이학박사 학위논문

Twists of elliptic curves
(타원곡선의 비틀림곡선)

2014년 8월

서울대학교 대학원

수리과학부

김 나 영

Twists of elliptic curves
(타원곡선의 비틀림곡선)

지도교수 변동호

이 논문을 이학박사 학위논문으로 제출함

2014년 4월

서울대학교 대학원

수리과학부

김 나 영

김 나 영의 이학박사 학위논문을 인준함

2014년 4월

위 원 장 조 영 현 (인)

부 위 원 장 변 동 호 (인)

위 원 강 석 진 (인)

위 원 오 병 권 (인)

위 원 김 창 헌 (인)

Twists of elliptic curves

A dissertation

submitted in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

to the faculty of the Graduate School of
Seoul National University

by

Nayoung Kim

Dissertation Director : Professor Dongho Byeon

Department of Mathematical Science
Seoul National University

August 2014

Abstract

Twists of elliptic curves

Nayoung Kim

Department of Mathematical Sciences

The Graduate School

Seoul National University

In this thesis, we investigate various properties of twists of elliptic curves.

First, let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$. Let D be a square-free integer and E^D the D-quadratic twist of E. In this thesis, we show that there are infinitely many elliptic curves $E/\mathbb{Q}$ such that for a positive portion of D, E^D has rank zero and satisfies the 3-part of the Birch and Swinnerton-Dyer conjecture. Previously only a finite number of such curves were known, due to James [J].

Second, let E/K be an elliptic curve with j-invariant 0 defined over a number field K. In this thesis, we give a simple condition on K which determines whether all cubic twists of E/K have the same root number or not. This is a cubic twist analogue to the work [DD] of Dokchitser and Dokchitser on quadratic twists of elliptic curves.

Finally, let K be a number field containing the third root of unity and $L = K(\sqrt[3]{D})$ be a cyclic extension over K of degree 3, where $D \in K$. Let E/K be an elliptic curve with j-invariant 0 defined over K and E_D the D-cubic twist of E. In this thesis, we show that if $\mathrm{Gal}(K(E[3])/K) \cong \mathbb{Z}_6$, then for any nonnegative integer $n \geq 0$, there are infinitely many $L = K(\sqrt[3]{D})$ such that the

cubic twist E_D/K has $\dim_{\mathbb{F}_3}\mathrm{Sel}_3(E_D/K) = 2n$. This is a cubic twist analogue of the work [MR] of Mazur and Rubin on quadratic twists of elliptic curves.

Key words : elliptic curve, cubic twist, quadratic twist, Selmer group, root number, Birch and Swinnerton-Dyer conjecture
Student Number : 2009-30844

Contents

Chapter 1

Introduction

The Mordell-Weil rank of elliptic curves and their average is a central subject in modern number theory, and there are many interesting questions about the rank. Specially, in this thesis we are interested in the average rank. This depends on how we collect a family of elliptic curves. One way for the average rank is that we consider all elliptic curves ordered in terms of their height. Another way is that we consider families of twists of elliptic curves. In particular, one has three natural kinds of families of twists: quadratic twists, cubic and quartic twists.

Among these twists, quadratic twists have been studied quite extensively, and there is a famous Goldfeld conjecture (1979) [G] which asserts that for every fixed elliptic curve over the rational field, the average rank of its quadratic twists is $\frac{1}{2}$.

Our aim in this thesis is to understand cubic twists of elliptic curves over arbitrary number field. Our central tools will be the root number and the Selmer group which give an information on the parity and upper bound of the Mordell-Weil rank, respectively, and they are computable. More precisely, we investigate

(1) the distribution of root numbers in families of cubic twists;

(2) the variation of 3-Selmer rank in families of cubic twists.

The contents of this thesis are divided into five chapters. Chapter 2 introduces the background and prerequisites. We give the definition of L-function and root number, and we list some standard conjectures about L-functions: the Hasse-Weil conjecture, the Birch and Swinnerton-Dyer conjecture, and the Tate-Shafarevich conjecture. Then we discuss what is the twists of elliptic curves and its natural classification. Lastly we study the Selmer and Shafarevich-Tate groups.

In Chapter 3, we consider the quadratic twist. We first introduce the Goldfelds's conjecture and Dokchitser and Dokchitser's theorem. Goldefeld conjecture is stated on an elliptic curve over the rational field. However the Goldfeld conjecture may not hold over number fields, and recently Dokchitser and Dokchitser [DD] gives a sufficient and necessary conditions which determines whether all quadratic twists of an elliptic curve have the same root number or not.

In the last section, we will consider a family of quadratic twists satisfying both the conditions of Vatsal [V] and Frey [F] which give the conditions such that quadratic twists has rank zero and the p-Selmer group of quadratic twists is trivial, respectively. Then we show that the p-part of the Birch and Swinnerton-Dyer conjecture is true for these quadratic twists:

Theorem 1 (Theorem 1.1 of [BK]). *Let $p \in \{3, 5, 7\}$ and $E/\mathbb{Q}$ be an optimal elliptic curve with a rational point P of order p and good, ordinary reduction at p. Suppose that $2, 3 \nmid N_E$, E has no additive reduction, and $\mathrm{ord}_q(j_E) \equiv 0$*

(mod p) *for each odd prime* $q|N_E$ *with* $q \equiv -1 \pmod{p}$. *Then*

$$\mathrm{ord}_p\left(\frac{L(E^D/\mathbb{Q},1)}{\Omega_{E^D/\mathbb{Q}}}\right) = \mathrm{ord}_p\left(\frac{\#Ш(E^D/\mathbb{Q})\prod_q c_q(E^D/\mathbb{Q})}{\#E^D(\mathbb{Q})^2_{\mathrm{tor}}}\right) = 0,$$

for every negative square-free integer D *prime to* pN_E *such that* $h(D) \not\equiv 0$ (mod p) *and*

$$\left(\frac{D}{q}\right) = \begin{cases} -1 & \text{if } E \text{ has split multiplicative reduction at } q, \\ 1 & \text{if } E \text{ has nonsplit multiplicative reduction at } q. \end{cases}$$

As a corollary we show that there are infinitely many elliptic curves over the rational field such that for a positive portion of D, $E^D/\mathbb{Q}$ has rank zero and satisfies the 3-part of the Birch and Swinnerton-Dyer conjecture:

Corollary 1.1 (Corollary 1.2 of [BK])**.** *For* $p = 3$*, there are infinitely many elliptic curves* $E/\mathbb{Q}$ *in Theorem 1.1 and for these elliptic curves, we have*

$$\#\{-X < D < 0 : D \text{ is square-free and } \mathrm{ord}_3\left(\frac{L(E^D/\mathbb{Q},1)}{\Omega_{E^D/\mathbb{Q}}}\right) = \mathrm{ord}_3\left(\frac{\#Ш(E^D/\mathbb{Q})\prod_q c_q(E^D/\mathbb{Q})}{\#E^D(\mathbb{Q})^2_{\mathrm{tor}}}\right) = 0\} \gg_E X.$$

Chaper 4 and 5 are concerned with the cubic twist. In Chapter 4, we first give a rank relation between cubic twist and cubic extentsion field for arbitrary base fields, then we prove that the average root number in a family of cubic twists of an fixed elliptic curve over $\mathbb{Q}$ is $\frac{1}{2}$. Lastly, we give a simple condition which determines whether all cubic twists of an elliptic curve have the same root number or not, this is an analogue of the work [DD] of Dokchitser and Dokchitser on quadratic twists:

Theorem 2 (Theorem 1.1. of [BK2]). *Let $E/K : y^2 = x^3 + a$ be an elliptic curve over a number field K. For cube-free $D \in K^*$, let $E_D/K : y^2 = x^3 + aD^2$ be the D-cubic twist of E. Then the root number $w(E_D/K)$ is constant for all $D \in K^*$ if and only if K contains $\sqrt{-3}$.*

In Chapter 5, we introduce the recent paper of Mazur and Rubin [MR2] concerning the 2-Selmer rank in families of quadratic twists of elliptic curves over arbitrary number fields. Then we generalize this paper to cubic twists setting. More precisely, we investigate the 3-Selmer rank in families of cubic twists of elliptic curves. We give sufficient conditions on an elliptic curve so that it has cubic twists of arbitrary (even) 3-Selmer rank:

Theorem 3 ([BK3], in preparation). *Let K be a number field containing a third root of unity. Suppose $E/K : y^2 = x^3 + a$ is an elliptic curve such that $\mathrm{Gal}(K(E[3])/K) \cong \mathbb{Z}_6$. Then for every integer $n \geq 0$, E has infinitely many cubic twists E_D/K such that $\dim_{\mathbb{F}_3} \mathrm{Sel}_3(E_D/K) = 2n$.*

Chapter 2

Preliminaries

In this chapter, we briefly explain the basic concepts which we will use throughout this thesis.

2.1 L-functions and root numbers

Let E/K be an elliptic curve over a number field K, and let v a finite place of K. We denote the residue field of K at v by k_v, the reduction of E at v by $\tilde{E}_v$, and let $q_v := \#k_v$.

The *L-function* of E/K is formally defined by the Euler product:

$$L(E/K, s) := \prod_v \left(1 - \frac{1 + q_v - \#\tilde{E}_v(k_v)}{q_v^s} + \frac{q_v}{q_v^{2s}}\right)^{-1}, \quad \left(Re(s) > \frac{3}{2}\right).$$

The Hasse-Weil conjecture asserts that $L(E/K, s)$ has an analytic continuation to the whole of $\mathbb{C}$ and the *modified Hasse-Weil L-function* of E/K is

$$\Gamma_{E/K}(s) := A^{s/2}\, \Gamma_K(s)\, L(E/K, s),$$

where $A = A_{E/K}$ and $\Gamma_K(s)$ are defined as follows:

(1) The constant $A_{E/K}$ is given by

$$A_{E/K} = N_E \cdot d_{K/\mathbb{Q}}^2,$$

where N_E is the conductor of E and $d_{K/\mathbb{Q}}$ is the discriminant of K.
(2) The gamma factor for the field K is

$$\Gamma_K(s) = [(2\pi)^{-s}\Gamma(s)]^n.$$

Then the modified Hasse-Weil L-function $\Gamma_{E/K}(s)$ satisfies the functional equation

$$\Gamma_{E/K}(s) = w(E/K)\,\Gamma_{E/K}(2-s),$$

where $w(E/K)$, called the *(global) root number* of E/K, equals 1 or -1. The root number has played an important role, since from the functional equation this number determines the parity of $\mathrm{ord}_{s=1}L(E/K,s)$ and under the parity conjecture the parity of the Mordell-Weil rank of E over K. However, such a functional equation is not yet known to exist in general. Therefore we adopt another representation-theoretic definition of the global root number which can be defined independent of any conjectures and is conjectured to be $w(E/K)$.

The *root number* is the product of the local root number over all places of K,

$$w(E/K) = \prod_v w(E/K_v),$$

with $w(E/K_v)$ defined using local Galois actions on the Tate module. More precisely, each $w(E/K_v)$ can be expressed in terms of a canonical representation $\sigma'_{E,v}$ of the Weil-Deligne representation of E/K_v:

$$w(E/K_v) = \frac{\epsilon(\sigma'_{E,v},\psi,dx)}{|\epsilon(\sigma'_{E,v},\psi,dx)|},$$

where ψ is any nontrivial unitary character of K_v and dx is any Haar measure on K_v (see for example, [R2]). The expression can be obtained from the coefficients of E by Rorlich [R], Kobayashi [K] and Dokchitser and Dokchitser [DD2].

2.2 Selmer and Shafarevich-Tate groups

Let E/K be an elliptic curve over a number field K. To study the arithmetic of the abelian group $E(K)$, let consider the map $[n] : E \to E$, which is multiplication by an integer n. Then there is an exact sequence of G_K-modules,

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{[n]} E \longrightarrow 0,$$

where $E[n]$ denotes the kernel of $[n]$. Taking Galois cohomology yields the long exact sequence

$$\begin{aligned} 0 \longrightarrow\ & E(K)[n] \longrightarrow E(K) \xrightarrow{[n]} E(K) \\ \xrightarrow{\delta}\ & H^1(K, E[n]) \longrightarrow H^1(K, E) \longrightarrow H^1(K, E[n]) \longrightarrow \cdots, \end{aligned}$$

and from this we obtain the short exact sequence

$$0 \longrightarrow E(K)/nE(K) \xrightarrow{\delta} H^1(K, E[n]) \longrightarrow H^1(K, E)[n] \longrightarrow 0.$$

By localizing at all places $\mathfrak{p}$ of K, we obtain the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/nE(K) & \xrightarrow{\delta} & H^1(K, E[n]) & \longrightarrow & H^1(K, E)[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & \searrow^{\alpha} & \downarrow & & \\ 0 & \longrightarrow & \bigoplus_{\mathfrak{p}} E(K_{\mathfrak{p}})/nE(K_{\mathfrak{p}}) & \xrightarrow{\delta} & \bigoplus_{\mathfrak{p}} H^1(K_{\mathfrak{p}}, E[n]) & \longrightarrow & \bigoplus_{\mathfrak{p}} H^1(K_{\mathfrak{p}}, E)[n] & \longrightarrow & 0. \end{array}$$

The *n-Selmer group* $\mathrm{Sel}_n(E/K)$ of E/K is the kernel of the map α, and the *Tate-Shafarevich group* of E/K is

$$Ш(E/K) := \ker\left(H^1(K,E) \to \bigoplus_{\mathfrak{p}} H^1(K_{\mathfrak{p}},E)\right).$$

By the definition of the Selmer group and Tate-Shafarevich group, we obtain the short exact sequence:

$$0 \longrightarrow E(K)/nE(K) \xrightarrow{\delta} \mathrm{Sel}_n(E/K) \longrightarrow Ш(E/K)[n] \longrightarrow 0.$$

From this short exact sequence, if p is a prime we have

$$\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/K) = \operatorname{rank} E/K + \dim_{\mathbb{F}_p} E(K)[p] + \dim_{\mathbb{F}_p} Ш(E/K)[p].$$

Thus, $\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/K)$ gives an upper bound for the rank of E/K.

Proposition 2.1. *The Selmer group* $\mathrm{Sel}_n(E/K)$ *is finite.*

2.3 Birch and Swinnerton-Dyer conjecture

Let E/K be an elliptic curve over a number field K with conductor N_E given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_1, a_2, a_3, a_4, a_6 \in K.$$

The set $E(K)$ of all K-rational points on E together with a point at infinity O forms an abelian group which is called the *Mordell-Weil Group* of the elliptic curve E/K. Then the Mordell and Weil theorem says that it is finitely generated. By the finitely generated abelian group theorem $E(K) \cong \mathbb{Z}^r \oplus T$, where r is a nonnegative integer and T is its torsion subgroup. We define r to be the *rank* of E/K, denoted by $\operatorname{rank} E/K$.

The Hasse-Weil conjecture says that the function $L(E/K, s)$ has an analytic continuation to the whole of $\mathbb{C}$. Granting the analytic continuation, we may state the following conjecture:

Conjecture 2.2 (Birch and Swinnerton-Dyer conjecture I)**.**

$$\mathrm{ord}_{s=1} L(E/K, s) = \mathrm{rank}\, E/K.$$

As an immediate consequence of the Hasse-Weil and BSD conjecture, we obtain the following conjecture.

Conjecture 2.3 (Parity conjecture)**.**

$$(-1)^{\mathrm{rank}\, E/K} = w(E/K),$$

where $w(E/K)$ is the root number of E/K.

The second form of the Birch and Swinnerton-Dyer conjecture predicts the precise leading Taylor coefficient of the L-function at $s = 1$. To state it, we require the Tate-Shafarevich conjecture.

Conjecture 2.4 (Tate-Shafarevich conjecture)**.** *$Ш(E/K)$ is finite.*

Conjecture 2.5 (Birch and Swinnerton-Dyer conjecture II)**.** *Let r be the rank of E/K. Then*

$$\frac{L^{(r)}(E/K, 1)}{r!\, \Omega_{E/K}} = \frac{\#Ш(E/K)\, R(E/K) \prod_{\mathfrak{p}} c_{\mathfrak{p}}(E/K)}{(\#E(K)_{tor})^2 \sqrt{\#\Delta_K}},$$

where $\Omega_{E/K}, Ш(E/K), R(E/K), c_{\mathfrak{p}}(E_D/\mathbb{Q})$ and Δ_K denote the real period, Tate-Shafarevich group, regulator, local Tamagawa number at each place $\mathfrak{p}$ of E/K and the discriminant of K, respectively.

2.4 Twists of elliptic curves

We continue to suppose that K is a number field, and E/K is an elliptic curve.

Definition 2.6. A *twist of* E/K is an elliptic curve E'/K that is isomorphic to E over an algebraic closure $\overline{K}$ of K. We treat two twists as equivalent if they are isomorphic over K. The set of twists of E/K, modulo K-isomorphism, is denoted by $\mathit{Twist}((E,O)/K)$.

