ELLiptic Curves with large Tate-Shafarevich Groups over a number field

KAZuo Matsuno

Abstract. Let $p$ be a prime number and let $K$ be a cyclic Galois extension of $\mathbb{Q}$ of degree $p$. We prove that the $p$-rank of the Tate-Shafarevich group over $K$ of elliptic curves defined over $\mathbb{Q}$ can be arbitrarily large.

1. Introduction

For an elliptic curve $E$ defined over a number field $K$, the Tate-Shafarevich group $\Sha(E/K)$ of $E$ over $K$ is defined to be the abelian group consisting of the isomorphism classes of principal homogeneous spaces for $E$ over $K$ which are everywhere locally trivial. We have the following description of $\Sha(E/K)$:

$$\Sha(E/K) = \ker(H^1(K, E(K)) \rightarrow \prod_v H^1(K_v, E(K_v))).$$

Here $v$ runs over all primes of $K$. In this paper, we discuss the size of the Tate-Shafarevich groups of elliptic curves over number fields. It is classically conjectured (but still unknown in general) that the Tate-Shafarevich group is finite for any elliptic curve over any number field of finite degree. Cassels, however, proved that there exists an elliptic curve defined over $\mathbb{Q}$ whose Tate-Shafarevich group has an arbitrarily large order. More precisely, Cassels [5] showed that the dimension over $\mathbb{F}_3$ of $\Sha(E/\mathbb{Q})[3]$, the 3-torsion subgroup of $\Sha(E/\mathbb{Q})$, is unbounded as $E$ varies over elliptic curves of $j$-invariant zero. After Cassels, the unboundedness of $\dim_{\mathbb{F}_p} \Sha(E/\mathbb{Q})[p]$ was studied by many authors and was proved for primes $p \leq 7$ or $p = 13$. See the papers [1], [2], [11], [16], [18], [20], and some other papers cited in those.

It is not easy to prove the unboundedness of $\dim_{\mathbb{F}_p} \Sha(E/\mathbb{Q})[p]$ for an arbitrary $p$ by extending the method given in the above papers because many of them used the fact that there exist infinitely many elliptic curves over $\mathbb{Q}$ (with different $j$-invariants) which have isogenies of degree $p$. It is known that there exist only finitely many such elliptic curves for $p = 11$ or $p \geq 17$. If we allow $K$ to vary over number fields of bounded degree and $E$ varies over elliptic curves over $K$, then the unboundedness of $\dim_{\mathbb{F}_p} \Sha(E/K)[p]$ has been proved for any $p$ by a similar method (cf. Kloosterman [15]). However, we cannot apply the same argument to showing the unboundedness for elliptic curves over a fixed number field $K$ when $p \geq 23$ since the modular curve $X_0(p)$ has genus greater than 1 and hence there exist only finitely many $K$-rational points on $X_0(p)$.

Received by the editors May 12, 2008.

2000 Mathematics Subject Classification. Primary 11G05.
The aim of this paper is to prove that $\dim_{\mathbb{F}_p} \text{III}(E/K)[p]$ is unbounded if $K$ is a fixed abelian field of degree $p$ and $E$ runs over elliptic curves over $\mathbb{Q}$. The main result is stated as follows.

**Theorem A.** Let $K$ be a Galois extension of $\mathbb{Q}$ such that $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}$ for a prime number $p$. Then, for any integer $k$, there exists an elliptic curve $E$ defined over $\mathbb{Q}$ satisfying $\dim_{\mathbb{F}_p} \text{III}(E/K)[p] \geq k$.

More precisely, we will prove the unboundedness of the $n$-ranks of Tate-Shafarevich groups of elliptic curves over a fixed cyclic extension of $\mathbb{Q}$ of degree $n$, where $n$ is a positive integer not divisible by 4. The main ingredient of the proof is the Cassels-Poitou-Tate global duality.

**Proposition B.** Let $E$ be an elliptic curve defined over $\mathbb{Q}$. Then, for any integer $k$, there exists a quadratic field $K$ satisfying $\dim_{\mathbb{F}_2} \text{III}(E/K)[2] \geq k$. 
2. Notation

For an abelian group $M$ and a positive integer $n$, we denote by $M[n]$ the subgroup of $M$ annihilated by $n$. If $M$ is a torsion abelian group, then we denote by $M^{(p)}$ the $p$-primary component of $M$ for each prime $p$, i.e., $M^{(p)} := \cup_{m}M[p^m]$. For a finite abelian group $M$, we denote by $rk_{\infty} M$ the largest integer $k$ such that $M$ contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{\oplus k}$. By definition, we have $rk_{\infty} M = rk_{\infty}(M[n])$ in any case, and $rk_{p} M = \dim_{\mathbb{F}_p} M$ if $pM = 0$ for a prime $p$.

For an elliptic curve $E$ defined over a number field $K$, we put $E[n] := E(\overline{K})[n]$. Then the $n$-Selmer group $Sel_n(E/K)$ of $E$ over $K$ is defined as follows:

$$ Sel_n(E/K) := \text{Ker}(H^1(K,E[n]) \to \prod_{v} H^1(K_v,E(\overline{K_v}))), $$

where $v$ runs over all primes of $K$. By definition, we have an exact sequence

$$ 0 \to E(K)/nE(K) \to Sel_n(E/K) \to \text{III}(E/K)[n] \to 0. $$

For a prime number $p$, we denote by $Sel_{p^{\infty}}(E/K)$ the inductive limit of $Sel_{p^{m}}(E/K)$ under the maps induced by the natural inclusions $E[p^m] \to E[p^{m+1}]$. We have

$$ Sel_{p^{\infty}}(E/K) = \text{Ker}(H^1(K,E[p^{\infty}]) \to \prod_{v} H^1(K_v,E(\overline{K_v}))), $$

where $E[p^{\infty}] = \cup_{m}E[p^m]$ is the group of all $p$-power torsion points of $E$.

3. Consequences of global duality

In this section, we recall some facts obtained from the global duality. We assume that $E$ is an elliptic curve defined over $\mathbb{Q}$.

