BEHAVIORS OF THE TATE–SHAFAREVICH GROUP OF ELLIPTIC CURVES UNDER QUADRATIC FIELD EXTENSIONS

by

Asuka Shiga

Abstract. — Let E be an elliptic curve defined over $\mathbb{Q}$. We study the behavior of the Tate–Shafarevich group of E under quadratic extensions $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$. First, we determine the cokernel of the restriction map $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E)[2] \to \bigoplus_p H^1(\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p), E)[2]$. Using this result, without assuming the finiteness of the Tate–Shafarevich group, we prove that the ratio $\frac{\#Ш(E/\mathbb{Q}(\sqrt{D}))[2]\cdot\#2Ш(E/\mathbb{Q}(\sqrt{D}))[4]}{\#Ш(E_D/\mathbb{Q})[2]}$ can grow arbitrarily large, where E_D denotes the quadratic twist of E by D. For elliptic curves of the form $E : y^2 = x^3 + px$ with p an odd prime, assuming the finiteness of the relevant Tate–Shafarevich groups, we prove two results: first, that $Ш(E_D/\mathbb{Q})[2] = 0$ for infinitely many square-free integers D, and second, that $\#Ш(E/\mathbb{Q}(\sqrt{D}))[2] \leq 4$ for infinitely many imaginary quadratic fields $\mathbb{Q}(\sqrt{D})$.

Contents

1. Introduction

Let K be a number field and M_K be the set of places of K. Let E be an elliptic curve over K. The Tate–Shafarevich group of E/K is defined as follows:

$$Ш(E/K) \overset{\mathrm{def}}{=} \mathrm{Ker}\left(\begin{array}{ccc} H^1(G_K, E) & \overset{\bigoplus_v \mathrm{res}_v}{\longrightarrow} & \bigoplus_{v \in M_K} H^1(G_{K_v}, E) \\ \cup & & \cup \\ [f] & \longmapsto & (\left[f\mid_{G_{K_v}} \right])_v \end{array} \right)$$

where K_v is the completion of K at the place v, and G_K, G_{K_v} are the absolute Galois groups of K, K_v respectively and $\mathrm{res}_v : H^1(G_K, E) \to H^1(G_{K_v}, E)$ is the restriction map of Galois cohomology. The Tate–Shafarevich group lives in the global Galois cohomology $H^1(G_K, E)$, which is isomorphic to the collection of equivalence classes of torsors, often denoted by $\mathrm{WC}(E/K)$, which is called the Weil–Châtelet group. Note that $\bigoplus_v \mathrm{res}_v$ is well-defined. Indeed, if a torsor C/K has good reduction at v, then its image in $H^1(G_{K_v}, E)$ vanishes since a genus 1 curve over a finite field always has a rational point.

Key words and phrases. — Elliptic curve, Tate–Shafarevich group, local global principle.

The Tate–Shafarevich group is a group that serves as an obstruction to the local-global principle for curves of genus 1. It is conjectured to be finite (Tate–Shafarevich conjecture), although this conjecture has not been proven. By contrast, the n-torsion subgroup of $Ш(E/K)$, that is, $Ш(E/K)[n] \overset{\text{def}}{=} \{a \in Ш(E/K) \mid na = 0\} = \mathrm{Ker}\left(H^1(G_K, E)[n] \overset{\text{res}}{\to} \bigoplus_{v\in M_K} H^1(G_{K_v}, E)[n]\right)$ is finite.

Let $L = K(\sqrt{D})/K$ be a quadratic extension. In this paper, we investigate the following question.

Question. — What are the behaviors of $\#Ш(E/L)[2]$ as a function of D? And how do they relate to the behaviors of $\#Ш(E_D/K)[2]$? Here, E_D/K is the quadratic twist of E/K by D.

In other words, this question examines the increase or decrease of counterexamples to the local-global principle under field extensions. When a torsor $[C/K] \in Ш(E/K)$ acquires an L-rational point through the field extension L/K, the image of $[C/K]$ in $Ш(E/L)$ becomes 0. However, the number of counterexamples to the local-global principle may increase over L, making the behavior of $\#Ш(E/L)$ relative to $\#Ш(E/K)$ intricate.

H. Yu explicitly expressed $\dfrac{\#Ш(E/L)}{\#Ш(E_D/K)}$ in terms of the order of local cohomology and global cohomology under the assumption that Tate–Shafarevich groups of elliptic curves are finite ([21]). Qiu provided the order of global cohomology and calculated examples of Yu's formula [16]. Independently of H. Yu's work, Clark proved $Ш(E/L)[n]$ can be made arbitrarily large by choosing an appropriate degree n extension L/K (Theorem 3 of [4]). He also mentioned H. Yu's work in Remark 3.8 of [4], noting that the case where $n = 2$ can be derived from Yu's formula if we assume the finiteness of the Tate-Shafarevich group. Matsuno provided an alternative proof for $n = 2$, $K = \mathbb{Q}$ of Clark's result by providing an inequality of the Selmer group (Proposition B of [11]). In contrast, it had been known earlier, according to Rohrlich, that $Ш(E_D/\mathbb{Q})[2]$ can be arbitrarily large when varying D [8]. M. Yu generalized this result to the quadratic number field with mild condition on elliptic curves [22]. Clark's result for the case $n = 2$ follows from Rohrlich and M. Yu-type results on the unboundedness of $Ш(E_D/K)[2]$. In the case of $K = \mathbb{Q}$, more strongly, we prove that $\dfrac{\#Ш(E/\mathbb{Q}(\sqrt{D}))[2]\#2Ш(E/\mathbb{Q}(\sqrt{D}))[4]}{\#Ш(E_D/\mathbb{Q})[2]}$ is unbounded above.

Theorem 1.1 **(Theorem 4.10).** — For arbitrary integer r and an elliptic curve over $\mathbb{Q}$, there exist infinitely many quadratic fields $\mathbb{Q}(\sqrt{D})$ such that

$$\frac{\#Ш(E/\mathbb{Q}(\sqrt{D}))[2]\#2Ш(E/\mathbb{Q}(\sqrt{D}))[4]}{\#Ш(E_D/\mathbb{Q})[2]} \geq r.$$

This theorem directly implies that both $\dfrac{Ш(E/\mathbb{Q}(\sqrt{D}))[2]^2}{Ш(E_D/\mathbb{Q})[2]}$ and $\#Ш(E/\mathbb{Q}(\sqrt{D}))[2]$ can be arbitrarily large. The presence of $2Ш(E/\mathbb{Q}(\sqrt{D}))[4]$ in the numerator suggests that the behavior of order 2 elements in the Tate–Shafarevich group under quadratic extensions is more complex than expected, due to their relationship with order 4 elements. For a comparison between Yu's formula and its 2-torsion subgroup version, see Remark 4.12 and Remark 4.13. In a simple case, we explain how the D in Theorem 4.10 can be chosen to be compatible with the D that makes $Ш(E_D/\mathbb{Q})[2]$ large. See Corollary 4.15.

In the proof of Theorem 4.10, we use Theorem 3.3 to avoid assuming the finiteness of the Tate-Shafarevich group.

Theorem 1.2 **(Theorem 3.3).** — Let E/K be an elliptic curve over K and n be a positive integer. Then,

$$\begin{array}{ccccc} X \coloneqq \mathrm{Coker}\Big(& H^1(G_K, E)[n] & \overset{\bigoplus_v \mathrm{res}_v}{\longrightarrow} & \bigoplus_{v\in M_K} H^1(G_{K_v}, E)[n] & \Big) \\ & \cup & & \cup & \\ & [f] & \longmapsto & (\left[f\mid_{G_{K_v}}\right])_v & \end{array}$$

is a finite group and $\#X \leq \#\mathrm{Sel}^n(E/K)$. When n is a prime number, $\#X = \#\mathrm{Sel}^n(E/K)$ holds.

In Cassels' "Arithmetic of curves of genus 1" parts I-VIII, the X in the theorem mentioned above was represented and studied using the Cyrillic letter Ж (see Appendix 2 of [3]). In Appendix 2 of [3], it is stated that there exists a duality between Ж and $\mathrm{Sel}^n(E/K)$ when n is a prime number. Despite the notable elegance of the theorem, citations of this result have been limited. Considering this, with an eye towards potential generalizations for arbitrary n, we have provided a detailed proof of this result using arguments that build upon the proof of the Cassels–Poitou–Tate duality (1.5. of Chapter 1 [5]) and Theorem 3.2.

The Tate–Shafarevich group is considered as an analogue of the ideal class group of number fields. The 2-torsion subgroup of the ideal class group can be calculated using what we call genus theory (see Theorem 5.3). According to that, the 2-torsion subgroup of the ideal class group of $\mathbb{Q}(\sqrt{D})$ grows arbitrarily large when D has many prime factors, and becomes small when D is prime. A similar phenomenon occurs for the Tate-Shafarevich group. The 2-torsion subgroup of the Tate-Shafarevich group $Ш(E/\mathbb{Q}(\sqrt{D}))[2]$ can grow arbitrarily large when D has many prime factors, as shown in Theorem 4.10. Regarding the possibility of decreasing, we prove that $Ш(E/\mathbb{Q}(\sqrt{D}))[2]$ becomes smaller when D is prime, although we cannot make it trivial in general. We also prove that $Ш(E_D/\mathbb{Q})[2]$ can be made trivial for infinitely many square-free integers D, under the assumption that the Tate–Shafarevich group is finite.

***Proposition 1.3* (Proposition 5.6).** — Let p be an odd prime, and let $E : y^2 = x^3 + px$ be an elliptic curve. Assume that Tate–Shafarevich group of elliptic curves are finite.

1. There exist infinitely many imaginary quadratic fields $K = \mathbb{Q}(\sqrt{D})$ such that $\#Ш(E/K)[2] \leq 4$. If $Ш(E/\mathbb{Q})$ contains an element of order 4, then for any quadratic number field $K = \mathbb{Q}(\sqrt{D})$, $\#Ш(E/K)[2] \neq 0$.
2. There exist infinitely many square-free integers D such that $Ш(E_D/\mathbb{Q})[2] = 0$.

Acknowledgement

I heartily thank my advisor Nobuo Tsuzuki for his constant encouragement and helpful comments and ideas. I would like to express my sincere gratitude for valuable comments from Professor Kazuo Matsuno. I would like to express my sincere gratitude to Professor Christian Wuthrich, who warmly answered my questions about the Tate-Shafarevich group through online forums and email. I would also like to express my gratitude to Kaoru Sano for engaging in valuable discussions. This work was supported by JSTSPRING, Grant Number JPMJSP2114.

2. Notation

Let us fix the notation as follows:

- K: a number field, O_K : ring of integers of K.
- M_K: the set of all places of K.
- K_v: the completion of K at place $v \in M_K$.
- G_L: the absolute Galois group of a field L, that is, $\mathrm{Gal}(\overline{L}/L)$.
- For an Abelian group A and an integer $n \geq 2$, we define $A[n]$(n-torsion subgroup of A) to be $\{a \in A \mid na = 0\}$ and nA to be $\{na \mid a \in A\}$.
- For an Abelian group A and a prime number p, we define $A[p^\infty]$(p-primary part of A) to be $A[p^\infty] := \{a \in A | \exists n \geq 0, p^n a = 0\}$.
- For a locally compact group A, A^* is the Pontryagin dual. For a group homomorphism $f : A \to B$ between locally compact group A and B, $f^* : B^* \to A^*$ is given by $g \mapsto g \circ f$.
- For a group homomorphism $f : N \to M$, $f(N)$ is the image of N under f.
- E/K: an elliptic curve defined over K.
- $\mathrm{rank}(E/K)$: the Mordell-Weil rank of elliptic curve E/K, Δ_E: discriminant of E/K.