Proposition 2.7 (X, Proposition 5.4 of [Sm])**.** *Let*

$$n := \begin{cases} 2 & \text{if } j(E) \neq 0, 1728 \\ 4 & \text{if } j(E) = 1728 \\ 6 & \text{if } j(E) = 0. \end{cases}$$

Then $\mathit{Twist}((E,O)/K)$ *is canonically isomorphic to* K^*/K^{*n}.

More precisely, choose a Weierstrass equation

$$E : y^2 = x^3 + ax + b$$

for E/K*, and let* $D \in K^*$*. Then the elliptic curve* $E_D \in \mathit{Twist}((E,O)/K)$ *corresponding to* $D \pmod{K^{*n}}$ *has the Weierstrass equation*

(i)	$E_D : y^2 = x^3 + aD^2x + bD^3$	*if* $j(E) \neq 0, 1728$*;*
(ii)	$E_D : y^2 = x^3 + aDx$	*if* $j(E) = 1728$ *(so* $b = 0$*);*
(iii)	$E_D : y^2 = x^3 + bD$	*if* $j(E) = 0$ *(so* $a = 0$*).*

From this proposition, we can conclude that there are families of quadratic, cubic, quartic and sextic twists. In this thesis, we mainly discuss quadratic and cubic twists:

- *Quadratic twists.* Let E be an elliptic curve over K given by the Weierstrass equation $y^2 = x^3 + ax^2 + bx + c$ and D be any square-free element of K^*, then the *quadratic twist* of E by D, denoted by E^D, is the curve defined by

$$E^D : y^2 = x^3 + aDx^2 + bD^2x + cD^3.$$

- *Cubic twists.* These twists can be defined on an elliptic curve over K with j-invariant equal to 0. More precisely, we may let E be an elliptic curve over K given by the Weierstrass equation $y^2 = x^3 + a$. Then for any cube-free element D of K^*, the *cubic twist* of E by D, denoted by E_D, is the curve defined by

$$E_D : y^2 = x^3 + aD^2.$$

Chapter 3

Quadratic twists

3.1 Goldfeld's conjecture

The average rank will depend on how we define the average. For this, we will consider the quadratic twists and cubic twists. At first, consider the asymptotic average rank in a family of quadratic twists ordered by the absolute value of D. In 1979, Goldefeld [G] conjectured that for every fixed elliptic curve over $\mathbb{Q}$, the average rank of its quadratic twists is $\frac{1}{2}$.

3.1.1 Goldfeld's conjecture over $\mathbb{Q}$

Fix for this section an elliptic curve E over $\mathbb{Q}$. Let D be a square-free integer, and let E^D be the the quadratic twist of E by D. Let

$$S(X) := \{\text{square-free } D \in \mathbb{Z} : |D| \leq X\}.$$

It is well-known that

$$\lim_{X\to\infty} \frac{\#\{D \in S(X) : w(E^D/\mathbb{Q}) = 1\}}{\#S(X)} = \frac{1}{2}$$

Suppose that the Parity conjecture hods. Then

$$\lim_{X\to\infty} \frac{\#\{D \in S(X) : \operatorname{rank} E/\mathbb{Q} \text{ is even}\}}{\#S(X)} = \lim_{X\to\infty} \frac{\#\{D \in S(X) : \operatorname{rank} E/\mathbb{Q} \text{ is odd}\}}{\#S(X)} = \frac{1}{2},$$

so we must have

$$\lim_{X\to\infty} \frac{\sum_{D\in S(X)} \operatorname{rank} E^D/\mathbb{Q}}{\sum_{D\in S(X)} 1} \geq \frac{1}{2}.$$

Under the Parity conjecture, the 'minimalistic conjecture' above becomes the Goldfeld's conjecture.

Conjecture 3.1 (Goldfeld's conjecture [G])**.**

$$\lim_{X\to\infty} \frac{\sum_{D\in S(X)} \operatorname{rank} E^D/\mathbb{Q}}{\sum_{D\in S(X)} 1} = \frac{1}{2}.$$

More precisely, if we assume the Parity conjecture, Goldfeld's conjecture asserts that

$$\begin{aligned} \operatorname{rank} E^D/\mathbb{Q} = 0 \quad &\text{for } 50\% \text{ square-free } D\text{'s}, \\ \operatorname{rank} E^D/\mathbb{Q} = 1 \quad &\text{for } 50\% \text{ square-free } D\text{'s}, \\ \operatorname{rank} E^D/\mathbb{Q} \geq 2 \quad &\text{for } \ 0\% \text{ square-free } D\text{'s}. \end{aligned}$$

3.1.2 No Goldfeld over number fields

Over number fields the Goldfeld's conjecture may not hold, because there is an elliptic curve such that its all quadratic twists have even rank. The simplest counterexample is CM curves:

Example 3.1 (See [DD]). Let $K = \mathbb{Q}(i)$ and $E/K : y^2 = x^3 + x$. This is a CM curve, becuase

$$\mathrm{End}_K E \cong \mathbb{Z}[i], \qquad [i](x, y) = (-x, iy).$$

Hence for every extension F of K, $E(F) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a $\mathbb{Q}(i)$-vector space, it is even-dimensional over $\mathbb{Q}$, so $\mathrm{rank}\,(E/F)$ is even. Thus for all $D \in K^*$,

$$\mathrm{rank}\, E^D/K = \mathrm{rank}\, E/K(\sqrt{D}) - \mathrm{rank}\, E/K \equiv 0 \pmod 2.$$

Also one can show that $w(E^D/K) = 1$ for all quadratic twist E^D of E/K.

Here is another example satisfying all quadratic twists have "$w = -1$".

Example 3.2 (See [DD]). The elliptic curve $E/\mathbb{Q} : y^2 = x^3 + \frac{5}{2}x^2 - 2x - 7$ $(121C1)$ has minimal discriminant 11^4, so it acquires everywhere good reduction over $\mathbb{Q}(\sqrt[3]{11})$. If we take $K = \mathbb{Q}(\zeta_3, \sqrt[3]{11})$, it is totally complex, E/K has everywhere good reduction, hence for all $D \in K^*$ we have

$$w(E^D/K) = w(E/K(\sqrt{D})) \cdot w(E/K) = 1 \cdot (-1)^{\#\{\mathfrak{p}|\infty\}} = -1,$$

because every $K(\sqrt{D})$ have totally complex places of even number.

Precisely, T. Dokchitser and V. Dokchitser gave the local conditions on an elliptic curve to guarantee that all of its quadratic twists have the same root number:

Theorem 3.2. ([DD]) *Let E/K be an elliptic curve. Then the following conditions are equivalent:*

(a) $w(E^D/K)$ is constant for all quadratic twists E^D of E.

(b) K has no real places, and E acquires everywhere good reduction over an abelian extension of K.

3.2 p-part of the Birch and Swinnerton-Dyer conjecture

Let $E/\mathbb{Q}$ be an elliptic curve of the conductor N_E given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$ and $L(E, s)$ its Hasse-Weil L-function. Let D be a square-free integer and $h(D)$ the class number of the quadratic field $\mathbb{Q}(\sqrt{D})$. Let E^D be the D-quadratic twist of E. Then it is given by

$$E^D : y^2 = x^3 + b_2Dx^2 + 8b_4D^2x + 16b_6D^3,$$

where $b_2 := a_1^2 + 4a_2$, $b_4 := 2a_4 + a_1a_3$, $b_6 := a_3^2 + 4a_6$.

If E^D has analytic rank zero, then the Birch and Swinnerton-Dyer conjecture asserts that

$$\frac{L(E^D/\mathbb{Q}, 1)}{\Omega_{E^D/\mathbb{Q}}} = \frac{\#Ш(E^D/\mathbb{Q}) \prod_q c_q(E^D/\mathbb{Q})}{\#E^D(\mathbb{Q})^2_{\text{tor}}}.$$

By the modularity theorem [BCDT], [TW], [Wi], every elliptic curve E defined over $\mathbb{Q}$ has a modular parametrization $\phi : X_0(N_E) \to E$. If for each isogenous curve E' with modular parametrization $\phi' : X_0(N_E) \to E'$ we have that $\phi' = \psi \circ \phi$ for some isogeny ψ, then we say that E is an *optimal* elliptic curve, often called a *strong Weil curve.* Every elliptic curve over $\mathbb{Q}$ has an optimal elliptic curve in its isogeny class and by the characterizing property this curve is unique.

In [V] Vatsal found explicit conditions which guarantee E^D has (analytic) rank zero. In [F] Frey found some conditions on E^D such that the p-Selmer group of E^D is trivial. In this section, we will consider a family of E^D satisfying

both of the conditions of Vatsal and Frey and show that the p-part of the Birch and Swinnerton-Dyer conjecture is true for these elliptic curves E^D.

Theorem 3.3. (Theorem 1.1 of [BK]) *Let $p \in \{3, 5, 7\}$ and $E/\mathbb{Q}$ be an optimal elliptic curve with a rational point P of order p and good reduction at p. Suppose that $2, 3 \nmid N_E$, E has no additive reduction, and $\mathrm{ord}_q(j_E) \equiv 0 \pmod{p}$ for each odd prime $q|N_E$ with $q \equiv -1 \pmod{p}$. Then*

$$\mathrm{ord}_p\left(\frac{L(E^D/\mathbb{Q}, 1)}{\Omega_{E^D/\mathbb{Q}}}\right) = \mathrm{ord}_p\left(\frac{\#Ш(E^D/\mathbb{Q}) \prod_q c_q(E^D/\mathbb{Q})}{\#E^D(\mathbb{Q})^2_{\mathrm{tor}}}\right) = 0,$$

for every negative square-free integer D prime to pN_E such that $h(D) \not\equiv 0 \pmod{p}$ and

$$\left(\frac{D}{q}\right) = \begin{cases} -1 & \text{if } E \text{ has split multiplicative reduction at } q, \\ 1 & \text{if } E \text{ has nonsplit multiplicative reduction at } q. \end{cases}$$

Remark 3.4. In (3.1) of [V], Vatsal remarks "Our result below may be viewed as a complement to the theorem of Frey, with the link being given by the Birch-Swinnerton-Dyer conjecture. It would be interesting to compare Frey's results to ours more explicty". Theorem 3.3 gives such comparison of the Vatsal's result with the Frey's one.

As a corollary we will show that there are infinitely many elliptic curves $E/\mathbb{Q}$ such that for a positive portion of D, E^D has rank zero and satisfies the 3-part of the Birch and Swinnerton-Dyer conjecture. Previously we know that there are finite number of elliptic curves for which a positive portion of the quadratic twists have rank zero and satisfy the 3-part of the Birch and Swinnerton-Dyer conjecture due to James [J].

Corollary 3.5. (Corollary 1.2 of [BK])
(1) *For $p = 3$, there are infinitely many elliptic curves $E/\mathbb{Q}$ in Theorem 3.3 and for these elliptic curves, we have*

$$\#\{-X < D < 0 : D \text{ is square-free and } \operatorname{ord}_3\left(\frac{L(E^D/\mathbb{Q},1)}{\Omega_{E^D/\mathbb{Q}}}\right) = \operatorname{ord}_3\left(\frac{\#Ш(E^D/\mathbb{Q})\prod_q c_q(E^D/\mathbb{Q})}{\#E^D(\mathbb{Q})^2_{\text{tor}}}\right) = 0\} \gg_E X.$$

(2) *For $p = 5$, there are infinitely many elliptic curves $E/\mathbb{Q}$ in Theorem 3.3 and for these elliptic curves, if there is at least one odd D_0 in Theorem 3.3 such that at least one prime factor of D_0 larger than $\frac{[\Gamma_0(1):\Gamma_0(4\cdot 5^2\cdot(4N_E)^4)]}{8} + 1$, we have*

$$\#\{-X < D < 0 : D \text{ is square-free and } \operatorname{ord}_5\left(\frac{L(E^D/\mathbb{Q},1)}{\Omega_{E^D/\mathbb{Q}}}\right) = \operatorname{ord}_5\left(\frac{\#Ш(E^D/\mathbb{Q})\prod_q c_q(E^D/\mathbb{Q})}{\#E^D(\mathbb{Q})^2_{\text{tor}}}\right) = 0\} \gg_E \frac{\sqrt{X}}{\log X}.$$

3.2.1 Calculation of Tamagawa numbers

Definition 3.6. If E is an elliptic curve over $\mathbb{Q}$ and p is a prime, the *Tamagawa number* (or *fudge factor*) $c_p(E/\mathbb{Q})$ is defined by

$$c_p(E/\mathbb{Q}) = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)],$$

where $E_0(\mathbb{Q}_p)$ is the subgroup of $E(\mathbb{Q}_p)$ consisting of those points whose reduction modulo p (on a minimal model of E at p) is nonsingular.

In particular, $c_p(E/\mathbb{Q}) = 1$ if $E/\mathbb{Q}$ has good reduction at p. The fundamental method for computing the Tamagawa number is Tate's algorithm [T]. Standard number theoretic computer packages, such as PARI, will compute these numbers very efficiently.

Let $\Delta(E/\mathbb{Q})$ denote the discriminant of a minimal model of $E/\mathbb{Q}$. The following is some well-known properties of the Tamagawa number.

Proposition 3.7. *Suppose E is an elliptic curve over $\mathbb{Q}$.*

1. *If E has split multiplicative reduction at p, then $c_p(E/\mathbb{Q}) = \mathrm{ord}_p(\Delta(E/\mathbb{Q}))$.*
2. *If E has nonsplit multiplicative reduction at p, then $c_p(E/\mathbb{Q}) \leq 2$ and $c_p(E/\mathbb{Q}) \equiv \mathrm{ord}_p(\Delta(E/\mathbb{Q})) \pmod 2$.*
3. *If E has additive reduction at p, then $c_p(E/\mathbb{Q}) \leq 4$.*

Proof. These are cases $1, 2a, 2b$, and 3 through 10, respectively, of Tate's algorithm [T]. □

Note that in [T], we have the following possibilities.

Kodaira type	$c_p(E/\mathbb{Q})$
I_ν $(\nu > 0)$	$1, 2$ or $v_p(\Delta(E/\mathbb{Q}))$
I_0, II, II^*	1
III, III^*	2
IV, IV^*	1 or 3
I_ν^* $(\nu \geq 0)$	2 or 4

Now, we consider the Tamagawa number of the quadratic twist of $E/\mathbb{Q}$. For convenience, we will write simply $c_p(D)$ for $c_p(E^D/\mathbb{Q})$.

Lemma 3.8. *Suppose that D, D' are the elements in $\mathbb{Q}^*$. If D/D' is a square in $\mathbb{Q}_p$, then $c_p(D) = c_p(D')$.*

Proof. Note that if D/D' is a square in $\mathbb{Q}_p$, then E^D is isomorphic to $E^{D'}$ over $\mathbb{Q}_p$. So by the definition of c_p, we get $c_p(D) = c_p(D')$. □

Proposition 3.9. *Let $E/\mathbb{Q} : y^2 = f(x)$. Suppose that D is a square-free integer, and p is a prime not dividing $2\Delta(E/\mathbb{Q})$. If $p \nmid D$ then $c_p(D) = 1$. If $p \mid D$ then*

$$c_p(D) = 1 + \{\textit{roots of } f(x) \textit{ in } \mathbb{Z}/p\mathbb{Z}\} = 1, 2, \textit{ or } 4.$$

Proof. If $p \nmid 2\Delta(E/\mathbb{Q})D$ then E^D has good reduction at p, so $c_p(D) = 1$. If $p \mid D$ but $p \nmid 2\Delta(E/\mathbb{Q})$ then we are in case 6 of Tate's algorithm [T]. □

Note that for every p not dividing $2\Delta(E/\mathbb{Q})$, the number of roots of $f(x)$ modulo p is at least as large as the number of roots of $f(x)$ in $\mathbb{Q}$. Thus if $p \mid D$ but $p \nmid 2\Delta(E/\mathbb{Q})$, then $c_p(D) \geq \#E(\mathbb{Q})[2]$.

The remaining situation, i.e. $p \mid 2\Delta(E/\mathbb{Q})$, is more complicated. However, for those primes, to determine $c_p(D)$ for every D, Lemma 3.8 shows that it is enough to compute $c_p(D)$ for D in a set of representatives of $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$. Note that $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ has order 4 if $p > 2$, and order 8 if $p = 2$ by the Hensel's lemma.

Example 3.3. Let $E/\mathbb{Q} : y^2 = x^3 - x$.

Then we have $\Delta(E/\mathbb{Q}) = 64$, and $x^3 - x$ factors into linear factors over $\mathbb{Q}$, so Proposition 3.9 shows that for $p > 2$ we have

$$c_p(D) = \begin{cases} 1 & \text{if } p \nmid D, \\ 4 & \text{if } p \mid D. \end{cases}$$

Tate's algorithm gives (alternatively, we can use PARI to compute)

$$c_2(1) = c_2(3) = c_2(-1) = c_2(-3) = 2,$$
$$c_2(2) = c_2(6) = c_2(-2) = c_2(-6) = 4,$$

and then by Lemma 3.8 we get that

$$c_2(D) = \begin{cases} 2 & \text{if } 2 \nmid D, \\ 4 & \text{if } 2 \mid D. \end{cases}$$

Therefore, we conclude that

$$\prod_p c_p(D) = \begin{cases} 2^{2\omega(D)+1} & \text{if } D \text{ is odd}, \\ 2^{2\omega(D)} & \text{if } D \text{ is even}, \end{cases}$$

where $\omega(D)$ is the number of prime divisors of D.