**Proposition 3.1.** Let $p$ be a prime number and $S$ a finite set of primes of $\mathbb{Q}$ containing $p$, the unique archimedean prime, and all bad reduction primes for $E$. Then $Sel_{p^{\infty}}(E/Q)$ coincides with the kernel of the map

$$ \varphi : H^1(Q_S/Q,E[p^{\infty}]) \to \prod_{v \in S} H^1(Q_v,E(\overline{Q_v}))(p), $$

where $Q_S$ denotes the maximal extension of $\mathbb{Q}$ unramified outside $S$. Furthermore, we have

$$ \text{rk}_p \text{Coker}(\varphi)[p] \leq \text{rank}_{Z_p} Sel_{p^{\infty}}(E/Q)^{\vee} + \text{rk}_p E(\mathbb{Q})[p], $$

where $Sel_{p^{\infty}}(E/Q)^{\vee}$ is the Pontryagin dual of $Sel_{p^{\infty}}(E/Q)$.

**Remark.** We have $\text{rank}_{Z_p} Sel_{p^{\infty}}(E/Q)^{\vee} = \text{rank}_{Z} E(\mathbb{Q})$ if $\text{III}(E/Q)^{(p)}$ is finite.

**Proof.** The first assertion is well-known (cf. [22, Corollary I.6.6]). The second assertion follows immediately from [8, (4) and Lemma 1.8]. \hfill $\square$

Let $K$ be a cyclic Galois extension of $\mathbb{Q}$ of finite degree. For a (non-archimedean or archimedean) prime $v$ of $\mathbb{Q}$, we define $W_{v,K}$ by

$$ W_{v,K} := \text{Ker}(H^1(Q_v,E(\overline{Q_v})) \to H^1(K_w,E(\overline{Q_v}))), $$

where $w$ is a prime of $K$ lying above $v$. The definition of $W_{v,K}$ is independent of the choice of $w$. It is known that $W_{v,K}$ is finite.
Proposition 3.2. Let $K/Q$ be a cyclic Galois extension with Galois group $G = \text{Gal}(K/Q)$. Suppose that the set $S$ in the statement of Proposition 3.1 contains the primes ramified in $K/Q$. Then $\text{Sel}_{p^\infty}(E/K)$ contains a subgroup $\mathcal{M}$ which sits in the following exact sequence:

$$(2)\quad 0 \rightarrow X \rightarrow \text{Sel}_{p^\infty}(E/Q) \rightarrow \mathcal{M} \rightarrow \left(\prod_{v \in S} W^{(p)}_{v,K}\right)/X' \rightarrow Y \rightarrow 0.$$ 

Here $X$, $X'$ and $Y$ are finite abelian $p$-groups satisfying

$$\text{rk}_p X, \text{rk}_p X' \leq \text{rk}_p E(Q)[p] + \delta,$$

$$\text{rk}_p Y \leq \text{rank}_{E_p} \text{Sel}_{p^\infty}(E/Q)^\vee + \text{rk}_p E(Q)[p],$$

where $\delta = 1$ if $p = 2$ and $\text{rk}_2 E(Q)[2] = 1$, and $\delta = 0$ if not.

Remark. The above $\mathcal{M}$ is of finite index in $\text{Sel}_{p^\infty}(E/K)^G$, the subgroup of $\text{Sel}_{p^\infty}(E/K)$ consisting of $G$-invariant elements. Moreover, we have $\mathcal{M} = \text{Sel}_{p^\infty}(E/K)^G$ if $E(Q)[p] = 0$.

Proof. Let $\mathcal{M}'$ be the image of the restriction map

$$H^1(Q_S/Q, E[p^\infty]) \rightarrow H^1(Q_S/K, E[p^\infty]).$$

Then we have the commutative diagram

$$
\begin{array}{cccccc}
0 & \rightarrow & H^1(G, E(K)[p^\infty]) & \rightarrow & H^1(Q_S/Q, E[p^\infty]) & \rightarrow & \mathcal{M}' & \rightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \rightarrow & \prod_{v \in S} W^{(p)}_{v,K} & \rightarrow & \prod_{v \in S} H^1(Q_v, E^{(p)}(Q_v)) & \rightarrow & \prod_{v \in S} H^1(K_v, E^{(p)}(Q_v)) & \rightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
& & \varphi & & \sigma & & \varphi_K & & \rho \\
\end{array}
$$

with exact rows. Put $\mathcal{M} = \text{Ker}(\varphi_K)$, $X = \text{Ker}(\psi)$ and $X' = \text{Im}(\psi)$, where $\varphi_K$ and $\psi$ are the vertical maps in the above diagram. By definition, $\mathcal{M}$ is contained in $\text{Sel}_{p^\infty}(E/K)$, and we have an exact sequence

$$0 \rightarrow X \rightarrow \text{Sel}_{p^\infty}(E/Q) \rightarrow \mathcal{M} \rightarrow \left(\prod_{v \in S} W^{(p)}_{v,K}\right)/X' \rightarrow \text{Coker}(\varphi)$$

by the snake lemma. By putting $Y$ as the image of the last map of this sequence, we obtain the exact sequence (2). The assertion on $\text{rk}_p Y$ follows immediately from Proposition 3.1. Since we have $\text{rk}_p X$, $\text{rk}_p X' \leq \text{rk}_p H^1(G, E(K)[p^\infty])$ by definition, the proof of this proposition is reduced to showing

$$(3)\quad \text{rk}_p H^1(G, E(K)[p^\infty]) \leq \text{rk}_p E(Q)[p] + \delta.$$ 

Let $K'$ be the maximal $p$-extension of $Q$ contained in $K$ and fix a generator $\sigma$ of $G' = \text{Gal}(K'/Q)$. Since $G'$ is cyclic, we have

$$H^1(G, E(K)[p^\infty]) \cong H^1(G', E(K')[p^\infty]) \cong \text{Ker}(N_{K'/Q}[(\sigma - 1)(E(K')[p^\infty])]),$$

where $N_{K'/Q} : E(K')[p^\infty] \rightarrow E(Q)[p^\infty]$ is the norm map. In particular, we have

$$\text{rk}_p H^1(G, E(K)[p^\infty]) \leq \text{rk}_p E(K')[p^\infty] = \text{rk}_p E(K')[p].$$