- E_D/K: the quadratic twist of E/K by a square-free integer D. Namely, if E/K is the elliptic curve defined by $y^2 = x^3+ax+b$, then the quadratic twist is an elliptic curve given by the equation $E_D : Dy^2 = x^3 + ax + b$. Quadratic twist E_D is isomorphic to E over $K(\sqrt{D})$ but not isomorphic over K. We fix an isomorphism $\tau : E(L) \cong E_D(L), (x, y) \mapsto (x, \frac{y}{\sqrt{D}})$.
- For an elliptic curve E/K, another elliptic curve E' and a nonzero isogeny $\phi : E \to E'$, the ϕ-Selmer group of E/K is defined as follows:

$$\mathrm{Sel}^{\phi}(E/K) \overset{\text{def}}{=} \mathrm{Ker}\Big(H^1(G_K, E[\phi]) \ \to \ \textstyle\prod_{v\in M_K} H^1(G_{K_v}, E)[\phi]\Big).$$

  When $E = E'$ and $\phi = [n]$ (multiplication-by-n map), we denote its Selmer group by $\mathrm{Sel}^n(E/K)$.

There exists an exact sequence

$$0 \to E(K)/nE(K) \to \mathrm{Sel}^n(E/K) \to Ш(E/K)[n] \to 0 \tag{1}$$

and $Ш(E/K)[n]$ is finite since n-Selmer group is finite (see Theorem 4.2 in Chapter X of [18]).

3. Local cohomology and Global cohomology

3.1. Switch local to global. — In this section, we determine the cokernel of the restriction map $H^1(G_K, E)[2] \to \bigoplus_{v\in M_K} H^1(G_{K_v}, E)[2]$ (Theorem 3.3). We denote this cokernel as X in Theorem 3.3. We prove that X is isomorphic to the dual of 2-Selmer group, which lives in the global cohomology $H^1(G_K, E[2])$.

Theorem 3.1 **(*cf.* [14], (8.6.10), Long Exact Sequence of Poitou–Tate)**

Let S be a nonempty set of primes of a number field K and assume that S contains all infinite places of K. Let K_S be the maximal unramified extension of K outside S and $G_S \coloneqq \mathrm{Gal}(K_S/K)$. Let M be a finite G_S module and $M' = \mathrm{Hom}(M, \mu)$ where μ is the group of roots of unity in ${K_S}^{\times}$. The following 9-term exact sequence exists:

$$\begin{array}{l} 0 \longrightarrow H^0(G_S, M) \xrightarrow{\alpha} \displaystyle\prod_{v\in S} H^0(G_{K_v}, M) \longrightarrow H^2(G_S, M')^* \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \big\downarrow \\ H^1(G_S, M')^* \longleftarrow \displaystyle\prod_{v\in S}{}' H^1(G_{K_v}, M) \xleftarrow[\beta]{} H^1(G_S, M) \\ \big\downarrow \\ H^2(G_S, M) \xrightarrow{\gamma} \displaystyle\bigoplus_{v\in S} H^2(G_{K_v}, M) \longrightarrow H^0(G_s, M')^* \longrightarrow 0. \end{array}$$

Here, α, β, and γ are localization maps and $\prod'_v$ is a restricted product with respect to unramified cohomology $H^1_{un}(G_{K_v}, M)$.

Theorem 3.2 **(*cf.* [7], 7.2, Lemma 2).** — Let S be a set of places of K containing all infinite places. Let K_S be the maximal unramified extension of K outside S and $G_S \coloneqq \mathrm{Gal}(K_S/K)$. Let M be a finite G_S-module.

Let p be a prime. If $pM = 0$ and $\dim_{\mathbb{F}_p} M \leq 2$ holds, then

$$\mathrm{Ker}\left(H^1(G_S, M) \xrightarrow{\beta} \prod_{v\in S}{}' H^1(G_{K_v}, M)\right) = 0.$$

Proof. — See [[7], Section 7.2, Lemma 2]. □

Theorem 3.3. — Let E/K be an elliptic curve and n be a positive integer. Then,

$$\begin{array}{ccc} X \coloneqq \mathrm{Coker}\Big(H^1(G_K, E)[n] & \overset{\bigoplus_v \mathrm{res}_v}{\longrightarrow} & \bigoplus_{v\in M_K} H^1(G_{K_v}, E)[n]\Big) \\ \cup & & \cup \\ [f] & \longmapsto & (\Big[f\mid_{G_{K_v}}\Big])_v \end{array}$$

is a finite group and $\#X \leq \#\mathrm{Sel}^n(E/K)$. When n is a prime number, $\#X = \#\mathrm{Sel}^n(E/K)$ holds.

Proof. — Let S be a finite subset of M_K containing the infinite places of K and the primes of bad reduction for E/K.

The exactness of the following sequence forms part of the long exact sequence in the Poitou–Tate duality (Theorem 3.1) when we set $M = E[n]$.

$$H^1(G_S, E[n]) \xrightarrow{\beta} \bigoplus_{v\in S} H^1(G_{K_v}, E[n]) \xrightarrow{\beta^*\circ\psi} H^1(G_S, E[n])^*$$

Here, $\psi \coloneqq \prod_{v\in S}\psi_v$, where ψ_v is the isomorphism given by the local Tate duality:

$$\psi_v \colon H^1(G_{K_v}, E[n]) \cong H^1(G_{K_v}, E[n])^*$$

(see [[14], Theorem 7.2.6]).

Let ι be the map that makes the following diagram commutative:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1(G_S, E[n]) & \xrightarrow{\beta} & \bigoplus_{v\in S} H^1(G_{K_v}, E[n]) & \xrightarrow{h} & \mathrm{Coker}\beta & \longrightarrow & 0 \\ & & \| & & \| & & \downarrow \iota & & \\ 0 & \longrightarrow & H^1(G_S, E[n]) & \xrightarrow{\beta} & \bigoplus_{v\in S} H^1(G_{K_v}, E[n]) & \xrightarrow{\beta^*\circ\psi} & H^1(G_S, E[n])^* . & & \end{array}$$

From the above diagram, ι is injective. Let us consider the following diagram.

$$\begin{array}{ccccc} & & \mathrm{Ker}\beta & \longrightarrow & \mathrm{Ker}\phi_S \\ & & \downarrow & & \downarrow \\ 0 & \longrightarrow & H^1(G_S, E[n]) & = & H^1(G_S, E[n]) \\ \downarrow & & \downarrow\beta & & \downarrow\phi_S \\ \bigoplus_{v\in S} H^1(G_{K_v}, E)[n]^* & \xrightarrow{\psi^{-1}\circ\lambda^*} & \bigoplus_{v\in S} H^1(G_{K_v}, E[n]) & \xrightarrow{\lambda} & \bigoplus_{v\in S} H^1(G_{K_v}, E)[n] \\ = \downarrow & & h\downarrow & & \\ \bigoplus_{v\in S} H^1(G_{K_v}, E)[n]^* & \xrightarrow{j} & \mathrm{Coker}\beta. & & \end{array}$$

Here, $\phi_S \overset{\mathrm{def}}{=} \lambda\circ\beta$ and $\lambda \coloneqq \bigoplus_{v\in S}\lambda_v$, where $\lambda_v : H^1(G_{K_v}, E[n]) \to H^1(G_{K_v}, E)[n]$ is the map induced by a short exact sequence $0 \to E[n] \to E \overset{\times n}{\to} E \to 0$ (see [[18], Section VIII.2]).

Note that

$$\bigoplus_{v\in S} H^1(G_{K_v}, E)[n]^* \overset{\psi^{-1}\circ\lambda^*}{\to} \bigoplus_{v\in S} H^1(G_{K_v}, E[n]) \overset{\lambda}{\to} \bigoplus_{v\in S} H^1(G_{K_v}, E)[n]$$

is an exact sequence because

$$\mathrm{Im}({\psi_v}^{-1}\circ{\lambda_v}^*) \cong \mathrm{Im}{\lambda_v}^* \cong (\mathrm{Im}\lambda_v)^* \cong (H^1(G_{K_v}, E)[n])^* \cong E(K_v)/nE(K_v) \cong \mathrm{Ker}\lambda_v$$

where the isomorphism $H^1(G_{K_v}, E)[n])^* \cong E(K_v)/nE(K_v)$ is given by the restricted Tate local duality (see [[19], Proposition 1]).

By the snake lemma, we obtain the following exact sequence

$$\mathrm{Ker}\beta \to \mathrm{Ker}\phi_S \to \bigoplus_{v\in S} H^1(G_{K_v}, E)[n]^* \xrightarrow{j} \mathrm{Coker}\beta.$$

We claim that the following diagram ⓐ is commutative.

$$\begin{array}{ccccccc} \mathrm{Ker}\beta & \longrightarrow & \mathrm{Ker}\phi_S & \longrightarrow & \bigoplus_{v\in S} H^1(G_{K_v}, E)[n]^* & \xrightarrow{\quad j \quad} & \mathrm{Coker}\beta \\ & & & & & {\scriptstyle \phi_S{}^*}\searrow & \downarrow{\scriptstyle \iota} \\ & & & & & & H^1(G_K, E[n])^* \end{array} \qquad \cdots ⓐ.$$

Indeed, this follows from the following diagram:

$$\begin{array}{ccc} \bigoplus_{v\in S} H^1(G_{K_v}, E)[n]^* & \xrightarrow{\quad j \quad} & \mathrm{Coker}\beta \\ {\scriptstyle \lambda^*}\downarrow \quad (1) & \overset{\phi_S{}^*}{\searrow} & \downarrow{\scriptstyle \iota} \\ \bigoplus_{v\in S} H^1(G_{K_v}, E[n])^* & \xrightarrow{\beta^*} & H^1(G_K, E[n])^* \\ {\scriptstyle \psi}\uparrow \quad & (2) & \uparrow{\scriptstyle \iota} \\ \bigoplus_{v\in S} H^1(G_{K_v}, E[n]) & \xrightarrow{\quad h \quad} & \mathrm{Coker}\beta. \end{array}$$

To prove the desired commutativity, it is sufficient to prove the commutativity of (1) and (2) of the above diagram because $h \circ \psi^{-1} \circ \lambda^* = j$. The commutativity of (1) follows directly from the definition of ϕ_S, and (2) is exactly the definition of ι, that is, $\iota \circ h = \beta^* \circ \psi$.

From the commutativity of the diagram ⓐ, we obtain the following exact sequence:

$$\mathrm{Ker}\beta \to \mathrm{Ker}\phi_S \to \bigoplus_{v\in S} H^1(G_{K_v}, E)[n]^* \xrightarrow{\phi_S{}^*} H^1(G_K, E[n])^*.$$

There is a canonical isomorphism $\mathrm{Ker}\phi_S \cong \mathrm{Sel}^n(E/K)$ (see [[13], Chapter I, Corollary 6.6]). By taking its Pontryagin dual, we obtain

$$H^1(G_K, E[n]) \to \bigoplus_{v\in S} H^1(G_{K_v}, E)[n] \to \mathrm{Sel}^n(E/K)^* \to (\mathrm{Ker}\beta)^*.$$

By taking the direct limit $\varinjlim_{S\subset M_K}$, we obtain the following exact sequence :

$$0 \to \mathrm{Sel}^n(E/K) \to H^1(G_K, E[n]) \xrightarrow{\phi} \bigoplus_{v\in M_K} H^1(G_{K_v}, E)[n] \xrightarrow{\epsilon} \mathrm{Sel}^n(E/K)^*.$$

We can conclude that $\#X \leq \#\mathrm{Sel}^n(E/K)$ from the following commutative diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Sel}^n(E/K) & \longrightarrow & H^1(G_K, E[n]) & \xrightarrow{\phi} & \bigoplus_{v\in M_K} H^1(G_{K_v}, E)[n] & \xrightarrow{\epsilon} & \mathrm{Sel}^n(E/K)^* \\ & & \downarrow\!\!\downarrow & & \downarrow\!\!\downarrow & & \| & & \\ 0 & \longrightarrow & Ш(E/K)[n] & \longrightarrow & H^1(G_K, E)[n] & \longrightarrow & \bigoplus_{v\in M_K} H^1(G_{K_v}, E)[n] & \longrightarrow & X \longrightarrow 0. \end{array}$$

Indeed, since $X \cong \mathrm{Coker}\phi$ injects into $\mathrm{Sel}^n(E/K)$, it follows that $\#X \leq \#\mathrm{Sel}^n(E/K)$.

When n is a prime number, $\mathrm{Ker}\beta = 0$ by Theorem 3.2. Therefore, ϵ is surjective, hence $\#X = \#\mathrm{Sel}^n(E/K)$.