3.2.2 Proof of Theorem 3.3

Theorem 3.10. (Corollary 3.4 of [V]) *Let p be an odd prime and $E/\mathbb{Q}$ be an elliptic curve with a rational point P of order p and good reduction at p. Assume that each prime of additive reduction is congruent to 1 modulo p. Then $L(E^D/\mathbb{Q}, 1) \neq 0$ for every negative square-free integer D prime to N_E such that $h(D) \not\equiv 0 \pmod{p}$ and*

$$\left(\frac{D}{q}\right) = \begin{cases} -1 & \text{if } E \text{ has additivie or} \\ & \text{split multiplicative reduction at } q, \\ -q \pmod{p} & \text{if } E \text{ has nonsplit multiplicative reduction at } q. \end{cases}$$

Remark 3.11. In fact, Vatsal (Theorem 2.10 and Theorem 3.3 of [V]) proved that for E^D in Theorem 3.10

$$\tau(\chi_D)\frac{L(E^D/\mathbb{Q},1)}{(-2\pi i)\Omega_f^-} \not\equiv 0 \pmod{p},$$

where $\tau(\chi_D)$ is the Gauss sum of the quadratic character χ_D and Ω_f^- is the canonical period of the cuspform f corresponding E. If E is optimal, then the imaginary period $\Omega_{E/\mathbb{Q}}^-$ of E is equal to $(-2\pi i)\,\Omega_f^-$ up to a p-adic unit (See Proposition 3.1 of [GV]). Since $\tau(\chi_D) = \sqrt{D}$ and $\Omega_{E/\mathbb{Q}}^-$ is equal to $\sqrt{D}\,\Omega_{E^D/\mathbb{Q}}$ up to a p-adic unit (See Theorem 3.2 of [Pa]), we have that if E is optimal, then

$$\frac{L(E^D/\mathbb{Q},1)}{\Omega_{E^D/\mathbb{Q}}} \not\equiv 0 \pmod{p}.$$

The following theorem is an effective form of [F].

Theorem 3.12. (Proposition 1.5 of [ABF]) *Let p be an odd prime and $E/\mathbb{Q}$ be an elliptic curve with a rational point P of order p and good reduction at p. Suppose that $2 \nmid N_E$, E has no additive reduction, and $\mathrm{ord}_q(j_E) \equiv 0 \pmod{p}$ for each odd prime $q|N_E$ with $q \equiv -1 \pmod{p}$. Then the p-Selmer group $\mathrm{Sel}_p(E^D/\mathbb{Q})$ of E^D is trivial for every negative square-free integer D prime to pN_E such that $h(D) \not\equiv 0 \pmod{p}$ and*

$$\left(\frac{D}{q}\right) = \begin{cases} -1 & \text{if } E \text{ has split multiplicative reduction at } q, \\ 1 & \text{if } E \text{ has nonsplit multiplicative reduction at } q. \end{cases}$$

Lemma 3.13. *Let p be an odd prime and $E/\mathbb{Q}$ be an elliptic curve with a rational point P of order p and good reduction at p. Assume that E has no additive reduction. For a prime $q(\neq 2,3)|N_E$,*

(1) *if P is a singular point in $\tilde{E}(\mathbb{F}_q)$, then E has split multiplicative reduction at q,*
(2) *if P is a non-singular point in $\tilde{E}(\mathbb{F}_q)$, then*

$$q \equiv \begin{cases} 1 \pmod{p} & \text{if } E \text{ has split multiplicative reduction at } q, \\ -1 \pmod{p} & \text{if } E \text{ has nonsplit multiplicative reduction at } q. \end{cases}$$

Proof. We may assume $P = (0,0)$ is a rational torsion point of order p. If $P = (0,0)$ is a singular point in $\tilde{E}(\mathbb{F}_q)$, then we easily see that $a_2 = a_3 = a_4 = a_6 = 0$. Since $y^2 + a_1xy - x^3 = y(y + a_1x) - x^3$, E has split multiplicative reduction at q. This proves the first part of the lemma. If P is a non-singular point in $\tilde{E}(\mathbb{F}_q)$, then p divides the order of the non-singular part $\tilde{E}(\mathbb{F}_q)_{ns}$ of $\tilde{E}(\mathbb{F}_q)$. So the second part comes from the order of $\tilde{E}(\mathbb{F}_q)_{ns}$, which is equal to $q-1$ if E has a split multiplicative reduction at q and is equal to $q+1$ if E has a nonsplit multiplicative reduction at q (See p.59 of [Mi]). □

From Theorem 3.10, Theorem 3.12 and Lemma 3.13, we obtain the following proposition.

Proposition 3.14. *Let p be an odd prime and $E/\mathbb{Q}$ be an elliptic curve with a rational point P of order p and good reduction at p. Suppose that $2, 3 \nmid N_E$, E has no additive reduction, and $\mathrm{ord}_q(j_E) \equiv 0 \pmod{p}$ for each odd prime $q|N_E$ with $q \equiv -1 \pmod{p}$. Then the p-Selmer group $\mathrm{Sel}_p(E^D/\mathbb{Q})$ of E^D is trivial and $L(E^D/\mathbb{Q}, 1) \neq 0$ for every negative square-free integer D prime to pN_E such that $h(D) \not\equiv 0 \pmod{p}$ and*

$$\left(\frac{D}{q}\right) = \begin{cases} -1 & \text{if } E \text{ has a split multiplicative reduction at } q, \\ 1 & \text{if } E \text{ has a nonsplit multiplicative reduction at } q. \end{cases}$$

Lemma 3.15. (p.59 of [Mi]) *Let $l \neq 2, 3$ be a prime, and $E/\mathbb{Q}$ be an elliptic curve given by*

$$E : y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{Z}.$$

Assume that this equation is minimal at l and E has bad reduction at l. Then

$$-2ab = \begin{cases} 0 \text{ in } \mathbb{F}_l & \text{if } E \text{ has additive reduction at } l, \\ \text{a square in } \mathbb{F}_l & \text{if } E \text{ has split multiplicative reduction at } l, \\ \text{a non-square in } \mathbb{F}_l & \text{if } E \text{ has nonsplit multiplicative reduction at } l. \end{cases}$$

Proof. Let's try to find a t such that an equation for $E/\mathbb{Q}$ is

$$\begin{aligned} y^2 &= (x-t)^2(x+2t) \\ &= x^3 - 3t^2x + 2t^3. \end{aligned}$$

For this, we have to choose t so that

$$t^2 = -\frac{a}{3}, \quad t^3 = \frac{b}{2}.$$

Hence $t = \frac{b/2}{-a/3} = -\frac{3b}{2a}$.

Now, we can rewrite the equation as

$$y^2 = 3t(x-t)^2 + (x-t)^3.$$

This has a singularity at $(t, 0)$. The point $(t, 0)$ is a cusp if $3t \equiv 0 \pmod{l}$, a node with rational tangents if $3t$ is a nonzero square in $\mathbb{F}_l$, and a node with non-rational tangents if $3t$ is a nonzero non-square in $\mathbb{F}_l$. Note that

$$-2ab = -2(-3t^2)(2t^3) = (2t^2)^2(3t)$$

and so $3t$ is zero or nonzero, a square or a non-square, according as $-2ab$ is. $\square$

From the above lemma, we can prove the following lemma which is needed to compute Tamagawa numbers of E^D in the proof of Theorem 3.3.

Lemma 3.16. *Let $E/\mathbb{Q}$ be an elliptic curve. Assume that E has no additive reduction. Then E^D has nonsplit multiplicative reduction at $q(\neq 2,3)|N_E$ for every negative square-free integer D such that*

$$\left(\frac{D}{q}\right) = \begin{cases} -1 & \text{if } E \text{ has split multiplicative reduction at } q, \\ 1 & \text{if } E \text{ has nonsplit multiplicative reduction at } q. \end{cases}$$

Proof. By assumption $q \neq 2, 3$, we may assume that E be a minimal Weierstrass equation at q of the form $y^2 = x^3 + ax + b$ for some $a, b \in \mathbb{Z}$. Then E^D is given by: $y^2 = x^3 + aD^2x + bD^3$ and this equation is also minimal at q. If E has split multiplicative reduction at q, then $(\frac{-2abD^5}{q}) = (\frac{-2ab}{q})(\frac{D}{q}) = 1 \cdot (-1) = -1$. If E has nonsplit multiplicative reduction at q, then $(\frac{-2abD^5}{q}) = (\frac{-2ab}{q})(\frac{D}{q}) = (-1) \cdot 1 = -1$. Thus E^D always has nonsplit multiplicative reduction at q by Lemma 3.15. □

Proof of Theorem 3.3. Suppose that E^D is the curve in Theorem 3.3. Then the p-Selmer group $\mathrm{Sel}_p(E^D/\mathbb{Q})$ of E^D is trivial and $L(E^D/\mathbb{Q}, 1) \neq 0$ by Proposition 3.14. Thus we have that $\operatorname{rank} E^D/\mathbb{Q} = 0$ by the work of Kolyvagin and $\operatorname{ord}_p\big(\#Ш(E^D/\mathbb{Q})\big) = 0$ by the usual Kummer exact sequence. Furthermore since E is optimal, we have $\frac{L(E^D/\mathbb{Q},1)}{\Omega_{E^D/\mathbb{Q}}} \not\equiv 0 \pmod{p}$ by the remark 3.11. The discriminant $\Delta(E^D)$ of E^D is equal to $2^{12} \cdot D^6 \cdot \Delta(E)$.

By the Tate's algorithm in [T], it is the case 6 of the Tate's algorithm and we have that $c_q(E^D/\mathbb{Q}) = 1, 2$, or 4 for $q|D$. And E^D has nonsplit multiplicative reduction at $q|N_E$ by Lemma 3.16, thus $c_q(E^D/\mathbb{Q}) = 1$ or 2 for $q|N_E$ (See Proposition 3.7(2)). And note that we can write down all the elliptic curves

over $\mathbb{Q}$ with a rational point of order p, up to isomorphism, and since it is enough to compute $c_2(E^D/\mathbb{Q})$ for D in a set of representatives of $\mathbb{Q}_2/(\mathbb{Q}_2^*)^2$, we can easily show that $c_2(E^D/\mathbb{Q}) = 1$.
Finally we have

$$\mathrm{ord}_p\left(\frac{L(E^D/\mathbb{Q},1)}{\Omega_{E^D/\mathbb{Q}}}\right) = \mathrm{ord}_p\left(\frac{\#Ш(E^D/\mathbb{Q})\prod_q c_q(E^D/\mathbb{Q})}{\#E^D(\mathbb{Q})^2_{\mathrm{tor}}}\right) = 0.$$

□

3.2.3 Proof of Corollary 3.5(1)

Let $\Phi(x) \in \mathbb{Z}[x]$ be a polynomial of degree k with positive leading coefficient. Then Perelli [Pe] and Brüdern, Kawada and Wooley [BKW] prove that almost all values of the polynomial $2\,\Phi(n)$ are the sum of two primes. With slight modification, Byeon, Jeon and Kim [BJK] obtain the following proposition.

Proposition 3.17 (Proposition 5.1 of [BJK])**.** *Let $\Phi(x) \in \mathbb{Z}[x]$ be a polynomial of degree k with positive leading coefficient and let A, B be positive odd integers such that $\gcd(A,B) = 1$. Let $\mathcal{E}_k(N;\Phi)$ denote the number of integers $n \in [1,N]$ for which the equation*

$$2\Phi(n) = As + Bt$$

has no solution in primes s, t. Then there is an absolute constant $c > 0$ such that

$$\mathcal{E}_k(N;\Phi) \ll_\Phi N^{1-c/k}.$$

Now we can prove Corollary 3.5(1).

Proof of Corollary 3.5(1). Let $p_1, \cdots, p_r$ and $q_1, \cdots, q_{r'}$ be different primes $\neq 2, 3$ such that $q_i \equiv 1 \pmod 3$ for all $i = 1, \cdots, r'$. Put $\Phi(x) := (3(2x +$

$1)+1)^3/2 \in \mathbb{Z}[x]$ and $A := 27p_1 \cdots p_r$, $B := q_1 \cdots q_{r'}$. Then there are infinitely many positive integers n of the form

$$2\Phi(n) = (3(2n+1)+1)^3 = 27p_1 \cdots p_r s + q_1 \cdots q_{r'} t$$

for some primes s, t by Proposition 3.17. We may assume that $s, t \neq 2, 3, p_i, q_j$. For such n, s, t, put $a := 3(2n+1)+1$ and $b := p_1 \cdots p_r s$. Let $E(a,b)$ be the elliptic curve defined by

$$E(a,b) : y^2 + axy + by = x^3.$$

Then $E(a,b)$ has the point $P = (0,0)$ of order 3 and the discriminant $\Delta(E(a,b))$ of $E(a,b)$ is

$$\Delta(E(a,b)) = b^3(a^3 - 27b) = p_1^3 \cdots p_r^3 s^3 q_1 \cdots q_{r'} t.$$

We can easily check that $2, 3 \nmid N_{E(a,b)}$, $E(a,b)$ has no additive reduction, and $\mathrm{ord}_q(j_{E(a,b)}) \equiv 0 \pmod 3$ for each odd prime $q | N_E$ with $q \equiv -1 \pmod 3$. Since the 3-isogeneous curve $E'(a,b) = E(a,b)/ < P >$ has no rational point of order 3 by Theorem 1.1 of [H], the isogeny class of $E(a,b)$ over $\mathbb{Q}$ is $\{E(a,b),\ E'(a,b)\}$. Since the optimal curve in the isogeny class should have a rational point of order 3 (See Theorem 1.2 of [Du]), $E(a,b)$ is optimal. Thus Corollary 3.5(1) follows from Theorem 3.3 and the work of Davenport and Heilbronn [DH] as improved by Nakagawa and Horie [NH]. □

3.2.4 Proof of Corollary 3.5(2)

Proposition 3.18. ([I]) *Let $F(x,y) = Ax^2 + Bxy + Cy^2$ be an irreducible quadratic form and m, n, r, r' be integers such that $nm \neq 0$. If $F(mx+r, ny+r')$ represents an integer prime to an arbitrary given non-zero integer , then*

$$\sum_{\substack{w \leq N\,:\,primes \\ w = F(mx+r, ny+r')}} 1 \quad \gg \quad \frac{N}{\log N}.$$

Now we can prove Corollary 3.5(2).

Proof of Corollary 3.5(2). Put $F(x,y) := x^2 - 11xy - y^2$. Then there are infinitely many primes $w \equiv 1 \pmod 5$ of the form $F(30x+1, 30y-1)$ by Proposition 3.18. For such x, y, put $u := 30x+1$, and $v := 30y-1$. Let $E(u,v)$ be an elliptic curve defined by:

$$E(u,v) : y^2 + (u-v)xy - u^2vy = x^3 - uvx^2.$$

Then $E(u,v)$ has the point $P = (0,0)$ of order 5 and the discriminant $\Delta(E(u,v))$ is

$$\Delta(E(u,v)) = u^5v^5(v^2 - 11uv - u^2) = -u^5v^5w.$$

We can easily check that $2, 3 \nmid N_{E(u,v)}$, $E(u,v)$ has no additive reduction, and $\mathrm{ord}_q(j_{E(u,v)}) \equiv 0 \pmod 5$ for each odd prime $q | N_E$ with $q \equiv -1 \pmod 5$. Furthermore $E(u,v)$ is optimal because the isogeny class of $E(u,v)$ is $\{E(u,v),\ E(u,v)/ < P >\}$ by the similar argument to the case $p = 3$. Thus Corollary 3.5(2) follows from Theorem 3.3 and Theorem 13 of [JO]. $\square$

Chapter 4

Cubic twists

We consider the curves $E_D : x^3 + y^3 = D$ over $\mathbb{Q}$, i.e., the elliptic curves $y^2 = x^3 - 432D^2$. The problem of determining whether an integer can be written as the sum of two rational cubes has a long history. Moreover, these are the "cubic twists" of the curve $E : x^3 + y^3 = 1$. In 1987, Zagier and Kramarz [ZK] examined these cubic twists, and they calculated the value of their L-functions and its derivative at 1 for all cube-free positive integers D less than $70,000$. Under the Birch and Swinnerton-Dyer conjecture, their calculations suggest that a positive proportion have the twists E_D of E have even rank ≥ 2, and a positive proportion have odd rank ≥ 3. Also, the percentages remaining constant as D grows.

In this direction, Mai [Ma] proved that the number of cube-free integers $D \leq X$ such that the analytic rank of E_D is even ≥ 2 is at least $CX^{2/3-\epsilon}$, where ϵ is arbitrarily small and C is a positive constant, for X large enough.

So if either a proportion of twists E_D of E having even rank ≥ 2 or one of twists E_D of E having odd rank ≥ 3 is positive, it would be a big difference between quadratic twists and cubic twists.

