, E[2])$$

denote the restriction map of group cohomology. Let $T$ be a finite set of places of $K$. Let

$$\mathrm{res}_T : H^1(K, E[2]) \to \bigoplus_{v \in T} H^1(K_v, E[2])$$

denote the sum of restriction maps.

**Definition 2.2.** Let $\chi \in \mathcal{C}(K)$. The 2-Selmer group $\mathrm{Sel}_2(E^\chi) \subset H^1(K, E[2])$ is the (finite) $\mathbf{F}_2$-vector space defined by the following exact sequence

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

where the rightmost map is the sum of the restriction maps, and $\chi_v$ is the restriction of $\chi$ to $G_{K_v}$. In particular, if $\chi$ is the trivial character, it is the classical 2-Selmer group of $E$.

We define various Selmer groups as follows.

**Definition 2.3.** Let $T$ be a finite set of places of $K$. Let $S = \{v_1, \ldots, v_k\}$ be a (finite) set of places such that $S \cap T = \varnothing$. Let $\psi_{v_j} \in \mathcal{C}(K_{v_j})$. Define

$$\begin{aligned}\mathrm{Sel}_2(E, \psi_{v_1}, \ldots, \psi_{v_k}) := \{x \in H^1(K, E[2]) \mid \mathrm{res}_v(x) \in \alpha_v(1_v) \text{ if } v \notin S,\\ \text{and } \mathrm{res}_{v_j}(x) \in \alpha_{v_j}(\psi_{v_j}) \text{ for } 1 \le j \le k\}.\end{aligned}$$

Define

$$\mathrm{Sel}_{2,T}(E, \psi_{v_1}, \ldots, \psi_{v_k}) := \{x \in \mathrm{Sel}_2(E, \psi_{v_1}, \ldots, \psi_{v_k}) \mid \mathrm{res}_T(x) = 0\}.$$

Define

$$\begin{aligned}\mathrm{Sel}_2^T(E, \psi_{v_1}, \ldots, \psi_{v_k}) := \{x \in H^1(K, E[2]) \mid \mathrm{res}_v(x) \in \alpha_v(1_v) \text{ if } v \notin S \cup T,\\ \text{and } \mathrm{res}_{v_j}(x) \in \alpha_{v_j}(\psi_{v_j}) \text{ for } 1 \le j \le k\}.\end{aligned}$$

For a place $v \notin S$, we simply write $\mathrm{Sel}_{2,v}(E, \psi_{v_1}, \ldots, \psi_{v_k})$, $\mathrm{Sel}_2^v(E, \psi_{v_1}, \ldots, \psi_{v_k})$ for $\mathrm{Sel}_{2,\{v\}}(E, \psi_{v_1}, \ldots, \psi_{v_k})$, $\mathrm{Sel}_2^{\{v\}}(E, \psi_{v_1}, \ldots, \psi_{v_k})$, respectively.

**Definition 2.4.** For convenience, we write $r_2(E^\chi), r_2(E, \psi_{v_1}, \ldots, \psi_{v_n})$ for $\dim_{\mathbf{F}_2}(\mathrm{Sel}_2(E^\chi)), \dim_{\mathbf{F}_2}(\mathrm{Sel}_2(E, \psi_{v_1}, \ldots, \psi_{v_n}))$, respectively.

The following theorem is due to [3, Theorem 3.9 and Lemma 5.2(ii)].

**Theorem 2.5 (Kramer, Klagsbrun-Mazur-Rubin).** *Let $\chi \in \mathcal{C}(K)$. We have*

$$r_2(E) - r_2(E^\chi) \equiv \sum_v h_v(\chi_v) (mod\ 2),$$

*where $\chi_v$ is the restriction of $\chi$ to $G_{K_v}$ and $h_v$ is given in Definition 1.2. Let $S = \{v_1, \ldots, v_k\}$ be a (finite) set of places. Let $\psi_{v_i} \in \mathcal{C}(K_{v_i})$. We have*

$$r_2(E, \psi_{v_1}, \ldots, \psi_{v_k}) - r_2(E) \equiv \sum_{i=1}^{k} h_{v_i}(\psi_{v_i}) (mod\ 2).$$

**Lemma 2.6.** *Let $\chi \in \mathcal{C}(K_v)$. Suppose that $\chi$ satisfies one of the following conditions:*

- *$\chi$ is trivial, or*
- *$E/K_v$ has good reduction, $v \nmid \infty$, and $\chi$ is unramified.*

*Then $h_v(\chi) = 0$, i.e., $\alpha_v(1_v) = \alpha_v(\chi)$.*

*Proof.* Let $L = \overline{K}_v^{\ker(\chi)}$. In either case, $\mathbf{N}(E(L)) = E(K_v)$ (in the second case, it follows from [5, Corollary 4.4]). Thus, by Lemma 1.3, the result follows. □

From now on, let $\Sigma$ denote a finite set of places of $K$ containing all primes above 2, all primes where $E$ has bad reduction, and all infinite places.

**Definition 2.7.** Define

$$\begin{aligned}\mathcal{P}_i &:= \{\mathfrak{q} : \mathfrak{q} \notin \Sigma \text{ and } \dim_{\mathbf{F}_2}(E(K_\mathfrak{q})[2]) = i\} \quad \text{for } 0 \le i \le 2, \text{ and}\\ \mathcal{P} &:= \mathcal{P}_0 \coprod \mathcal{P}_1 \coprod \mathcal{P}_2 = \{\mathfrak{q} : \mathfrak{q} \notin \Sigma\}.\end{aligned}$$

Although $\mathcal{P}_i$ and $\mathcal{P}$ depend on the choice of $\Sigma$ and $E$, we suppress them from the notation.

**Remark 2.8.** By [10, Lemma 2.11(i)], if $\mathfrak{q} \in \mathcal{P}$, we have

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

Hence, if $\mathfrak{q} \in \mathcal{P}_i$ and $\chi \in \mathcal{C}(K_\mathfrak{q})$, we have $\dim_{\mathbf{F}_2}(\alpha_\mathfrak{q}(\chi)) = i$.

**Lemma 2.9.** *Let $\mathfrak{q} \in \mathcal{P}_i$. Suppose that $\chi \in \mathcal{C}_{\mathrm{ram}}(K_\mathfrak{q})$. Then $\alpha_\mathfrak{q}(1_\mathfrak{q}) \cap \alpha_\mathfrak{q}(\chi) = \{0\}$, and $h_\mathfrak{q}(\chi) = i$.*

*Proof.* See [7, Lemma 2.11]. □

**Theorem 2.10.** *Let $T$ be a finite set of places of $K$. Let $v_1, \ldots, v_k \notin T$ be places and $\psi_{v_j} \in \mathcal{C}(K_{v_j})$. The images of right hand restriction maps of the following exact sequences are orthogonal complements with respect to the pairing given by the sum of pairings (2) of the places $v \in T$*

$$\begin{aligned}&0 \longrightarrow \mathrm{Sel}_2(E, \psi_{v_1}, \ldots, \psi_{v_k})\\ &\quad \longrightarrow \mathrm{Sel}_2^T(E, \psi_{v_1}, \ldots, \psi_{v_k}) \longrightarrow \bigoplus_{v \in T} H^1(K_v, E[2])/\alpha_v(1_v),\\ &0 \longrightarrow \mathrm{Sel}_{2,T}(E, \psi_{v_1}, \ldots, \psi_{v_k}) \longrightarrow \mathrm{Sel}_2(E, \psi_{v_1}, \ldots, \psi_{v_k}) \longrightarrow \bigoplus_{v \in T} \alpha_v(1_v).\end{aligned}$$