□

3.2. Local vs Global. — The local cohomology of elliptic curves at bad primes (especially those with additive reduction) remains mysterious, but we can calculate it at primes of good reduction. In this section, we prove that we can increase the contributions from local cohomology while suppressing the contributions from global cohomology.

Theorem 3.4. — Let E/K be an elliptic curve over K. Let $L = K(\sqrt{D})$ be a quadratic extension of K. Let σ be a generator of $\mathrm{Gal}(L/K)$. We define $\mathrm{tr} : E(L) \to E(K)$ by $P \mapsto P+P^{\sigma}$. Then,

$$\#H^1(\mathrm{Gal}(L/K), E(L)) = \#\mathrm{Coker}(\mathrm{tr}) \times 2^{\mathrm{rank}(E_D/K)-\mathrm{rank}(E/K)}$$

holds. In particular, $\#H^1(\mathrm{Gal}(L/K), E(L)) \leq 2^{\mathrm{rank}(E_D/K)} \times \#E(K)[2]$

Proof. — For the former, see [[16], Theorem 1.5]. The latter immediately follows from the fact that there is a surjection from $E(K)/2E(K)$ to $\mathrm{Coker}(\mathrm{tr})$.

□

Proposition 3.5. — Let L be a quadratic extension of K. Let $v \in M_K$ be a place that is not above 2 and let w a place of L above v. Let E/K be an elliptic curve. Let k be the residue field of K_v and $\tilde{E}/k$ be the reduction of E/K mod v.

(1) Suppose v is an unramified place of L/K and is a good place of E/K. It holds that $H^1(\mathrm{Gal}(L_w/K_v), E(L_w)) = 0$.
(2) $H^1(\mathrm{Gal}(L_w/K_v), E(L_w))$ is a finite group.
(3) Suppose v is a ramified place of L/K and is a good place of E/K. It holds that

$$\#H^1(\mathrm{Gal}(L_w/K_v), E(L_w)) = \#\tilde{E}(k)[2].$$

Proof. — (1) See [[12], Corollary 4.4].

(2) We have an inflation-restriction exact sequence:

$$0 \to H^1(\mathrm{Gal}(L_w/K_v), E(L_w)) \xrightarrow{\mathrm{inf}} H^1(G_{K_v}, E) \xrightarrow{\mathrm{res}} H^1(G_{L_w}, E).$$

From Tate duality, the dual of this sequence is

$$E(L_w) \xrightarrow{\mathrm{tr}} E(K_v) \to H^1(\mathrm{Gal}(L_w/K_v), E(L_w))^* \to 0.$$

Thus, $H^1(\mathrm{Gal}(L_w/K_v), E(L_w)) \cong E(K_v)/\mathrm{tr}(E(L_w))$ holds (see [[12], Proposition 4.2] for this isomorphism and [[19], equation (12)] for the relation $\mathrm{res}^* = \mathrm{tr}$).

There exists a surjective map from the weak Mordell–Weil group $\frac{E(K_v)}{2E(K_v)}$ to $\frac{E(K_v)}{\mathrm{tr}(E(L_w))}$. Because $\frac{E(K_v)}{2E(K_v)} \subset H^1(G_{K_v}, E[2])$, it is sufficient to prove $H^1(G_{K_v}, E[2])$ is finite. Let $M = K_v(E[2])$. Then M/K_v is a finite Galois extension. Because $H^1(G_M, E[2]) \cong (M^{\times}/M^{\times 2})^2$ is finite and $\#H^1(\mathrm{Gal}(M/K_v), E(M)[2])$ is finite, we see that $H^1(G_{K_v}, E[2])$ is finite because of the exact sequence $0 \to H^1(\mathrm{Gal}(M/K_v), E(M)[2]) \xrightarrow{\mathrm{inf}} H^1(G_{K_v}, E[2]) \xrightarrow{\mathrm{res}} H^1(G_M, E[2])$.

(3) From (2), it is sufficient to prove $\#\dfrac{E(K_v)}{\mathrm{tr}(E(L_w))} = \#\tilde{E}(k)[2]$. There exists an exact sequence:

$$0 \to \frac{E_1(K_v)}{\mathrm{tr}(E_1(L_w))} \to \frac{E(K_v)}{\mathrm{tr}(E(L_w))} \xrightarrow{\text{reduction}} \frac{\tilde{E}(k)}{2\tilde{E}(k)} \to 0$$

where E_1 denotes the kernel of reduction. Note that reduction is well-defined since L_w/K_v is a ramified extension. Let us prove that the group on the left-hand side is trivial. Indeed, $E_1(K_v) \cong \hat{E}(M)$, where M is the maximal ideal of O_K and $\hat{E}(M)$ is the group associated with the formal group $\hat{E}$, which is a 2-divisible group. For all $a \in E_1(K_v)$, there exists $b \in E_1(K_v)$ such that $a = 2b = \mathrm{tr}(b)$. Then we can conclude that $\#H^1(\mathrm{Gal}(L_w/K_v), E(L_w))) = \#\dfrac{E(K_v)}{\mathrm{tr}(E(L_w))} = \#\dfrac{\tilde{E}(k)}{2\tilde{E}(k)} = \#\tilde{E}(k)[2]$.

□

Remark 3.6. — When L/K is a quadratic extension and there is a choice of $w \in M_L$ above $v \in M_K$, v splits completely. Since $H^1(\mathrm{Gal}(L_w/K_v), E(L_w)) = 0$ in this case, the choice of w is not an issue. More generally, for a Galois extension L/K of degree n, it can be shown

that $H^1(\mathrm{Gal}(L_w/K_v), E(L_w))$ is independent of the choice of $w \mid v$. Similarly to (1) and (2) of Proposition 3.5, it can be proven that $H^1(\mathrm{Gal}(L_w/K_v), E(L_w))$ is a finite group that vanishes for almost all v.

Theorem 3.7 **(*cf.* J.Hoffstein and W.Luo appendixed by Rohrlich [8])**

For any elliptic curve A over $\mathbb{Q}$, there exist infinitely many square-free integers $D \in \mathbb{Z}$ such that $\mathrm{rank}(A_D/\mathbb{Q}) = 0$ and the number of prime factors of D is no greater than 4.

Proposition 3.8. — Let K be a number field. Suppose that there exists a quadratic extension $K(\sqrt{d})$ of K such that $\mathrm{rank}(A_d/K) = 0$ for arbitrary elliptic curve A over K and the number of prime factors of d is no greater than some constant a. Then for an arbitrary integer $r \in \mathbb{Z}$ and arbitrary elliptic curve E/K, there exist infinitely many quadratic extensions $L = K(\sqrt{D})/K$ such that

$$g(D) \coloneqq \frac{\#\bigoplus_{v\in M_K} H^1(\mathrm{Gal}(L_w/K_v), E(L_w))}{\#H^1(\mathrm{Gal}(L/K), E(L))} \geq r.$$

Proof. — By Theorem 3.4, it is sufficient to prove there exists infinitely many D such that

$$\frac{\#\bigoplus_{v\in M_K} H^1(\mathrm{Gal}(L_w/K_v), E(L_w))}{2^{\mathrm{rank}(E_D/K)}} \geq r.$$

For an arbitrary r, there exists an integer R such that $4^{R-a} \geq r$. For this R, there exist infinitely many prime elements $v_i (1 \leq i \leq R)$ of O_K such that :

(1) split completely in the Hilbert calss field of $K(E[2])$
(2) E/K has good reduction at v_i and not above 2.

For such prime elements v of O_K, $K_v(E[2]) = K_v$ since v splits completely in $K(E[2])$, thus $E(\overline{K_v})[2] = E(K_v)[2]$ injects into $\tilde{E}(k_v)[2]$, and therefore $\#\tilde{E}(k_v)[2] = 4$ where k_v is the residue field of K_v. Thus if v is a ramified prime of quadratic extension $L = K(\sqrt{D})$ of K, $\#H^1(\mathrm{Gal}(L_w/K_v), E(L_w)) = 4$ holds by Proposition 3.5. By setting $A = E_{v_1v_2\cdots v_R}$, there exists a quadratic extension $K(\sqrt{D_R})/K$ such that $\mathrm{rank}(E_{v_1v_2\cdots v_RD_R}/K) = 0$ and the number of prime factors of D_R is no greater than 4. Let us take D as $D = v_1 \cdots v_R D_R$. Because the number of prime factors of D_R is no greater than a, the number of ramified places of K under quadratic extension $L = K(\sqrt{v_1v_2\cdots v_RD_R})/K$ which satisfies condition (1), (2) is $R - a$ or more. Thus, taking $L = K(\sqrt{v_1v_2\cdots v_RD_R})$,

$$\frac{\#\bigoplus_{v\in M_K} H^1(\mathrm{Gal}(L_w/K_v), E(L_w))}{2^{\mathrm{rank}(E_D/K)}} \geq \frac{4^{R-a}}{2^{\mathrm{rank}(E_D/K)}} \geq \frac{4^{R-a}}{2^0} \geq r.$$

In this configuration, there are infinitely many ways to choose the prime factor v, which means there are also infinitely many ways to choose D. □

Remark 3.9. — In particular, when $K = \mathbb{Q}$, Theorem 3.7 implies that for all $r \in \mathbb{Z}$ and all elliptic curves E/K, there exist infinitely many square-free integers D such that $g(D) \geq r$. If we can determine that $\mathrm{rank}(E_D/K)$ does not grow significantly compared to $4^{\omega(\Delta_{E_D})}$, where $\omega(\Delta_{E_D})$ is the number of prime factors of Δ_{E_D}, this result can be generalized to cases where $K \neq \mathbb{Q}$.

4. Increasing $Ш(E/\mathbb{Q}(\sqrt{D}))[2]$ and $Ш(E_D/\mathbb{Q})[2]$

4.1. Trace and twist. — In this section, we investigate the relationship between $\mathrm{tr}(Ш(E/L)[2])$ and $\#Ш(E_D/K)[2]$. The Galois group naturally acts on $Ш(E/L)$ by acting on the coefficients of torsors, and we can explicitly calculate this action cohomologically.

Definition 4.1 **($\mathrm{Gal}(L/K)$ acts on $Ш(E/L)$).** — Let G be a group and H be a normal finite index subgroup of G. Let M be a G-module. G/H acts on $H^1(H, M)$ by $(\overline{g} * X)(h) = gX(g^{-1}hg)$. Here, g is a lift of $\bar{g} \in G/H$ in G, and $gX(g^{-1}hg)$ does not depend on the lift modulo coboundary.

When $G = G_K$ and $H = G_L$ and $M = E$, the Galois group $\mathrm{Gal}(L/K) \cong G/H$ acts on $Ш(E/L)[2] \subset H^1(G_L, E)$ as described above.

***Definition 4.2* (Corestriction and trace).** — In the case $[G:H]=2$, let σ be a generator of G/H. There is a map $\mathrm{cor} : H^1(H,M) \to H^1(G,M)$ called corestriction which satisfies $\mathrm{cor} \circ \mathrm{res} = [2]$ and $\mathrm{tr} = \mathrm{res} \circ \mathrm{cor}$ where $\mathrm{tr} : H^1(H,M) \to H^1(H,M)$ be a map defined by $X \mapsto X + \sigma * X$.

Explicitly, $\mathrm{cor} : H^1(H,M) \to H^1(G,M)$ can be expressed as follows.

$$H^1(H,M) \to H^1(G,M) \text{ is given by } X \mapsto \left[g \mapsto \begin{cases} X(g) + (\sigma * X)(g) & \text{if } g \in H, \\ X(g\sigma) + (\sigma * X)(g\sigma) & \text{if } g \in G - H \end{cases} \right].$$

This is indeed a trace map if we restrict it to $H^1(H,M)$. When $G = G_K, H = G_L, M = E$, the map $\mathrm{cor} : H^1(G_L,E) \to H^1(G_K,E)$ and $\mathrm{tr} : H^1(G_L,E) \to H^1(G_L,E)$ induce maps $\mathrm{cor} : Ш(E/L)[2] \to Ш(E/K)[2]$ and $\mathrm{tr} : Ш(E/L)[2] \to Ш(E/L)[2]$.