Also, cubic twists are less known than quadratic twists. In this chapter,

we investigate analogous properties which we know the properties of quadratic twists. First, we give a rank relation between cubic twists and cubic extension field for any number field K. Next, we prove that the asymptotic average root number in a family of cubic twists of an elliptic curve is $\frac{1}{2}$, like quadratic twists. Finally, we give a simple condition on the base field K which determines whether all cubic twists of give elliptic curve over K have the same root number or not. This is a cubic twist analogue to the work [DD2] of Dokchitser and Dokchitser on quadratic twists of elliptic curves.

4.1 General properties of cubic twists

For a quadratic twist case, it is well-known that:

> Let E/K be an elliptic curve, let $D \in K^*$ be such that $L = K(\sqrt{D})$ is a quadratic extension, and let E^D/K be the quadratic twist. Then
>
> $$\operatorname{rank} E/L = \operatorname{rank} E/K + \operatorname{rank} E^D/K. \tag{4.1}$$

Indeed, let φ be an isomorphism satisfying

$$\varphi : E \to E^D, \qquad (x, y) \mapsto (Dx, D^{3/2}y),$$

σ denote a complex conjugation of $\mathrm{Gal}(L/K)$, and χ denote a quadratic character satisfying $\chi(\sigma) = \sqrt{D}^{\sigma}/\sqrt{D}$. Then

$$\varphi(x, y)^{\sigma} = \chi(\sigma)\varphi(x, y) = \varphi(x, \pm y).$$

This shows that φ exchanges the ± 1-eigenspaces of σ. Consider $E(L)$ as a $\mathbb{Z}[G]$-module, then the $+1$-eigenspace of $E(L)$ is $E(K)$ and -1-eigenspace is $E^D(K)$. (See X, §3, Example 2.4 of [Sm]).

Lemma 4.1. (Corollary 3.4 of [St]) *Let K be a number field such that $\sqrt{-3} \notin K$, and let $E : y^2 = x^3 + a$ be an elliptic curve over K. Then we have*

$$\operatorname{rank} E/K(\sqrt{-3}) = 2 \operatorname{rank} E/K.$$

Proof. Consider the quadratic twist $E^{-3} : y^2 = x^3 - 27a$. Then

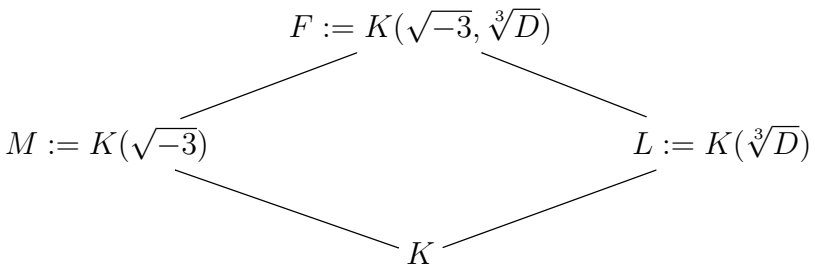
$$\varphi : E \to E^{-3}, \qquad (x, y) \mapsto \left(-\frac{x^3 + 4a}{x^2}, -\frac{y(x^3 - 8a)}{x^3} \right).$$

is a K-isogeny of degree 3. Since K-rational rank is an K-isogeny invariant, we have that $\operatorname{rank} E/K = \operatorname{rank} E^{-3}/K$. Combining this with (4.1) proves the lemma. □

Proposition 4.2. *Let $E : y^2 = x^3 + a$ be an elliptic curve over a number field K, let $D \in K^*$ be such that $L = K(\sqrt[3]{D})$ is a cubic extension of K, and let $E_D : y^2 = x^3 + aD^2$ be the cubic twist of E/K. Then*

$$\operatorname{rank} E/K(\sqrt[3]{D}) = \operatorname{rank} E/K + \operatorname{rank} E_D/K + \operatorname{rank} E_{D^2}/K.$$

Proof. It is well-known that the special case where K contains $\sqrt{-3}$ holds the desired equation (For example, see Corollary 2.4 of [St]). In general case, i.e. K doesn't contain $\sqrt{-3}$, consider the following diagram:



From the special case we get

$$\operatorname{rank} E/F = \operatorname{rank} E/M + \operatorname{rank} E_D/M + \operatorname{rank} E_{D^2}/M,$$

and by Lemma 4.1 we have

$$\begin{aligned} \operatorname{rank} E/F &= 2 \operatorname{rank} E/L \\ \operatorname{rank} E/M &= 2 \operatorname{rank} E/K \\ \operatorname{rank} E_D/M &= 2 \operatorname{rank} E_D/K \\ \operatorname{rank} E_{D^2}/M &= 2 \operatorname{rank} E_{D^2}/K. \end{aligned}$$

Thus we complete the proof. □

4.2 Distribution of cubic twists with root number 1

Let $E/\mathbb{Q}$ be an elliptic curve of the conductor N_E, and for a square-free integer D let E^D be a quadratic twist of E. Then

$$L(E/\mathbb{Q}(\sqrt{D}), s) = L(E/\mathbb{Q}, s)\, L(E^D/\mathbb{Q}, s).$$

By the work of Breuil, Conrad, Diamond, Taylor and Wiles [BCDT] [TW] [Wi], $L(E/\mathbb{Q}, s)$ has an analytic continuation to $\mathbb{C}$ and satisfies the functional equation

$$\Gamma_{E/\mathbb{Q}}(s) = N_E^{s/2}(2\pi)^{-s}\Gamma(s)\, L(E/\mathbb{Q}, s) = w(E/\mathbb{Q})\, \Gamma_{E/\mathbb{Q}}(2-s).$$

If we let $L(E/\mathbb{Q}, s) = \sum_{n\geq 1} a_n n^{-s}$, then

$$L(E^D/\mathbb{Q}, s) = \sum_{n\geq 1} \chi_D(n)\, a_n n^{-s},$$

where $\chi_D(\cdot) = \left(\frac{D}{\cdot}\right)$ is the usual Kronecker character, has an analytic continuation and the functional equation

$$\Gamma_{E^D/\mathbb{Q}}(s) = w(E/\mathbb{Q})\,\chi_D(-N_E)\,\Gamma_{E^D/\mathbb{Q}}(2-s).$$

Hence from this functional equation we can show that

$$\begin{aligned} w(E^D/\mathbb{Q}) &= +1 \quad \text{for 50\% square-free integers } D\text{'s}, \\ w(E^D/\mathbb{Q}) &= -1 \quad \text{for 50\% square-free integers } D\text{'s}. \end{aligned}$$

Now, we consider the case of cubic twists. Mai [Ma] consider the elliptic curve $E : X^3 + Y^3 = 1$ which has a Weierstrass form of $y^2 = x^3 - 432$, and prove that the set of $\{$cubic twist E_D of E $: w(E_D/\mathbb{Q}) = 1\}$ has density $\frac{1}{2}$ in the set of cubic twists E_D of E. In this section, we prove that it holds for every elliptic curve $y^2 = x^3 + a$ over the rational field.

Theorem 4.3. *Let $E : y^2 = x^3 + a$ be an elliptic curve defined over $\mathbb{Q}$. Then the set of $\{$cube-free $D : w(E_D/\mathbb{Q}) = 1\}$ has density $\frac{1}{2}$ in the set $\{$cube-free $D\}$.*

4.2.1 Calculation of local root numbers

Let us first collect a general list of local root number formula. It is well-known that:

$$w(E/K_v) = \begin{cases} +1 & \text{if } E/K_v \text{ has good} \\ & \text{or non-split multiplicative reduction;} \\ -1 & \text{if } v \text{ is infinite} \\ & \text{or } E/K_v \text{ has split multiplicative reduction.} \end{cases}$$

At places of additive reduction, Rohrlich [R] gives the following formula for $w(E/K_v)$ when $K_v = \mathbb{Q}_p$ with $p \geq 5$, and Conrad, Conrad and Helfgott [CCH] prove that the formula can be extended for any K_v with its residual characteristic ≥ 5.

Theorem 4.4. (Proposition 2, 3 of [R], Theorem 3.1 of [CCH]) *Let K_v be a local field, with residue field of characteristic $p \geq 5$ and normalized valuation v. Let E/K_v be an elliptic curve with additive reduction. We denote the usual discriminant of a Weierstrass model for E/K_v by Δ, and the quadratic residue symbol on the residue field of K_v by $\left(\frac{}{k_v}\right)$.*

(1) Assume E has potentially good reduction. Define $e = 12/\gcd(v(\Delta), 12)$. We have $e \in \{1, 2, 3, 4, 6\}$, and the local root number $w(E/K_v)$ can be computed by the following formula:

$$w(E/K_v) = \begin{cases} 1 & \text{if } e = 1, \\ \left(\frac{-1}{k_v}\right) & \text{if } e = 2 \text{ or } 6, \\ \left(\frac{-3}{k_v}\right) & \text{if } e = 3, \\ \left(\frac{-2}{k_v}\right) & \text{if } e = 4. \end{cases}$$

(2) If E has potentially multiplicative reduction, then $w(E/K_v) = \left(\frac{-1}{k_v}\right)$.

In [K], Kobayashi gives a formula for the local root number $w(E/K_v)$ with any local field K_v of *odd* residue characteristic.

Theorem 4.5. (Theorem 1.1 of [K])
Let K_v be a local field, with residue field of odd characteristic and normalized valuation v. Let E/K_v be an elliptic curve with potentially good reduction. We denote the Hilbert symbol of K_v by $(\ ,\ )_{K_v}$.

(1) If the Kodaira-Néron type of E is I_0 or I_0^*, then

$$w(E/K_v) = \left(\frac{-1}{k_v}\right)^{v(\Delta)/2}.$$

(2) If the Kodaira-Néron type of E is III or III^*, then

$$w(E/K_v) = \left(\frac{-2}{k_v}\right).$$

(3) If the Kodaira-Néron type of E is II, IV, IV^* or II^*, there exists a Weierstrass equation such that $y^2 = x^3 + ax^2 + bx + c$ with $3 \nmid v(c)$. Then for such equation, we have

$$w(E/K_v) = \delta\ (\Delta,\, c)_{K_v} \left(\frac{v(c)}{k_v}\right)^{v(\Delta)} \left(\frac{-1}{k_v}\right)^{\frac{v(\Delta)(v(\Delta)-1)}{2}}$$

where $\delta = \pm 1$ and $\delta = 1$ if and only if $\Delta^{\frac{1}{2}} \in K_v$.

Thus $w(E/K_v)$ have been classified except at places above 2. In [DD2], Dokchitser and Dokchitser complete the remaining case. However for an elliptic curve $E : y^2 = x^3 + a$, the local root number $w(E/K_v)$ at places above 2 can be easily computed by Kobayashi. (Note that Dokchitser and Dokchitser [D-D2, Section 4] inform the misprints in [K, Proposition 6.1].)

Theorem 4.6. (Proposition 6.1 of [K]) *Let K_v be a local field, with residue field of even characteristic and normalized valuation v. Let E/K_v be an elliptic curve $E : y^2 = x^3 + a$ of the conductor N_E. Then*

$$w(E/K_v) = \begin{cases} (-1,\, a)_{K_v} & \text{if } v(\Delta) \equiv 0 \pmod 3 \text{ or } \sqrt{-3} \in K_v; \\ (-1)^{\frac{N_E}{2}}\ (3,\ a)_{K_v} & \text{otherwise.} \end{cases}$$

4.2.2 Proof of Theorem 4.3

Using the formula in Theorem 4.4 (1), Theorem 4.5, and Theorem 4.6 we can show the following lemma.

Lemma 4.7. *Let a be a six power free integer with factorization $a = 3^y a_3$, where $3 \nmid a_3$. Let D be a cube-free integer. Then $E_D : y^2 = x^3 + aD^2$ has the root number*

$$w(E_D/\mathbb{Q}) = -\prod_p w(E_D/\mathbb{Q}_p)$$

where for $p \geq 5$,

$$\text{if } p \nmid a, \quad w(E_D/\mathbb{Q}_p) = \begin{cases} -1 & \text{if } p \mid D \text{ and } p \equiv 2 \pmod 3 \\ +1 & \text{elsewhere} \end{cases}$$

$$\text{if } p \,||\, a, \quad w(E_D/\mathbb{Q}_p) = \begin{cases} -1 & \text{if } p \equiv 3 \pmod 4 \\ +1 & \text{elsewhere} \end{cases}$$

for $p = 2$,

$$\text{if } 2 \nmid a, \quad w(E_D/\mathbb{Q}_p) = \begin{cases} +1 & \text{if } 2^2 \,||\, D \text{ and } a \equiv 1 \pmod 4 \\ -1 & \text{elsewhere} \end{cases}$$

$$\text{if } 2 \,||\, a, \quad w(E_D/\mathbb{Q}_p) = \begin{cases} -1 & \text{if } a \equiv -2 \pmod 8 \\ +1 & \text{elsewhere} \end{cases}$$

and for $p = 3$,

$$\text{if } 3 \nmid a, \quad w(E_D/\mathbb{Q}_3) = \begin{cases} -1 & \text{if } a \equiv 1, 2 \pmod 9 \text{ and } D \equiv \pm 4 \pmod 9; \\ & \quad a \equiv 4, 8 \pmod 9 \text{ and } D \equiv \pm 2 \pmod 9; \\ & \quad a \equiv 5, 7 \pmod 9 \text{ and } D \equiv \pm 1 \pmod 9; \\ & \quad a \equiv 1 \pmod 3 \text{ and } 3 \,||\, D; \text{ or if} \\ & \quad a \equiv 2 \pmod 3 \text{ and } 3^2 \,||\, D \\ 1 & \text{otherwise} \end{cases}$$

$$\text{if } 3 \,||\, a, \quad w(E_D/\mathbb{Q}_3) = \begin{cases} -1 & \text{if } a \equiv 3, 15 \pmod{27} \text{ and } D \equiv \pm 6 \pmod{27}; \\ & \quad a \equiv 6, 12 \pmod{27} \text{ and } D \equiv \pm 3 \pmod{27}; \\ & \quad a \equiv 21, 24 \pmod{27} \text{ and } D \equiv \pm 12 \pmod{27}; \\ & \quad a \equiv 3 \pmod 9 \text{ and } 3 \nmid D; \text{ or if} \\ & \quad a \equiv 6 \pmod 9 \text{ and } 3^2 \,||\, D \\ 1 & \text{otherwise} \end{cases}$$

Remark 4.8. If there is a prime factor p such that $p^{2n} \mid a$ for some integer $n > 0$, consider it as the factor of D. So using Lemma 4.7 we can calculate the local root number $w(E_D/\mathbb{Q})$ for any curves $E_D : y^2 = x^3 + aD^2$.

By a slight generalization of the proof of Theorem 2 of [Ma], we can easily obtain the following lemma.

Lemma 4.9. *For distinct primes* $p_1, \cdots, p_k$,

$$\sum_{\substack{D \text{ cube-free} \le X \\ \tau_2(D) \text{ is even} \\ D \equiv D_0 \pmod{3^l} \\ \mathrm{ord}_{p_i}(D) = c_i (1 \le i \le k)}} 1 \;=\; \frac{1}{2} \sum_{\substack{D \text{ cube-free} \le X \\ D \equiv D_0 \pmod{3^l} \\ \mathrm{ord}_{p_i}(D) = c_i (1 \le i \le k)}} 1 \;+\; O(\sqrt{X} \log X),$$

where $\tau_2(D)$ *is the number of distinct primes* $p \equiv 2 \pmod 3$ *such that* $p \mid D$.

Now we can prove Theorem 4.3.

Proof of Theorem 4.3. Let $E/\mathbb{Q} : y^2 = x^3 + a$ with a six power free integer a, and let $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ be the factorization of a into distinct prime powers, $e_i \geq 1$ for all i. Then for a cube-free integer D, let E_D be the cubic twist

$$E_D : y^2 = x^3 + aD^2.$$

Let D and D' be two cube-free integers such that

(1) $D \equiv D' \pmod{27}$,

(2) $\mathrm{ord}_2(D) = \mathrm{ord}_2(D')$,

(3) $\mathrm{ord}_{p_i}(D) = \mathrm{ord}_{p_i}(D')$ for all $1 \leq i \leq k$.

Then $w(E_D/\mathbb{Q}_p) = w(E_{D'}/\mathbb{Q}_p)$ for all primes p by Lemma 4.7, so we will divide the cases as follows:

$$\sum_{\substack{\text{cube-free } D \leq X \\ w(E_D/\mathbb{Q})=1}} 1 \quad = \quad \sum_{D_0} \sum_{(c,c_1,\cdots,c_k)} \sum_{\substack{\text{cube-free } D \leq X \\ w(E_D/\mathbb{Q})=1 \\ D \equiv D_0 \pmod{3^l} \\ (q,q_1,\cdots,q_k)=(c,c_1,\cdots,c_k)}} 1$$

where $(q, q_1, \cdots, q_k) := (ord_2(D), ord_{p_1}(D), \cdots, ord_{p_k}(D))$.