*In particular,*

$$\begin{aligned}&\dim_{\mathbf{F}_2}(\mathrm{Sel}_2^T(E, \psi_{v_1}, \ldots, \psi_{v_k})) - \dim_{\mathbf{F}_2}(\mathrm{Sel}_{2,T}(E, \psi_{v_1}, \ldots, \psi_{v_k}))\\ &= \Sigma_{v \in T} \dim_{\mathbf{F}_2}(\alpha_v(1_v)) = \Sigma_{v \in T} \frac{1}{2} \dim_{\mathbf{F}_2}(H^1(K_v, E[2])).\end{aligned}$$

*Proof.* The thoerem follows from the Global Poitou-Tate Duality. For example, see [6, Theorem 2.3.4]. □

**Corollary 2.11.** *Suppose* $T=\{\mathfrak{q}_1,\dots,\mathfrak{q}_n\}$, *where* $\mathfrak{q}_i\in\mathcal{P}$. *Let* $\psi_i\in\mathcal{C}_{\mathrm{ram}}(K_{\mathfrak{q}_i})$. *Let* $v_0\notin T$ *be a place and* $\psi_{v_0}\in\mathcal{C}(K_{v_0})$. *Suppose that the map*

$$\mathrm{res}_T:\mathrm{Sel}_2(E,\psi_{v_0})\to\bigoplus_{v\in T}\alpha_v(1_v)$$

*is surjective. Then we have*

(i) $\mathrm{Sel}_2(E,\psi_{v_0})=\mathrm{Sel}_2^T(E,\psi_{v_0})$, *and*

(ii) $\mathrm{Sel}_2(E,\psi_1,\dots,\psi_n,\psi_{v_0})=\mathrm{Sel}_{2,T}(E,\psi_{v_0})$.

*Proof.* The first assertion is clear because the orthogonality in Theorem 2.10 shows that the image of

$$\mathrm{res}_T:\mathrm{Sel}_2^T(E,\psi_{v_0})\to\bigoplus_{v\in T}H^1(K_v,E[2])/\alpha_v(1_v)$$

is trivial. Lemma 2.9 shows that

$$\mathrm{Sel}_2(E,\psi_{v_0})\cap\mathrm{Sel}_2(E,\psi_1,\dots,\psi_n,\psi_{v_0})=\mathrm{Sel}_{2,T}(E,\psi_{v_0}),$$

where the intersection is taken in $H^1(K,E[2])$. Now the second assertion is easy to see. □

**Corollary 2.12.** *Let* $\mathfrak{q}$ *be a place and let* $v_1,\dots,v_k$ *be places of* $K$ *not equal to* $\mathfrak{q}$. *Let* $\psi_{v_j}\in\mathcal{C}(K_{v_j})$. *For any* $\phi_\mathfrak{q},\eta_\mathfrak{q}\in\mathcal{C}(K_\mathfrak{q})$, *we have*

$$|r_2(E,\psi_{v_1},\dots,\psi_{v_k},\phi_\mathfrak{q})-r_2(E,\psi_{v_1},\dots,\psi_{v_k},\eta_\mathfrak{q})|\le\dim_{\mathbf{F}_2}(\alpha_\mathfrak{q}(1_\mathfrak{q})).$$

*Proof.* In Theorem 2.10, take $T=\{\mathfrak{q}\}$. Note that $\mathrm{Sel}_2(\psi_{v_1},\dots,\psi_{v_k},\phi_\mathfrak{q})$ and $\mathrm{Sel}_2(\psi_{v_1},\dots,\psi_{v_k},\eta_\mathfrak{q})$ contains $\mathrm{Sel}_{2,\mathfrak{q}}(\psi_{v_1},\dots,\psi_{v_k})$ and are contained in $\mathrm{Sel}_2^\mathfrak{q}(\psi_{v_1},\dots,\psi_{v_k})$, where the result easily follows from Theorem 2.10. □

## 3. Increasing 2-Selmer rank by twisting

Let $E$ be an elliptic curve over a number field $K$ and let $\Sigma$ be as in previous section.

**Lemma 3.1.** *Let* $\mathfrak{q}$ *be a prime of* $K$ *such that* $\mathfrak{q}\nmid 2$. *Then*

(i) *if all the points of* $E[4]$ *are* $K_{\mathfrak{q}}$*-rational and* $\chi$ *is a nontrivial quadratic character, then* $E^{\chi}(K_{\mathfrak{q}})[4] = E^{\chi}(K_{\mathfrak{q}})[2] \cong (\mathbf{Z}/2\mathbf{Z})^2$*;*

(ii) *if* $E(K_{\mathfrak{q}})[4] = E(K_{\mathfrak{q}})[2]$*, then the map* $E(K_{\mathfrak{q}})[2] \to E(K_{\mathfrak{q}})/2E(K_{\mathfrak{q}})$ *via the projection is an isomorphism.*

*Proof.* The first assertion (i) is obvious from the definition of quadratic twists. For (ii), multiplication by 2 is surjective on the pro-(prime to 2) part of $E(K_{\mathfrak{q}})$, so only the pro-2 part $E(K_{\mathfrak{q}})[2^\infty]$ contributes to $E(K_{\mathfrak{q}})/2E(K_{\mathfrak{q}})$, hence $E(K_{\mathfrak{q}})[2] = E(K_{\mathfrak{q}})[2^\infty]/2E(K_{\mathfrak{q}})[2^\infty] \cong E(K_{\mathfrak{q}})/2E(K_{\mathfrak{q}})$. □

The following generalizes methods that are used in the proof of Proposition 5.1 in [7].

**Theorem 3.2.** *Let* $E$ *be an elliptic curve over a number field* $K$*. Then there exist infinitely many* $\chi \in \mathcal{C}(K)$ *such that* $r_2(E^{\chi}) = r_2(E) + 2$*.*

*Proof.* If $\mathrm{Gal}(K(E[2])/K) \cong S_3$ or $A_3$, the result follows from [10, Proposition 6.6]. Therefore, from now on, we assume that $\mathrm{Gal}(K(E[2])/K)$ has order 1 or 2, i.e., there exists a non-trivial rational 2-torsion point $P \in E(K)[2]$. Let $\theta$ be the formal product of 8, and all places in $\Sigma$ not dividing 2. In particular, $\theta$ is divisible by primes where $E$ has bad reduction. Let $K[\theta]$ be the maximal 2-subextension of $K(\theta)$, where $K(\theta)$ is the ray class field modulo $\theta$.

Let $L$ be a Galois extension containing $K(E[4])K[\theta]$ such that the image of the restriction map

$$\mathrm{Sel}_2(E) \subseteq H^1(K, E[2]) \to H^1(L, E[2]) = \mathrm{Hom}(G_L, E[2])$$

is trivial. Choose a prime (Chebotarev's density theorem) $\mathfrak{q} \notin \Sigma$ so that $\mathfrak{q}$ is unramified in $L/K$ and $\mathrm{Frob}_{\mathfrak{q}}|_L = 1$. Note that the restriction map $H^1(K, E[2]) \to H^1(K_{\mathfrak{q}}, E[2])$ factors through the restriction $H^1(K, E[2]) \to H^1(L, E[2])$ because $\mathfrak{q}$ splits completely in $L/K$, so $\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_2(E)) = 0$ and

$$\mathrm{Sel}_2(E) = \mathrm{Sel}_{2,\mathfrak{q}}(E).$$

Moreover, there exists an odd integer $k$ such that $\mathfrak{q}^k = (d)$ for some $d \in K^{\times}$ such that $d \equiv 1 \pmod{\theta}$. Note the following properties of the extension $K(\sqrt{d})/K$:

- $\mathfrak{q}$ is ramified in $K(\sqrt{d})/K$,
- If $v \notin \Sigma$ and $v \neq \mathfrak{q}$, then $v$ is unramified in $K(\sqrt{d})/K$, and
- If $v \in \Sigma$, then $v$ splits in $K(\sqrt{d})/K$.

Therefore by Lemma 2.6, the local conditions of $\mathrm{Sel}_2(E)$ and $\mathrm{Sel}_2(E^d)$ are the same except at $\mathfrak{q}$, where two local conditions intersect trivially by Lemma 2.9. By Corollary 2.12 and the fact that $\mathrm{Sel}_2(E) = \mathrm{Sel}_{2,\mathfrak{q}}(E)$, we have $0 \leq r_2(E^d) - r_2(E) \leq 2$. Moreover since $\mathfrak{q} \in \mathcal{P}_2$, Theorem 2.5 and Lemma 2.9 prove that

$$r_2(E^d) = r_2(E) \text{ or } r_2(E) + 2. \tag{3}$$

By our choice of a prime $\mathfrak{q}$, we have $E[4] \subset E(K_\mathfrak{q})$. By Lemma 3.1, $P$ has a nonzero local Kummer image for $E^d$ at $\mathfrak{q}$. Therefore $\mathrm{res}_\mathfrak{q}(\mathrm{Sel}_2(E^d)) \neq 0$, where $\mathrm{res}_\mathfrak{q} : \mathrm{Sel}_2(E^d) \to H^1(K_\mathfrak{q}, E[2])$ is the restriction map. Hence $\mathrm{Sel}(E^d)$ contains $\mathrm{Sel}_2(E)(= \mathrm{Sel}_{2,\mathfrak{q}}(E))$ properly, i.e., $r_2(E^d) \geq r_2(E) + 1$. Therefore by (3), we have $r_2(E^d) = r_2(E) + 2$. Since the only constraint on our choice of $\mathfrak{q}$ is $\mathrm{Frob}_\mathfrak{q}|_L = 1$ and there are infinitely many such primes (Chebotarev's density theorem), we have infinitely many quadratic twists with the desired property. □

**Remark 3.3.** A similar argument can show the following theorem: Let $C_f$ be a hyperelliptic curve over a number field $K$ given by an affine model

$$y^2 = f(x),$$

where $n := \deg(f) > 1$ is odd. Let $J$ be the Jacobian of $C_f$. If $K$ contains a root of $f$, then for any given natural number $r$, there exist infinitely many quadratic twists $J^\chi$ such that $\dim_{\mathbf{F}_2}(\mathrm{Sel}_2(J^\chi/K)) \geq r$ (In [10], the author discusses the cases when $\mathrm{Gal}(f) \cong A_n$ or $S_n$. In such cases, the result is even stronger. See [10, Theorem 6.7]).

## 4. Changing the parity of 2-Selmer rank by twisting

Recall that $\Sigma$ is a finite set of places of $K$ containing all places where $E$ has bad reduction, all primes above 2, and all infinite places. We enlarge $\Sigma$, if necessary, so that $\mathrm{Pic}(O_{K,\Sigma}) = 1$, where $O_{K,\Sigma}$ denote the ring of $\Sigma$-integers. For the rest of the paper, we put $n := |\Sigma|$. Let $\Delta_E$ denote the discriminant of some model of the elliptic curve $E$.

**Lemma 4.1.** $\dim_{\mathbf{F}_2}(O_{K,\Sigma}^\times/(O_{K,\Sigma}^\times)^2) = n$.

*Proof.* It is well-known that $O_{K,\Sigma}^\times \cong \mathbf{Z}^{n-1} \oplus \mathbf{Z}/m\mathbf{Z}$, where $m = \#\{\text{roots of unity in } K\}$ is divisible by 2 (for example, see [8, Proposition 6.1.1]). □

**Lemma 4.2.** *Let $\mathfrak{q} \notin \Sigma$ (so $\mathfrak{q} \nmid 2$) be a prime of $K$ and suppose $g \in \mathrm{Hom}(\mathcal{O}_{\mathfrak{q}}^{\times}, \{\pm 1\})$ is non-trivial. Then $g(b) = \mathrm{Frob}_{\mathfrak{q}}(\sqrt{b})/\sqrt{b}$ for all $b \in \mathcal{O}_{K,\Sigma}^{\times}$. In particular, if $\psi \in \mathcal{C}_{\mathrm{ram}}(K_{\mathfrak{q}})$, then $\psi(b) = \mathrm{Frob}_{\mathfrak{q}}(\sqrt{b})/\sqrt{b}$ for all $b \in \mathcal{O}_{K,\Sigma}^{\times}$.*

*Proof.* We have

$$\mathrm{Hom}(\mathcal{O}_{\mathfrak{q}}^{\times}, \{\pm 1\}) = \mathrm{Hom}(\mathcal{O}_{\mathfrak{q}}^{\times}/(\mathcal{O}_{\mathfrak{q}}^{\times})^2, \{\pm 1\}) \cong \mathbf{Z}/2\mathbf{Z}$$

because $\mathcal{O}_{\mathfrak{q}}^{\times}/(\mathcal{O}_{\mathfrak{q}}^{\times})^2 \cong \mathbf{Z}/2\mathbf{Z}$. Note that $b \in (\mathcal{O}_{\mathfrak{q}}^{\times})^2$ if and only if $\mathrm{Frob}_{\mathfrak{q}}(\sqrt{b}) = \sqrt{b}$, where the assertion follows. □

**Lemma 4.3.** *The image of the restriction map*

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

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

*Proof.* Global Class Field Theory and the condition $\mathrm{Pic}(\mathcal{O}_{K,\Sigma}) = 1$ show the equalities. It is clear that the image is as stated. □

**Proposition 4.4.** *Let $v_0 \in \Sigma$ and $\psi_{v_0} \in \mathcal{C}(K_v)$. Suppose that $\psi_{v_0}(\mathcal{O}_{K,\Sigma}^{\times}) = 1$. Then there exists $\chi \in \mathcal{C}(K)$ such that $\mathrm{Sel}_2(E^{\chi}) = \mathrm{Sel}_2(E, \psi_{v_0})$*

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

- $f_{v_0} = \psi_{v_0}$,
- $f_v = 1_v$ for $v \in \Sigma \backslash \{v_0\}$, and
- $g_{\mathfrak{p}}$ is trivial for $\mathfrak{p} \notin \Sigma$.

By Lemma 4.3, there exists a character $\chi \in \mathcal{C}(K)$ such that for $\mu \in \Sigma$ and $\nu \notin \Sigma$, $\chi_{\mu} = f_{\mu}$ and $\chi_{\nu}|_{\mathcal{O}_{\nu}^{\times}} = g_{\nu}$, where $\chi_{\mu}, \chi_{\nu}$ are restrictions of $\chi$ to $K_{\mu}^{\times}, K_{\nu}^{\times}$ via the local reciprocity maps, respectively. Now one can see the local conditions for $\mathrm{Sel}_2(E^{\chi})$ and $\mathrm{Sel}_2(E, \psi_{v_0})$ are the same everywhere by Lemma 2.6. □

**Lemma 4.5.** *Let $v_0$ be a place in $\Sigma$ and let $T$ be a (finite) set of primes such that $T \cap \Sigma = \varnothing$. Suppose that $\psi_{v_0} \in \mathcal{C}(K_{v_0})$. Then there exist infinitely many* *primes $\mathfrak{q} \notin \Sigma \cup T$ for which there exists a character $\chi \in \mathcal{C}(K)$ satisfying the following conditions.*

(i) $\chi_{v_0} = \psi_{v_0}$,

(ii) $\chi_v = 1_v$ *for* $v \in \Sigma \backslash \{v_0\}$,

(iii) $\chi_\omega$ *is ramified for* $\omega \in T$,

(iv) $\chi_\mathfrak{p}$ *is unramified for* $\mathfrak{p} \notin \Sigma \cup T \cup \{\mathfrak{q}\}$,

(v) $\chi_\mathfrak{q}$ *is ramified,*

*where $\chi_{v_0}, \chi_v, \chi_\omega, \chi_\mathfrak{p}, \chi_\mathfrak{q}$ are restrictions of $\chi$ to $K_{v_0}^\times, K_v^\times, K_\omega^\times, K_\mathfrak{p}^\times, K_\mathfrak{q}^\times$ via the local reciprocity maps, respectively.*

*Proof.* Let $\beta_1, \dots, \beta_n$ be a basis of $O_{K,\Sigma}^\times/(O_{K,\Sigma}^\times)^2$. Choose a prime $\mathfrak{q}$ such that

$$\mathrm{Frob}_\mathfrak{q}(\sqrt{\beta_i})/\sqrt{\beta_i} = \psi_{v_0}(\beta_i) \cdot \prod_{\omega \in T} \mathrm{Frob}_\omega(\sqrt{\beta_i})/\sqrt{\beta_i} \tag{4}$$

for all $i$, where the existence is guaranteed by Chebotarev's density theorem. Put $f_\mu \in \mathrm{Hom}(K_\mu^\times, \{\pm 1\})$ for $\mu \in \Sigma$ and $g_\nu \in \mathrm{Hom}(\mathcal{O}_\nu^\times, \{\pm 1\})$ for $\nu \notin \Sigma$ such that

- $f_{v_0} = \psi_{v_0}$,
- $f_v = 1_v$ for $v \in \Sigma \backslash \{v_0\}$,
- $g_\omega$ is not trivial for $\omega \in T$,
- $g_\mathfrak{p}$ is trivial for $\mathfrak{p} \notin \Sigma \cup T \cup \{\mathfrak{q}\}$, and
- $g_\mathfrak{q}$ is not trivial.

By Lemma 4.2, we have

$$g_\mathfrak{q}(\beta_i) = f_{v_0}(\beta_i) \cdot \prod_{v \in \Sigma \backslash \{v_0\}} f_v(\beta_i) \cdot \prod_{\omega \in T} g_\omega(\beta_i) \cdot \prod_{\mathfrak{p} \notin \Sigma \cup \{\mathfrak{q}\} \cup T} g_\mathfrak{p}(\beta_i).$$

By Lemma 4.3, this means that there exists a character $\chi \in \mathcal{C}(K)$ such that for $\mu \in \Sigma$ and $\nu \notin \Sigma$, $\chi_\mu = f_\mu$ and $\chi_\nu|_{\mathcal{O}_\nu^\times} = g_\nu$, where $\chi_\mu, \chi_\nu$ are restrictions of $\chi$ to $K_\mu^\times, K_\nu^\times$ via the local reciprocity maps, respectively. It is easy to see $\chi$ satisfies the desired conditions. For example, for $\omega \in T$, $\chi_\omega|_{\mathcal{O}_\omega^\times} = g_\omega$, and this shows that $\chi_\omega$ is ramified since $g_\omega(\mathcal{O}_\omega^\times) \neq 1$ by our construction. □

**Proposition 4.6.** *Let $v_0 \in \Sigma$ and $\psi_{v_0} \in \mathcal{C}(K_{v_0})$.*

(i) *If* $\psi_{v_0}(\Delta_E) = -1$ *and* $\mathrm{Gal}(K(E[2])/K) \cong \mathbf{Z}/2\mathbf{Z}$*, there exist infinitely many* $\varphi \in \mathcal{C}(K)$ *such that* $r_2(E^\varphi/K) = r_2(E, \psi_{v_0}) + 1$*.*

(ii) *If* $\psi_{v_0}(\Delta_E) = 1$*, there exist infinitely many* $\varphi \in \mathcal{C}(K)$ *such that* $r_2(E^\varphi/K) = r_2(E, \psi_{v_0}) + 2$*.*

(iii) *Suppose that* $\psi_{v_0}(\Delta_E) = 1$ *and there exists an element* $c \in \mathrm{Sel}_2(E, \psi_{v_0})$*. Let* $T = \varnothing$ *and choose* $\mathfrak{q}$ *and* $\chi$ *as in Lemma 4.5. Suppose that* $\mathrm{res}_\mathfrak{q}(c) \neq 0$*. Then there exist infinitely many* $\varphi \in \mathcal{C}(K)$ *such that* $r_2(E^\varphi/K) = r_2(E, \psi_{v_0})$*.*

*Proof.* For (i) and (ii), let $T = \varnothing$ and we begin with choosing $\mathfrak{q}$ and $\chi$ as in Lemma 4.5. Note that the local conditions for $\mathrm{Sel}_2(E^\chi)$ and $\mathrm{Sel}_2(E, \chi_{v_0})$ are the same everywhere except possibly at $\mathfrak{q}$ by Lemma 2.6. Thus Corollary 2.12 shows that $|r_2(E^\chi) - r_2(E, \chi_{v_0})| \leq 2$. The conditions in (i) and the product formula imply $\chi_\mathfrak{q}(\Delta_E) = \psi_{v_0}(\Delta_E) = -1$, so $\Delta_E \notin (K_\mathfrak{q}^\times)^2$, which shows that $E(K_\mathfrak{q})[2] \cong \mathbf{Z}/2\mathbf{Z}$. Hence Theorem 2.5, Lemma 2.9 prove that $r_2(E^\chi)$ is $r_2(E, \psi_{v_0}) - 1$, or $r_2(E, \psi_{v_0}) + 1$. Then (i) follows from Theorem 3.2. For (ii), the condition $\psi_{v_0}(\Delta_E) = 1$ and the product formula imply $\chi_\mathfrak{q}(\Delta_E) = 1$, so $\Delta_E \in (K_\mathfrak{q}^\times)^2$, which shows that $E(K_\mathfrak{q})[2] \cong (\mathbf{Z}/2\mathbf{Z})^2$ or $E(K_\mathfrak{q})[2] = 0$. Then Theorem 2.5, Lemma 2.9 show that $r_2(E^\chi)$ is $r_2(E, \psi_{v_0}) - 2$, or $r_2(E, \psi_{v_0})$ or $r_2(E, \psi_{v_0}) + 2$ and the rest follows from Theorem 3.2. To see (iii), note that the condition $\mathrm{res}_\mathfrak{q}(c) \neq 0$ rules out the possibility for $r_2(E^\chi)$ to be $r_2(E, \psi_{v_0}) + 2$ in the proof of (ii) (for otherwise, $r_2(E^\chi) \geq \dim_{\mathbf{F}_2}(\mathrm{Sel}_{2,\mathfrak{q}}(E^\chi)) + 3$ and this would mean $r_2(E^\chi) \geq \dim_{\mathbf{F}_2}(\mathrm{Sel}_2^\mathfrak{q}(E^\chi)) + 1$, which is absurd). □

**Lemma 4.7.** *Suppose that* $K$ *has a real place* $v_0$*, so* $K_{v_0} \cong \mathbf{R}$*. Let* $\eta \in \mathcal{C}(K_{v_0})$ *be the sign character. Then*

$$h_{v_0}(\eta) = \begin{cases} 0 & \textit{if } \dim_{\mathbf{F}_2}(E(K_{v_0})[2]) = 1, \\ 1 & \textit{if } \dim_{\mathbf{F}_2}(E(K_{v_0})[2]) = 2. \end{cases}$$

*Proof.* The image $\mathbf{N}(E(\mathbf{C}))$ of the norm map

$$\mathbf{N} : E(\mathbf{C}) \to E(\mathbf{R})$$

is the connected component of the identity of $E(\mathbf{R})$, i.e., $\mathbf{N}(E(\mathbf{C})) \cong \mathbf{R}/\mathbf{Z}$, where the result follows by Lemma 1.3. □

**Lemma 4.8.** *Let $M = K(E[2])$. The restriction map*

$$H^1(K, E[2]) \to H^1(M, E[2]) = \mathrm{Hom}(G_M, E[2]) \tag{5}$$

*is an injection.*

*Proof.* The Inflation-Restriction Sequence shows that the kernel of (5) is $H^1(M/K, E[2])$. It is well-known that $H^1(\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}), E[2]) = 0$ (note rhat $\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}) \cong S_3$). For the rest cases, let $\sigma$ be a generator of the cyclic group $\mathrm{Gal}(M/K)$. One can see $\mathrm{Ker}(\sigma+1) = \mathrm{Im}(\sigma-1)$, so the cohomology group vanishes. □

**Theorem 4.9.** *If $K$ has a real embedding, there exist infinitely many $\chi \in \mathcal{C}(K)$ such that $r_2(E^\chi) = r_2(E) + 1$.*

*Proof.* Let $M = K(E[2])$. We assume $\mathrm{Gal}(M/K)$ has order 1 or 2, since otherwise we already know the result holds by [7, Theorem 1.5] and Theorem 3.2. We let $v_0$ be a real place, so that $K_{v_0} \cong \mathbf{R}$. Let $\psi_{v_0} \in \mathcal{C}(K_{v_0})$ denote the sign character, i.e., $\psi_{v_0}$ sends negative numbers to $-1$.

Case 1: $E[2] \subset E(K)$. We have $E(K_{v_0}) \cong \mathbf{R}/\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$. Therefore, there exists a point $P \in E(K)[2]$ that is not divisible by 2 in $E(K_{v_0})$. One can see $\mathrm{res}_{v_0}(\overline{P}) \neq 0$, where $\overline{P}$ is the image of $P$ in the map $E(K) \to E(K)/2E(K) \to \mathrm{Sel}_2(E) \subset H^1(K, E[2])$, because the image of $P$ in $E(K_{v_0})/2E(K_{v_0})$ is not trivial. The restriction map $\mathrm{Sel}_2(E)/\mathrm{Sel}_{2,v_0}(E) \to \alpha_{v_0}(1_{v_0})$ is an isomorphism (since $\mathrm{res}_{v_0}(\mathrm{Sel}_2(E)) \neq 0$) and the restriction map $\mathrm{Sel}_2(E, \psi_{v_0})/\mathrm{Sel}_{2,v_0}(E) \to \alpha_{v_0}(\psi_{v_0})$ is an injection. Therefore, Theorem 2.5 and Lemma 4.7 show that $r_2(E, \psi_{v_0}) = r_2(E) - 1$. Then the result follows from Proposition 4.6(ii).

Case 2: $\mathrm{Gal}(M/K) \cong \mathbf{Z}/2\mathbf{Z}$ and $E(K_{v_0}) \cong \mathbf{R}/\mathbf{Z}$ (i.e., $\psi_{v_0}(\Delta_E) = -1$). We have $\mathrm{Sel}_2(E) = \mathrm{Sel}_2(E, \psi_{v_0})$ since $\alpha_{v_0}(1_v), \alpha_{v_0}(\psi_{v_0}) \subset H^1(\mathbf{R}, E[2]) = 0$ in this case. The result follows form Proposition 4.6(i).

Case 3: $\mathrm{Gal}(M/K) \cong \mathbf{Z}/2\mathbf{Z}$ and $E(K_{v_0}) \cong \mathbf{R}/\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ ($\Delta_E \notin (K^\times)^2$ and $\psi_{v_0}(\Delta_E) = 1$). Suppose that $\beta_1, \ldots, \beta_{n-1}, \Delta_E$ form a basis of $\mathcal{O}_{K,\Sigma}^\times/(\mathcal{O}_{K,\Sigma}^\times)^2$. By Corollary 2.12, we have $|r_2(E, \psi_{v_0}) - r_2(E)| \leq 1$. Then $r_2(E, \psi_{v_0}) = r_2(E) + 1$ or $r_2(E) - 1$ by Theorem 2.5 and Lemma 4.7. If $r_2(E, \psi_{v_0}) = r_2(E) - 1$, Proposition 4.6(ii) proves the result. Hence for the rest of the proof, we assume $r_2(E, \psi_{v_0}) = r_2(E) + 1$. Choose $c \in \mathrm{Sel}_2(E, \psi_{v_0}) \backslash \mathrm{Sel}_2(E)$. Then $\mathrm{res}_{v_0}(c) \neq 0$. Let $\tilde{c}$ denote the image of $c$ in the map (5) in Lemma 4.8. Let $L := M(\sqrt{\beta_1}, \ldots, \sqrt{\beta_{n-1}})$ and $N := \overline{M}^{\ker(\tilde{c})}$ (we identify $\overline{K}$ and $\overline{M}$).

(i) First, suppose that $N \not\subset L$. Choose $\mathfrak{q} \in \mathcal{P}_2$ so that

- $\mathfrak{q}$ is unramified in $NL/M$
- $\mathrm{Frob}_{\mathfrak{q}}(\sqrt{\beta_i})/\sqrt{\beta_i} = \psi_{v_0}(\beta_i)$,
- $\mathrm{Frob}_{\mathfrak{q}}|_{\mathrm{Gal}(N/M)} \neq 1$, i.e., $N \not\subset K_{\mathfrak{q}}$.

It is possible because $N \not\subset L$. Note that $\mathfrak{q}$ is chosen as in Lemma 4.5 for $T = \varnothing$ (see (4)). Then $\mathrm{res}_{\mathfrak{q}}(c) \neq 0$ since $N \not\subset K_{\mathfrak{q}}$. The result follows from Proposition 4.6(iii).

(ii) Now we assume that $N \subset L$. By choosing a basis again, we may assume that $\psi_{v_0}(\beta_1) = -1$ and $\psi_{v_0}(\beta_2) = \psi_{v_0}(\beta_3) = \cdots = \psi_{v_0}(\beta_{n-1}) = \psi_{v_0}(\Delta_E) = 1$. Since $\mathrm{res}_{v_0}(c) \neq 0$, we have $N \not\subset M(\sqrt{\beta_2}, \sqrt{\beta_3}, \ldots, \sqrt{\beta_{n-1}})(= L \cap K_{v_0})$. Choose $\mathfrak{q} \in \mathcal{P}_2$ so that

- $\mathfrak{q}$ is unramified in $L/K$
- $\mathrm{Frob}_{\mathfrak{q}}(\sqrt{\beta_i})/\sqrt{\beta_i} = \psi_{v_0}(\beta_i)$.