Proposition 4.3. — $\#\mathrm{tr}(Ш(E/L)[2]) \geq \dfrac{\#\mathrm{cor}(Ш(E/L)[2])}{\#H^1(\mathrm{Gal}(L/K), E(L))}$.

Proof. — Since $\mathrm{tr} = \mathrm{res} \circ \mathrm{cor}$, there exists a map $\mathrm{cor}(Ш(E/L)[2]) \xrightarrow{\mathrm{res}} \mathrm{tr}(Ш(E/L)[2])$. By the inflation-restriction sequence, $\mathrm{Ker}(\mathrm{res})$ is contained in $H^1(\mathrm{Gal}(L/K), E(L))$. By applying the first isomorphism theorem to res, we obtain the inequality. □

Theorem 4.4. — Let

$$\langle\ ,\rangle_K : Ш(E/K)[2] \times Ш(E/K)[2] \to \mathbb{Z}/2\mathbb{Z},$$
$$\langle\ ,\rangle_L : Ш(E/L)[2] \times Ш(E/L)[2] \to \mathbb{Z}/2\mathbb{Z}$$

be the Cassels–Tate pairing. Then,

(1) The kernel on each side is $Ш(E/K)[2] \cap 2Ш(E/K) = 2Ш(E/K)[4]$ and $2Ш(E/L)[4]$, respectively.
(2) $\langle a, \mathrm{cor}(a')\rangle_K = \langle \mathrm{res}(a), a'\rangle_L$.

Proof. — For (1), see [[19], Theorem 3.2]. See also [[20], Theorem 15]. For (2), see [[21],Theorem 8]. □

Corollary 4.5. —

$$\#\mathrm{cor}(Ш(E/L)[2]) \geq \frac{\#Ш(E/K)[2]}{\#2Ш(E/L)[4]\#H^1(\mathrm{Gal}(L/K), E(L))}.$$

Proof. — By Theorem 4.4 (1), the Cassels–Tate pairing induces non-degenerate pairings

$$\langle\ ,\ \rangle'_K : \frac{Ш(E/K)[2]}{2Ш(E/K)[4]} \times \frac{Ш(E/K)[2]}{2Ш(E/K)[4]} \to \mathbb{Z}/2\mathbb{Z},$$
$$\langle\ ,\ \rangle'_L : \frac{Ш(E/L)[2]}{2Ш(E/L)[4]} \times \frac{Ш(E/L)[2]}{2Ш(E/L)[4]} \to \mathbb{Z}/2\mathbb{Z}.$$

Let $\mathrm{res}' : \dfrac{Ш(E/K)[2]}{2Ш(E/K)[4]} \to \dfrac{Ш(E/L)[2]}{2Ш(E/L)[4]}$ and $\mathrm{cor}' : \dfrac{Ш(E/L)[2]}{2Ш(E/L)[4]} \to \dfrac{Ш(E/K)[2]}{2Ш(E/K)[4]}$ be the map induced by $\mathrm{res} : Ш(E/K)[2] \to Ш(E/L)[2], \mathrm{cor} : Ш(E/L)[2] \to Ш(E/K)[2]$ respectively.

By Theorem 4.4 (2), $\langle a + 2Ш(E/K)[4], \mathrm{cor}'(a' + 2Ш(E/L)[4])\rangle'_K := \langle a, \mathrm{cor}(a')\rangle_K = \langle \mathrm{res}(a), a'\rangle_L =: \langle \mathrm{res}'(a + 2Ш(E/K)[4]), a' + 2Ш(E/L)[4]\rangle'_L$ holds.

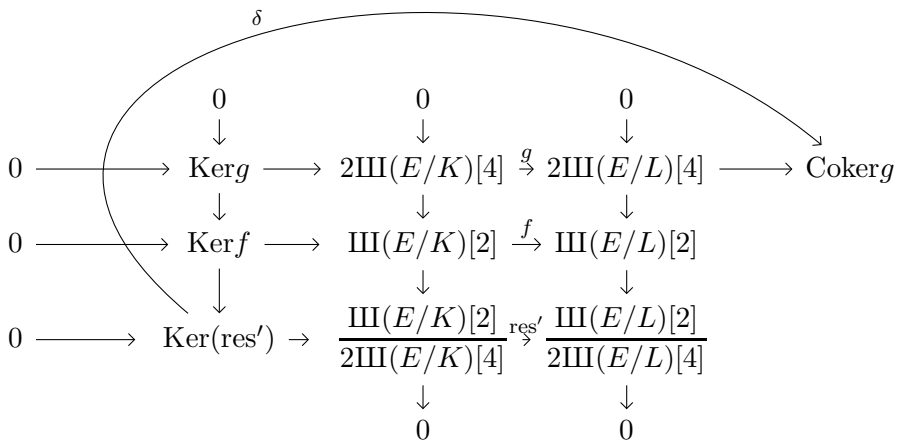
Therefore, the following diagram is commutative, where the vertical map is an isomorphism induced by $\langle\ ,\ \rangle'_L$. Note that these two vertical arrows are isomorphisms because the induced pairing is non-degenerate.

$$\begin{array}{ccc} \dfrac{Ш(E/K)[2]}{2Ш(E/K)[4]} & \xrightarrow{\mathrm{res}'} & \dfrac{Ш(E/L)[2]}{2Ш(E/L)[4]} \\ \cong\downarrow & & \downarrow\cong \\ \left(\dfrac{Ш(E/K)[2]}{2Ш(E/K)[4]}\right)^* & \xrightarrow[\mathrm{cor}'^*]{} & \left(\dfrac{Ш(E/L)[2]}{2Ш(E/L)[4]}\right)^* \end{array}$$

From this commutative diagram,

$$\#\mathrm{cor}'(\frac{Ш(E/L)[2]}{2Ш(E/L)[4]}) = \#\mathrm{cor}'^{*}((\frac{Ш(E/K)[2]}{2Ш(E/K)[4]})^{*}) = \#\mathrm{res}'(\frac{Ш(E/K)[2]}{2Ш(E/K)[4]}) \tag{2}$$

holds. Let us consider the following diagram. For simplicity, we abbreviate $\mathrm{res} : Ш(E/K)[2] \to Ш(E/L)[2]$ as f, and denote by g the map induced by f on $2Ш(E/K)[4]$.



By applying the snake lemma to this diagram, we obtain an exact sequence:

$$0 \to \mathrm{Ker}g \to \mathrm{Ker}f \to \mathrm{Ker}(\mathrm{res}') \to \mathrm{Im}\delta \to 0.$$

Because $\mathrm{Ker}f \subset H^1(\mathrm{Gal}(L/K), E(L))$, we obtain

$$\begin{aligned} \#\mathrm{Ker}(\mathrm{res}') &= \frac{\#\mathrm{Ker}f\,\#\mathrm{Im}\delta}{\#\mathrm{Ker}g} \\ &\leq \frac{\#H^1(\mathrm{Gal}(L/K), E(L))\,\#\mathrm{Coker}g}{\#\mathrm{Ker}g} = \frac{\#H^1(\mathrm{Gal}(L/K), E(L))\,\#2Ш(E/L)[4]}{\#2Ш(E/K)[4]}. \end{aligned} \tag{3}$$

Here, the last equality holds because of the exactness of

$$0 \to \mathrm{Ker}g \to 2Ш(E/K)[4] \xrightarrow{g} 2Ш(E/L)[4] \to \mathrm{Coker}g \to 0.$$

Therefore,

$$\begin{aligned} \#\mathrm{cor}(Ш(E/L)[2]) \geq \#\mathrm{cor}'(\frac{Ш(E/L)[2]}{2Ш(E/L)[4]}) &= \#\mathrm{res}'(\frac{Ш(E/K)[2]}{2Ш(E/K)[4]}) \text{ (by (2))} \\ &= \frac{\#Ш(E/K)[2]}{\#\mathrm{Ker}(\mathrm{res}')\#2Ш(E/K)[4]} \\ &\geq \frac{\#Ш(E/K)[2]}{\#2Ш(E/L)[4]\#H^1(\mathrm{Gal}(L/K), E(L))} \text{ (by (3))}. \end{aligned}$$

□

Proposition 4.6. — Let L/K be a quadratic extension and $L = K(\sqrt{D})$. Then,

$$\#\mathrm{tr}(Ш(E/L)[2]) \geq \frac{\#Ш(E_D/K)[2]}{4^{\mathrm{rank}(E/K)}\#E(K)[2]^2\#2Ш(E/L)[4]}$$

holds.

Proof. — Let $\phi : Ш(E/L) \cong Ш(E_D/L)$ be an isomorphism induced by $\tau : E(L) \cong E_D(L), (x,y) \mapsto (x, \frac{y}{\sqrt{D}})$. The following commutative diagram exists.

$$\begin{array}{ccc} Ш(E/L) & \xrightarrow{\mathrm{tr}} & Ш(E/L) \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi} \\ Ш(E_D/L) & \xrightarrow[1-\sigma]{} & Ш(E_D/L) \end{array}$$

From this diagram, $\#\mathrm{tr}(Ш(E/L)[2]) = \#\mathrm{tr}(Ш(E_D/L)[2])$ for 2-torsions.

By applying Proposition 4.3, Corollary 4.5, and Theorem 3.4 , we obtain the inequality.

□

4.2. Main theorem. — Let us consider the inflation-restriction sequence

$$0 \to H^1(\mathrm{Gal}(L/K), E(L)) \overset{\mathrm{inf}}{\to} H^1(G_K, E) \overset{\mathrm{res}}{\to} H^1(G_L, E)^{\mathrm{Gal}(L/K)}.$$

Taking the 2-torsion subgroup of this sequence , we obtain an exact sequence

$$0 \to H^1(\mathrm{Gal}(L/K), E(L)) \overset{\mathrm{inf}}{\to} H^1(G_K, E)[2] \overset{\mathrm{res}}{\to} H^1(G_L, E)[2]^{\mathrm{Gal(L/K)}}.$$

Note that $H^1(\mathrm{Gal}(L/K), E(L))$ is a 2-torsion group, that is, $2H^1(\mathrm{Gal}(L/K), E(L)) = 0$ because $\#\mathrm{Gal}(L/K) = 2$.

Consider the local-global version of this diagram, and draw the following diagram with exact rows and columns:

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & \mathrm{Ker}F & \longrightarrow & Ш(E/K)[2] & \longrightarrow & \mathrm{Ker}H & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & H^1(\mathrm{Gal}(L/K), E(L)) & \xrightarrow{\mathrm{inf}} & H^1(G_K, E)[2] & \xrightarrow{\mathrm{res}} & \mathrm{res}(H^1(G_K, E)[2]) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle G} & & \downarrow{\scriptstyle H} & & \\ 0 & \longrightarrow & \bigoplus_{v\in M_K} H^1(\mathrm{Gal}(L_w/K_v), E(L_w)) & \longrightarrow & \bigoplus_{v\in M_K} H^1(G_{K_v}, E)[2] & \longrightarrow & \bigoplus_{v\in M_K} \mathrm{res}(H^1(G_{K_v}, E)[2]) & & \\ & & \downarrow & & \downarrow & & & & \\ & & \mathrm{Coker}F & \xrightarrow{j} & X & & & & \\ & & \downarrow & & \downarrow & & & & \\ & & 0 & & 0. & & & & \end{array}$$

FIGURE 1. A key diagram

Notably, by Theorem 3.3, $X \cong \mathrm{Sel}^2(E/K)$ holds.

Lemma 4.7. — $\#\mathrm{Ker}H = \dfrac{\#Ш(E/K)[2]\#\bigoplus_{v\in M_K} H^1(\mathrm{Gal}(L_w/K_v), E(L_w))}{\#j(\mathrm{Coker}F)\#H^1(\mathrm{Gal}(L/K), E(L))}$.

Proof. — By applying the snake lemma,

$$0 \to \mathrm{Ker}F \to Ш(E/K)[2] \to \mathrm{Ker}H \to \mathrm{Coker}F \to j(\mathrm{Coker}F) \to 0.$$

We obtain $\#\mathrm{Ker}H = \dfrac{\#Ш(E/K)[2]\#\mathrm{Coker}F}{\#j(\mathrm{Coker}F)\#\mathrm{Ker}F}$. The left vertical exact sequence implies $\dfrac{\#\mathrm{Coker}F}{\#\mathrm{ker}F} = \dfrac{\#\bigoplus_{v\in M_K} H^1(\mathrm{Gal}(L_w/K_v), E(L_w))}{\#H^1(\mathrm{Gal}(L/K), E(L))}$, thus the proposition follows.

□

In the Figure 1, Ker$H$ lives in Ш$(E/L)[2]$. Henceforth, we shall prove that the ratio of the order of Ш$(E/L)[2]$ to that of Ker$H$ is related to $\#$Ш$(E_D/K)[2]$.

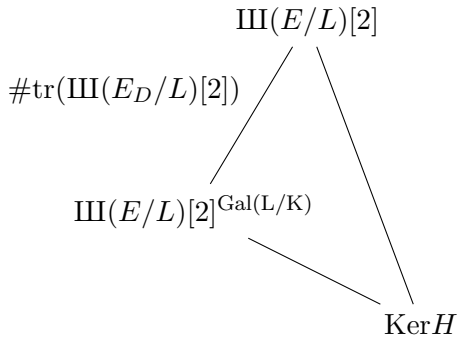


FIGURE 2. The gap between Ker$H$ and Ш$(E/L)[2]$

Lemma 4.8. — $\dfrac{\#Ш(E/L)[2]}{\#\mathrm{Ker}H} \geq \#\mathrm{tr}(Ш(E/L)[2])$.

Proof. — Since $\mathrm{Ker}H \subset Ш(E/L)[2]^{\mathrm{Gal}(L/K)} \subset Ш(E/L)[2]$ and

$$\frac{Ш(E/L)[2]}{Ш(E/L)[2]^{\mathrm{Gal}(L/K)}} \cong (\sigma - 1)Ш(E/L)[2] = \mathrm{tr}(Ш(E/L)[2]),$$

we obtain $\#Ш(E/L)[2] \geq \#\mathrm{tr}(Ш(E/L)[2])\#\mathrm{Ker}H$. □

By combining Lemma 4.7 and Lemma 4.8 and Proposition 4.6, we obtain

$$\begin{aligned}
\#Ш(E/L)[2] &\geq \#\mathrm{tr}(Ш(E/L)[2])\#\mathrm{Ker}H \quad \text{(by Lemma 4.8)} \\
&\geq \frac{\#Ш(E_D/K)[2]}{4^{\mathrm{rank}(E/K)}\#E(K)[2]^2\#2Ш(E/L)[4]}\#\mathrm{Ker}H \quad \text{(by Proposition 4.6)} \\
&\geq \frac{\#Ш(E/K)[2]\#Ш(E_D/K)[2]\#\bigoplus_{v\in M_K} H^1(\mathrm{Gal}(L_w/K_v), E(L_w))}{4^{\mathrm{rank}(E/K)}\#E(K)[2]^2\#j(\mathrm{Coker}F)\#H^1(\mathrm{Gal}(L/K), E(L))\#2Ш(E/L)[4]} \quad \text{(by Lemma 4.7).}
\end{aligned}$$

Because

$$\begin{aligned}
\#j(\mathrm{Coker}F) &\leq \#X = \#\mathrm{Sel}^2(E/K) \text{(by Theorem 3.3)} \\
&= \#\frac{E(K)}{2E(K)} \times \#Ш(E/K)[2] \text{(by exact sequence 1)} \\
&= \#E(K)[2] \times 2^{\mathrm{rank}(E/K)} \times \#Ш(E/K)[2]
\end{aligned}$$

holds, we obtain the following inequality.

Proposition 4.9. — Let E/K be an elliptic curve and let L/K be a quadratic field extension of a number field. Then,

$$\frac{\#Ш(E/L)[2]\#2Ш(E/L)[4]}{\#Ш(E_D/K)[2]} \geq \frac{1}{\#E(K)[2]^3 \times 2^{3\mathrm{rank}(E/K)}} \cdot \frac{\#\bigoplus_{v\in M_K} H^1(\mathrm{Gal}(L_w/K_v), E(L_w))}{\#H^1(\mathrm{Gal}(L/K), E(L))}$$

holds.

Theorem 4.10. — For arbitrary integer r and an elliptic curve over $\mathbb{Q}$, there exist infinitely many quadratic fields $\mathbb{Q}(\sqrt{D})$ such that

$$\frac{\#Ш(E/\mathbb{Q}(\sqrt{D}))[2]\#2Ш(E/\mathbb{Q}(\sqrt{D}))[4]}{\#Ш(E_D/\mathbb{Q})[2]} \geq r.$$

Proof. — Proposition 4.9 states that the unboundedness of $g(D)$ implies the unboundedness of $\dfrac{\#Ш(E/\mathbb{Q}(\sqrt{D}))[2]\#2Ш(E/\mathbb{Q}(\sqrt{D}))[4]}{\#Ш(E_D/\mathbb{Q})[2]}$. Remark 3.9 states that $g(D)$ is indeed unbounded when $K = \mathbb{Q}$. Therefore, we can conclude that $\dfrac{\#Ш(E/\mathbb{Q}(\sqrt{D}))[2]\#2Ш(E/\mathbb{Q}(\sqrt{D}))[4]}{\#Ш(E_D/\mathbb{Q})[2]}$ is unbounded above. □

Remark 4.11. — In this paper, we restrict our consideration to the case of the 2-torsion subgroup of the Tate–Shafarevich group. This focus is motivated by the fact that $\#Ш(E/\mathbb{Q}(\sqrt{D})[n] = \#Ш(E_D/\mathbb{Q})[n]\#Ш(E/\mathbb{Q})[n]$ where n is an odd number. This is because $\mathrm{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$ acts on the odd abelian group $Ш(E/\mathbb{Q}(\sqrt{D}))[n]$, and thus $Ш(E/\mathbb{Q}(\sqrt{D}))[n]$ decomposes into a direct sum of $Ш(E/\mathbb{Q}(\sqrt{D}))[n]^+ := \{a \in Ш(E/\mathbb{Q}(\sqrt{D}))[n] \mid \sigma * a = a\} = Ш(E/\mathbb{Q})[n]$ and $Ш(E/L)[n]^- := \{a \in Ш(E/\mathbb{Q}(\sqrt{D}))[n] \mid \sigma * a = -a\}$. For the definition of the action denoted by $*$, see Definition 4.1. The isomorphism $Ш(E/\mathbb{Q}(\sqrt{D}))[n]^- \cong Ш(E_D/\mathbb{Q})[n]$ follows from the commutative diagram in the proof of Proposition 4.6 and the isomorphism $Ш(E_D/\mathbb{Q}(\sqrt{D}))[n]^{\mathrm{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})} \cong Ш(E_D/\mathbb{Q})[n]$.

Remark 4.12. — Let K be a number field and E/K be an elliptic curve over K. Let $L = K(\sqrt{D})$ be a quadratic extension of K. H. Yu explicitly expressed the formula for $\#Ш(E/L)$ under the assumption that the Tate–Shafarevich group of elliptic curves over K are finite, that is,

$$\frac{\#Ш(E/L)}{\#Ш(E_D/K)} = \frac{\#Ш(E/K)}{\#\mathrm{Coker}(\mathrm{trace} : E(L) \to E(K))} \cdot \frac{\#\bigoplus_{v\in M_K} H^1(\mathrm{Gal}(L_w/K_v), E(L_w))}{\#H^1(\mathrm{Gal}(L/K), E(L))}$$

(see [[21], Main Theorem]).

Combining Yu's formula with Remark 3.9, we know that $\#Ш(E/\mathbb{Q}(\sqrt{D}))/\#Ш(E_D/\mathbb{Q})$ is unbounded from above under the assumption that Tate–Shafarevich group of elliptic curves are finite.

Compare the following diagram from Yu's paper with the Figure 1.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \mathrm{Ker}F' & \longrightarrow & Ш(E/K) & \longrightarrow & \mathrm{Ker}H' & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & H^1(\mathrm{Gal}(L/K), E(L)) & \xrightarrow{\inf} & H^1(G_K, E) & \xrightarrow{\mathrm{res}} & \mathrm{res}(H^1(G_K, E)) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle F'} & & \downarrow{\scriptstyle G'} & & \downarrow{\scriptstyle H'} & & \\
0 & \longrightarrow & \bigoplus_{v\in M_K} H^1(\mathrm{Gal}(L_w/K_v), E(L_w)) & \longrightarrow & \bigoplus_{v\in M_K} H^1(G_{K_v}, E) & \longrightarrow & \bigoplus_{v\in M_K} \mathrm{res}(H^1(G_{K_v}, E)) & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & \mathrm{Coker}F' & \xrightarrow{j} & \widehat{E(K)}^* & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

In this paper, X plays the role that $\widehat{E(K)}^*$ (Pontryagin dual of profinite completion of $E(K)$) plays in the diagram above. However, the explicit formula relating $\dfrac{\#Ш(E/L)[2]}{\#Ш(E_D/K)[2]}$ to $\dfrac{\#\bigoplus_{v\in M_K} H^1(\mathrm{Gal}(L_w/K_v), E(L_w))}{\#H^1(\mathrm{Gal}(L/K), E(L))}$, remains unknown.

Remark 4.13. — Whether the ratio $\dfrac{Ш(E/\mathbb{Q}(\sqrt{D}))[2]}{Ш(E_D/\mathbb{Q})[2]}$ can become arbitrarily large is a problem of interest, but no resolution has been reached. If one proves that $2Ш(E/\mathbb{Q}(\sqrt{D}))[4]$ does

not grow significantly compared to $\bigoplus_p H^1(\mathrm{Gal}(\mathbb{Q}_p(\sqrt{D})/\mathbb{Q}_p), E(\mathbb{Q}_p(\sqrt{D})))$, the proof will be complete.

Theorem 4.14 (*cf.* **Rohrlich [8]**). — For arbitrary integer $r \in \mathbb{Z}$ and arbitrary $E/\mathbb{Q}$, there exists a square free integer D such that $Ш(E_D/\mathbb{Q})[2] \geq r$.

Let us explain, in a simple case, how the D in Main Theorem Theorem 4.10 and Theorem 4.14 can be chosen compatibly.

Corollary 4.15. — For an arbitrary $r \in \mathbb{Z}$ and an arbitrary elliptic curve $E/\mathbb{Q} : y^2 = x^3 + ax^2 + bx$ with the condition $\dfrac{b}{a^2-4b} \notin \mathbb{Q}^{\times 2}$, there exists a square-free integer D such that $\dfrac{\#Ш(E/\mathbb{Q}(\sqrt{D}))[2]\#2Ш(E/\mathbb{Q}(\sqrt{D}))[4]}{Ш(E_D/\mathbb{Q})[2]} \geq r$ and $\#Ш(E_D/\mathbb{Q})[2] \geq r$.

Proof. — $E/\mathbb{Q}$ has a Weierstrass form $E : y^2 = x^3 + ax^2 + bx$ and let E' be $E' : y^2 = x^3 - 2ax^2 + (a^2-4b)x$. Let $\phi : E \to E'$ be $(x,y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2}\right)$ be degree 2 isogeny and $\hat{\phi}$ be its dual.