For a prime factor $p \neq 2, 3$ of D with $p \nmid a$, the condition $w(E_D/\mathbb{Q}_p) = -1$ is equivalent to $p \equiv 2 \pmod 3$. Thus, the global root number $w(E_D/\mathbb{Q})$ is completely determined by the parity of $\tau_2(D)$. Therefore, by Lemma 4.9

$$\begin{aligned} \sum_{\substack{\text{cube-free } D \leq X \\ w(E_D/\mathbb{Q})=1}} 1 \quad &= \quad \frac{1}{2} \sum_{D_0} \sum_{(c,c_1,\cdots,c_k)} \sum_{\substack{\text{cube-free } D \leq X \\ D \equiv D_0 \pmod{3^l} \\ (q,q_1,\cdots,q_k)=(c,c_1,\cdots,c_k)}} 1 \quad + \quad O(\sqrt{X} \log X) \\ &= \quad \frac{1}{2} \sum_{\text{cube-free } D \leq X} 1 \quad + \quad O(\sqrt{X} \log X). \end{aligned}$$

□

4.3 Elliptic curves with all cubic twists of the same root number

Recall that Dokchitser and Dokchitser [DD] consider an elliptic curve E/K all of whose quadratic twists have the same global root number, and they gave the conditions on E/K which determine whether it is such a curve. In this section, we give an answer to the analogous question for cubic twists, i.e., to determine which elliptic curves have the same global root number over all its cubic twists.

Lemma 4.10 (Corollary 6.3 of [K])**.** *Let $E : y^2 = x^3 + a$ be an elliptic curve over a number field K. If K contains $\mathbb{Q}(\sqrt{-3})$, then $w(E/K) = 1$.*

Remark 4.11. The Parity conjecture and Lemma 4.10 imply that if $K \ni \sqrt{-3}$, every elliptic curve $E : y^2 = x^3 + a$ over a number field K has the Mordell-Weil group $E(K)$ of even rank. On the other hand, using the complex multiplication $[\zeta_3]$ of E/K, where ζ_3 is a primitive cubic root of unity and $[\zeta_3](x, y) = (\zeta_3 x, y)$, we can show this without the Parity conjecture, because $E(K)$ is a direct sum of two-dimensional subspaces with the bases of the form $\{P, [\zeta_3]P\}$.

Theorem 4.12. (Theorem 1.1. of [BK2]) *Let $E : y^2 = x^3 + a$ be an elliptic curve over a number field K. For a cube-free $D \in K^*$, let $E_D : y^2 = x^3 + aD^2$ be the cubic twist of E. Then the root number $w(E_D/K)$ is constant for all $D \in K^*$ if and only if K contains $\sqrt{-3}$.*

Proof. By Lemma 4.10, it suffices to show the necessary condition. Suppose that $K \not\ni \sqrt{-3}$. Then it suffices to find $D, D' \in K^*/(K^*)^3$ such that $D \neq k^3 D'$

for any $k \in K^*$ and

$$w(E_D/K) \neq w(E_{D'}/K).$$

Using the Chebotarev density theorem for the cyclotomic extension $K(\sqrt{-3})$ over K, we can show that there are infinitely many prime numbers p with $p \equiv 2 \pmod 3$ such that some $\mathfrak{p} \,|\, p$ in K has the residual degree $f(\mathfrak{p} \,|\, p) = 1$. So we can pick $\mathfrak{p} \,|\, p$ in K satisfying the following three conditions:

(a1) The prime number p is $\neq 2, 3$, and $p \equiv 2 \pmod 3$.

(a2) The residual degree $f(\mathfrak{p} \,|\, p)$ is 1.

(a3) $\mathfrak{p}$ doesn't contain the coefficient a of E.

Let v' be the finite place of K corresponding to the prime ideal $\mathfrak{p}$, and let $\pi \in K^*$ be a local uniformizer of v' such that for all the other finite places v of K, $v(\pi) = 0$. On the other hand, we can easily find $D \in K^*/(K^*)^3$ satisfying the following three properties:

(b1) $3 \nmid v(aD^2)$ for all places v over 3 of K.

(b2) $v(\Delta(E_D/K)) \equiv 0 \pmod 3$ for all places v over 2 of K.

(b3) $v'(D) = 0$.

Now, we show that the following two twists of E have different root numbers:

$$E_D : y^2 = x^3 + aD^2, \;\; E_{\pi D} : y^2 = x^3 + a\pi^2 D^2.$$

We first compare their local root numbers over K_v with the residue characteristic ≥ 5. For all these $v(\neq v')$, the assumption $v(\pi) = 0$ implies that the numbers e in Theorem 4.4(1) for E_D and $E_{\pi D}$ are same, and, therefore, we can conclude that $w(E_D/K_v) = w(E_{\pi D}/K_v)$. For the v', E_D has good reduction at

v' by the conditions (a1) and (b1), and so $w(E_D/K_{v'}) = 1$. Also, since π is a local uniformizer, the number e in Theorem 4.4(1) is 3, and hence we have

$$w(E_{\pi D}/K_{v'}) = \left(\frac{-3}{k_{v'}}\right) = \left(\frac{-3}{p}\right)^{f(\mathfrak{p}|p)} = \left(\frac{p}{3}\right) = -1$$

by the conditions (a1), (a2). For a place v with the residue characteristic 3, E_D/K_v and $E_{\pi D}/K_v$ are of type II, IV, IV^* or II^* by (a1). Then the formulas in Theorem 4.5 (3) for E_D and $E_{\pi D}$ are same, and thus

$$w(E_D/K_v) = w(E_{\pi D}/K_v).$$

Finally, for a place v with the residue characteristic 2, we have

$$w(E_D/K_v) = (-1\,,\, aD^2)_{K_v} = (-1\,,\, a)_{K_v} = (-1\,,\, a\pi^2 D^2)_{K_v} = w(E_{\pi D}/K_v)$$

by Theorem 4.6. Furthermore, for a fixed π, there are infinitely many $D \in K^*/(K^*)^3$ satisfying the property (b1)-(b3), and the involution $D \leftrightarrow \pi D$ on K^*/K^{*3} changes the sign of $w(E_D/K)$. Thus, taking $D' := \pi D$ completes the proof of theorem. □

It is interesting to note that the condition which determines whether all cubic twists of E/K has the same root number or not depends only on the base field.

Remark 4.13. In particular, if $K \ni \sqrt{-3}$ then $w(E_D/K) = 1$ for all $D \in K^*$, and if $K \not\ni \sqrt{-3}$ then there are infinitely many E_D/K such that $w(E_D/K) = 1$ and $w(E_D/K) = -1$, respectively.

Chapter 5

Selmer groups of twists of elliptic curves

In this chapter, we first introduce the paper of Mazur and Rubin (2010) [MR2]. They investigate the variation of the 2-Selmer rank in quadratic twist families of elliptic curves over number fields. They give sufficient conditions on an elliptic curve so that it has twists of arbitrary 2-Selmer rank, and give lower bounds for the number of quadratic twists that have a given 2-Selmer rank.

For the most part the proofs avoid the big guns of late 20th century elliptic curve theory, e.g. no use of modular forms methods nor Kolyvagin's Euler systems methods. Instead, they manage to their own circumvent big machinery in place of clever calculations using cocycles and number fields.

We will check that whether each statement of this paper holds for the cubic twists case. Moreover, we will extend their paper to cubic twists.

5.1 Mazur and Rubin's results

In [MR2], Mazur and Rubin study the variation of the 2-Selmer rank in quadratic twist families of elliptic curves over number fields. They give sufficient conditions on an elliptic curve so that it has twists of arbitrary 2-Selmer rank.

Note that not all elliptic curves have quadratic twists of every 2-Selmer rank. The theorem [DD] of Dokchitser and Dokchitser, combined with the Tate-Shafarevich conjecture, predicts that E/K has constant 2-Selmer parity, meaning that 2-Selmer ranks of all quadratic twists of E/K have the same parity, if and only K is totally imaginary and E acquired everywhere good reduction over an abelian extension of K. They expect that constant parity and the existence of rational 2-torsion are the only obstructions to having twists of every 2-Selmer rank:

Conjecture 5.1 (Conjecture 1.3 of [MR2])**.** *Suppose K is a number field and E is an elliptic curve over K. For $n \in \mathbb{N}$ and $X \in \mathbb{R}_{\geq 0}$, let*

$$N_r(E, X) := \#\{\textit{quadratic } F/K : \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^F/K) = r \textit{ and } \mathbb{N}_{K/\mathbb{Q}}\mathfrak{f}(F/K) < X\},$$

where $\mathfrak{f}(F/K)$ denotes the finite part of the conductor of F/K.
(i) *If $r \geq \dim_{\mathbb{F}_2} E(K)[2]$ and $r \equiv \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E/K) \pmod 2$, $N_r(E, X) \gg X$.*
(ii) *If K has a real embedding, or if E/K does not acquire everywhere good reduction over an abelian extension of K, then $N_r(E, X) \gg X$ for every $r \geq \dim_{\mathbb{F}_2} E(K)[2]$.*

The condition $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^F/K) \geq \dim_{\mathbb{F}_2} E(K)[2]$ holds for all quadratic twists, because $E(K)[2] \cong E^F(K)[2]$ for all quadratic twists and by the Kummer exact sequence $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E/K) \geq \dim_{\mathbb{F}_2} E(K)[2]$.

In this direction, they prove the following theorem.

Theorem 5.2 (Corollary 1.9 of [MR2]). *Suppose K is a number field. There are elliptic curves E over K such that for every $r \geq 0$, E has many quadratic twists E^F/K with $\dim_{\mathbb{F}_2}\mathrm{Sel}_2(E^F/K) = r$.*

Note that in the statements above, the phrase "E has many cubic twists" means that the number of such twists, ordered by $\mathbb{N}_{K/\mathbb{Q}}\mathfrak{f}(L/K)$, is $\gg X/(\log X)^c$ for some $c \in \mathbb{R}$.

As applications, they obtain two important results. The first settles an open question mentioned to by Poonen.

Theorem 5.3 (Theorem 1.1 of [MR2]). *If K is a number field, then there is an elliptic curve E over K with $E(K) = 0$.*

The second relies on a weak version of the Tate-Shafarevich conjecture.

Theorem 5.4 (Theorem 1.2 of [MR2]). *Suppose that for every number field K and every elliptic curve E/K, $\dim_{\mathbb{F}_2}Ш(E/K)[2]$ is even. Then for every number field K, Hilbert's Tenth Problem is undecidable, i.e. has negative answer, over the ring of integers of K.*

5.2 Twisting commutative algebraic groups

Much of the technical machinery for this section is drawn from Sections 4 and 5 of [MRS].

5.2.1 The Weil restriction of scalars

Let L/K be a finite Galois extension of fields with Galois group G, and let V be a commutative algebraic group over K.

Definition 5.5 (See for example §1.3 of [W] or Definition 2.2 of [Sb])**.** The *Weil restriction of scalars* of V from L to K, denoted by $\mathrm{Res}_K^L V$, is a commutative algebraic group over K along with a homomorphism

$$\eta_{L/K} : \mathrm{Res}_K^L V \to V$$

defined over L, with the universal property that for every variety X over K, the map

$$\mathrm{Hom}_K(X, \mathrm{Res}_K^L V) \xrightarrow{\sim} \mathrm{Hom}_L(X, V), \qquad f \mapsto \eta_{L/K} \circ f$$

is an isomorphism.

Note that the universal property defines $\mathrm{Res}_K^L V$ uniquely up to K-isomorphism, and for every commutative K- algebra A, there is an isomorphism

$$(\mathrm{Res}_K^L V)(A) \cong V(A \otimes_K L).$$

In particular, $(\mathrm{Res}_K^L V)(K) \cong V(L)$.

Example 5.1 (See §2.1.2 of [Sb]). Suppose K is a number field and suppose $E : y^2 = x^3 + ax + b$ is an elliptic curve over K. Suppose D is a non-square in K^* and let $L := K(\sqrt{D})$ be a quadratic extension of K. Let $E^D : y^2 = x^3 + aD^2x + bD^3$ be the quadratic twist of E by D. Define

$$\phi : E \xrightarrow{\sim} E^D \qquad (x, y) \mapsto (Dx, D\sqrt{D}y),$$

an isomorphism defined over L and $T := \{\, (P,\, \phi(P)) \in E \times E^D \mid 2P = 0 \,\}$. Then $\mathrm{Res}_K^L E$ is $(E \times E^D)/T$ with the following homomorphism

$$\eta_{L/K} : (E \times E^D)/T \to E, \qquad (P, Q) \mapsto P + \phi^{-1}(Q).$$

For a cubic twist case, we obtain the following new result.

Theorem 5.6. *Suppose K is a number field containing a primitive 3rd root of unity ω and let $E : y^2 = x^3 + a$ $(a \in K)$ be an elliptic curve over K. Suppose D is a non-cube in K^* and let $L := K(\sqrt[3]{D})$ be a cubic Galois extension of K. Let $E_D : y^2 = x^3 + aD^2$ be the cubic twist of E by D. Define*

$$\begin{aligned} \phi_1 : E &\xrightarrow{\sim} E_D \qquad (x, y) \mapsto (D^{\frac{2}{3}}x, Dy), \\ \phi_2 : E &\xrightarrow{\sim} E_{D^2} \qquad (x, y) \mapsto (D^{\frac{4}{3}}x, D^2 y), \end{aligned}$$

isomorphisms defined over L and $T := \{\, (P, \phi_1(P), \phi_2(P)) \in E \times E_D \times E_{D^2} \mid 3P = 0 \}$. Then $\mathrm{Res}_K^L E$ is $(E \times E_D \times E_{D^2})/T$ with the following homomorphism

$$\eta_{L/K} : (E \times E_D \times E_{D^2})/T \to E, \qquad (P, Q, R) \mapsto P + \phi_1^{-1}(Q) + \phi_2^{-1}(R).$$

Proof. We will show that $(E \times E_D \times E_{D^2})/T$ satisfies the universal property of $\mathrm{Res}_K^L E$ with $\eta_{L/K}$. Suppose X is a variety over K and suppose $\varphi \in \mathrm{Hom}_L(X, E)$. Let $[3]^{-1} : E \to E\,/E[3]$ be the inverse map of the induced isomorphism from multiplication by 3, let

$$\lambda : E\,/E[3] \to (E \times E_D \times E_{D^2})/T, \qquad P \mapsto \big(P,\, \phi_1(P),\, \phi_2(P)\big) \pmod T,$$

and let σ be the generator of $G = \mathrm{Gal}(L/K)$ which maps $\sqrt[3]{D}$ to $\sqrt[3]{D}\,\omega$. Define

$$\tilde{\varphi} := \lambda \circ [3]^{-1} \circ \varphi + (\lambda \circ [3]^{-1} \circ \varphi)^{\sigma} + (\lambda \circ [3]^{-1} \circ \varphi)^{\sigma^2} \in \mathrm{Hom}_K\big(X,\, (E \times E_D \times E_{D^2})/\,T\,\big).$$

Then we have that

$$\begin{aligned}
&\eta_{L/K} \circ\ \lambda \circ [3]^{-1} \circ \varphi &&= \varphi,\\
&\eta_{L/K} \circ (\lambda \circ [3]^{-1} \circ \varphi)^{\sigma} &&= 0 \quad (\because \phi_1^{\sigma} = [\omega]\phi_1,\ \phi_2^{\sigma} = [\omega]^2\phi_2,\ [1+\omega+\omega^2] = [0]),\\
&\eta_{L/K} \circ (\lambda \circ [3]^{-1} \circ \varphi)^{\sigma^2} &&= 0 \quad (\text{by the same reason}),
\end{aligned}$$

where $[\omega] : (x, y) \mapsto (\omega^2 x, y)$ is an endomorphism of E, E_D, and E_{D^2}. So $\eta_{L/K} \circ \tilde{\varphi} = \varphi$.