Since $G'$ is a $p$-group, $\text{rk}_p E(K')[p] = 0$ if and only if $\text{rk}_p E(Q)[p] = 0$. This implies $\text{rk}_2 E(K')[2] \leq \text{rk}_2 E(Q)[2] + \delta$ for $p = 2$. If $p$ is odd, then $K'$ contains no primitive $p$-th root of unity. Hence we have $\text{rk}_p E(K')[p] \leq 1$ for any odd $p$, which implies $\text{rk}_p E(Q)[p] = \text{rk}_p E(K')[p]$. Thus we obtain the inequality (3) for any $p$. The proof has been completed. □
Remark. We cannot remove the term $\delta$ in (3). In fact, if we take $E$ as the elliptic curve defined by $y^2 = (x - 1)(x^2 + x - 1)$, the curve 40A3 in [9], and take $K$ as the cyclotomic field of conductor 5, then we have $E(\mathbb{Q})[2^\infty] \cong \mathbb{Z}/4\mathbb{Z}$ and $E(K)[2^\infty] = E(\mathbb{Q}(\sqrt{5}))[2^\infty] \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. One sees that the norm map $N_{K/\mathbb{Q}}$ is the zero map and $(\sigma - 1)(E(K)[2^\infty]) = 2E(\mathbb{Q})[2^\infty]$, where $\sigma$ is a generator of $G = \text{Gal}(K/\mathbb{Q})$. Therefore, $H^1(G, E(K)[2^\infty]) \cong \text{Ker}(N_{K/\mathbb{Q}})/(\sigma - 1)(E(K)[2^\infty]) \cong (\mathbb{Z}/2\mathbb{Z})^\oplus 2$, which implies $\text{rk}_2 H^1(G, E(K)[2^\infty]) = 2 = \text{rk}_2 E(\mathbb{Q})[2] + 1$.

**Corollary 3.3.** For any prime number $p$ and any positive integer $e$, we have

$$\text{rk}_{p^e} \text{Sel}_{p^e}(E/K) \geq \sum_{v \in S} \text{rk}_{p^e} W_{v,K} - 2\text{rk}_{p} E(\mathbb{Q})[p] - \delta,$$

where $\delta$ and $S$ are as in Proposition 3.2.

**Proof.** Let $\mathcal{M}$, $X'$ and $Y$ be as in Proposition 3.2. Put $r = \text{rank}_{\mathbb{Z}_p} E(\mathbb{Q})^\vee$ and $t = \text{rk}_p E(\mathbb{Q})[p]$. By the exact sequence (2) in Proposition 3.2, the maximal divisible subgroup $D$ of $\mathcal{M}$ is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^{\oplus r}$ and we have an exact sequence of finite abelian $p$-groups:

$$\mathcal{M}/D \longrightarrow \left( \prod_{v \in S} W_{v,K}^{(p)} \right)/X' \longrightarrow Y \longrightarrow 0.$$

Although the $p^e$-rank is not “additive” for short exact sequences in general, the above sequence implies the inequality

$$\text{rk}_{p^e} \mathcal{M}/D \geq \sum_{v \in S} \text{rk}_{p^e} W_{v,K}^{(p)} - \text{rk}_p X' - \text{rk}_p Y.$$

Therefore, as an abelian group, $\mathcal{M}$ is isomorphic to the direct sum of $(\mathbb{Q}_p/\mathbb{Z}_p)^{\oplus r}$ and a finite abelian $p$-group whose $p^e$-rank is not less than $\sum_{v \in S} \text{rk}_{p^e} W_{v,K}^{(p)} - r - 2t - \delta$.

Since $\mathcal{M}$ is a subgroup of $\text{Sel}_{p^e}(E/K)$ and there exists a surjection $\text{Sel}_{p^e}(E/K) \twoheadrightarrow \text{Sel}_{p^e}(E/K)[p^e]$, we have

$$\text{rk}_{p^e} \text{Sel}_{p^e}(E/K) \geq \text{rk}_{p^e} \mathcal{M}[p^e] \geq r + \sum_{v \in S} \text{rk}_{p^e} W_{v,K}^{(p)} - r - 2t - \delta$$

$$= \sum_{v \in S} \text{rk}_{p^e} W_{v,K} - 2t - \delta.$$

The proof has been completed. \qed

Remark. In the case $e = 1$, one can improve the assertion of the above corollary as

$$\text{rk}_p \text{Sel}_p(E/K) \geq \sum_{v \in S} \text{rk}_p W_{v,K} - \text{rk}_p E(\mathbb{Q})[p]$$

by using the fact that the kernel of $\text{Sel}_p(E/K) \twoheadrightarrow \text{Sel}_{p^e}(E/K)[p]$ is isomorphic (as an abelian group) to $E(K)[p]$. 


4. Large Selmer groups

In this section, we give some sufficient conditions for $W_{\ell,K}$ to be nontrivial. By Corollary 3.3, this enables us to construct elliptic curves defined over $\mathbb{Q}$ which have large Selmer groups over $K$. We keep the assumptions that the elliptic curve $E$ is defined over $\mathbb{Q}$ and $K$ is a cyclic Galois extension of $\mathbb{Q}$.

**Lemma 4.1.** Let $\ell$ be a prime number satisfying the following conditions for a positive integer $n$ prime to $\ell$.

(i) $E$ has split multiplicative reduction at $\ell$.

(ii) The inertia degree of $\ell$ in $K/\mathbb{Q}$ is divisible by $n$.

(iii) The Tamagawa factor $c_\ell$ of $E$ at $\ell$ is divisible by $n$.

Then $W_{\ell,K}$ contains a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z}$, i.e., $\text{rk}_n W_{\ell,K} \geq 1$.

**Proof.** Fix a prime $l$ of $K$ lying above $\ell$. Let $L$ be the maximal unramified extension of $\mathbb{Q}_l$ in $K_1$ and put $G' = \text{Gal}(L/\mathbb{Q}_l)$. Then we have an injection $H^1(G', E(L)) \hookrightarrow W_{\ell,K}$ by the inflation-restriction sequence. Hence it suffices to show that $H^1(G', E(L))$ has an element of order $n$. If we denote by $E_0(L)$ the subgroup of $E(L)$ consisting of the points with non-singular reduction, then we have

$$H^1(G', E(L)) \cong H^1(G', E(L)/E_0(L))$$

(cf. [21, Proposition 4.3]). By the assumption (i) and the fact that $L/\mathbb{Q}_l$ is unramified, $E(L)/E_0(L)$ is a cyclic group of order $c_\ell$ and $G'$ acts trivially on it. Hence we have

$$H^1(G', E(L)) \cong \text{Hom}(G', E(L)/E_0(L)) \cong \mathbb{Z}/g\mathbb{Z},$$

where $g$ is the greatest common divisor of $c_\ell$ and the order of $G'$. By (ii) and (iii), $g$ is divisible by $n$. Thus the claim has been proved.