The following inequality holds because there exists an exact sequence: $0 \to E'(\mathbb{Q})[\hat{\phi}]/\phi(E(\mathbb{Q})[2]) \to \mathrm{Sel}^{\phi}(E/\mathbb{Q}) \to \mathrm{Sel}^2(E/\mathbb{Q})$ (see [17], lemma 9.1).

$$\#Ш(E_D/\mathbb{Q})[2] = \frac{\#\mathrm{Sel}^2(E_D/\mathbb{Q})}{\#E_D(\mathbb{Q})/2E_D(\mathbb{Q})} \geq \frac{\#\mathrm{Sel}^{\phi}(E_D/\mathbb{Q})}{\#\mathrm{Sel}^{\hat{\phi}}(E'_D/\mathbb{Q})} \times \frac{1}{2 \times 2^{\mathrm{rank}(E_D/\mathbb{Q})} \times E(\mathbb{Q})[2]}.$$

Here, $\dfrac{\#\mathrm{Sel}^{\phi}(E_D/\mathbb{Q})}{\#\mathrm{Sel}^{\hat{\phi}}(E'_D/\mathbb{Q})}$ is what we call the Tamagawa ratio. By Theorem 2.2 of [9],

$$\frac{\#\mathrm{Sel}^{\phi}(E_D/\mathbb{Q})}{\#\mathrm{Sel}^{\hat{\phi}}(E'_D/\mathbb{Q})} \geq \prod_{p|D \text{ and } p\nmid\Delta_E} \frac{1}{2}\#\frac{E'_D(\mathbb{Q}_p)[2]}{\phi(E_D(\mathbb{Q}_p)[2])}$$

holds. Let $h(D) \coloneqq \prod_{p|D \text{ and } p\nmid\Delta_E} \frac{1}{2}\#\frac{E'_D(\mathbb{Q}_p)[2]}{\phi(E_D(\mathbb{Q}_p)[2])}$, it is sufficient to prove $\forall r \in \mathbb{Z}, \exists D$: square free such that $\dfrac{h(D)}{2^{\mathrm{rank}(E_D/\mathbb{Q})}} \geq r$ and $g(D) = \dfrac{\bigoplus_{p\in M_{\mathbb{Q}}} H^1(\mathrm{Gal}(\mathbb{Q}_p(\sqrt{D})/\mathbb{Q}_p), E(\mathbb{Q}_p(\sqrt{D}))}{2^{\mathrm{rank}(E_D/\mathbb{Q})}} \geq r$.

The calculation of $\#\dfrac{E'_D(\mathbb{Q}_p)[2]}{\phi(E_D(\mathbb{Q}_p)[2])}$ is as follows.

- When $E(\mathbb{Q}_p)[2] \cong \mathbb{Z}/2\mathbb{Z}$ and $E'(\mathbb{Q}_p)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\#\dfrac{E'_D(\mathbb{Q}_p)[2]}{\phi(E_D(\mathbb{Q}_p)[2])} = 4$.
- When $E(\mathbb{Q}_p)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $E'(\mathbb{Q}_p)[2] \cong \mathbb{Z}/2\mathbb{Z}$, $\#\dfrac{E'_D(\mathbb{Q}_p)[2]}{\phi(E_D(\mathbb{Q}_p))[2]} = 1$.
- When $E(\mathbb{Q}_p)[2] \cong \mathbb{Z}/2\mathbb{Z}$ and $E'(\mathbb{Q}_p)[2] \cong \mathbb{Z}/2\mathbb{Z}$ or $E(\mathbb{Q}_p)[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$ and $E'(\mathbb{Q}_p)[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$, $\#\dfrac{E'_D(\mathbb{Q}_p)[2]}{\phi(E_D(\mathbb{Q}_p)[2])} = 2$.

For arbitrary $r \in \mathbb{Z}$, let us take R such that $2^{R-4} \geq r$. By the condition $\dfrac{b}{a^2-4b} \notin \mathbb{Q}^{\times 2}$, $\mathbb{Q}(E[2]) \neq \mathbb{Q}(E'[2])$. By the Chebotarev density theorem, there exist infinitely many primes p that satisfy the following conditions:

(1) p does not split completely in $\mathbb{Q}(E[2])/\mathbb{Q}$, then, $E(\mathbb{Q}_p)[2] \cong \mathbb{Z}/2\mathbb{Z}$
(2) p splits completely in $\mathbb{Q}(E'[2])/\mathbb{Q}$, then, $E'(\mathbb{Q}_p)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Take $p_1, \cdots, p_R$ that satisfy the conditions (1) and (2). Take prime numbers $l_1, \cdots, l_R$ that satisfy the conditions $E(\mathbb{Q}_{l_i})[2] \cong \mathbb{Z}/2\mathbb{Z}$ and l_i is a good prime of $E/\mathbb{Q}$. There exists a square-free integer D_R with prime factors no greater than 4 such that $\mathrm{rank}(E_D/\mathbb{Q}) = 0$, where $D = p_1 \cdots p_R l_1 \cdots l_R D_R$ by Theorem 3.7. For this D, $\dfrac{h(D)}{2^{\mathrm{rank}(E_D/\mathbb{Q})}} \geq r$ and $g(D) \geq r$ hold.

□

5. Decreasing $Ш(E/\mathbb{Q}(\sqrt{D}))[2]$ and $Ш(E_D/\mathbb{Q})[2]$

In this section, we prove that for a prime p, there exist infinitely many quadratic fields $K = \mathbb{Q}(\sqrt{D})$ for the elliptic curve $E : y^2 = x^3 + px$, such that $Ш(E_D/\mathbb{Q})[2] = 0$ and $\#Ш(E/K)[2] \leq 4$ respectively under the assumption that Tate–Shafarevich group is finite.

Let us recall the theory of the descent using the two 2-isogenies ϕ and $\hat{\phi}$ as described in [18]. Let E/K be an elliptic defined by $E : y^2 = x^3 + ax (a \in \mathbb{Z})$. Let $E' : y^2 = x^3 - 4ax$. Let $\phi : E \to E'$ be $(x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(a-x^2)}{x^2}\right)$ be degree 2 isogeny and $\hat{\phi}$ be its dual. Let

$$S_{E/K} \coloneqq \{v \in M_K : E \text{ has bad reduction at } v, \text{infinite places}\}.$$

When we fix $E/\mathbb{Q}$, $\#S$ depends on K. Let $H^1(G_K, E[\phi]; S)$ be

$$H^1(G_K, E[\phi]; S) \stackrel{\text{def}}{=} \{[\sigma] \in H^1(G_K, E[\phi]) \mid \sigma \text{ is unramified outside } S\}$$

where unramified outside S means restriction of σ to inertia group $I_v \coloneqq \mathrm{Gal}(\overline{{K_v}^{nr}}/{K_v}^{\mathrm{nr}})$ at $v \notin S$ is trivial. The Selmer group $K(S, 2)$ of a field, which is a finite group, is defined as

$$K(S, 2) \stackrel{\text{def}}{=} \{\bar{d} \in K^\times/{K^\times}^2 \mid v(d) \equiv 0 \bmod 2, \forall v \notin S\}$$

The Selmer group $\mathrm{Sel}^\phi(E/K)$ is embedded into $K(S, 2)$ via

$$\mathrm{Sel}^\phi(E/K) \subset H^1(G_K, E[\phi]; S) \cong K(S, 2)$$

where the last isomorphism $K(S, 2) \cong H^1(G_K, E[\phi]; S)$ is given by $\overline{d} \mapsto [f_d : \sigma \mapsto \frac{\sqrt{d}^\sigma}{\sqrt{d}}]$. Here, $(-)^\sigma$ denotes the action of $\sigma \in G_K$ on elements of $\overline{K}$. Note that f_d is unramified outside S if only if $v(d) \equiv 0 \mod 2$ for $v \notin S$. Here, note that we identify $E[\phi] \cong \mu_2$ as a trivial G_K-module.

Let C_d be the image of $\overline{d}$ by the composition $K(S, 2) \cong H^1(G_K, E[\phi]; S) \subset H^1(G_K, E[\phi]) \twoheadrightarrow WC(E/K)[\phi]$. [[18], Proposiiton 4.9] shows that C_d is isomorphic over K to a projective closure of $dy^2 = d^2 - 4ax^4$ in $\mathbb{P}_K(1, 2, 1)$. The Selmer group is cut out from $K(S, 2)$ by the condition that corresponding torsors has a rational points locally at bad primes in S. Let C_d and C'_d be the curves defined by the equations $dy^2 = d^2 - 4ax^4$ and $dy^2 = d^2 + 16ax^4$, respectively. Then,

$$\mathrm{Sel}^\phi(E/K) \cong \left\{ \bar{d} \in K(S, 2) \;\middle|\; \begin{array}{l} C_d(K_v) \neq \emptyset, \forall v \in S, \\ C_d : dy^2 = d^2 - 4ax^4 \end{array} \right\}.$$

By replacing $a \mapsto -4a$, we obtain the following.

$$\mathrm{Sel}^{\hat{\phi}}(E'/K) \cong \left\{ \bar{d} \in K(S, 2) \;\middle|\; \begin{array}{l} C'_d(K_v) \neq \emptyset, \forall v \in S, \\ C'_d : dy^2 = d^2 + 16ax^4 \end{array} \right\}.$$

Remark 5.1. — When we write $C_d : dy^2 = d^2 - 4ax^4$, it precisely represents the projective curve obtained by embedding $dy^2 = d^2 - 4ax^4$ into the weighted projective space $\mathbb{P}(1, 2, 1)$. Simply taking the projective closure in $\mathbb{P}^2$ would result in a singular point at $[0 : 1 : 0]$, which cannot be adopted as a torsor. Therefore, to eliminate the singular point, we glue together two nonsingular affine curves, $C_0 : dy^2 = d^2 - 4ax^4$ and $C_1 : dv^2 = d^2u^4 - 4a$, using the relation $u = \frac{1}{x}, v = \frac{y}{x^2}$. Specifically, we embed these curves into $\mathbb{P}(1, 2, 1)$ as follows: $i : C_0 \to \mathbb{P}(1, 2, 1)$ given by $(x, y) \mapsto [x : y : 1]$ and $v : C_1 \to \mathbb{P}(1, 2, 1)$ given by $(u, v) \mapsto [1 : v : u]$. We then define the curve C_d in $\mathbb{P}_K(1, 2, 1)$ as $C_d = i(C_0) \cup v(C_1)$. The projective closure of affine part of C_d has two points

$$[1 : \pm\sqrt{\frac{-4a}{d}} : 0]$$

at infinity in $\mathbb{P}_K(1, 2, 1)$.

The following inequality gives an upper bound for the order of $Ш(E/K)[2]$.

Proposition 5.2. — Let E/K be an elliptic curve. Let $\phi : E \to E'$ be an isogeny of degree 2 and $\hat{\phi} : E' \to E$ be the dual isogeny of ϕ. The following inequality holds:

$$\dim_{\mathbb{F}_2} Ш(E/K)[2] \leq \dim_{\mathbb{F}_2} \mathrm{Sel}^{\phi}(E/K) + \dim_{\mathbb{F}_2} \mathrm{Sel}^{\hat{\phi}}(E'/K) - \dim_{\mathbb{F}_2} \frac{E'(K)[\hat{\phi}]}{\phi(E(K)[2])} - \dim_{\mathbb{F}_2} \frac{E(K)}{2E(K)}.$$

Proof. — There exists an exact sequence:

$$0 \to E'(K)[\hat{\phi}]/\phi(E(K)[2]) \to \mathrm{Sel}^{\phi}(E/K) \to \mathrm{Sel}^{2}(E/K) \xrightarrow{\phi} \mathrm{Sel}^{\hat{\phi}}(E'/K)$$

(see [[17], lemma 9.1]). Thus,

$$\dim_{\mathbb{F}_2} \mathrm{Sel}^{2}(E/K) \leq \dim_{\mathbb{F}_2} \mathrm{Sel}^{\phi}(E/K) + \dim_{\mathbb{F}_2} \mathrm{Sel}^{\hat{\phi}}(E'/K) - \dim_{\mathbb{F}_2} \frac{E'(K)[\hat{\phi}]}{\phi(E(K)[2])}. \tag{4}$$

Therefore,

$$\begin{aligned}
&\dim_{\mathbb{F}_2} Ш(E/K)[2] \\
&= \dim_{\mathbb{F}_2} \mathrm{Sel}^{2}(E/K) - \dim_{\mathbb{F}_2} \frac{E(K)}{2E(K)} \text{ (by exact sequence (1))} \\
&\leq \dim_{\mathbb{F}_2} \mathrm{Sel}^{\phi}(E/K) + \dim_{\mathbb{F}_2} \mathrm{Sel}^{\hat{\phi}}(E'/K) + \dim_{\mathbb{F}_2} \frac{E(K)}{2E(K)} - \dim_{\mathbb{F}_2} \frac{E'(K)[\hat{\phi}]}{\phi(E(K)[2])} \text{ (by inequality(4))}.
\end{aligned}$$

□

From this point forward, we will limit our discussion to elliptic curves of the form $E : y^2 = x^3 + px$ where p is a prime number. In this case, note that $\#E'_D(\mathbb{Q})[\hat{\phi}_D]/\phi_D(E_D(\mathbb{Q})[2]) = 2$.