On the other hand, for any $(P, Q, R) \in (E \times E_D \times E_{D^2})/T$

$$\begin{aligned}
(P,Q,R) &\overset{\eta_{L/K}}{\longmapsto} && P + \phi_1^{-1}(Q) + \phi_2^{-1}(R)\\
&\overset{[3]^{-1}}{\longmapsto} && P' + \phi_1^{-1}(Q') + \phi_2^{-1}(R')\\
&\overset{\lambda}{\longmapsto} && \Big(P' + \phi_1^{-1}(Q') + \phi_2^{-1}(R'),\\
& && \quad \phi_1(P') + Q' + \phi_1(\phi_2^{-1}(R')),\\
& && \quad \phi_2(P') + \phi_2(\phi_1^{-1}(Q')) + R'\Big) \pmod{T},\\
(P,Q,R) &\overset{(\lambda \circ [3]^{-1} \circ \eta_{L/K})^{\sigma}}{\longmapsto} && \Big(P' + [\omega]^2\phi_1^{-1}(Q') + [\omega]\phi_2^{-1}(R'),\\
& && \quad [\omega]\phi_1(P') + Q' + [\omega]^2\phi_1(\phi_2^{-1}(R')),\\
& && \quad [\omega]^2\phi_2(P') + [\omega]\phi_2(\phi_1^{-1}(Q')) + R'\Big),\\
(P,Q,R) &\overset{(\lambda \circ [3]^{-1} \circ \eta_{L/K})^{\sigma^2}}{\longmapsto} && \Big(P' + [\omega]\phi_1^{-1}(Q') + [\omega]^2\phi_2^{-1}(R'),\\
& && \quad [\omega]^2\phi_1(P') + Q' + [\omega]\phi_1(\phi_2^{-1}(R')),\\
& && \quad [\omega]\phi_2(P') + [\omega]^2\phi_2(\phi_1^{-1}(Q')) + R'\Big),
\end{aligned}$$

where P' (resp. Q', R') is an element satisfying $[3]P' = P$ (resp. $[3]Q' = Q$, $[3]R' = R$). So $(\lambda \circ [3]^{-1} \circ \eta_{L/K}) + (\lambda \circ [3]^{-1} \circ \eta_{L/K})^{\sigma} + (\lambda \circ [3]^{-1} \circ \eta_{L/K})^{\sigma^2} = \mathrm{id}$, and hence for every $f \in \mathrm{Hom}_K(X, (E \times E_D \times E_{D^2})/T$, we have

$$\begin{aligned}
&\widetilde{(\eta_{L/K} \circ f)}\\
&= (\lambda \circ [3]^{-1} \circ \eta_{L/K} \circ f) + (\lambda \circ [3]^{-1} \circ \eta_{L/K} \circ f)^{\sigma} + (\lambda \circ [3]^{-1} \circ \eta_{L/K} \circ f)^{\sigma^2}\\
&= (\lambda \circ [3]^{-1} \circ \eta_{L/K}) \circ f + (\lambda \circ [3]^{-1} \circ \eta_{L/K})^{\sigma} \circ f + (\lambda \circ [3]^{-1} \circ \eta_{L/K})^{\sigma^2} \circ f\\
&= f.
\end{aligned}$$

Therefore, the map $\mathrm{Hom}_K\big(X, (E \times E_D \times E_{D^2})/T\big) \to \mathrm{Hom}_L(X, E)$ defined by $f \mapsto \eta_{L/K} \circ f$ is an isomorphism. □

5.2.2 Twisting commutative algebraic groups

Let L/K be a finite Galois extension of fields with Galois group G, and let K^s be a separable closure of K with $G_K := \mathrm{Gal}(K^s/K)$. Suppose that V is a commutative algebraic group over K, suppose $\mathcal{I}$ is a free $\mathbb{Z}$-module of finite rank with a continuous right action of G_K (the modules are given the discrete topology), and suppose there is a ring homomorphism $\mathbb{Z} \to \mathrm{End}_K(V)$. In particular, view $\mathbb{Z}$ as a free rank one $\mathbb{Z}$-module with trivial G_K-action.

Definition 5.7 (See Definition 1.1 of [MRS] and §2.2 of [Sb], respectively)**.** (1) Let $d := \mathrm{rank}_{\mathbb{Z}}(\mathcal{I})$, and fix an $\mathbb{Z}$-module isomorphism $j : \mathbb{Z}^d \xrightarrow{\sim} \mathcal{I}$. Let $c_{\mathcal{I}} \in H^1(K, \mathrm{Aut}_{K^s}(V^d))$ be the image of the cocycle $(\gamma \mapsto j^{-1}j^{\gamma})$ under the composition

$$H^1(K, \mathrm{GL}_d(\mathbb{Z})) \longrightarrow H^1(K, \mathrm{Aut}_K(V^d)) \longrightarrow H^1(K, \mathrm{Aut}_{K^s}(V^d))$$

induced by the homomorphism $\mathbb{Z} \to \mathrm{End}_K(V)$. Define $\mathcal{I} \otimes_{\mathbb{Z}} V$ to be the twist of V^d by the cocycle $c_{\mathcal{I}}$, i.e., $\mathcal{I} \otimes_{\mathbb{Z}} V$ is the unique commutative algebraic group over K with an isomorphism $\phi : V^d \xrightarrow{\sim} \mathcal{I} \otimes_{\mathbb{Z}} V$ defined over K^s such that for every $\gamma \in G_K$,

$$c_{\mathcal{I}}(\gamma) = \phi^{-1} \circ \phi^{\gamma}.$$

(2) For each $g \in G_K$, consider $\eta_{L/K}^g \in \mathrm{Hom}_L(\mathrm{Res}_K^L V, V)$. By the universal property of $\mathrm{Res}_K^L V$, there is $g_{L/K,V} \in \mathrm{Hom}_K(\mathrm{Res}_K^L V, \mathrm{Res}_K^L V)$ such that $\eta_{L/K} \circ$

$g_{L/K,V} = \eta_{L/K}^g$. Define a ring homomorphism

$$-_V : \mathbb{Z}[G] \to \mathrm{End}_K(\mathrm{Res}_K^L V), \qquad \sum_{g\in G} a_g\, g \mapsto a_g\, g_{L/K,V}.$$

Proposition 5.8 (Proposition 4.2 of [MRS])**.** *If $\mathbb{Z}[G]/\mathcal{I}$ is a projective $\mathbb{Z}$-module,*

$$\mathcal{I} \otimes_{\mathbb{Z}} V = \bigcap_{\alpha\in\mathcal{I}^\perp} \ker\left(\alpha_V : \mathrm{Res}_K^L V \to \mathrm{Res}_K^L V\right),$$

where $\mathcal{I}^\perp := \{\alpha \in \mathbb{Z}[G] : \alpha\mathcal{I} = 0\}$ is the ideal of $\mathbb{Z}[G]$.

5.2.3 Abelian twists

Suppose that L/K is an *abelian* extension with $G = \mathrm{Gal}(L/K)$, and E is an elliptic curve defined over K. For a cyclic extension F of K in L with $H = \mathrm{Gal}(L/F)$, define

$$e_H := \frac{1}{|G|} \sum_{g\in G} \sum_{\substack{\chi\in\hat{G}\\ \ker(\chi)=H}} \chi(g)\, g^{-1} \in \mathbb{Q}[G].$$

Let $\mathbb{Q}[G]_F := e_H\, \mathbb{Q}[G]$, a simple $\mathbb{Q}[G]$-submodule of $\mathbb{Q}[G]$. Then the action of G on $\mathbb{Q}[G]_F$ is the unique irreducible representation of G contained in $\mathbb{Q}[G]$ whose kernel is H, and the semisimple group ring $\mathbb{Q}[G]$ decomposes

$$\mathbb{Q}[G] = \bigoplus_{\substack{F:\text{cyclic}\\ K\subseteq F\subseteq L}} \mathbb{Q}[G]_F.$$

Definition 5.9 (Definition 5.1 of [MRS])**.** For every cyclic extension F of K in L, define

$$\mathcal{I}_F := \mathbb{Q}[G]_F \cap \mathbb{Z}[G] \quad \text{and} \quad A_F := \mathcal{I}_F \otimes_{\mathbb{Z}} E.$$

If d is a positive integer, let $\Phi_d \in \mathbb{Z}[x]$ be the d-th cyclotomic polynomial, and let $\Psi_d(x) := (x^d - 1)/\Phi_d(x) \in \mathbb{Z}[x]$. In the case L/K is cyclic, $\mathcal{I}_L$ can easily be obtained:

Proposition 5.10 (Lemma 5.4 of [MRS]). *If L/K is cyclic of degree n with a generator σ, then*

$$\mathcal{I}_L = \Psi_n(\sigma)\,\mathbb{Z}[G] \quad \textit{and} \quad \mathcal{I}_L^{\perp} = \Phi_n(\sigma)\,\mathbb{Z}[G].$$

Example 5.2 (See §2.2.2 of [Sb]). Suppose K is a number field and suppose $E : y^2 = x^3 + ax + b$ is an elliptic curve over K. Suppose D is a non-square in K^* and let $L := K(\sqrt{D})$ be a quadratic extension of K with $\mathrm{Gal}(L/K) = \sigma$. Let $E^D : y^2 = x^3 + aD^2x + bD^3$ be the quadratic twist of E by D. Recall that by Example 5.1 $\mathrm{Res}_K^L E$ is $(E \times E^D)/T$, where $T = \{P, \phi(P)) \in E \times E^D | 2P = O\}$. The image of σ under Definition 5.7(2) is

$$\sigma_E(P, Q) = (P, -Q),$$

and hence

$$\Phi_2(\sigma)_E(P, Q) = (\sigma + 1)_E(P, Q) = (2P, O).$$

Thus by Proposition 5.8 and Proposition 5.10, we have

$$\begin{aligned} A_L := \mathcal{I}_L \otimes_{\mathbb{Z}} E &= \ker\big(\Phi_2(\sigma)_E : \mathrm{Res}_K^L E \to \mathrm{Res}_K^L E\big) \\ &= \{(P, Q) \in (E \times E^D)/T \,|\, (2P, O) \equiv (O, O) \pmod{T}\} \\ &= \{(P, Q) \in (E \times E^D)/T \,|\, P \in E[2]\} \cong E^D. \end{aligned}$$

For a cubic twist case, we obtain the following new result.

Theorem 5.11. *Suppose K is a number field containing a primitive 3rd root of unity ω and let $E : y^2 = x^3 + a$ be an elliptic curve over K. Suppose D is a non-cube in K^* and let $L := K(\sqrt[3]{D})$ be a cubic Galois extension of K. Let $E_D : y^2 = x^3 + aD^2$ be the cubic twist of E by D. Then A_L is $E_D \times E_{D^2}$ inside $\mathrm{Res}^L_K E$.*

Proof. We continue the with notations K , L , σ , E , E_D , T , $\eta_{L/K}$, $\widetilde{\cdot}$ in Theorem 5.6. Recall that $\mathrm{Res}^L_K E$ is $(E \times E_D \times E_{D^2})\,/\,T$ with the homomorphism $\eta_{L/K}$. Note that for the $\sigma \in \mathrm{Gal}(L/K)$, its induced endomorphism $\sigma_E \in \mathrm{End}_K(\mathrm{Res}^L_K E)$ defined in Definition 5.7(2) is precisely

$$\sigma_E(P,Q,R) = \widetilde{\eta^\sigma_{L/K}}\,(P,Q,R) = (P,\, [\omega]^2 Q,\, [\omega]R),$$

and hence $\Phi_3(\sigma)_E$ is given by

$$\Phi_3(\sigma)_E(P,Q,R) = (\sigma^2+\sigma+1)_E(P,Q,R) = (\,3P,\, O\,,\, O\,).$$

Thus by Proposition 5.8 and Proposition 5.10, we have

$$\begin{aligned} A_L := \mathcal{I}_L \otimes_{\mathbb{Z}} E &= \ker\big(\Phi_3(\sigma)_E : \mathrm{Res}^L_K E \to \mathrm{Res}^L_K E\big) \\ &= \{(P,Q,R) \in (E \times E_D \times E_{D^2})/\,T \,|\, (3P,O,O) \equiv (O,O,O) (\mathrm{mod}\, T)\} \\ &= \{(P,Q,R) \in (E \times E_D \times E_{D^2})/\,T \,|\, P \in E[3]\}. \end{aligned}$$

We claim that

$$\mathrm{im}\,(E_D \times E_{D^2} \hookrightarrow \mathrm{Res}^L_K E) \;=\; \{(P,Q,R) \in (E \times E_D \times E_{D^2})/\,T \mid\; P \in E[3]\,\},$$

where the left side is the image of $E_D \times E_{D^2} \hookrightarrow E \times E_D \times E_{D^2} \twoheadrightarrow (E \times E_D \times E_{D^2})/T$. To prove it, let $(P,Q,R) \in (E \times E_D \times E_{D^2})/\,T$ with $P \in E[3]$. Then

$$\begin{aligned} (P,Q,R) &= \big(P,\, \phi_1(P),\, \phi_2(P)\big) + \big(O,\, Q-\phi_1(P),\, R-\phi_2(P)\big) \\ &\equiv \big(O,\, Q-\phi_1(P),\, R-\phi_2(P)\big) \pmod{T} \\ &\in \mathrm{im}\,(E_D \times E_{D^2} \hookrightarrow \mathrm{Res}^L_K E), \end{aligned}$$

and the other inclusion is clear. Therefore, A_L is $E_D \times E_{D^2}$ inside $\mathrm{Res}_K^L E$. $\square$

5.3 Local conditions

For this section, fix a number field K and a cyclic extension L/K of degree 3 with $G := \mathrm{Gal}(L/K)$. Let R_L be the maximal order of $\mathbb{Q}[G]_L$. Then R_L has a unique prime ideal above 3, which we denote by $\mathfrak{p}_L$.

Definition 5.12 (See Definition 2.1 of [MR2] and Definition 4.3 of [MR])**.** Suppose E is an elliptic curve over K. For every place $\mathfrak{p}$ of K, let $H^1_f(K_\mathfrak{p}, E[3])$ denote the image of the Kummer map

$$E(K_\mathfrak{p})/3E(K_\mathfrak{p}) \longrightarrow H^1(K_\mathfrak{p}, E[3]),$$

and let $H^1_g(K_\mathfrak{p}, A_L[3])$ denote the image of the Kummer map

$$A_L(K_\mathfrak{p})/\mathfrak{p}_L A_L(K_\mathfrak{p}) \longrightarrow H^1(K_\mathfrak{p}, A_L[\mathfrak{p}_L]).$$

Lemma 5.13.

(i) *If* $\mathfrak{p} \nmid 3\infty$ *then* $\dim_{\mathbb{F}_3}(H^1_f(K_\mathfrak{p}, E[3])) = \dim_{\mathbb{F}_3}(E(K_\mathfrak{p})[3])$.

(ii) *If* $\mathfrak{p} \nmid 3\infty$ *and* E *has good reduction at* v*, then*

$$H^1_f(K_\mathfrak{p}, E[3]) \cong E[3]/(\mathrm{Frob}_\mathfrak{p} - 1)E[3]$$

with the isomorphism given by evaluating cocycles at the Frobenius automorphism $\mathrm{Frob}_\mathfrak{p}$.

Proof. Suppose $\mathfrak{p} \nmid 3\infty$, and let l be the residue characteristic of $\mathfrak{p}$. There is the theorem of Lutz (Proposition VII.6.3 of [Sm]) which states that

$$E(K_\mathfrak{p}) \cong T \oplus \mathbb{Z}_l^{[K_\mathfrak{p}:\mathbb{Q}_l]},$$

where T is a finite group. So under the isomorphism

$$H^1_f(K_\mathfrak{p}, E[3]) \cong E(K_\mathfrak{p})/3E(K_\mathfrak{p}),$$

$H^1_f(K_\mathfrak{p}, E[3])$ and $E(K_\mathfrak{p})[3]$ are (finite dimensional) $\mathbb{F}_3$-vector spaces of the same dimension.

If in addition E has good reduction at $\mathfrak{p}$, then by Lemma 19.3 of [C]

$$H^1_f(K_\mathfrak{p}, E[3]) = H^1(K_\mathfrak{p}^{\mathrm{ur}}/K_\mathfrak{p}, E[3]) \cong E[3]/(\mathrm{Frob}_\mathfrak{p} - 1)E[3].$$

□

Definition 5.14 (See Definition 4.3 of [MR])**.** Suppose E is an elliptic curve over K. Define the Selmer groups

$$\mathrm{Sel}_3(E/K) := \ker\Big(H^1(K, E[3]) \longrightarrow \bigoplus_\mathfrak{p} H^1(K_\mathfrak{p}, E[3])/H^1_f(K_\mathfrak{p}, E[3])\Big),$$
$$\mathrm{Sel}_{\mathfrak{p}_L}(A_L/K) := \ker\Big(H^1(K, A_L[\mathfrak{p}_L]) \longrightarrow \bigoplus_\mathfrak{p} H^1(K_\mathfrak{p}, A_L[\mathfrak{p}_L])/H^1_g(K_\mathfrak{p}, A_L[\mathfrak{p}_L])\Big).$$

We denote

$$d_3(E/K) := \dim_{\mathbb{F}_3}\mathrm{Sel}_3(E/K),$$
$$d_3(A_L/K) := \dim_{\mathbb{F}_3}\mathrm{Sel}_{\mathfrak{p}_L}(A_L/K).$$

Remark 5.15. Let E be an elliptic curve over K, and A_L be the abelian variety over K as given by Definition 5.9. Then there is a natural identification of G_K-modules $E[p] = A_L[\mathfrak{p}_L]$ inside $\mathrm{Res}^L_K E$ (see Proposition 4.1 and Remark 4.2 of [MR]). This allows us to view $\mathrm{Sel}_3(E/K)$, $\mathrm{Sel}_{\mathfrak{p}_L}(A_L/K) \subset H^1(K, E[3])$, defined by different sets of local Selmer structure. Also, view $H^1_g(K_\mathfrak{p}, A_L[3]) \subset H^1(K_\mathfrak{p}, E[3])$, defined by the image of the composition

$$A_L(K_\mathfrak{p})/\mathfrak{p}_L A_L(K_\mathfrak{p}) \to H^1(K_\mathfrak{p}, A_L(\mathfrak{p}_L)) \cong H^1(K_\mathfrak{p}, E[3]).$$

With slight modification of the proof of Lemma 2.5 of [MR2], we obtain the following lemma.