**Lemma 4.2.** Let $\ell$ be a prime number satisfying the following conditions for a positive integer $n$ prime to $\ell$.

(i) $E$ has good reduction at $\ell$.

(ii) The ramification index of $\ell$ in $K/\mathbb{Q}$ is divisible by $n$.

(iii) $E(\mathbb{Q}_l)$ contains an element of order $n$.

Then $W_{\ell,K}$ contains a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

**Proof.** Since we have an isomorphism $E(\mathbb{Q}_l)/nE(\mathbb{Q}_l) \overset{\sim}{\longrightarrow} H^1(\mathbb{Q}_l, E(\mathbb{Q}_l))[n]$ by the Tate local duality (cf. [22, Corollary I.3.4]), there exists an element $\alpha \in H^1(\mathbb{Q}_l, E(\mathbb{Q}_l))$ of order $n$ by the assumption (iii). By [19, Corollary 1], $\alpha$ becomes trivial over $K_1$ under the assumptions (i) and (ii), i.e., $\alpha \in W_{\ell,K}$. Thus, $W_{\ell,K}$ contains an element of order $n$, as desired.

By these lemmas, we obtain a lower bound of Selmer groups.

**Definition.** For a cyclic Galois extension $K$ over $\mathbb{Q}$ of degree $n$, let $T_{E,K}$ be the set of prime numbers $\ell \nmid n$ satisfying the assumptions either of Lemmas 4.1 or 4.2. Denote by $t_{E,K}$ the cardinality of $T_{E,K}$.

**Proposition 4.3.** Let $K$ be a cyclic Galois extension of $\mathbb{Q}$ of degree $n$. Then we have

$$\text{rk}_n \text{Sel}_n(E/K) \geq t_{E,K} - 2\max\{\text{rk}_p E(\mathbb{Q})/p \mid p|n\} - \delta' \geq t_{E,K} - 4,$$

where $\delta' = 1$ if $n$ is even and $\text{rk}_2 E(\mathbb{Q})/2 = 1$, and $\delta' = 0$ if not.
Proof. By Lemmas 4.1 and 4.2, we have \( \text{rk}_n(W_{\ell,K}) \geq 1 \) for any \( \ell \in T_{E,K} \). Hence the assertion follows immediately from Corollary 3.3.

By using this lower bound, we have the following results on the unboundedness of \( p \)-Selmer groups.

**Corollary 4.4.** Let \( p \) be a prime number. Then, for any cyclic Galois extension \( K/\mathbb{Q} \) of degree \( p \), we have

\[
\sup \{ \dim_{\mathbb{Q}_p} \text{Sel}_p(E/K) \mid E \text{ is defined over } \mathbb{Q} \} = +\infty.
\]

**Proof.** For any positive integer \( k \), take prime numbers \( \ell_1, \ldots, \ell_k \) not equal to \( p \) which remain primes in \( K \). Then there exists an elliptic curve \( E' \) defined over \( \mathbb{Q} \) whose \( j \)-invariant is equal to \((\ell_1 \cdots \ell_k)^{-p}\). We can take a quadratic twist \( E \) of \( E' \) such that \( E \) has split multiplicative reduction at each \( \ell_i \). Since \( \text{ord}_{\ell_i}(j_E) = \text{ord}_{\ell_i}(j_{E'}) = -p \), the Tamagawa factor of \( E \) at \( \ell_i \) is equal to \( p \). Therefore, the primes \( \ell_1, \ldots, \ell_k \) satisfy the conditions of Lemma 4.1, i.e., \( \ell_1, \ldots, \ell_k \in T_{E,K} \). By Proposition 4.3, we have \( \dim_{\mathbb{Q}_p} \text{Sel}_p(E/K) \geq k - 4 \), which implies the assertion of this corollary. \( \square \)

**Corollary 4.5.** Let \( p \) be a prime number. For any elliptic curve \( E \) defined over \( \mathbb{Q} \), we have

\[
\sup \{ \dim_{\mathbb{Q}_p} \text{Sel}_p(E/K) \mid K/\mathbb{Q} \text{ is a cyclic extension of degree } p \} = +\infty.
\]

**Proof.** There exist infinitely many odd prime numbers which split completely in the extension \( \mathbb{Q}(E[p])/\mathbb{Q} \). For any positive integer \( k \), take such primes \( \ell_1, \ldots, \ell_k \) at which \( E \) has good reduction. Then \( E[p] \) is contained in \( E(\mathbb{Q}_{\ell_i}) \) for each \( i \). By a property of the Weil pairing, \( \mathbb{Q}_{\ell_i}^{\times} \) contains a primitive \( p \)-th root of unity, i.e., \( \ell_i \equiv 1 \mod p \). Hence there exists an abelian field \( K \) of degree \( p \) and of conductor \( \ell_1 \cdots \ell_k \). Then the primes \( \ell_1, \ldots, \ell_k \) satisfy the conditions of Lemma 4.2, i.e., \( \ell_1, \ldots, \ell_k \in T_{E,K} \). Thus, we have \( \dim_{\mathbb{Q}_p} \text{Sel}_p(E/K) \geq k - 4 \) by Proposition 4.3. This implies the assertion. \( \square \)