Clearly, $L \cap K_{\mathfrak{q}} = M(\sqrt{\beta_2}, \ldots, \sqrt{\beta_{n-1}})$. Note that $\mathfrak{q}$ is chosen as in Lemma 4.5 for $T = \varnothing$ (see (4)). Therefore $\mathrm{res}_{\mathfrak{q}}(c) \neq 0$, since $N \subset K_{\mathfrak{q}}$ would mean $N \subset M(\sqrt{\beta_2}, \ldots, \sqrt{\beta_{n-1}})$, which is a contradiction. Then the theorem follows from Proposition 4.6(iii). □

**Theorem 4.10.** *Suppose that $E$ has multiplicative reduction at a prime $v_0$, where $v_0 \nmid 2$. Then there exist (infinitely many) $\chi \in \mathcal{C}(K)$ such that $r_2(E^\chi) = r_2(E) + 3$. If moreover, $E(K)[2] \cong \mathbf{Z}/2\mathbf{Z}$ and $v_0(\Delta_E)$ is odd where $v_0$ denote the normalized valuation of $K_{v_0}$, then there exist (infinitely many) $\chi \in \mathcal{C}(K)$ such that $r_2(E^\chi) = r_2(E) + 1$.*

*Proof.* If $E(K)[2] = 0$, [7, Theorem 1.5] and Theorem 3.2 prove the stronger statement that $A_E = \mathbf{Z}_{\geq 0}$. Suppose that $E(K)[2] \neq 0$. Choose the (nontrivial) quadratic unramified character $\psi_{v_0} \in \mathcal{C}(K_{v_0})$. By local class field theory, $\psi_{v_0}(\Delta_E) = 1$ if and only if $v_0(\Delta_E)$ is even. By Corollary 2.12, we have $|r_2(E) - r_2(E, \psi_{v_0})| \leq 2$. Therefore, [4, Propositions 1 and 2(a)] and Theorem 2.5 show that $r_2(E) - r_2(E, \psi_{v_0})$ is either $-1$ or 1. Let $T = \varnothing$ and choose $\mathfrak{q}$ and $\chi$ as in Lemma 4.5. If $\psi_{v_0}(\Delta_E) = 1$, [4, Propositions 1 and 2(a)] shows that $h_{v_0}(\psi_{v_0}) = 1$. Then Proposition 4.6(ii) and Theorem 3.2 prove the first assertion. If $\psi_{v_0}(\Delta_E) = -1$ (so $E(K)[2] \cong \mathbf{Z}/2\mathbf{Z}$), [4, Propositions 1 and 2(a)] shows that $h_{v_0}(\psi_{v_0}) = 0$, so $\mathrm{Sel}_2(E) = \mathrm{Sel}_2(E, \psi_{v_0})$. Therefore the second assertion follows from Proposition 4.6(i). □

## 5. An upper bound for $t_E$

We continue to assume that $E$ is an elliptic curve over a number field $K$. Recall that $t_E$ is the smallest number in the set $A_E = \{r_2(E^\chi) : \chi \in \mathcal{C}(K)\}$. In this section, we study $t_E$. Let $s_2$ be the number of complex places of $K$.

**Example 5.1.** Let $E_{(m)}$ be the elliptic curve over $K$ defined by the equation

$$E_{(m)} : y^2 + xy = x^3 - 128m^2x^2 - 48m^2x - 4m^2. \tag{6}$$

Suppose that $1 + 256m^2 \notin (K^\times)^2$. Then $E_{(m)}$ has a single point $(-1/4, 1/8)$ of order 2 in $E_{(m)}(K)$. In [2], Klagsbrun shows that $t_{E_{(m)}} \geq s_2 + 1$. Note that in this paper $r_2(E)$ is defined (slightly) differently from that defined in [2] (In [2], the author subtracts the contribution of rational 2-torsion points from $\dim_{\mathbf{F}_2}(\mathrm{Sel}_2(E))$ for the "2-Selmer rank"). As his example suggests, $t_E$ can be a lot bigger than the trivial lower bound $\dim_{\mathbf{F}_2}(E(K)[2])$.

**Remark 5.2.** If $K$ contains $\sqrt{1 + 256m^2}$, then $E(K)$ contains all 2-torsion points. In this case, we still can prove $t_{E_{(m)}} \geq s_2$ using the argument in [2]. Note that all Lemmas and Propositions in Section 3 in *op. cit.* can be proved by the exactly same methods. However, in the proof of Proposition 4.1 in *op. cit.*, now the map from $\mathrm{Sel}_\phi(E)$ to $\mathrm{Sel}_2(E)$ is injective and $\dim_{\mathbf{F}_2}(\mathrm{Sel}_{\hat{\phi}}(E'/K)) \geq 0$, so $r_2(E) \geq \mathrm{ord}_2(\mathcal{T}(E/E'))$ is the correct lower bound we can get from applying the argument of the proof of Proposition 4.1 in *op. cit.*.

For the rest of the paper, we let $|\Sigma| = n$ and $E[2] \subset E(K)$. Note that this means if $v \notin \Sigma$, then $v \in \mathcal{P}_2$. For a character $\chi \in \mathcal{C}(K)$ and a place $v$, we write $\chi_v \in \mathcal{C}(K_v)$ for the restriction of $\chi$ to $K_v^\times$ via the local reciprocity map. Let $L = K(\sqrt{\mathcal{O}_{K,\Sigma}^\times})$. Let $v_0 \in \Sigma$ and $\psi_{v_0} \in \mathcal{C}(K_{v_0})$. We discuss an upper bound for $t_E$ from now on.

**Definition 5.3.** If $\mathfrak{q} \notin \Sigma$, the composition map

$$\mathrm{Sel}_2(E, \psi_{v_0}) \xrightarrow{\mathrm{res}_\mathfrak{q}} \mathrm{Hom}_{ur}(G_{K_\mathfrak{q}}, E[2]) \cong E[2]$$

is given by sending $c \in \mathrm{Sel}_2(E, \psi_{v_0}) \subset \mathrm{Hom}(G_K, E[2])$ to $c(\mathrm{Frob}_\mathfrak{q})$, where $\mathrm{Frob}_\mathfrak{q}$ is a Frobenius automorphism at $\mathfrak{q}$ (note that $\mathrm{res}_\mathfrak{q}(c) \neq 0$ if and only if $c(\mathrm{Frob}_\mathfrak{q}) \neq 0$).

**Lemma 5.4.** *Suppose that $\phi_1, \dots, \phi_n$ are homomorphisms from $\mathbf{F}_2^m$ to $\mathbf{F}_2^2$ where $m = n + k$ and $1 \le k \le n$ such that $\cap_{i=1}^n \ker(\phi_i) = \{0\}$. Then there exist $i_1, \dots, i_k$ such that $\phi_{i_1} \times \cdots \times \phi_{i_k} : \mathbf{F}_2^m \to (\mathbf{F}_2^2)^k$ sending $v \in \mathbf{F}_2^m$ to $(\phi_{i_1}(v), \dots, \phi_{i_k}(v))$ is surjective.*

*Proof.* Define $s_j = \dim_{\mathbf{F}_2}(\mathrm{Im}(\phi_1 \times \cdots \times \phi_j))$. Then clearly $s_j = s_{j-1}$ or $s_j = s_{j-1} + 1$ or $s_j = s_{j-1} + 2$. Then there are at least $k$ many $j$ such that $s_j = s_{j-1} + 2$. Collect all $j$ such that $s_j = s_{j-1} + 2$ and name them $i_1 < \cdots < i_k < \cdots$. Then it is easy to see $\phi_{i_1} \times \cdots \times \phi_{i_k}$ is surjective. □

**Proposition 5.5.** *Let $v_0 \in \Sigma$ and $\psi_{v_0} \in \mathcal{C}(K_{v_0})$. Then $r_2(E, \psi_{v_0}) \le 2n$.*

*Proof.* Clearly, we have $\mathrm{Sel}_2(E, \psi_{v_0}) \subseteq \mathrm{Hom}(G_K, E[2])$. For all nonzero $s \in \mathrm{Sel}_2(E, \psi_{v_0})$, we claim that $\overline{K}^{\ker(s)} \subseteq L = K(\sqrt{\mathcal{O}_{K,\Sigma}^\times})$. Indeed, for any quadratic extension $K(\sqrt{a})/K$, where all primes not in $\Sigma$ are unramified, one can replace $a$ with an element in $\mathcal{O}_{K,\Sigma}^\times$ because $\mathrm{Pic}(O_{K,\Sigma}) = 1$. Now the claim follows easily once we note that $\overline{K}^{\ker(s)}$ is a compositum of (possibly the same) quadratic extensions, where all primes not in $\Sigma$ are unramified. Therefore, $\mathrm{Sel}_2(E, \psi_{v_0}) \subseteq \mathrm{Hom}(\mathrm{Gal}(L/K), E[2])$ by the Inflation-Restriction Sequence. By Lemma 4.1, $\dim_{\mathbf{F}_2}(\mathrm{Gal}(L/K)) = n$, whence the result. □

**Theorem 5.6.** *Suppose $E[2] \subset E(K)$. If $r_2(E, \psi_{v_0}) = n + k$ for $2 \le k \le n$, then there exist $E^\chi$ such that $r_2(E^\chi) = n - k + 2$. In particular $t_E \le n + 1$.*

*Proof.* Let $\beta_1, \dots, \beta_n$ be a basis of $\mathcal{O}_{K,\Sigma}^\times/(\mathcal{O}_{K,\Sigma}^\times)^2$. Let $L = K(\sqrt{\beta_1}, \dots, \sqrt{\beta_n})$. Define $\sigma_i \in \mathrm{Gal}(L/K)$ so that $\sigma_i(\sqrt{\beta_i}) = -\sqrt{\beta_i}$ and $\sigma_i(\sqrt{\beta_j}) = \sqrt{\beta_j}$ for $j \ne i$. Note that an element $s \in \mathrm{Sel}_2(E, \psi_{v_0})$ is determined by $s(\sigma_1), \dots, s(\sigma_n) \in E[2]$. Define $t_i \in \mathrm{Hom}(\mathrm{Sel}_2(E, \psi_{v_0}), E[2])$ sending $s \in \mathrm{Sel}_2(E, \psi_{v_0})$ to $s(\sigma_i)$. Applying Lemma 5.4, without loss of generality, we may assume $t_1 \times \cdots \times t_k$ is a surjection from $\mathrm{Sel}_2(E, \psi_{v_0})$ to $E[2]^k$. In other words, there exist $s_{2i-1}, s_{2i}$ for $0 \le i \le k$ such that

- $s_{2i-1}(\sigma_i) = P_1$ and $s_{2i}(\sigma_i) = P_2$, where $P_1, P_2 \in E[2]$ is a basis of $E[2]$,
- $s_{2i-1}(\sigma_j) = s_{2i}(\sigma_j) = 0$ for $1 \le j \ne i \le k$.

For $1 \le i \le k$, let $\omega_i \in \mathcal{P}_2$ be a prime such that $\mathrm{Frob}_{\omega_i} = \sigma_i$ in $\mathrm{Gal}(L/K)$. Then by Definition 5.3 we have that

(i) $\mathrm{res}_{\omega_i}(s_{2i-1})$ and $\mathrm{res}_{\omega_i}(s_{2i})$ generate $\alpha_{\omega_i}(1_{\omega_i}) = \mathrm{Hom}_{\mathrm{ur}}(G_{K_{\omega_i}}, E[2])$, and

(ii) $\mathrm{res}_{\omega_j}(s_{2i-1}) = \mathrm{res}_{\omega_j}(s_{2i}) = 0$ for $1 \le j \ne i \le k$.

Let $T = \{\omega_1, \dots, \omega_k\}$. Let $\psi_i \in \mathcal{C}_{\mathrm{ram}}(K_{\omega_i})$. Then by Corollary 2.11 and Theorem 2.10, we have $\mathrm{Sel}_2(E, \psi_{v_0}) = \mathrm{Sel}_2^T(E, \psi_{v_0})$ and

$$r_2(E, \psi_1, \dots, \psi_k, \psi_{v_0}) = r_2(E, \psi_{v_0}) - 2k. \tag{7}$$

By Lemma 4.5, there exist $\mathfrak{q} \in \mathcal{P}_2 \backslash T$ and $\chi \in \mathcal{C}(K)$ so that

- $\chi_{v_0} = \psi_{v_0}$
- $\chi_v = 1_v$ for $v \in \Sigma \backslash \{v_0\}$,
- $\chi_\omega$ is ramified for $\omega \in T$,
- $\chi_\mathfrak{p}$ is unramified for $\mathfrak{p} \notin \Sigma \cup T \cup \{\mathfrak{q}\}$, and
- $\chi_\mathfrak{q}$ is ramified.

Then $\mathrm{Sel}_2(E^\chi) = \mathrm{Sel}_2(E, \chi_{\omega_1}, \dots, \chi_{\omega_k}, \psi_{v_0}, \chi_\mathfrak{q})$. Theorem 2.5, Lemma 2.9, and Corollary 2.12 show

$$|r_2(E, \chi_{\omega_1}, \dots, \chi_{\omega_k}, \psi_{v_0}, \chi_\mathfrak{q}) - r_2(E, \chi_{\omega_1}, \dots, \chi_{\omega_k}, \psi_{v_0})|$$

is even and less than or equal to 2, so by (7), we have $r_2(E^\chi) = r_2(E, \psi_{v_0}) - 2k-2$ or $r_2(E, \psi_{v_0}) - 2k$ or $r_2(E, \psi_{v_0}) - 2k+2$. In any case, by Theorem 3.2, there exist infinitely many $\varphi \in \mathcal{C}(K)$ such that $r_2(E^\varphi/K) = r_2(E, \psi_{v_0}) - 2k + 2 = n + k - 2k + 2 < n + 1$. Proposition 5.5 with putting $\psi_{v_0} = 1_{v_0}$ shows that $t_E \leq n + 1$. $\square$

**Lemma 5.7.** *Suppose that there exist* $c_1, c_2 \in \mathrm{Sel}_2(E, \psi_{v_0})$ *such that* $\mathrm{res}_\omega(c_1)$ *and* $\mathrm{res}_\omega(c_2)$ *generate* $\alpha_\omega(1_\omega) = \mathrm{Hom}_{\mathrm{ur}}(G_\omega, E[2])$ *for some prime* $\omega \notin \Sigma$. *Then there exist infinitely many* $\varphi \in \mathcal{C}(K)$ *such that* $r_2(E^\varphi/K) = r_2(E, \psi_{v_0})$.

*Proof.* Let $T = \{\omega\}$. By Lemma 4.5, there exist infinitely many $\mathfrak{q} \notin \Sigma \cup T$ for which there exists a character $\chi \in \mathcal{C}(K)$ such that

- $\chi_{v_0} = \psi_{v_0}$,
- $\chi_v = 1_v$ for $v \in \Sigma \backslash \{v_0\}$,
- $\chi_\omega$ is ramified,
- $\chi_\mathfrak{p}$ is unramified for all $\mathfrak{p} \notin \Sigma \cup T \cup \{\mathfrak{q}\}$, and
- $\chi_\mathfrak{q}$ is ramified.

Note that $\mathrm{Sel}_2(E^\chi) = \mathrm{Sel}_2(E, \psi_{v_0}, \chi_\omega, \chi_\mathfrak{q})$ by Lemma 2.6. Let $S = \{\omega, \mathfrak{q}\}$. Then $r_2(E, \psi_{v_0}) \geq \dim_{\mathbf{F}_2}(\mathrm{Sel}_{2,S}(E^\chi)) + 2$, since by the condition on $c_1, c_2, \omega$

the following map is surjective

$$\mathrm{res}_\omega : \mathrm{Sel}_2(E, \psi_{v_0})/\mathrm{Sel}_{2,S}(E^\chi) \to \mathrm{Hom}_{\mathrm{ur}}(G_{K_\omega}, E[2]).$$

Note that $c_1, c_2, c_1 + c_2 \in \mathrm{Sel}_2^S(E^\chi) \backslash \mathrm{Sel}_2(E^\chi)$ since $\alpha_\omega(1_\omega) \cap \alpha_\omega(\chi_\omega) = \{0\}$ (Lemma 2.9). Therefore $\dim_{\mathbf{F}_2}(\mathrm{Sel}_2^S(E^\chi)) \geq r_2(E^\chi) + 2$. Theorem 2.10 shows that $\dim_{\mathbf{F}_2}(\mathrm{Sel}_2^S(E^\chi)) - \dim_{\mathbf{F}_2}(\mathrm{Sel}_{2,S}(E^\chi)) = 4$. Then it follows that $r_2(E, \psi_{v_0}) \geq r_2(E^\chi)$ and $r_2(E, \psi_{v_0}) \equiv r_2(E^\chi) \pmod 2$ by Theorem 2.5. Then the assertion follows from Theorem 3.2. □

**Theorem 5.8.** *If $E$ does not satisfy the constant 2-Selmer parity condition, then $t_E \leq n$.*

*Proof.* If $r_2(E) \equiv n \pmod 2$, the result follows from Theorem 5.6. From now on, we assume that $r_2(E) \not\equiv n \pmod 2$. Since $E$ does not satisfy the constant 2-Selmer parity, there exist $v_0 \in \Sigma$ and $\psi_{v_0} \in \mathcal{C}(K_{v_0})$ such that $r_2(E, \psi_{v_0}) \equiv n \pmod 2$ by Theorem 2.5 (note that since $E[2] \subset E(K)$, all primes outside $\Sigma$ are in $\mathcal{P}_2$, so twisting locally at primes not in $\Sigma$ does not change the parity by Lemma 2.6 and Lemma 2.9). If $r_2(E, \psi_{v_0}) \leq n - 2$ or $r_2(E, \psi_{v_0}) \geq n + 2$, then the result follows from Proposition 4.6(ii), Theorem 5.6, respectively. Let $r_2(E, \psi_{v_0}) = n$. If $\psi_{v_0}(\mathcal{O}_{K,\Sigma}^\times) = 1$, Proposition 4.4 shows the result. Now let $\beta_1, \ldots, \beta_n$ be a basis of $\mathcal{O}_{K,\Sigma}^\times/(\mathcal{O}_{K,\Sigma}^\times)^2$ such that $\psi_{v_0}(\beta_1) = -1$ and $\psi_{v_0}(\beta_2) = \psi_{v_0}(\beta_3) = \cdots = \psi_{v_0}(\beta_n) = 1$.

Define $\sigma_1, \ldots, \sigma_n$ and $t_1, \ldots, t_n$ as in the proof of Theorem 5.6. If $\dim_{\mathbf{F}_2}(\mathrm{Im}(t_1)) \geq 1$, let $c \in \mathrm{Sel}_2(E, \psi_{v_0})$ and $c(\sigma_1) \neq 0$. Choose $\mathfrak{q}$ ($T = \varnothing$) as in Lemma 4.5, i.e., $\mathrm{Frob}_\mathfrak{q} = \sigma_1$ in $L/K$ (see (4)). Then $c(\mathrm{Frob}_\mathfrak{q}) = c(\sigma_1) \neq 0$, so Definition 5.3 shows $\mathrm{res}_\mathfrak{q}(c) \neq 0$. Then the result follows from Proposition 4.6(iii). Therefore for the rest of the proof, assume that $\dim_{\mathbf{F}_2}(\mathrm{Im}(t_1)) = 0$. Then without loss of generality, we may assume $\dim_{\mathbf{F}_2}(\mathrm{Im}(t_2)) = 2$. Choose $\omega \notin \Sigma$ so that $\mathrm{Frob}_\omega = \sigma_2$ in $\mathrm{Gal}(L/K)$. Then Definition 5.3 shows that there exist $c_1, c_2 \in \mathrm{Sel}_2(E, \psi_{v_0})$ such that $\mathrm{res}_\omega(c_1)$ and $\mathrm{res}_\omega(c_2)$ generate $\mathrm{Hom}_{\mathrm{ur}}(G_{K_\omega}, E[2])$. Now Lemma 5.7 completes the proof. □

## Acknowledgements

The author is very grateful to his advisor Karl Rubin for helpful suggestions and discussion. The author also thanks to the referee for careful reading the manuscript and many comments.

## References


[1] T. Dokchitser and V. Dokchitser, *Root numbers and parity of ranks of elliptic curves*, J. Reine Angew. Math. **658** (2011), 39–64.

[2] Z. Klagsbrun, *Elliptic curves with a lower bound on* 2*-Selmer ranks of quadratic twists*, Math. Res. Lett. **19** (2012), no. 5, 1137–1143.

[3] Z. Klagsbrun, B. Mazur, and K. Rubin, *Disparity in Selmer ranks of quadratic twists of elliptic curves*, Ann. of Math. (2) **178** (2013), no. 1, 287–320.

[4] K. Kramer, *Arithmetic of elliptic curves upon quadratic extension*, Trans. Amer. Math. Soc. **264** (1981), no. 1, 121–135.

[5] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

[6] B. Mazur and K. Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799, viii+96.

[7] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), no. 3, 541–575.

[8] J. Neukirch, *Algebraic number theory*, Vol. 322 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Springer-Verlag, Berlin (1999), `ISBN 3-540-65399-6`. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[9] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, Vol. 323 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Springer-Verlag, Berlin, second edition (2008), `ISBN 978-3-540-37888-4`.

[10] M. Yu, *Selmer ranks of twists of hyperelliptic curves and superelliptic curves*, J. Number Theory **160** (2016), 148–185.



Department of Mathematics
University of California, Irvine
Irvine, CA 92697, USA
*E-mail address*: `myungjuy@math.uci.edu`


Received November 23, 2015