Lemma 5.16. *Let K be a number field containing ω, and let $L := K(\sqrt[3]{D})$ be a cubic extension of K with $\sqrt[3]{-4a} \notin L \setminus K$. Suppose $E : y^2 = x^3 + a$ is an elliptic curve over K, and let E_D and E_{D^2} be cubic twists of E over K given by $E_D : y^2 = x^3 + aD^2$ and $E_{D^2} : y^2 = x^3 + aD^4$, respectively. Then*

$$d_3(E/K) + d_3(E_D/K) + d_3(E_{D^2}/K) \equiv d_3(E/L) \pmod 2.$$

Proof. Using the Cassels pairing, Proposition 2.1 of [MR] gives us that

$$\mathrm{corank}_{\mathbb{Z}_3}(\mathrm{Sel}_{3^\infty}(E/K)) \equiv d_3(E/K) + \dim_{\mathbb{F}_3} E(K)[3] \pmod 2.$$

The natural map

$$\mathrm{Sel}_{3^\infty}(E/K) \oplus \mathrm{Sel}_{3^\infty}(E_D/K) \oplus \mathrm{Sel}_{3^\infty}(E_{D^2}/K) \longrightarrow \mathrm{Sel}_{3^\infty}(E/L)$$

has finite kernel and cokernel, so

$$\begin{aligned}\mathrm{corank}_{\mathbb{Z}_3}(\mathrm{Sel}_{3^\infty}(E/K)) + \mathrm{corank}_{\mathbb{Z}_3}(\mathrm{Sel}_{3^\infty}(E_D/K)) + \mathrm{corank}_{\mathbb{Z}_3}(\mathrm{Sel}_{3^\infty}(E_{D^2}/K)) \\ = \mathrm{corank}_{\mathbb{Z}_3}(\mathrm{Sel}_{3^\infty}(E/L)).\end{aligned}$$

Note that

$$E[3] = \{O, (0, \pm\sqrt{a}), (\sqrt[3]{-4a}, \pm\sqrt{-3a}), \\ (\sqrt[3]{-4a}\,\omega, \pm\sqrt{-3a}), (\sqrt[3]{-4a}\,\omega^2, \pm\sqrt{-3a})\}$$

so we have that $E_D(K)[3] \cong E_{D^2}(K)[3]$, and by assumption $\sqrt[3]{-4a} \notin L \setminus K$, we have that $E(K)[3] = E(L)[3]$. Therefore, we prove the congruence of the lemma. □

Fix for the rest of this section an elliptic curve E/K and let Δ_E be the discriminant of some model of E.

Definition 5.17 (See Definition 4.5 of [MR])**.** For every place $\mathfrak{p}$ of K, we define an invariant $\delta_\mathfrak{p} \in \mathbb{Z}/2\mathbb{Z}$ by

$$\delta_\mathfrak{p}(E, L/K) := \dim_{\mathbb{F}_3} \left(H^1_f(K_\mathfrak{p}, E[3])/H^1_{f\cap g}(K_\mathfrak{p}, E[3])\right) \pmod 2,$$

where $H^1_{f\cap g}(K_\mathfrak{p}, E[3]) := H^1_f(K_\mathfrak{p}, E[3]) \cap H^1_g(K_\mathfrak{p}, E[3])$.

Theorem 5.18 (Corollary 4.6 of [MR])**.** *Suppose that S is a set of primes of K containing all primes above 3, all primes ramified in L/K, and all primes where E has bad reduction. Then*

$$d_3(E/K) \equiv d_3(A_L/K) + \sum_{\mathfrak{p}\in S} \delta_\mathfrak{p}(E, L/K) \pmod 2.$$

Moreover, if $\mathfrak{p} \notin S$ then

$$H^1_f(K_\mathfrak{p}, E[3]) = H^1_g(K_\mathfrak{p}, E[3]) = H^1(K^{\mathrm{ur}}_\mathfrak{p}/K_\mathfrak{p}, E[3]).$$

Suppose that $\mathfrak{p}$ is a place of K and $\mathfrak{P}$ is a place of L above $\mathfrak{p}$. Let $L_\mathfrak{p} := K_\mathfrak{p} \otimes_K L$, and let $G = \mathrm{Gal}(L/K)$ act on L_v via its action on L. Let $N_{L/K} : E(L_\mathfrak{p}) \to E(K_\mathfrak{p})$ and $N_{L_\mathfrak{P}/K_\mathfrak{p}} : E(L_\mathfrak{P}) \to E(K_\mathfrak{p})$ denote the norm (or trace) maps.

Lemma 5.19. *Under the isomorphism $H^1_f(K_\mathfrak{p}, E[3]) \cong E(K_\mathfrak{p})/3E(K_\mathfrak{p})$, we have*

$$H^1_{f\cap g}(K_\mathfrak{p}, E[3]) \cong N_{L_\mathfrak{P}/K_\mathfrak{p}} E(L_\mathfrak{P})/3E(K_\mathfrak{p}).$$

Proof. By Proposition 5.2 of [MR]

$$H^1_{f\cap g}(K_\mathfrak{p}, E[3]) \cong \left(E(K_\mathfrak{p}) \cap N_{L/K}E(L_\mathfrak{p})\right)/3E(K_\mathfrak{p}) = N_{L/K}E(L_\mathfrak{p})/3E(K_\mathfrak{p}).$$

Since L/K is cyclic,

$$N_{L/K}E(L_\mathfrak{p}) = N_{L_\mathfrak{P}/K_\mathfrak{p}}E(L_\mathfrak{P}).$$

This proves the lemma. □

Lemma 5.20.

(i) If $\mathfrak{p}$ splits in L/K, then $H^1_f(K_\mathfrak{p}, E[3]) = H^1_g(K_\mathfrak{p}, E[3])$.

(ii) If $\mathfrak{p} \nmid 3\infty$ and $E(K_\mathfrak{p})[3] = 0$, then $H^1_f(K_\mathfrak{p}, E[3]) = 0$.

(iii) If $\mathfrak{p}$ is real and $(\Delta_E)_\mathfrak{p} < 0$, then $\delta_\mathfrak{p}(E, L/K) = 0$.

(iv) If E has good reduction at $\mathfrak{p}$ and $\mathfrak{p}$ is unramified in L/K, then $\delta_\mathfrak{p}(E, L/K) = 0$.

Proof. If $\mathfrak{p}$ splits in L/K, then $N_{L_\mathfrak{P}/K_\mathfrak{p}}$ is surjective. Since $N_{L_\mathfrak{P}/K_\mathfrak{p}}E(L_\mathfrak{P}) = N_{L/K}E(L_\mathfrak{p})$, so we have $H^1_f(K_\mathfrak{p}, E[3]) = H^1_g(K_\mathfrak{p}, E[3])$ by Proposition 5.2 of [MR].

If $\mathfrak{p} \nmid 3\infty$ and $E(K_\mathfrak{p})[3] = 0$, then $H^1_f(K_\mathfrak{p}, E[3]) = 0$ by Lemma 5.13(i).

If $\mathfrak{p}$ is real and $(\Delta_E)_\mathfrak{p} < 0$, then $E(K_\mathfrak{p}) \cong \mathbb{R}/\mathbb{Z}$ is connected and $\delta_\mathfrak{p}(E, L/K) = 0$.

If E has good reduction at $\mathfrak{p}$ and $\mathfrak{p}$ is unramified in L/K, then Lemma 5.5 of [MR] asserts that $N_{L_\mathfrak{P}/K_\mathfrak{p}}$ is surjective so we have $\delta_\mathfrak{p}(E, L/K) = 0$ by Lemma 5.19. □

Lemma 5.21. *If $\mathfrak{p} \nmid 3\infty$, E has good reduction at $\mathfrak{p}$, and $L_\mathfrak{P}/K_\mathfrak{p}$ is nontrivial and totally ramified, then*

$$H^1_{f\cap g}(K_\mathfrak{p}, E[3]) = 0 \quad \textit{and} \quad \delta_\mathfrak{p}(E, L/K) \equiv \dim_{\mathbb{F}_3} E(K_\mathfrak{p})[3] \pmod 2.$$

Proof. For such $\mathfrak{p}$, Lemma 5.5(ii) of [MR] asserts that $N_{L_\mathfrak{P}/K_\mathfrak{p}}E(L_\mathfrak{P}) = 3E(K_\mathfrak{p})$. So the first assertion of the lemma follows from Lemma 5.19. The second directly from Theorem 5.6 of [MR]. □

5.4 Comparing Selmer groups

We continue to fix a number field K, a cyclic extension L/K of degree 3, an elliptic curve E/K.

Definition 5.22. If T is a finite set of places of K, let

$$\mathrm{loc}_T : H^1(K, E[3]) \longrightarrow \bigoplus_{\mathfrak{p}\in T} H^1(K_\mathfrak{p}, E[3]).$$

Define strict and relaxed 3-Selmer groups $\mathcal{S}_T \subset \mathcal{S}^T \subset H^1(K, E[3])$ by the exactness of

$$0 \longrightarrow \mathcal{S}^T \longrightarrow H^1(K, E[3]) \longrightarrow \bigoplus_{\mathfrak{p} \notin T} H^1(K_\mathfrak{p}, E[3])/H^1_f(K_\mathfrak{p}, E[3]),$$

$$0 \longrightarrow \mathcal{S}_T \longrightarrow \mathcal{S}^T \xrightarrow{\mathrm{loc}_T} \bigoplus_{\mathfrak{p} \in T} H^1(K_\mathfrak{p}, E[3]).$$

Then by definition $\mathcal{S}_T \subset \mathrm{Sel}_3(E/K) \subset \mathcal{S}^T$, and we define

$$V_T := \mathrm{loc}_T(\mathrm{Sel}_3(E/K)) \subset \bigoplus_{\mathfrak{p} \in T} H^1_f(K_\mathfrak{p}, E[3]),$$
$$V_T^L := \mathrm{loc}_T(\mathrm{Sel}_{\mathfrak{p}_L}(A_L/K)) \subset \bigoplus_{\mathfrak{p} \in T} H^1_g(K_\mathfrak{p}, E[3]).$$

Lemma 5.23. $\dim_{\mathbb{F}_3} \mathcal{S}^T - \dim_{\mathbb{F}_3} \mathcal{S}_T = \sum_{\mathfrak{p} \in T} \dim_{\mathbb{F}_3} H^1_g(K_v, E[3])$.

Proof. We have exact sequences

$$0 \longrightarrow \mathrm{Sel}_3(E/K) \longrightarrow \mathcal{S}^T \xrightarrow{\mathrm{loc}_T} \bigoplus_{\mathfrak{p} \in T} (H^1(K_\mathfrak{p}, E[3])/H^1_f(K_\mathfrak{p}, E[3]))$$

$$0 \longrightarrow \mathcal{S}_T \longrightarrow \mathrm{Sel}_3(E/K) \xrightarrow{\mathrm{loc}_T} \bigoplus_{\mathfrak{p} \in T} H^1_f(K_\mathfrak{p}, E[3]).$$

By Poitou-Tate global duality, the images of the right-hand maps are orthogonal complements under the non degenerate sum of the local Tate pairings, so their $\mathbb{F}_3$-dimensions sum to $\sum_{\mathfrak{p} \in T} \dim_{\mathbb{F}_3} H^1_f(K_\mathfrak{p}, E[3])$. The lemma follows directly. □

Proposition 5.24. *Suppose that all of the following places split in L/K:*

- *all primes where E has bad reduction, and*
- *all primes above* 3.

Let T be the set of (finite) places $\mathfrak{p}$ of K such that L/K is ramified at $\mathfrak{p}$. Then

$$d_3(A_L/K) = d_3(E/K) - \dim_{\mathbb{F}_3} V_T + d$$

for some d satisfying

$$0 \leq d \leq \dim_{\mathbb{F}_3} \left(\bigoplus_{\mathfrak{p} \in T} H^1_f(K_\mathfrak{p}, E[3])/V_T \right),$$

$$d \equiv \dim_{\mathbb{F}_3} \left(\bigoplus_{\mathfrak{p} \in T} H^1_f(K_\mathfrak{p}, E[3])/V_T \right) \pmod 2.$$

Proof. If $\mathfrak{p} \notin T$, then $H^1_f(K_\mathfrak{p}, E[3]) = H^1_g(K_\mathfrak{p}, E[3])$ by Theorem 5.18 and Lemma 5.20(i). Therefore we have $\mathcal{S}_T \subset \mathrm{Sel}_{\mathfrak{p}_L}(A_L/K) \subset \mathcal{S}^T$, and we have exact sequences

$$0 \longrightarrow \mathcal{S}_T \longrightarrow \mathrm{Sel}_3(E/K) \xrightarrow{\mathrm{loc}_T} V_T \longrightarrow 0$$

$$0 \longrightarrow \mathcal{S}_T \longrightarrow \mathrm{Sel}_{\mathfrak{p}_L}(A_L/K) \xrightarrow{\mathrm{loc}_T} V_T^L \longrightarrow 0.$$

We deduce that

$$d_3(A_L/K) = d_3(E/K) + \dim_{\mathbb{F}_3} V_T^L - \dim_{\mathbb{F}_3} V_T. \tag{5.1}$$

Let

$$t := \sum_{\mathfrak{p} \in T} \dim_{\mathbb{F}_3} H^1_f(K_\mathfrak{p}, E[3]).$$

By Lemma 5.21 we have $\mathrm{Sel}_3(E/K) \cap \mathrm{Sel}_{\mathfrak{p}_L}(A_L/K) = \mathcal{S}_T$, and by the remark above we also have $\mathrm{Sel}_3(E/K) + \mathrm{Sel}_{\mathfrak{p}_L}(A_L/K) \subset \mathcal{S}^T$. Hence by above exact sequences and Lemma 5.21,

$$\dim_{\mathbb{F}_3} V_T + \dim_{\mathbb{F}_3} V_T^L \leq \dim_{\mathbb{F}_3}(\mathcal{S}^T/\mathcal{S}_T) = t. \tag{5.2}$$

By Theorem 2.7 and Lemma 5.20(i), $\delta_{\mathfrak{p}}(E, L/K) = 0$ if $\mathfrak{p} \notin T$, and by Lemma 5.13(i) and Lemma 5.21,

$$\sum_{\mathfrak{p}\in T} \delta_{\mathfrak{p}}(E, L/K) = t,$$

so $d_3(A_L/K) \equiv d_3(E/K) + t \pmod 2$ by Theorem 5.18. Comparing this with (5.1) and by (5.2), we see that

$$\dim_{\mathbb{F}_3} V_T^L \equiv t - \dim_{\mathbb{F}_3} V_T = \dim_{\mathbb{F}_3} \left(\bigoplus_{\mathfrak{p}\in T} H_f^1(K_{\mathfrak{p}}, E[3])/V_T \right) \pmod 2,$$

$$0 \leq \dim_{\mathbb{F}_3} V_T^L \leq t - \dim_{\mathbb{F}_3} V_T = \dim_{\mathbb{F}_3} \left(\bigoplus_{\mathfrak{p}\in T} H_f^1(K_{\mathfrak{p}}, E[3])/V_T \right).$$

If we let $d := \dim_{\mathbb{F}_3} V_T^L$, then the conclusion of proposition follows. □

Corollary 5.25. *Suppose $E, L/K$, and T are as in Proposition 5.24.*

(i) If $\dim_{\mathbb{F}_3}(\bigoplus_{\mathfrak{p}\in T} H_f^1(K_{\mathfrak{p}}, E[3])/V_T) \leq 1$, then

$$d_3(A_L/K) = d_3(E/K) - 2\dim_{\mathbb{F}_3} V_T + \sum_{\mathfrak{p}\in T} \dim_{\mathbb{F}_3} H_f^1(K_{\mathfrak{p}}, E[3]).$$

(ii) If $E(K_{\mathfrak{p}})[3] = 0$ for every $\mathfrak{p} \in T$, then $d_3(A_L/K) = d_3(E/K)$.

Proof. The first assertion follows directly from Proposition 5.24. For (ii), suppose $E(K_{\mathfrak{p}})[3] = 0$ for every $\mathfrak{p} \in T$. Then by Lemma 5.13(i) $E(K_{\mathfrak{p}}) = 3E(K_{\mathfrak{p}})$, and by Lemma 5.5(ii) of [MR] $N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} E(L_{\mathfrak{P}}) = 3E(K_{\mathfrak{p}})$, so $N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} E(L_{\mathfrak{P}}) = E(K_{\mathfrak{p}})$. Thus by Lemma 5.19, $H_f^1(K_{\mathfrak{p}}, E[3]) = H_g^1(K_{\mathfrak{p}}, E[3])$ and equal to 0. Therefore, $\mathrm{Sel}_{\mathfrak{p}_L}(A_L/K)$ and $\mathrm{Sel}_3(E/K)$ have the same local Selmer structures for all places. □

For Lemma 5.28, we review some basic properties of group cohomology.

Proposition 5.26 (inflation-restriction exact sequence)**.** *Let G be a group, $H \triangleleft G$ a normal subgroup and M a G-module. Then the following sequence*

$$0 \longrightarrow H^1(G/H, M^H) \xrightarrow{\text{Inf}} H^1(G, M) \xrightarrow{\text{Res}} H^1(H, M)$$

is exact.

Lemma 5.27 (Appendix B, Exercises B.3 of [Sm])**.** *With notation as above,*

(i) there is a natural action of G/H on $H^1(H, M)$,

(ii) there is an exact sequence

$$0 \longrightarrow H^1(G/H, M^H) \longrightarrow H^1(G, M) \longrightarrow H^1(H, M)^{G/H}.$$

Proof. First, let us see that G acts on $H^1(H, M)$: if $f : H \to M$ is a crossed homomorphism, define

$$(gf)(h) := g^{-1} f(ghg^{-1}).$$

Then we have

$$\begin{aligned}(gf)(ab) &= g^{-1} f(gabg^{-1}) = g^{-1} f(gag^{-1}gbg^{-1}) \\ &= g^{-1}\left(gag^{-1} f(gbg^{-1}) + f(gag^{-1})\right) = ag^{-1} f(gbg^{-1}) + g^{-1} f(gag^{-1}) \\ &= a(gf)(b) + (gf)(a),\end{aligned}$$

so gf is a crossed homomorphism. If $f(h) = hx - x$ for some $x \in M$, $(gf)(h) = h(g^{-1}x) - g^{-1}x$, so gf is also a 1-coboundary and this defines an action of the group G on $H^1(H, M)$. A direct calculation shows that, if $h' \in H$ then

$$(gh'f)(h) = hg^{-1} f(gh'^{-1}g^{-1}) + g^{-1} f(ghg^{-1}) + h'^{-1}g^{-1} f(gh'g^{-1}),$$

so we have

$$\begin{aligned} & g^{-1}f(gh'^{-1}g^{-1}) + h'^{-1}g^{-1}f(gh'g^{-1}) \\ =& f(h'^{-1}g^{-1}) - f(g^{-1}) + f(g^{-1}) - f(h'^{-1}g^{-1}) \\ =& 0, \end{aligned}$$

and hence gf and $gh'f$ differ by a 1-coboundary, thus they are equal in $H^1(H, M)$. Therefore G/H acts on $H^1(H, M)$.

Next, we claim that there is an exact sequence

$$0 \longrightarrow H^1(G/H, M^H) \longrightarrow H^1(G, M) \longrightarrow H^0(G/H, H^1(H, M)).$$

By the inflation-restriction sequence, the only thing we have to prove is that $\mathrm{Im}(\mathrm{Res}) \subseteq H^0(G/H, H^1(H, M))$. Take a crossed homomorphism $f : G \to M$. A direct calculation show that

$$(gf)(h) = hf(g^{-1}) + f(h) + g^{-1}f(g),$$

but we have

$$f(g^{-1}) + g^{-1}f(g) = f(g^{-1}) + f(1) - f(g^{-1}) = 0,$$

so g and gf differ by a 1-coboundary, hence they are equal in $H^1(H, M)$. This completes the proof of the claim. By the Hochschild-Serre spectral sequence we have the form

$$H^r(G/H, H^s(H, M)) \Rightarrow H^{r+s}(G, M),$$

which completes the proof. □

Let $M := K(E[3])$, and $\Gamma := \mathrm{Gal}(M/K)$. Then either $\Gamma \cong \mathbb{Z}_6$ or $\Gamma \cong \mathbb{Z}_2$.

Lemma 5.28. *Suppose* $\mathrm{Gal}(M/K) \cong \mathbb{Z}_6$*, and* c_1, c_2 *are cocyles representing* $\mathbb{F}_3$*-independent elements of* $H^1(K, E[3])$*. Then there is a* $\gamma \in G_K$ *such that* $\gamma|_{MK^{ab}} = 1$ *and* $c_1(\gamma), c_2(\gamma)$ *are an* $\mathbb{F}_3$*-basis of* $E[3]$*.*

Proof. By the assumption $\Gamma \cong \mathbb{Z}_6$, $E[3]$ is an irreducible Γ-module. And

$$H^1(\mathbb{Z}_6, E[3]) \cong H^1(\mathbb{Z}_6, \mathbb{Z}_3) \times H^1(\mathbb{Z}_6, \mathbb{Z}_3) \cong \mathrm{Ext}^1_{\mathbb{Z}_6}(\mathbb{Z}, \mathbb{Z}_3) \times \mathrm{Ext}^1_{\mathbb{Z}_6}(\mathbb{Z}, \mathbb{Z}_3) = 0,$$

so the restriction map

$$H^1(K, E[3]) \to \mathrm{Hom}(G_M, E[3])^\Gamma$$

is injective. Let $\tilde{c_1}, \tilde{c_2}$ be the distinct nonzero elements of $\mathrm{Hom}(G_M, E[3])^\Gamma$ obtained by restricting c_1, c_2 to G_M.

For $i = 1, 2$ let N_i be the fixed field of $\ker(\tilde{c_i})$. Then $\tilde{c_i} : \mathrm{Gal}(N_i/M) \to E[3]$ is nonzero and Γ-equivariant, so it must be an isomorphism.

Let $N = N_1 \cap N_2$. Since $\tilde{c_i}$ identifies $\mathrm{Gal}(N_i/N)$ with a Γ-stable subgroup of $E[3]$, we either have $N_1 = N_2$ or $N_1 \cap N_2 = M$.

If $N_1 = N_2$, then $\tilde{c_1}, \tilde{c_2} : \mathrm{Gal}(N/M) \to E[3]$ are different isomorphisms, so we can find $\tau \in \mathrm{Gal}(N/M)$ such that $\tilde{c_1}(\tau)$ and $\tilde{c_2}(\tau)$ are $\mathbb{F}_3$-independent.

If $N_1 \cap N_2 = M$, then again we can find $\tau \in \mathrm{Gal}(N_1N_2/M)$ such that $\tilde{c_1}(\tau)$ and $\tilde{c_2}(\tau)$ are $\mathbb{F}_3$-independent.

Since Γ acts trivially on $\mathrm{Gal}((MK^{\mathrm{ab}} \cap N_1N_2)/M)$, but $\mathrm{Gal}(N_1N_2/M) \cong E[3]$ or $E[3]^2$ has nonzero quotients on which Γ acts trivially, we have $MK^{\mathrm{ab}} \cap N_1N_2 = M$. Thus we can choose $\gamma \in G_M$ such that $\gamma|_{MK^{\mathrm{ab}}} = 1$ and $\gamma|_{N_1N_2} = \tau$. This γ has the desired properties. □

5.5 Twisting to equal the Selmer rank

Fix a number field K which contains ω, where ω is a primitive 3rd root of unity, and fix an elliptic curve $E : y^2 = x^3 + a$ over K with $E(K)[3] = 0$. Let Δ be the discriminant of and integral model of E. Let $N := K(3^*\Delta\infty)$, the ray class field of K modulo $3^*\infty$ and all infinite places, and let $M := K(E[3])$. Let S be the set of elements of order 2 in $\mathrm{Gal}(M/K)$. Define a set of primes of K

$$\mathcal{P} := \{\mathfrak{p} : \mathfrak{p} \text{ is unramified in } NM/K \text{ and } \mathrm{Frob}_{\mathfrak{p}}(M/K) \subset S\}$$

and two sets of ideals $\mathcal{N}_1 \subset \mathcal{N}$ of K

$$\mathcal{N} := \{\mathfrak{a} : \mathfrak{a} \text{ is a cubefree product of primes in } \mathcal{P}\},$$
$$\mathcal{N}_1 := \{\mathfrak{a} \in \mathcal{N} : [\mathfrak{a}, N/K] = 1\},$$

where $[\,\cdot\,, N/K]$ is the global Artin symbol.

Note that since $E(K)[3] = 0$ we have $\mathrm{Gal}(M/K) = \mathbb{Z}_2$ or $\mathbb{Z}_6$, depending on whether K is containing $\sqrt[3]{-4a}$ or not, so $|S| = 2$.

Lemma 5.29. *There is a positive real constant C such that*

$$|\{\mathfrak{a} \in \mathcal{N}_1 : \mathbb{N}_{K/\mathbb{Q}}\mathfrak{a} < X\}| \geq (C + o(1))\frac{X}{(\log X)^{1-|S|/[M:K]}}$$

Proof. By Lemma 4.1 of [MR2]. □

Proposition 5.30. *Suppose $\mathfrak{a} \in \mathcal{N}_1$. Then there is a cyclic cubic extension L/K of conductor $\mathfrak{a}$ such that $d_3(A_L/K) = d_3(E/K)$.*

Proof. Fix $\mathfrak{a} \in \mathcal{N}_1$. Then $\mathfrak{a}$ is principal, with a totally positive generator $\alpha \equiv 1 \pmod{3^*\Delta}$. Let $L := K(\sqrt[3]{\alpha})$. Then all primes above 3, all primes of bad reduction, and all infinite places split in L/K. If $\mathfrak{p}$ ramifies in L/K then $\mathfrak{p}|\mathfrak{a}$, so $\mathfrak{p} \in \mathcal{P}$. Thus the Frobenius of $\mathfrak{p}$ in $\mathrm{Gal}(M/K)$ has order 2, which shows that $E(K_\mathfrak{p})[3] = 0$. Now the proposition follows from Corollary 3.4(ii). □

Now, let $\mathfrak{f}(L/K)$ denote the finite part of the conductor of L/K. Then we have the following new result.

Theorem 5.31. *Suppose $n \geq 0$ is an integer, and $d_3(E/K) = n$. Then*

$$N_n(E, X) := |\{\textit{cubic extension } L/K : d_3(A_L/K) = n \textit{ and } \mathbb{N}_{K/\mathbb{Q}}\mathfrak{f}(L/K) < X\}| \gg \frac{X}{(\log X)^\alpha},$$

for some $\alpha \in \mathbb{R}$. .

Proof. By above Lemma 5.29 and Proposition 5.30. □

5.6 Twisting to lower and raise the Selmer rank

Fix a number field K which contains ω, where ω is a primitive 3rd root of unity, and fix an elliptic curve $E : y^2 = x^3 + a$ over K.

Proposition 5.32. *Suppose E/K is an elliptic curve such that $\mathrm{Gal}(M/K) \cong \mathbb{Z}_6$, and $n > 0$ is an integer.*

(i) If $d_3(E/K) \geq 2n$, then E has a cubic twist A_L over K such that

$$d_3(A_L/K) = d_3(E/K) - 2n.$$

(ii) E has a cubic twist A'_L over K such that

$$d_3(A'_L/K) = d_3(E/K) + 2n.$$

Proof. Let $M := K(E[3])$, and let Δ be the discriminant of E. Let $K(3^*\Delta\infty)$ denote the ray class field of K modulo the product of $3^*\Delta\infty$ and all infinite places. Let N be a Galois extension of K containing $MK(3^*\Delta\infty)$, large enough so that the restriction of $\mathrm{Sel}_3(E/K)$ to N is zero.

(i) Since $d_3(E/K) \geq 2n$, we can choose cocyles $c_1, c_2, \cdots, c_{2n}$ representing $\mathbb{F}_3$-independent elements of $\mathrm{Sel}_3(E/K)$. By Lemma 5.28 we can find $\gamma_1, \cdots, \gamma_n \in G_K$ such that

- $\gamma_i|_{MK(3^*\Delta\infty)} = 1$ for all $1 \leq i \leq n$,
- $c_{2i-1}(\gamma_i), c_{2i}(\gamma_i)$ are an $\mathbb{F}_3$-basis of $E[3]$ for all $1 \leq i \leq n$.

For each $1 \leq i \leq n$, let $\mathfrak{p}_i$ be a prime of K where E has good reduction, not dividing 3, whose Frobenius in $\mathrm{Gal}(N/K)$ is the conjugacy class of γ_i. Then $\mathfrak{p}_i$ has a totally positive generator $\alpha_i \equiv 1 \pmod{3^*\Delta}$. Let $L = K(\sqrt[3]{\alpha_1 \cdots \alpha_n})$. Then all places $\mathfrak{p}$ dividing $3^*\Delta\infty$ split in L/K, and $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ are all primes that ramifies in L/K.

We will apply Corollary 5.25(i) with $T = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_n\}$. Since E has good reduction at all $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$, it follows from Lemma 5.13(ii) that

$$H^1_f(K_{\mathfrak{p}_i}, E[3]) \cong E[3]/(\mathrm{Frob}_{\mathfrak{p}_i} - 1)E[3] = E[3]/(\gamma_i - 1)E[3] = E[3].$$

The localization map $\mathrm{loc}_T : \mathrm{Sel}_3(E/K) \to \bigoplus_{\mathfrak{p}_i \in T} H^1_f(K_{\mathfrak{p}_i}, E[3])$ is given by evaluation of cocycles at $\mathrm{Frob}_{\mathfrak{p}_i} = \gamma_i$, so by our choice of γ_i, the classes $\mathrm{loc}_T(c_{2i-1})$ and $\mathrm{loc}_T(c_{2i})$ generate $H^1_f(K_{\mathfrak{p}_i}, E[3])$. Therefore we have

$$\dim_{\mathbb{F}_3} V_T = \sum_{1 \leq i \leq n} \dim_{\mathbb{F}_3} H^1_f(K_{\mathfrak{p}_i}, E[3]) = 2n,$$

and Corollary 5.25(i) yields $d_3(A_L/K) = d_3(E/K) - 2n$, as desired.

(ii) Now, we can find $\delta_1, \cdots, \delta_n \in G_K$ such that

- $\delta_i|_{MK(3^*\Delta\infty)} = 1$ for all $1 \leq i \leq n$,
- $\big(\mathrm{Sel}_3(E/K)\big)(\delta_i) = 0$ for all $1 \leq i \leq n$.

For each $1 \leq i \leq n$, let $\mathfrak{q}_i$ be a prime of K not dividing $3^*\Delta\infty$, whose Frobenius in $\mathrm{Gal}(N/K)$ is the conjugacy class of δ_i. Then $\mathfrak{q}_i$ has a totally positive generator $\beta_i \equiv 1 \pmod{3^*\Delta\infty}$. Let $L' = K(\sqrt[3]{\beta_1 \cdots \beta_n})$. Then all places $\mathfrak{p}$ dividing $3^*\Delta\infty$ split in L', and $\mathfrak{q}_i, \cdots, \mathfrak{q}_n$ are all primes that ramifies in L'/K.

Let $T' = \{\mathfrak{q}_1, \cdots, \mathfrak{q}_n\}$. Since E has good reduction at all $\mathfrak{q}_1, \cdots, \mathfrak{q}_n$, we have

$$H^1_f(K_{\mathfrak{q}_i}, E[3]) \cong E[3]/(\delta_i - 1)E[3] = E[3],$$

so

$$\sum_{1 \leq i \leq n} \dim_{\mathbb{F}_3} H^1_f(K_{\mathfrak{q}_i}, E[3]) = 2n.$$

Further, the localization maps

$$\mathrm{loc}_{T'} : \mathrm{Sel}_3(E/K) \to \bigoplus_{\mathfrak{q}_i \in T'} H^1_f(K_{\mathfrak{q}_i}, E[3]) \to \bigoplus_{1 \leq i \leq n} E[3]/(\delta_i - 1)E[3]$$

are given by evaluation of cocycles at $\mathrm{Frob}_{\mathfrak{q}_i} = \delta_i$. Hence by our choice $(\mathrm{Sel}_3(E/K))$ $(\delta_i) = 0$, we have $\mathrm{loc}_T(\mathrm{Sel}_3(E/K)) = 0$. Thus we conclude that

$$d_3(A_{L'}/K) = d_3(E/K) - 2 \cdot 0 + 2n = d_3(E/K) + 2n.$$

□

Proposition 5.33. *Let $D \in K$ and $L = K(\sqrt[3]{D})$ be a cyclic extension of degree 3 over K. Suppose that all of the following places split in L/K:*

- *all primes where E has bad reduction,*
- *all primes above* 3.

Then we have

$$\mathrm{Sel}_{\mathfrak{p}_L}(E_D/K) = \mathrm{Sel}_{\mathfrak{p}_L}(E_{D^2}/K).$$

Proof. By Proposition 2.1 and Theorem 6.1 of [HHW], $\mathrm{Sel}_{\mathfrak{p}_L}(E_{D^\alpha}/K)$ consists of some elements $t \in K^*/(K^*)^3$ such that the homogeneous curve $C_{D^\alpha,t}$: $X^3 - tY^3 = -54\sqrt{\frac{a}{-27}}D^\alpha t^2 Z^3$ has a K_v-rational point for every $v \in M_K$, where $\alpha = 1$ or 2. Suppose that D is a cube in K_v for all primes v where E has bad reduction, which is equivalent to the condition. Then D^2 is also a cube in K_v for all primes v where E has bad reduction. So $C_{D,t}$ has a K_v-rational point for every $v \in M_K$ if and only if $C_{D^2,t}$ has a K_v-rational point for every $v \in M_K$. Thus we have $\mathrm{Sel}_{\mathfrak{p}_L}(E_D/K) = \mathrm{Sel}_{\mathfrak{p}_L}(E_{D^2}/K)$. □

Lemma 5.34. *Let E_D be a cubic twist of E.*

(i) If $E[3] = 0$, then $E_D[3] = 0$.

(ii) If we let $M' = K(E_D[3])$, then we have $\mathrm{Gal}(M/K) = \mathrm{Gal}(M'/K)$.

Proof. Recall that E is given by $y^2 = x^3 + a$, and let $P(x', y')$ be a non-trivial 3-torsion point on E. