LARGE SHAFAREVICH-TATE GROUPS OVER QUADRATIC NUMBERIELDS

MYUNGJUN YU

Abstract. Let $E$ be an elliptic curve over the rational field $\mathbb{Q}$. Let $K$ be a quadratic extension over $\mathbb{Q}$. We show that (under mild conditions on $E$) for every $r > 0$, there are infinitely many quadratic twists $E^d/\mathbb{Q}$ of $E/\mathbb{Q}$ such that $\dim F_2(\Sha(E^d/K)[2]) > r$.

1. Introduction

Let $E$ be an elliptic curve over a number field $F$. The group of rational points $E(F)$ is known to be a finitely generated abelian group and its rank is called the Mordell-Weil rank, denoted by $\text{rk}(E(F))$. The Mordell-Weil rank is one of the most interesting and mysterious invariants in the study of elliptic curves. In general, it is very difficult to compute the Mordell-Weil rank, and we often study various Selmer groups, which give upper bounds for the Mordell-Weil rank. These Selmer groups also contain the information of another very important object, called the Shafarevich-Tate group. Precisely, one can define the Shafarevich-Tate group of $E/F$ as follows.

$\Sha(E/F) := \ker \left( H^1(F, E(F)) \to \prod_v H^1(F_v, E(F_v)) \right)$,

where $v$ varies over the places of $F$.

It is conjectured that $\Sha(E/F)$ is finite, but one may wonder whether the order of $\Sha(E/F)$ can be arbitrarily large. Since it is often easier to study its $p$-torsion part (for a prime $p$) instead, a natural question one can ask is: “can $\Sha(E/F)[p]$ be arbitrarily large?”

Cassels [2] first showed the unboundedness of $\text{dim}_{\mathbb{F}_p}(\Sha(E/\mathbb{Q})[3])$ as $E$ varies over elliptic curves over $\mathbb{Q}$. Showing the unboundedness of $\text{dim}_{\mathbb{F}_p}(\Sha(E/\mathbb{Q})[p])$ has been successful for some primes including 2, 3, 5, 7 and 13. For related results, see [1], [4], [9], and [10]. They use the fact that there are infinitely many elliptic curves over $\mathbb{Q}$ with rational $p$-isogenies, so this idea doesn’t seem to work for all primes $p$.

If $F$ is allowed to vary (with bounded degree over $\mathbb{Q}$), Kloosterman [7] showed that for any $p$, $\text{dim}_{\mathbb{F}_p}(\Sha(E/F)[p])$ is unbounded (as $E$ also varies). Clark and Sharif [3] proved that for any elliptic curve $E/\mathbb{Q}$, $\text{dim}_{\mathbb{F}_p}(\Sha(E/F)[p])$ is unbounded when $F$ varies over degree $p$ (not necessarily Galois) extensions over $\mathbb{Q}$.

If $F$ is a fixed Galois extension of degree $p$ over $\mathbb{Q}$, Matsumoto [11] proved that $\text{dim}_{\mathbb{F}_p}(\Sha(E/F)[p])$ is unbounded as $E$ varies over elliptic curves over $\mathbb{Q}$. It is important to note that the unboundedness of $\text{dim}_{\mathbb{F}_p}(\Sha(E/\mathbb{Q})[p])$ does not imply that of $\text{dim}_{\mathbb{F}_p}(\Sha(E/F)[p])$ since the kernel of the restriction map

$\Sha(E/\mathbb{Q})[p] \to \Sha(E/F)[p]$
could be also large in size under the condition that \([F : \mathbb{Q}] = p\). We give a further discussion of Matsuno’s result when \(p = 2\) in Remark 1.4.

Now let \(D\) be a squarefree integer and let \(K = \mathbb{Q}(\sqrt{D})\) be a quadratic number field. For a squarefree integer \(d\), we write \(E^d\) for the quadratic twist of \(E\) by \(\mathbb{Q}(\sqrt{d})/\mathbb{Q}\). In this paper, we improve Matsuno’s theorem when \(p = 2\) by showing \(\dim_{\mathbb{F}_2}(\text{Sel}_2(E^d/K)[2])\) is unbounded as \(E^d\) varies over quadratic twists of a fixed elliptic curve \(E/\mathbb{Q}\) (under mild conditions on \(E\)).

More precisely, the main theorem of this paper is

**Theorem 1.1.** Let \(E\) be an elliptic curve over \(\mathbb{Q}\) with no non-trivial rational 2-torsion point. Let \(\Delta\) be the discriminant of a model of \(E\). If \(K \neq \mathbb{Q}(\sqrt{\Delta})\), then for every \(r > 0\), there exist infinitely many quadratic twists \(E^d\) of \(E\) over \(\mathbb{Q}\) such that

\[
\dim_{\mathbb{F}_2}(\text{III}(E^d/K)[2]) - \dim_{\mathbb{F}_2}(\text{III}(E^d/\mathbb{Q})[2]) > r.
\]

As an immediate consequence, we have

**Corollary 1.2.** Let \(E/\mathbb{Q}\), \(K\), and \(r\) be as in the previous theorem. Then there exist infinitely many quadratic twists \(E^d\) of \(E\) over \(\mathbb{Q}\) such that

\[
\dim_{\mathbb{F}_2}(\text{III}(E^d/K)[2]) > r.
\]

**Remark 1.3.** In an appendix to [5], Rohrlich proved that for every \(r > 0\), there exists \(E^d/\mathbb{Q}\) such that

\[
\dim_{\mathbb{F}_2}(\text{III}(E^d/\mathbb{Q})[2]) > r.
\]

Note that the above corollary is not a direct consequence of Rohrlich’s theorem since the kernel of the restriction map

\[
\text{III}(E^d/\mathbb{Q})[2] \to \text{III}(E^d/K)[2]
\]

can be also large as mentioned above.

**Remark 1.4.** What Matsuno [11] proved in the case \(p = 2\) is as follows. Let \(A/\mathbb{Q}\) be an elliptic curve defined by the equation

\[
y^2 + xy = x^3 + 8mx^2 + lm,
\]

with certain restrictions on the prime divisors of \(l\) and \(m\). Then Corollary 1.2 holds when \(E\) is replaced by \(A\).

1.1. **Strategy of the proof.** For a number field \(F\) and an elliptic curve \(E/F\), we have a short exact sequence

\[(1) \quad 0 \rightarrow E(F)/2E(F) \rightarrow \text{Sel}_2(E/F) \rightarrow \text{III}(E/F)[2] \rightarrow 0.\]

It follows that

\[(2) \quad \dim_{\mathbb{F}_2}(\text{Sel}_2(E/F)) = \text{rk}(E(F)) + \dim_{\mathbb{F}_2}(E(F)[2]) + \dim_{\mathbb{F}_2}(\text{III}(E/F)[2]).\]

We will construct \(E^d\) so that the following conditions are all satisfied.

(i) \(\text{rk}(E^d(\mathbb{Q})) = \text{rk}(E^d(K))\),

(ii) \(\dim_{\mathbb{F}_2}(\text{Sel}_2(E^d(\mathbb{Q}))) < a\) for a fixed constant \(a\),

(iii) \(\dim_{\mathbb{F}_2}(\text{Sel}_2(E^d(K))) \gg 0\).

Then, by (2), (i) and (ii), we have \(\text{rk}(E^d(K)) < a\) and \(\dim_{\mathbb{F}_2}(\text{III}(E^d(\mathbb{Q}))[2]) < a\). Therefore it follows from (2) and (iii) that

\[
\dim_{\mathbb{F}_2}(\text{III}(E^d/K)[2]) - \dim_{\mathbb{F}_2}(\text{III}(E^d/\mathbb{Q})[2]) \gg 0.
\]
2. Selmer ranks over $K$

Let $E$ be an elliptic curve over $\mathbf{Q}$ with no non-trivial rational 2-torsion point. We write $q$ for a prime of $\mathbf{Q}$. Let $\mathbf{Q}_q$ denote the $q$-adic completion of $\mathbf{Q}$.

**Definition 2.1.** We define

$$W_{q,K} := \ker \left( H^1(\mathbf{Q}_q, E(\mathbf{Q}_q)) \to H^1(K_q, E(\mathbf{Q}_q)) \right),$$

where $q$ is a prime of $K$ above $q$ and $K_q$ is the completion of $K$ at $q$.

**Lemma 2.2.** Let $q$ be an odd prime such that $\dim_{\mathbf{F}_2}(E(\mathbf{Q}_q)[2]) = 2$. Suppose $E$ has additive reduction at $q$ and suppose $q$ is inert in $K/\mathbf{Q}$. Then

(i) $E(K_q)[2\infty] = E(K_q)[2] = E[2]$

(ii) $\dim_{\mathbf{F}_2}(W_{q,K}) = 2$.

**Proof.** It follows from [15, Proposition VII.5.4(a)] that $E$ has additive reduction over $K_q$. By [15, Theorem VII.6.1], we have $[E(K_q) : E_0(K_q)] \leq 4$. Since $E_0(K_q)$ is divisible by 2, (i) follows. We now show (ii). By the inflation-restriction sequence, we have

$$W_{q,K} \cong H^1(K_q/\mathbf{Q}_q, E(K_q)) \cong H^1(K_q/\mathbf{Q}_q, E(\mathbf{Q}_q)[2\infty]) \cong \text{Hom}(K_q/\mathbf{Q}_q, E[2]),$$

where the second isomorphism follows from decomposing $E(K_q)$ into the direct sum of 2-primary part and non 2-primary part (note that $[K_q : \mathbf{Q}_q] = 2$). Then (ii) easily follows.

Define $A_E$ to be the set of primes $q$ of $\mathbf{Q}$ satisfying the conditions of Lemma 2.2.

We write Sel$_2(E/K)$ for the classical 2-Selmer group of $E/K$ (see Definition 3.7).

**Proposition 2.3.** We have

$$\dim_{\mathbf{F}_2}(\text{Sel}_2(E/K)) \geq 2|A_E|.$$

**Proof.** The proposition immediately follows from the remark after [11, Corollary 3.3] and Lemma 2.2(ii). \(\square\)

3. Selmer ranks over $\mathbf{Q}$

We continue to assume that $E/\mathbf{Q}$ has no non-trivial rational 2-torsion point. Let $d$ be a squarefree integer.

**Lemma 3.1.** Let $q$ be an odd prime. Then

$$\dim_{\mathbf{F}_2}(E(\mathbf{Q}_q)/2E(\mathbf{Q}_q)) = \dim_{\mathbf{F}_2}(E(\mathbf{Q}_q)[2]).$$

**Proof.** See for example, [13, Lemma 2.2(i)]. \(\square\)

**Definition 3.2.** Let $G_E$ be the set of odd primes where $E$ has good reduction. For $0 \leq i \leq 2$, define

$$\mathcal{P}_{E,i} = G_E \cap \{ q : \dim_{\mathbf{F}_2}(E(\mathbf{Q}_q)[2]) = i \}.$$

**Remark 3.3.** If $q \in G_E$, then $\mathbf{Q}(E[2])$ is an unramified extension of $\mathbf{Q}$ at $q$, where $\mathbf{Q}(E[2])$ is the smallest extension of $\mathbf{Q}$ that contains the coordinates of all points of $E[2]$. Write $\text{Frob}_q$ for the Frobenius automorphism at $q$ in $\text{Gal}(\mathbf{Q}(E[2])/\mathbf{Q})$. Then by [6, Lemma 4.3], we have

(i) $\text{Frob}_q$ has degree 3 if and only if $q \in \mathcal{P}_{E,0}$,

(ii) $\text{Frob}_q$ has degree 2 if and only if $q \in \mathcal{P}_{E,1}$. 


(iii) \( \text{Frob}_q = 1 \) if and only if \( q \in \mathcal{P}_{E,2} \).

**Definition 3.4.** Let \( v \) be a place of \( \mathbb{Q} \). For \( d_v \in \mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^2 \), define the image
\[
\alpha_v(d_v) := \text{Im} \left( E^{d_v}(\mathbb{Q}_v)/2E^{d_v}(\mathbb{Q}_v) \to H^1(\mathbb{Q}_v, E^{d_v}[2]) \cong H^1(\mathbb{Q}_v, E[2]) \right),
\]
where the first map is the Kummer map for multiplication by 2 on \( E^{d_v} \) and the second map is induced by the canonical isomorphism \( E^{d_v}[2] \cong E[2] \).

**Remark 3.5.** For \( d \in \mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^2 \), note that \( \alpha_v(d) \) only depends on the image of \( d \) in \( \mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^2 \).

We recall the Tate local duality:

**Theorem 3.6.** The Weil pairing and cup product induce a nondegenerate pairing
\[
\langle \ , \rangle_v : H^1(\mathbb{Q}_v, E[2]) \times H^1(\mathbb{Q}_v, E[2]) \to H^2(\mathbb{Q}_v, \{\pm 1\}) \cong \mathbb{F}_2.
\]

**Proof.** See [14, Theorem 7.2.6]. \( \square \)

Define the restriction map at \( v \)
\[
\text{res}_v : H^1(\mathbb{Q}, E[2]) \to H^1(\mathbb{Q}_v, E[2]).
\]

**Definition 3.7.** The 2-Selmer group \( \text{Sel}_2(E^d/\mathbb{Q}) \subset H^1(\mathbb{Q}, E[2]) \) is the (finite) \( \mathbb{F}_2 \)-vector space defined by the following exact sequence
\[
0 \to \text{Sel}_2(E^d/\mathbb{Q}) \to H^1(\mathbb{Q}, E[2]) \to \prod_v H^1(\mathbb{Q}_v, E[2])/\alpha_v(d),
\]
where the rightmost map is the sum of \( \text{res}_v \). In particular, if \( d = 1 \), it is the classical 2-Selmer group of \( E/\mathbb{Q} \).

We define various Selmer groups as follows.

**Definition 3.8.** Let \( S \) be a finite set of places of \( \mathbb{Q} \). Define
\[
\text{Sel}_{2,S}(E^d/\mathbb{Q}) := \left\{ x \in \text{Sel}_2(E^d/\mathbb{Q}) : \text{res}_q(x) = 0 \text{ for all } q \in S \right\}.
\]

Define
\[
\text{Sel}_2^S(E^d/\mathbb{Q}) := \left\{ x \in H^1(\mathbb{Q}, E[2]) : \text{res}_q(x) \in \alpha_q(d) \text{ for all } q \notin S \right\}.
\]

If \( S = \{v\} \), we simply write \( \text{Sel}_{2,v}(E^d/\mathbb{Q}) \) and \( \text{Sel}_2^v(E^d/\mathbb{Q}) \) for \( \text{Sel}_{2,S}(E^d/\mathbb{Q}) \) and \( \text{Sel}_2^S(E^d/\mathbb{Q}) \), respectively.

**Theorem 3.9.** Let \( S \) be a finite set of places of \( \mathbb{Q} \). 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 (3) of the places \( v \in S \)
\[
0 \to \text{Sel}_2(E/\mathbb{Q}) \to \text{Sel}_2^S(E/\mathbb{Q}) \to \bigoplus_{v \in S} H^1(\mathbb{Q}_v, E[2])/\alpha_v(1),
\]
\[
0 \to \text{Sel}_{2,S}(E/\mathbb{Q}) \to \text{Sel}_2(E/\mathbb{Q}) \to \bigoplus_{v \in S} \alpha_v(1).
\]

In particular,
\[
\dim_{\mathbb{F}_2}(\text{Sel}_2^S(E/\mathbb{Q})) - \dim_{\mathbb{F}_2}(\text{Sel}_{2,S}(E/\mathbb{Q})) = \sum_{v \in S} \dim_{\mathbb{F}_2}(\alpha_v(1)).
\]

**Proof.** See [12, Theorem 2.3.4]. \( \square \)
Corollary 3.10. Let $T$ be a set of places containing all places $v$, where the local conditions of $E$ and $E^d$ are not the same, i.e., $\alpha_v(1) \neq \alpha_v(d)$. Then

$$|\dim_{F_2}(\text{Sel}_2(E/Q)) - \dim_{F_2}(\text{Sel}_2(E^d/Q))| \leq \sum_{v \in T} \dim_{F_2}(\alpha_v(1)).$$

Proof. We have

$$\text{Sel}_{2,T}(E/Q) \subseteq \text{Sel}_2(E/Q), \text{Sel}_{2}(E^d/Q) \subseteq \text{Sel}_{2}^T(E/Q).$$

Then the corollary is an immediate consequence of Theorem 3.9.

Lemma 3.11. For $0 \leq i \leq 2$, let $q$ be an odd prime in $\mathcal{P}_{E,i}$. Let $v_q$ be the normalized (additive) valuation of $Q_q$. For $d_q \in Q_q^{\times}$, if $v_q(d_q)$ is odd, then

$$\alpha_q(1) \cap \alpha_q(d_q) = 0.$$

Proof. Note that the condition $v_q(d_q)$ is odd is equivalent to the condition that $Q_q(\sqrt{d_q})$ is a ramified (quadratic) extension of $Q_q$. The lemma follows from Lemma 2.11.

For $A \subset H^1(Q, E[2])$, we write $\text{res}_q(A)$ for the image of $A$ under $\text{res}_q$.

Lemma 3.12. Let $q$ be an odd prime in $\mathcal{P}_{E,2}$. There exists $d_q \in Q_q^{\times}$ such that $v_q(d_q)$ is odd and

$$\dim_{F_2}(\alpha_q(d_q) \cap \text{res}_q(\text{Sel}_2^q(E/Q))) \leq \dim_{F_2}(\alpha_q(1) \cap \text{res}_q(\text{Sel}_2^q(E/Q))).$$

Proof. For such $q$, we have $\dim_{F_2}(\text{res}_q(\text{Sel}_2^q(E/Q))) = 2$ by Theorem 3.9. For simplicity, let

$$X := \alpha_q(1) \cap \text{res}_q(\text{Sel}_2^q(E/Q)).$$

If $\dim_{F_2}(X) = 2$, there is nothing to show. If $\dim_{F_2}(X) = 1$, then for any $d_q \in K_q^{\times}$, we have $\dim_{F_2}(\alpha_q(d_q) \cap \text{res}_q(\text{Sel}_2^q(E/Q))) = 1$ by Lemma 3.11 and Theorem 2.5 and Lemma 2.9. If $X = 0$, choose $c_q$, $d_q \in Q_q^{\times}$ so that $Q_q(\sqrt{c_q})$ and $Q_q(\sqrt{d_q})$ are distinct ramified extension over $Q_q$. By Lemma 3.9 and Proposition 3.10(i)], without loss of generality, we can assume

$$\alpha_q(c_q) = \text{res}_q(\text{Sel}_2^q(E/Q)),
\alpha_q(d_q) \cap \text{res}_q(\text{Sel}_2^q(E/Q)) = 0,$$

so the lemma follows.

Proposition 3.13. Assume that $E/Q$ has no rational 2-torsion point. Let $q_1, q_2, \ldots, q_s$ be elements of $\mathcal{P}_{E,2}$. Then there exist infinitely many squarefree odd integers $d$ such that the following conditions are satisfied.

(i) $\dim_{F_2}(\text{Sel}_2(E^d/Q)) \leq \dim_{F_2}(\text{Sel}_2(E/Q))$.

(ii) Every prime divisor of $d$ is in $\mathcal{P}_{E,0} \cup \mathcal{P}_{E,2}$ (in particular if $q|d$, $E$ has good reduction at $q$).

(iii) The prime factors of $d$ in $\mathcal{P}_{E,2}$ are exactly $q_1, q_2, \ldots, q_s$.

Proof. By induction, it is enough to find $d$ so that (i),(ii) hold and $\mathcal{P}_{E,2}$ contains only one prime that divides $d$. This is a consequence of Lemma 3.12 and Lemma 6.4 (and its proof).

\(^1\)Typo: the conclusion of Lemma 6.4 should be \(\text{Sel}_2(J^N/K) = \text{Sel}_2(J, \psi_1)\) not \(\text{Sel}_2(J^N/K) = \text{Sel}_2(J, \chi_d)\).
Lemma 3.14. Suppose \( E/\mathbb{Q} \) has a good reduction at an odd prime \( q \). If \( q \mid d \), then \( E^d \) has additive reduction at \( q \).

Proof. See, for example, [15, Proposition VII.5.1(c)]. \( \square \)

4. Proof of Theorem 1.1

Recall \( K = \mathbb{Q}(\sqrt{D}) \) for a squarefree integer \( D \). First, we fix an integer \( c \) such that
\[
\dim_{\mathbb{F}_2}(\text{Sel}_2(E/\mathbb{Q})) \leq c.
\]
By the argument of subsection 1.1, it is enough to find (infinitely many) \( E^d \) such that (i),(ii), and (iii) in subsection 1.1 are satisfied. Since \( K \neq \mathbb{Q}(\sqrt{\Delta}) \), we have that
\[
\mathbb{Q}(E[2]) \cap K = \mathbb{Q}.
\]
Then the Chebotarev density theorem implies that for any \( s > 0 \), we can choose \( q_1, q_2, \ldots, q_s \in \mathcal{P}_{E,2} \) so that \( q_i \)'s are inert in \( K/\mathbb{Q} \). In virtue of Proposition 3.13 and Lemma 3.14, we may assume \( E \) (by replacing it with some quadratic twist) satisfies
\[
\begin{align*}
&\bullet |A_E| \gg 0, \\
&\bullet \dim_{\mathbb{F}_2}(\text{Sel}_2(E/\mathbb{Q})) \leq c.
\end{align*}
\]

Let \( S \) be a set of primes of \( \mathbb{Q} \) containing 2, primes where \( E \) has bad reduction, and divisors of \( D \). By [5, Theorem] (for \( E^P \)) and a Kolyvagin’s theorem [8], there are infinitely many squarefree odd integers \( d \) satisfying
\[
\begin{align*}
&\bullet \text{\( d \)} \text{ has at most } 4 \text{ prime factors}, \\
&\bullet \text{rk}(E^{Dd}(\mathbb{Q})) = 0, \text{ and} \\
&\bullet \text{For all } q \in S, \ d \in (\mathbb{Q}_q^\times)^2.
\end{align*}
\]
Then
\[
\text{rk}(E^{d}(K)) = \text{rk}(E^{d}(\mathbb{Q})) + \text{rk}(E^{dD}(\mathbb{Q})) = \text{rk}(E^{d}(\mathbb{Q}))
\]
which is (i) in subsection 1.1. Note that the last condition on the choice of \( d \) implies that \( E \) and \( E^d \) have the same local conditions except at the (prime) divisors of \( d \) and the archimedean place (by Remark 3.10 and [18, Lemma 2.6]). Then Corollary 3.10 proves that
\[
\dim_{\mathbb{F}_2}(\text{Sel}_2(E^d/\mathbb{Q})) \leq c + 10,
\]
so (ii) in subsection 1.1 holds. Also, by the choice of \( d \), it is clear that \( A_E \subseteq A_{E^d} \).

Finally, (iii) in subsection 1.1 follows from Proposition 2.3.

Remark 4.1. In the proof of Theorem 1.1, we constructed \( E^d \) with a large number of primes where \( E^d \) has additive reduction. In particular, \( d \) has many prime divisors. It would be interesting to know whether it is possible to find \( E^d \) with a large (2-torsion part of) Shafarevich-Tate group over \( K \) with a small number of prime divisors of \( d \).

References
[1] R. Bölling. Die Ordnung der Shafarewitsch-Tate-Gruppe kann beliebig groß werden. Math. Nachr., 67:157–179, 1975.
[2] J. W. S. Cassels. Arithmetic on curves of genus 1. VI. The Tate-šafarevič group can be arbitrarily large. J. Reine Angew. Math., 214/215:65–70, 1964.
[3] P. L. Clark and S. Sharif. Period, index and potential. III. Algebra Number Theory, 4(2):151–174, 2010.
LARGE SHAFAREVICH-TATE GROUPS

[4] T. Fisher. Some examples of 5 and 7 descent for elliptic curves over $\mathbb{Q}$. *J. Eur. Math. Soc. (JEMS)*, 3(2):169–201, 2001.

[5] J. Hoffstein and W. Luo. Nonvanishing of $L$-series and the combinatorial sieve. *Math. Res. Lett.*, 4(2-3):435–444, 1997. With an appendix by David E. Rohrlich.

[6] Z. Klagsbrun, B. Mazur, and K. Rubin. Disparity in Selmer ranks of quadratic twists of elliptic curves. *Ann. of Math. (2)*, 178(1):287–320, 2013.

[7] R. Kloosterman. The $p$-part of the Tate-Shafarevich groups of elliptic curves can be arbitrarily large. *J. Théor. Nombres Bordeaux*, 17(3):787–800, 2005.

[8] V. A. Kolyvagin. Finiteness of $E(\mathbb{Q})$ and $\mu(E, \mathbb{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(3):522–540, 670–671, 1988.

[9] K. Kramer. A family of semistable elliptic curves with large Tate-Shafarevich groups. *Proc. Amer. Math. Soc.*, 89(3):379–386, 1983.

[10] K. Matsuno. Construction of elliptic curves with large Iwasawa $\lambda$-invariants and large Tate-Shafarevich groups. *Manuscripta Math.*, 122(3):289–304, 2007.

[11] K. Matsuno. Elliptic curves with large Tate-Shafarevich groups over a number field. *Math. Res. Lett.*, 16(3):449–461, 2009.

[12] B. Mazur and K. Rubin. Kolyvagin systems. *Mem. Amer. Math. Soc.*, 168(799):viii+96, 2004.

[13] B. Mazur and K. Rubin. Ranks of twists of elliptic curves and Hilbert’s tenth problem. *Invent. Math.*, 181(3):541–575, 2010.

[14] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[15] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[16] M. Yu. 2-Selmer near-companion curves. 2016. https://arxiv.org/abs/1610.01195.

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

[18] M. Yu. On 2-Selmer ranks of quadratic twists of elliptic curves. *Math. Res. Lett.*, 24(5):1565–1583, 2017.

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109-1043, USA
E-mail address: myungjuy@umich.edu