Theorem 5.3 **(*cf.* Genus theory, [1, Theorem 8, p. 247]).** — Let $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field and Cl_K be the ideal class group of K. Then $\#\mathrm{Cl}_K[2] = 2^{r-1}$ holds where r is the number of prime factors of the discriminant of K.

Lemma 5.4. — Let p be an odd prime, and let $E : y^2 = x^3 + px$ be an elliptic curve.

Let $S \coloneqq S_{E/K}$. Suppose that an imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$ satisfies the following conditions: $|D| \neq p$ is a prime number such that $D \equiv 5 \bmod 8$ and p does not split in $K = \mathbb{Q}(\sqrt{D})/\mathbb{Q}$. Then, we have the following.

(1) $\#K(S,2) = 8$.
(2) Assume that $Ш(E/K)$ is finite. Then $\#Ш(E/K)[2] \leq 4$.

Proof. — (1) Define a group of S-units as $O_{K,S}{}^{\times} \overset{\text{def}}{=} \{a \in K \mid v(a) = 0, \forall v \notin S\}$ and define the S-ideal class group $\mathrm{Cl}(K,S)$ as the ideal class group of $O_{K,S}$. There is the following exact sequence ([15], Proposion 12.6):

$$1 \to O_{K,S}{}^{\times}/O_{K,S}{}^{\times 2} \to K(S,2) \to \mathrm{Cl}(K,S)[2] \to 1.$$

To prove $\#K(S,2) = 8$, let us prove $\mathrm{Cl}(K,S) = 1$ and $\#O_{K,S}^{\times}/O_{K,S}^{\times}{}^2 = 8$. Because $|D|$ is a prime, $\mathrm{Cl}_K[2] = 1$ by Theorem 5.3. Hence, Cl_K is an abelian group of odd order. There is a surjection from Cl_K to $\mathrm{Cl}(K,S)$. Therefore, the order of $\mathrm{Cl}(K,S)$ is odd. Hence, $\mathrm{Cl}(K,S)[2] = 1$.

Let us consider $O_{K,S}{}^{\times}/O_{K,S}^{\times}{}^2$. From Dirichlet's S-unit theorem, $O_{K,S}{}^{\times} \cong \mu(K) \times \mathbb{Z}^{\#S-1}$ where $\mu(K)$ is the group of roots of unity. Since $D \equiv 5 \bmod 8$, 2 does not split in K, and p does not split in K by hypothesis, $\#S = 3$. Since $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, $\mu(K) = \{\pm 1\}$. From the above, $O_{K,S}{}^{\times}/O_{K,S}^{\times}{}^2 \cong (\mathbb{Z}/2\mathbb{Z})^3$. Therefore, $\#K(S,2) = \#O_{K,S}{}^{\times}/O_{K,S}^{\times}{}^2 \times \#\mathrm{Cl}(K,S)[2] = 8$ holds. □

(2) Let $\dim_{\mathbb{F}_2}\mathrm{Sel}^{\phi}(E/K) = a$ and $\dim_{\mathbb{F}_2}\mathrm{Sel}^{\hat{\phi}}(E'/K) = b$. By (1), $a, b \leq 3$. The $\hat{\phi}$-Selmer group is,

$$\mathrm{Sel}^{\hat{\phi}}(E'/K) \cong \{\bar{d} \in K(S,2) \mid C'_d(\mathbb{Q}_p) \neq \emptyset, \forall p \in \{2, p, \infty\}\}.$$

When $D \equiv 5 \bmod 8$, $C'_2 : 2y^2 = 4 + px^4$ does not have a root in $\mathbb{Q}_2(\sqrt{D}) = \mathbb{Q}_2(\sqrt{5})$. Note that $\mathbb{Q}_2(\sqrt{5}) = \mathbb{Q}_2(\zeta_3)$ is an unramified extension of $\mathbb{Q}_2$, thus 2-adic valuation v_2 takes integer

valuation. If C_2' had a $\mathbb{Q}_2(\sqrt{5})$-rational point (x, y), looking at the 2-adic valuation v_2 of both sides, we obtain $1 + 2v_2(y) = \min\{2, 4v_2(x)\}$. But the left-hand side is odd and the right-hand side is even, which is a contradiction. Also, points at infinity of C_2' are $[1 : \pm 4\sqrt{\frac{p}{2}} : 0] = [1 : \pm 4\sqrt{2p} : 0]$ by Remark 5.1. Because $\sqrt{2p} \notin \mathbb{Q}_2(\sqrt{5})$, there are no points at infinity. Thus, we obtain that $2 \notin \mathrm{Sel}^{\hat{\phi}}(E'/K)$. Thus, $b \leq 2$, we can conclude $\dim_{\mathbb{F}_2} Ш(E/K)[2] \leq a+b-1-1 \leq 3$ by Proposition 5.2. Because $\dim_{\mathbb{F}_2} Ш(E/K)[2]$ is even when $Ш(E/K)$ is finite (see [[18], Section X, Remark 6.3]), $\dim_{\mathbb{F}_2} Ш(E/K)[2] \leq 2$ holds.

□

Lemma 5.5. — Let p be an odd prime, and let $E : y^2 = x^3 + px$ be an elliptic curve.

(1) When $p \equiv 1 \bmod 4$, we take an imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$ that satisfies the following conditions:
- $l := -D \neq p$ is a prime number,
- $D \equiv 1 \bmod 4$,
- p does not split in $K = \mathbb{Q}(\sqrt{D})/\mathbb{Q}$.

Assume that $Ш(E_D/\mathbb{Q})$ is finite. Then, $Ш(E_D/\mathbb{Q})[2] = 0$.

(2) When $p \equiv 3 \bmod 4$, we take an imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$ that satisfies the following conditions:
- $l := -D \neq p$ is a prime number,
- $D \equiv 3 \bmod 4$,
- p splits in $K = \mathbb{Q}(\sqrt{D})/\mathbb{Q}$.

Assume that $Ш(E_D/\mathbb{Q})$ is finite. Then, $Ш(E_D/\mathbb{Q})[2] = 0$.

Proof. — First, let us establish the common preliminary setup for both cases (1) and (2). Let $S' := S_{E_D/\mathbb{Q}}$. Since $-D$ is a prime number, $S' = \{2, p, -D, \infty\}$ and

$$\#\mathbb{Q}(S', 2) = \#\{(-1)^{n_1} 2^{n_2} p^{n_3} (-D)^{n_4} \mid 0 \leq n_1, n_2, n_3, n_4 \leq 1\} = 16.$$

Let $\phi_D : E_D \to E_D', (x, y) \mapsto (\frac{y^2}{x^2}, \frac{y(aD^2-x^2)}{x^2})$ be a degree 2 isogeny and $\hat{\phi}_D$ be dual isogeny. Let $\dim_{\mathbb{F}_2} \mathrm{Sel}^{\phi_D}(E_D/\mathbb{Q}) = e, \dim_{\mathbb{F}_2} \mathrm{Sel}^{\hat{\phi}_D}(E_D'/\mathbb{Q}) = f$. Since $\#\mathbb{Q}(S', 2) = 16, e, f \leq 4$.

Let $T_d : dy^2 = d^2 - 4pD^2x^4$ and $T_d' : dy^2 = d^2 + pD^2x^4$.

The ϕ_D-Selmer group and $\hat{\phi}_D$-Selmer group are as follows:

$$\mathrm{Sel}^{\phi_D}(E_D/\mathbb{Q}) \cong \left\{ \bar{d} \in \mathbb{Q}(S', 2) \mid T_d(\mathbb{Q}_v) \neq \emptyset, \forall v \in \{2, p, \infty\} \right\},$$

$$\mathrm{Sel}^{\hat{\phi}_D}(E_D'/\mathbb{Q}) \cong \left\{ \bar{d} \in \mathbb{Q}(S', 2) \mid T_d'(\mathbb{Q}_v) \neq \emptyset, \forall v \in \{2, p, \infty\} \right\}.$$

For curves T_d and T_d', we first determine their points at infinity: By Remark 5.1, the points at infinity of T_d are $[1 : \pm 2D\sqrt{\frac{-p}{d}} : 0]$. Similarly, the points at infinity of T_d' are $[1, \pm D\sqrt{\frac{p}{d}}, 0]$.

For both (1) and (2), $\left(\frac{p}{l}\right) = -1$ holds true. Indeed, when $p \equiv 1 \bmod 4$, since p does not split in $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$, $\left(\frac{D}{p}\right) = -1$, and from the quadratic reciprocity law, $\left(\frac{l}{p}\right) \cdot \left(\frac{p}{l}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{l-1}{2}} = (-1)^{\frac{p-1}{2}}$ and $\left(\frac{l}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)$, we obtain $\left(\frac{p}{l}\right) = -1$. When $p \equiv 3 \bmod 4$, $\left(\frac{D}{p}\right) = 1$, and from the quadratic reciprocity law, $\left(\frac{l}{p}\right) \cdot \left(\frac{p}{l}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{l-1}{2}} = 1$ and $\left(\frac{l}{p}\right) = (-1)^{\frac{p-1}{2}} = -1$, we obtain $\left(\frac{p}{l}\right) = -1$.

We prove that $T_D : y^2 = D - 4pDx^4, T_{pD} : y^2 = pD - 4Dx^4, T_{2pD} : y^2 = 2pD - 2Dx^4, T_{2D} : y^2 = 2D - 2pDx^4$ do not have $\mathbb{Q}_l$-rational points. For each curve, if there exists a $\mathbb{Q}_l$-rational point (x, y), then the Hilbert symbol $(A, B)_l$ of $A(x^2)^2 + By^2 = 1$ must be 1. We compute the Hilbert symbols mod l for these quadratic forms: For T_D : $(\frac{1}{D}, 4p)_l = (p, D)_l$. For T_{pD} : $(\frac{1}{pD}, \frac{4}{p})_l = (pD, p)_l = (p, D)_l$. For T_{2pD} : $(\frac{1}{2pD}, \frac{1}{p})_l = (2pD, p)_l = (p, D)_l$. For

$T_{2D} : (\frac{1}{2D}, p)_l = (2D, p)_l = (p, D)_l$. Since $\left(\frac{p}{l}\right) = -1$, we have $(p, D)_l = -1$. Therefore, all the above Hilbert symbols equal -1, which proves that none of these curves have $\mathbb{Q}_l$-rational points in the affine part. Moreover, there are no points at infinity because $\sqrt{pl}, \sqrt{l}, \sqrt{2l}, \sqrt{2pl} \notin \mathbb{Q}_l$. As a consequence, we conclude that $D, pD, 2pD, 2D \notin \mathrm{Sel}^{\phi_D}(E_D/\mathbb{Q})$.

Note that $-p \in \mathrm{Sel}^{\phi_D}(E_D/\mathbb{Q})$ since the points at infinity are $[1 : \pm 2D : 0]$. Therefore, $-pD, -D, -2D, -2pD \notin \mathrm{Sel}^{\phi_D}(E_D/\mathbb{Q})$. Since we have determined that 8 out of 16 elements of $\mathbb{Q}(S', 2)$ do not belong to $\mathrm{Sel}^{\phi_D}(E_D/\mathbb{Q})$, if we can show that one of the remaining T_d has no $\mathbb{Q}_v$-rational point for some $v \in S'$, then we can prove that $e \leq 2$.