We conclude this section by giving a proof of Proposition B in the introduction. Let \( E \) be an elliptic curve defined over \( \mathbb{Q} \) with conductor \( N \). As in the proof of Corollary 4.5, take odd prime numbers \( \ell_1, \ldots, \ell_k \nmid N \) which split completely in the Galois extension \( \mathbb{Q}(E[2])/\mathbb{Q} \). By results of Waldspurger (cf. [4, Theorem in Section 0]) and Kolyvagin ([17]), there exists a quadratic field \( K \) such that all \( \ell_1, \ldots, \ell_k \) ramify in \( K/\mathbb{Q} \) and \( \text{rank}_{E'}(\mathbb{Q}) = 0 \), where \( E' \) is the quadratic twist of \( E \) corresponding to \( K \). Then we have \( \text{rank}_{E}(K) = \text{rank}_{E}(\mathbb{Q}) + \text{rank}_{E'}(\mathbb{Q}) = \text{rank}_{E}(\mathbb{Q}) \). By Corollary 3.3 and Lemma 4.2, we have \( \dim_{\mathbb{Q}_p} \text{Sel}_2(E/K) \geq k - 4 \) and

\[
\dim_{\mathbb{Q}_p} \text{III}(E/K)[2] \geq \dim_{\mathbb{Q}_p} \text{Sel}_2(E/K) - \text{rank}_{E}(K) - 2 \geq k - 6 - \text{rank}_{E}(\mathbb{Q}).
\]

Since \( \text{rank}_{E}(\mathbb{Q}) \) is independent of \( k \), this completes the proof of Proposition B by taking \( k \) arbitrarily large.

## 5. Large Tate-Shafarevich groups

In this section, we prove the following result, which implies the statement of Theorem A in the introduction for odd primes \( p \).
Lemma 1. Let $A$ be the Frobenius element at $m$ and the image of $A$ at $m$. We can indeed find such primes by using the Chebotarev density theorem. (After Theorem 3.) Moreover, if we define the subgroup $P$ such that the image of a point $A$ is the reduction at $\ell$, we can take odd positive integers $s$. Let $F(x) := (2ax - d_0)(2bx + c_0) \in \mathbb{Z}[x]$. By assumption, we have $8ab(ac_0 + bd_0) \neq 0$. Moreover, for any prime $p$, there is an integer $e$ such that $F(e) \neq 0 (\mod p)$. Then there exist infinitely many positive integers $e'$ such that $F(e')$ has at most 5 prime factors (cf. [13, Chapter 10]).

Proof. We may assume $a$ is negative. Take odd integers $c_0$ and $d_0$ satisfying $ac_0 + bd_0 = 1$ and consider the polynomial $F(x) := (2ax - d_0)(2bx + c_0) \in \mathbb{Z}[x]$. By assumption, we have $8ab(ac_0 + bd_0) \neq 0$. Moreover, for any prime $p$, there is an integer $e$ such that $F(e) \neq 0 (\mod p)$. Then there exist infinitely many positive integers $e'$ such that $F(e')$ has at most 5 prime factors (cf. [13, Chapter 10]).

Take such an $e'$ so that both $c = c_0 + 2be'$ and $d = d_0 - 2ae'$ are positive. These $c$ and $d$ satisfy the assertion of this lemma.

We can indeed find such primes by using the Chebotarev density theorem. (After taking $m_1, \ldots, m_k$ satisfying (A2) and (A3), take $\ell_1 \not| n$ such that the fixed field of the Frobenius element at $\ell_1$ in $\text{Gal}(\mathbb{Q}(\sqrt{-1}, \sqrt{m_1}, \ldots, \sqrt{m_k})/\mathbb{Q})$ is $\mathbb{Q}(\sqrt{-1}, \sqrt{m_2}, \ldots, \sqrt{m_k})$, and so on.) By Lemma 5.2 below, which is proved by using a result in [13], we can take odd positive integers $s$ and $t$ such that

$$st\ell_1 \cdots \ell_k - 16tm_1^n \cdots m_k^n = 1$$

and $st$ has at most 5 prime factors.

Lemma 5.2. Let $a$ and $b$ be nonzero coprime integers. If $ab$ is even and negative, then there exist odd positive integers $c$ and $d$ such that $ac + bd = 1$ and $cd$ has at most 5 prime factors.

Proof. We may assume $a$ is negative. Take odd integers $c_0$ and $d_0$ satisfying $ac_0 + bd_0 = 1$ and consider the polynomial $F(x) := (2ax - d_0)(2bx + c_0) \in \mathbb{Z}[x]$. By assumption, we have $8ab(ac_0 + bd_0) \neq 0$. Moreover, for any prime $p$, there is an integer $e$ such that $F(e) \neq 0 (\mod p)$. Then there exist infinitely many positive integers $e'$ such that $F(e')$ has at most 5 prime factors (cf. [13, Chapter 10]).

Take such an $e'$ so that both $c = c_0 + 2be'$ and $d = d_0 - 2ae'$ are positive. These $c$ and $d$ satisfy the assertion of this lemma.

Put $l = s\ell_1 \cdots \ell_k$ and $m = tm_1^n \cdots m_k^n$. Let $A$ be the elliptic curve defined by the Weierstrass equation

$$y^2 + xy = x^3 + 8mx^2 + lmx.$$  

The discriminant $\Delta_A$ of this curve is $\Delta_A = l^2m^2 = m^2(16m + 1)^2$. As shown in [18, Lemma 1], $A$ is semistable and $A[2] \subset A(\mathbb{Q})$. In fact, the points $P_1 = (0, 0), P_2 = (-4m, 2m)$ and $P_3 = (-\frac{1}{2}, \frac{1}{2})$ have order 2. Furthermore, $A$ has split multiplicative reduction at $\ell_1, \ldots, \ell_k, m_1, \ldots, m_k$ (cf. [18, p. 383]). We have an isomorphism

$$\lambda_K : H^1(K, A[2]) \xrightarrow{\sim} K = \{(x, y, z) \in (K^x/K^x)^{\oplus 3} \mid xyz = 1\}$$

such that the image of a point $P \in A(K) \setminus A(K)[2]$ under the composite map

$$A(K) \rightarrow A(K)/2A(K) \rightarrow H^1(K, A[2]) \xrightarrow{\lambda_K} K$$

is $(x(P), x(P) + 4m, x(P) + \frac{1}{2})$, where $x(P)$ is the $x$-coordinate of $P$ (cf. [18, Section 3]). Moreover, if we define the subgroup $K_v$ of $(K_v^x/K_v^x)^{\oplus 3}$ for a prime $v$ of $K$, similarly, then there is an isomorphism $\lambda_K : H^1(K_v, A[2]) \xrightarrow{\sim} K_v$ compatible with $\lambda_K$, and the image of $A(K_v)/2A(K_v)$ in $K_v$ has been described explicitly (cf. [3] and [18,
Corollary 5.5. Let \( h \) denote the 2-rank of the \( \Sigma \)-ideal class group \( \text{Cl}_\Sigma(K) \) of \( K \). Then we have \( \dim_{\mathbb{F}_2} \mathcal{K}_\Sigma / \mathcal{L} \leq 14n + 2h \).

Proof. We have an exact sequence

\[
1 \longrightarrow (\mathcal{O}_\Sigma^\times / \mathcal{O}_\Sigma^{\times 2})^{\oplus 2} \longrightarrow \mathcal{K}_\Sigma \longrightarrow (\text{Cl}_\Sigma(K)[2])^{\oplus 2} \longrightarrow 1,
\]

where \( \mathcal{O}_\Sigma^\times \) is the group of \( \Sigma \)-units of \( K \). Since \( K \) is a totally real field of degree \( n \), there exist exactly \( n \) archimedean primes. Since \( 2st \) has at most 6 prime factors, the number of non-archimedean primes in \( \Sigma \) is at most \( 6n + 2k \) by (A3). Hence we have \( \dim_{\mathbb{F}_2} (\mathcal{O}_\Sigma^\times / \mathcal{O}_\Sigma^{\times 2}) \leq 7n + 2k \). This implies

\[
\dim_{\mathbb{F}_2} \mathcal{K}_\Sigma - \dim_{\mathbb{F}_2} \mathcal{L} \leq 2(7n + 2k) + 2h - 4k = 14n + 2h
\]
as desired. \( \square \)

The following proposition is proved by an argument given in [18, Section 2].

Proposition 5.4. \( \mathcal{L} \cap \lambda_K(\text{Sel}_2(A/K)) = \{1\} \).

Proof. Take an element \( (x, y, z) \in \mathcal{L} \cap \lambda_K(\text{Sel}_2(A/K)) \) and suppose \( y \) is represented by \( q := \ell_1^{e_1} \cdots \ell_k^{e_k} m_1^{f_1} \cdots m_k^{f_k} \) \((e_i, f_j \in \{0, 1\})\). It is known that \( y \) is contained in the kernel of the natural map \( K^\times / K^{\times 2} \longrightarrow K_{\ell_i}^\times / K_{\ell_i}^{\times 2} \) for any \( i \) (cf. [3, Section 4], [18, Section 2]). This implies that \( \text{ord}_{\ell_i}(y) = 0 \), i.e., \( e_i = 0 \). Moreover, we have \( f_j = 0 \) since \( m_j \notin K_{\ell_i}^{\times 2} \) and \( m_j \in K_{\ell_i}^\times \) for any \( j \neq i \) by (A4). (Recall that \( n = [K : \mathbb{Q}] \) is odd.) Thus, \( y \) is trivial in \( K^\times / K^{\times 2} \). Similar argument shows that \( z \) is trivial since the image of \( z \) in \( K_{m_j}^\times / K_{m_j}^{\times 2} \) should be trivial for any \( j \) and \( \left( \frac{z}{m_j} \right) = (-1)^{\delta_{i,j}} \) by (A1) and (A4). This proves the assertion. \( \square \)

By this proposition, \( \text{Sel}_2(A/K) \) can be regarded as a subgroup of \( \mathcal{K}_\Sigma / \mathcal{L} \). We obtain the following upper bound of the Mordell-Weil rank of \( A \) over \( K \).

Corollary 5.5. \( \text{rank}_2 A(K) \leq 14n + 2h - 2 \).

Proof. By Lemma 5.3 and Proposition 5.4, we have \( \dim_{\mathbb{F}_2} \text{Sel}_2(A/K) \leq 14n + 2h \). The assertion follows from the exact sequence (1) and the fact \( \dim_{\mathbb{F}_2} A(K)[2] = 2 \). \( \square \)

Combining this with Proposition 4.3, we have the following lower bound of the \( n \)-rank of the Tate-Shafarevich group of \( A \) over \( K \).
Corollary 5.6. We have $\text{rk}_n \, \text{III}(A/K)[n] \geq k - 14n - 2h - 8$.

Proof. If $m_j$ does not divide $st$, then the Tamagawa factor of $A$ at $m_j$ is equal to $2n$, i.e., $m_j \in T_{A,K}$. Since $A(Q)[n] = 0$ by [18, Lemma 3], we have $\text{rk}_n(\text{Sel}_n(A/K)) \geq t_{A,K} \geq k - 5$ by Proposition 4.3. Since $A(K)/nA(K)$ is isomorphic to a direct sum of $(\mathbb{Z}/n\mathbb{Z})^{2\text{rank}_2(A(K))}$ and a cyclic group of order dividing $n$, the assertion follows from Corollary 5.5 and the exact sequence (1).

Although Corollary 5.6 is sufficient for proving Theorem A for odd primes $p$, in order to complete the proof of Theorem 5.1, we show that the 2-rank of the Tate-Shafarevich group over $K$ also becomes large if we replace the curve $A$ with its 2-isogenous curve $B$ below as in [18].

Let $B$ be the elliptic curve over $\mathbb{Q}$ defined by the equation

$$y^2 + xy = x^3 - 16mx^2 - 8mx - m.$$  

The discriminant $\Delta_B$ of this curve is $lm$ and there exists an isogeny $f : A \to B$ of degree 2 defined over $\mathbb{Q}$. The following lower bound on the 2-rank of $\text{III}(B/K)[2]$ is enough to prove Theorem 5.1.

Proposition 5.7. We have $\dim_{\mathbb{F}_2} \, \text{III}(B/K)[2] \geq 2k - 17$.

Remark. We give here a proof based on a result of Cassels [6] as in [16]. One can also obtain a similar lower bound by the same argument as given in Kramer’s paper [18].