Let evaluate f. When $d < 0$, $T'_d(\mathbb{R}) = \emptyset$. Thus, $d \notin \mathrm{Sel}^{\hat{\phi}_D}(E_D/\mathbb{Q})$. Affine parts of $T'_2 : 2y^2 = 4 + pD^2x^4$, $T'_{2pl} : 2y^2 = 4pl + lx^4$ and $T'_{2p} : 2y^2 = 4p + D^2x^4$ do not have $\mathbb{Q}_2$-rational points because $1 + 2\mathrm{ord}_2(y) = \min\{2, 4\mathrm{ord}_2(x)\}$ does not hold. Also, note that $T'_2, T'_{2p}, T'_{2l}, T'_{2pl}$ do not have points at infinity since either $\sqrt{2p}, \sqrt{2}, \sqrt{2pl}$ nor $\sqrt{2l}$ do not belong to $\mathbb{Q}_2$. Since we have shown that 12 out of 16 elements do not belong to $\mathrm{Sel}^{\hat{\phi}_D}(E'_D/\mathbb{Q})$, $f \leq 2$, if we can show that one of the remaining T_d has no $\mathbb{Q}_v$-rational point for some $v \in S'$, then we can prove that $f \leq 1$.

In what follows, we prove that both e and f can be reduced by 1 in each of cases (1) and (2).

(1) Let us evaluate e. We claim that $T_{-1} : y^2 = -1 + 4pl^2x^4$ does not have $\mathbb{Q}_l$-rational points. Indeed, when $x, y \in \mathbb{Z}_l$, $y^2 \equiv -1 \bmod l$ does not hold since $\left(\frac{-1}{l}\right) = -1$. When $v_l(x) < 0$, $v_l(y) = 1 + 2v_l(x)$. Set $v_l(x) \coloneqq -a$ $(a > 0)$. We can put $x = l^{-a}x'$, $y = l^{1-2a}y'$ where $x', y' \in {\mathbb{Z}_l}^{\times}$. We obtain $y'^2 = -l^{4a-2} + 4px'^4$ and p should be a square modulo l. This contradicts the fact that $\left(\frac{p}{l}\right) = -1$. Thus, $v_l(x) \geq 0$. In this case, $x, y \in \mathbb{Z}_l$ and we have already shown that there are no $\mathbb{Q}_l$-rational points in this case. There are no points at infinity since $\sqrt{p} \notin \mathbb{Q}_l$. Therefore, $-1 \notin \mathrm{Sel}^{\hat{\phi}_D}(E'_D/\mathbb{Q})$. Since we have shown that 9 out of 16 elements do not belong to $\mathrm{Sel}^{\hat{\phi}_D}(E'_D/\mathbb{Q})$, we can conclude that $e \leq 2$.

Let us evaluate f. We claim that $T'_l(\mathbb{Q}_p) = \emptyset$ where $T'_l : y^2 = l + plx^4$. Indeed, When $p \equiv 1 \bmod 4$, $\left(\frac{1}{l}, -p\right)_p = (-1)^{\frac{p+1}{2}} = -1$ and there are no points at infinity since $\sqrt{-pl} \notin \mathbb{Q}_p$. Thus, $l \notin \mathrm{Sel}^{\hat{\phi}_D}(E'_D/\mathbb{Q})$. Since we have shown that 13 out of 16 elements do not belong to $\mathrm{Sel}^{\hat{\phi}_D}(E'_D/\mathbb{Q})$, we can conclude that $f \leq 1$. Thus, $\dim_{\mathbb{F}_2} Ш(E_D/\mathbb{Q})[2] \leq e + f - 1 - 1 \leq 2 + 1 - 1 - 1 = 1$. Because $\dim_{\mathbb{F}_2} Ш(E_D/\mathbb{Q})[2]$ is even, $\dim_{\mathbb{F}_2} Ш(E_D/\mathbb{Q})[2] = 0$ holds. Thus, $\dim_{\mathbb{F}_2} Ш(E_D/\mathbb{Q})[2] \leq e + f - 1 - 1 \leq 2 + 1 - 1 - 1 = 1$. Since $\dim_{\mathbb{F}_2} Ш(E_D/\mathbb{Q})[2]$ is even (see [[18], Remark 6.3]), $\dim_{\mathbb{F}_2} Ш(E_D/\mathbb{Q})[2] = 0$ holds.

(2) Let us evaluate e. We claim that $T_{-1}(\mathbb{Q}_l) = \emptyset$ where $T_{-1} : y^2 = -1 + 4pl^2x^4$. Indeed, Hilbert symbol $\left(-1, 4pl^2\right)_p = (-1, p)_p = (-1)^{\frac{p-1}{2}} = -1$ and there is no points at infinity because $\sqrt{p} \notin \mathbb{Q}_l$. Since we have shown that 9 out of 16 elements do not belong to $\mathrm{Sel}^{\hat{\phi}_D}(E'_D/\mathbb{Q})$, we can conclude that $e \leq 2$.

Let us evaluate f. Since $l \equiv 1 \bmod 4$, affine part of $T'_l : y^2 = l + plx^4$ does not have $\mathbb{Q}_l$-rational points because $\left(-p, \frac{1}{l}\right)_l = (-p, l)_l = \left(\frac{p}{l}\right)\left(\frac{-1}{l}\right) = -(-1)^{\frac{l-1}{2}} = -1$. Also, note that T'_l does not have $\mathbb{Q}_l$-rational points at infinity because $\sqrt{pl}$ does not belong to $\mathbb{Q}_l$. Since we have shown that 13 out of 16 elements do not belong to $\mathrm{Sel}^{\hat{\phi}_D}(E'_D/\mathbb{Q})$, $f \leq 1$. Thus, $\dim_{\mathbb{F}_2} Ш(E_D/\mathbb{Q})[2] \leq e + f - 1 - 1 \leq 2 + 1 - 1 - 1 = 1$. Since $\dim_{\mathbb{F}_2} Ш(E_D/\mathbb{Q})[2]$ is even, $\dim_{\mathbb{F}_2} Ш(E_D/\mathbb{Q})[2] = 0$ holds.

□

Proposition 5.6. — Let p be an odd prime, and let $E : y^2 = x^3 + px$ be an elliptic curve. Assume that Tate–Shafarevich group of elliptic curves are finite.

(1) There exist infinitely many imaginary quadratic fields $K = \mathbb{Q}(\sqrt{D})$ such that $\#Ш(E/K)[2] \leq 4$. If $Ш(E/\mathbb{Q})$ contains an element of order 4, then for any quadratic number field $K = \mathbb{Q}(\sqrt{D})$, $\#Ш(E/K)[2] \neq 0$.
(2) There exist infinitely many square-free integers D such that $Ш(E_D/\mathbb{Q})[2] = 0$.

Proof. — (1) By Lemma 5.4, this holds because there exist infinitely many prime numbers $-D$ such that $D \equiv 5 \bmod 8$ and p does not split in $K = \mathbb{Q}(\sqrt{D})/\mathbb{Q}$.

Let $C \in Ш(E/\mathbb{Q})$ be an element of order 4. If C is trivial in $Ш(E/\mathbb{Q}(\sqrt{D}))$ for some D, the order (period), which is 4, would have to divide index, which is 2. This is a contradiciton. Thus any K cannot trivialize C in $Ш(E/K)$. This implies $Ш(E/K)$ has an element of order 2.

(2) By Lemma 5.5, this holds because there exist infinitely many prime numbers $-D$ such that $D \equiv 3 \bmod 4$ and p splits in $K = \mathbb{Q}(\sqrt{D})/\mathbb{Q}$. Also, there exist infinitely many prime numbers $-D$ such that $D \equiv 1 \bmod 4$ and p does not split in $K = \mathbb{Q}(\sqrt{D})/\mathbb{Q}$. □

Example 5.7. — Let $p = 17$. Using MAGMA [2], we compute:

```
K<b>:=QuadraticField(-2);
A:=EllipticCurve([K!0,0,0,17,0]);
Sel2:=TwoSelmerGroup(A); Sel2;
Q := QuadraticTwist(A, -2); // Compute the quadratic twist of A by -2
rank := Rank(Q); // Calculate the rank of the quadratic twist rank;
```

This computation shows that $E : y^2 = x^3 + 17x$ satisfies $Ш(E/\mathbb{Q}(\sqrt{-2}))[2] = 0$. Also, $Ш(E/\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ holds (see [[18], Proposition 6.5]). By the contrapositive of Proposition 5.4 (2), $Ш(E/\mathbb{Q})[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Example 5.8. — Let $p = 257$ be the fourth Fermat prime. Using MAGMA [2], we compute:

```
A := EllipticCurve([0,0,0,257,0]);
MordellWeilShaInformation(A: ShaInfo := true);
```

This computation shows that the Tate–Shafarevich group $Ш(E/\mathbb{Q})$ of the elliptic curve $E : y^2 = x^3 + 257x$ has an element of order 4. Thus, by Proposition 5.6 (2), there exists no quadratic field $\mathbb{Q}(\sqrt{D})$ such that $Ш(E/\mathbb{Q}(\sqrt{D}))[2] = 0$.

Remark 5.9. — It remains unknown whether there exist finite extensions $L/\mathbb{Q}$ such that $Ш(E/L)[2] = 0$.

References

[1] I. Borevich, I. R. Shafarevich, Number theory. Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20 Academic Press, New York-London 1966.

[2] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., 24 (1997), 235-265.

[3] J.W.S. Cassels, Arithmetic on curves of genus 1. VII. The dual exact sequence. Journal für die reine und angewandte Mathematik 216: 150-158, 1964.

[4] P. L. Clark and S. Sharif, Period, index and potential Sha. Algebra and Number Theory 4, No. 2, 151-174, 2010.

[5] J. Coates, R. Sujatha: Galois Cohomology of Elliptic Curves. Tata Institute of Fundamental Research/Narosa Publication House, Mumbai, 2000.

[6] E. V. Flynn and C. Grattoni. Descent via isogeny on elliptic curves with large rational torsion subgroups. Journal of Symbolic Computation, 43(4):293–303, 2008.

[7] K. Haberland, Galois cohomology of algebraic number fields, Deutscher Verlag der Wissenschaften, Berlin , 1978.

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

[9] Z. Klagsbrun, R.J.L. Oliver, The Distribution of 2-Selmer Ranks of quadratic twists of elliptic curves with paritial two-torsion. Mathematika;62(1):67-78, 2016.

[10] V. A. Kolyvagin, Finiteness of $E(Q)$ and $Ш(E/Q)$ for a class of Weil curves, Math.USSR Izvestiya 32, 523-541, 1989.

[11] K. Matsuno, Elliptic curves with large Tate–Shafarevich groups over a number field, Math. Research Letters 16, no. 3, 449–461, 2009.

[12] B. Mazur, Rational points of Abelian varieties with values in towers of number fields, Invent. math, 18, 183-266, 1972.

[13] J. S. Milne, Arithmetic Duality Theorems, 2nd edition, BookSurge, LLC, 2006.

[14] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of number fields (Die Grundlehren der mathematischen Wissenschaften, v. 323) Springer, c2008 2nd ed. Corr. 2nd printing, 2013.

[15] B. Poonen, and Edward F. Schaefer, Explicit descent for Jacobians of cyclic coevers of the projective line. Journal für die reine und angewandte Mathematik 488 : 141-188, 1997.

[16] D. Qiu, On Quadratic Twists of Elliptic Curves and Some Applications of a Refined Version of Yu's Formula, Communications in Algebra, 42(12), 5050–5064, 2014.

[17] E. F. Schaefer and M. Stoll. How to do a p-descent on an elliptic curve. Trans. Amer. Math. Soc. 356 (2004), 1209–1231.

[18] J. H. Silverman, The arithmetic of elliptic curves, Springer, 2nd edition 2009.

[19] J. Tate, WC-group over p-adic fields, Séminaire Bourbaki, 1957–58, exposé 156.

[20] C. Wuthrich, Selmer groups [Lecture notes], University of Nottingham (2022), https://www.maths.nottingham.ac.uk/plp/pmzcw/download/baskerville_selmer_groups.pdf

[21] H. Yu, On Tate-Shafarevich groups over Galois extensions, Israel Journal of Mathematics. 141, 211–220, 2004.

[22] M. Yu , Large Shafarevich-Tate groups over quadratic number fields, Journal of Number Theory, 199, 98-109, 2019.

Asuka Shiga

,

Mathematical Institute, Graduate School of Science,
Tohoku University, 6-3 Aramakiaza, Aoba, Sendai, Miyagi 980-8578, Japan.
E-mail : otheiio323.com@gmail.com