Proof. Since $n = [K : \mathbb{Q}]$ is odd, the kernel of the restriction map $\text{III}(B/\mathbb{Q}) \to \text{III}(B/K)$ has no element of order 2. Hence we have only to show $\dim_{\mathbb{F}_2} \, \text{III}(B/\mathbb{Q})[2] \geq 2k - 17$. Let $g : B \to A$ be the dual isogeny of $f$. We have the following relation between the Selmer groups $\text{Sel}_f(A/\mathbb{Q})$ and $\text{Sel}_g(B/\mathbb{Q})$ associated with the isogenies $f$ and $g$ (cf. [16, Theorem 1]):

$$\dim_{\mathbb{F}_2} \text{Sel}_g(B/\mathbb{Q}) \geq \dim_{\mathbb{F}_2} \text{Sel}_f(A/\mathbb{Q}) + \sum_q (u_{A,q} - u_{B,q}) - 1.$$

Here $q$ runs over all prime numbers at which $A$ and $B$ have bad reduction and we denote by $u_{A,q}$ and $u_{B,q}$ the normalized 2-adic valuations of the Tamagawa factors of $A$ and $B$ at $q$. Since $A$ and $B$ are semistable and $\Delta_A = \Delta_B^2$, we have $u_{A,q} \geq u_{B,q}$ for any prime $q$ at which $A$ and $B$ have bad reduction. Moreover, we have $u_{A,q} - u_{B,q} = 1$ if $q$ is one of the primes $\ell_1, \ldots, \ell_k, m_1, \ldots, m_k$ since both $A$ and $B$ have split multiplicative reduction at $q$. Hence we have

$$\dim_{\mathbb{F}_2} \text{Sel}_g(B/\mathbb{Q}) \geq \dim_{\mathbb{F}_2} \text{Sel}_f(A/\mathbb{Q}) + 2k - 1 \geq 2k - 1.$$

By the exact sequence

$$B(\mathbb{Q})[2] \longrightarrow A(\mathbb{Q})[f] \longrightarrow \text{Sel}_g(B/\mathbb{Q}) \longrightarrow \text{Sel}_2(B/\mathbb{Q})$$

(cf. [16, Proposition 1]), we have $\dim_{\mathbb{F}_2} \text{Sel}_2(B/\mathbb{Q}) \geq \dim_{\mathbb{F}_2} \text{Sel}_g(B/\mathbb{Q}) - 1 \geq 2k - 2$. By the same argument as in the proof of Proposition 5.4 and Corollary 5.5, we have $\text{rank}_2(B(\mathbb{Q})) = \text{rank}_2(A(\mathbb{Q})) \leq 14$ (see also the proof of Corollary 6.2). Therefore, we have $\dim_{\mathbb{F}_2} \, \text{III}(B/K)[2] \geq 2k - 2 - 14 - 1 = 2k - 17$ by (1) and the fact that $B(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$. \qed
The isogeny \( f : A \to B \) induces an isomorphism \( \text{III}(A/K)[n] \cong \text{III}(B/K)[n] \) since the degree of \( f \) is prime to \( n \). Hence we have
\[
\text{rk}_2 \text{II}(B/K) \geq k - 14n - 2h - 8
\]
by Corollary 5.6 and Proposition 5.7. Thus the elliptic curve \( E = B \) with \( k = \kappa + 14n + 2h + 8 \) satisfies the assertion of Theorem 5.1.

6. The case \( p = 2 \)

In this section, we complete the proof of Theorem A for \( p = 2 \). The proof is obtained by combining Proposition 4.3 with a result of Hoffstein-Luo [14], a variant of Waldspurger’s result on the behavior of central values of the Hasse-Weil \( L \)-functions under quadratic twists.

Let \( K \) be a quadratic field with fundamental discriminant \( D \). For an arbitrary positive integer \( k \), take distinct odd primes \( \ell_1, \cdots, \ell_k, m_1, \cdots, m_k \) satisfying the conditions \((A1),(A3)\) and \((A4)\) in the preceding section. (We can indeed take such primes by the Chebotarev density theorem; \( \ell_1 \) is taken so that the fixed field of the Frobenius element in \( \text{Gal}(\mathbb{Q}(\sqrt{-1}, \sqrt{D}, \sqrt{m_1}, \cdots, \sqrt{m_k})/\mathbb{Q}) \) is \( \mathbb{Q}(\sqrt{-1}, \sqrt{Dm_1}, \sqrt{m_2}, \cdots, \sqrt{m_k}) \).) Then, by Lemma \( 5.2 \), there exist odd positive integers \( s \) and \( t \) such that \( st \ell_1 \cdots \ell_k - 16tm_1 \cdots m_k = 1 \) and \( st \) has at most 5 prime factors. Let \( A \) be an elliptic curve defined by the equation \((5)\) with \( l = s\ell_1 \cdots \ell_k \) and \( m = tm_1 \cdots m_k \) (not same as in the preceding section). The following proposition is proved by using a result of [14]. We denote by \( E_a \) the quadratic twist of an elliptic curve \( E \) over \( \mathbb{Q} \) corresponding to a quadratic extension \( \mathbb{Q}(\sqrt{a})/\mathbb{Q} \).

**Proposition 6.1.** There exists a square-free integer \( d \) with at most 4 prime factors such that \( \text{rank}_\mathbb{Z} A_d(K) = \text{rank}_\mathbb{Z} A_d(\mathbb{Q}) \), \( d \equiv 1 \mod 8 \), and \( \left( \frac{d}{p} \right) = 1 \) for any prime \( q \) dividing \( 2Dlm \).

**Proof.** Let \( S \) be the set of prime numbers dividing \( 2Dlm \). By applying [14, Theorem] to \( A_D \) and \( S \), we obtain an integer \( d \) with at most 4 prime factors which satisfies \( L(A_{Dd},1) \neq 0 \) and \( \left( \frac{d}{q} \right) = 1 \) for any \( q \in S \). Here \( L(A_{Dd},s) \) is the Hasse-Weil \( L \)-function of \( A_{Dd} \). By a result of Kolyvagin on the Birch and Swinnerton-Dyer conjecture ([17]), we have \( \text{rank}_\mathbb{Z} A_{Dd}(\mathbb{Q}) = 0 \). This implies
\[
\text{rank}_\mathbb{Z} A_d(K) = \text{rank}_\mathbb{Z} A_d(\mathbb{Q}) + \text{rank}_\mathbb{Z} A_{Dd}(\mathbb{Q}) = \text{rank}_\mathbb{Z} A_d(\mathbb{Q})
\]
as desired.

By the argument of Kramer [18] used in the preceding section, we obtain the following upper bound of the Mordell-Weil rank of \( A_d \) over \( K \).

**Corollary 6.2.** We have \( \text{rank}_\mathbb{Z} A_d(K) = \text{rank}_\mathbb{Z} A_d(\mathbb{Q}) \leq 20 \).

**Proof.** If we put \( d = 4e + 1 \), then \( A_d \) has a Weierstrass equation
\[
y^2 + xy = x^3 + (8md + e)x^2 + lmd^2x.
\]
The discriminant of this Weierstrass model is \( l^2m^2d^6 \) and \( A_d(\mathbb{Q}) \) contains \( A_d[2] \). As in the preceding section, \( \text{Sel}_2(A_d/\mathbb{Q}) \) is regarded as a subgroup of
\[
\mathbb{Q}_\Sigma = \{ (x,y,z) \in (\mathbb{Q}^\times/\mathbb{Q}^\times)^{\oplus 3} \mid xyz = 1, \overline{\ord}_q(x) = \overline{\ord}_q(y) = 0 \text{ for any } q \not\in \Sigma \},
\]
where $\Sigma$ is the set of prime numbers dividing $2dlm$. Moreover, any nonzero element of $\text{Sel}_2(A_d/Q)$ is not contained in the subgroup of $Q_{\Sigma}$ generated by the classes of $(q, q, 1)$ and $(q, 1, q)$ for all $q \in \{\ell_1, \ldots, \ell_k, m_1, \ldots, m_k\}$ since the assumption $\left(\frac{d}{q}\right) = 1$ implies the local condition at $q$ for defining the 2-Selmer group does not change by the quadratic twist corresponding to $Q(\sqrt{d})$ (see the proof of Proposition 5.4). Hence we have

$$\dim_{\mathcal{O}_{\Sigma}} \text{Sel}_2(A_d/Q) \leq \dim_{\mathcal{O}_{\Sigma}} Q_{\Sigma} - 4k = 2(2k + 5 + 4 + 2) - 4k = 22.$$ 

This implies $\text{rank}_{\mathcal{O}} A_d(Q) \leq \dim_{\mathcal{O}_{\Sigma}} \text{Sel}_2(A_d/Q) - \dim_{\mathcal{O}} A_d(Q)[2] \leq 20$, as desired. \hfill \Box

**Corollary 6.3.** We have $\dim_{\mathcal{O}} \text{III}(A_d/K)[2] \geq 2k - 31$.

**Proof.** Since $A_d$ has split multiplicative reduction with even Tamagawa factor at each $q \in \{\ell_1, \ldots, \ell_k, m_1, \ldots, m_k\}$ not dividing $st$ and any such $q$ remains prime in $K$, we have $t_{A_d,K} \geq 2k - 5$. By Proposition 4.3, we have $\dim_{\mathcal{O}} \text{Sel}_2(A_d/K) \geq 2k - 9$. Hence we have $\dim_{\mathcal{O}} \text{III}(A_d/K)[2] \geq 2k - 9 - \dim_{\mathcal{O}} A_d(K)/2A_d(K) \geq 2k - 31$ by (1) and Corollary 6.2. \hfill \Box

By taking $k$ large arbitrarily, this corollary implies that the 2-rank of $\text{III}(A_d/K)[2]$ is unbounded as $d$ varies. The proof of Theorem A has been completed.

We can also give a proof of Theorem A for $p = 2$ by considering the 2-rank of $\text{III}(B_d/K)$ instead of $\text{III}(A_d/K)$. As in the preceding section, we can show that

$$\dim_{\mathcal{O}} \text{III}(B_d/Q)[2] = \dim_{\mathcal{O}} \text{Sel}_2(B_d/Q) - \text{rank}_{\mathcal{O}} B_d(Q) - \dim_{\mathcal{O}} B_d(Q)[2]$$

by using [16, Theorem 1] and Corollary 6.2. (Recall that $B_d$ is isogenous to $A_d$ and $B_d$ has semistable reduction at any prime not dividing $d$.) As we remarked before, this does not imply the assertion of Theorem A immediately since $\text{Ker}(\text{III}(B_d/Q) \to \text{III}(B_d/K))$ may have a large subgroup of exponent 2 in general. However, we can apply the following lemma in this case.

**Lemma 6.4.** Let $F'/F$ be a Galois extension of number fields such that $[F': F]$ is a prime $p$. For any elliptic curve $E$ defined over $F$ satisfying $\text{rank}_{\mathcal{O}} E(F') = \text{rank}_{\mathcal{O}} E(F)$, we have

$$\dim_{\mathcal{O}_p} \text{III}(E/F')[p] \geq \dim_{\mathcal{O}_p} \text{III}(E/F)[p] - 2.$$ 

**Proof.** By the inflation-restriction sequence, the kernel of the restriction map $\text{III}(E/F') \to \text{III}(E/F)$ is regarded as a subgroup of $H^1(G, E(F'))$, where $G = \text{Gal}(F'/F)$. We have only to prove that the $p$-rank of $H^1(G, E(F'))$ is at most 2. If we denote by $T$ the torsion subgroup of $E(F')$, then $G$ acts trivially on the free $\mathbb{Z}$-module $E(F')/T$. Indeed, $P^p - P$ is contained in $T$ for any $P \in E(F')$ and any $\sigma \in G$ by the assumption $\text{rank}_{\mathcal{O}} E(F') = \text{rank}_{\mathcal{O}} E(F)$. Hence we have $H^1(G, E(F')/T) = \text{Hom}(G, E(F')/T) = 0$. On the other hand, $H^1(G, T)$ is of exponent $p$ and its $p$-rank is not greater than $\dim_{\mathcal{O}_p} T[p] \leq 2$. The claim is proved. \hfill \Box

Since $\text{rank}_{\mathcal{O}} B_d(Q) = \text{rank}_{\mathcal{O}} B_d(K)$ by Proposition 6.1, we have $\dim_{\mathcal{O}} \text{III}(B_d/K)[2] \geq 2k - 32$. This implies the assertion of Theorem A for $p = 2$. 


Acknowledgements

The author would like to thank Yoshitaka Hachimori for helpful discussions, and the referee for valuable suggestions. The author was partially supported by KAKENHI (Grant-in-Aid for Young Scientists (B)) 18740013.

References

[17] V. A. Kolyvagin, Finiteness of E(Q) and III(E, Q) for a subclass of Weil curves, Math. USSR-Izv. 32 (1989), 523–541.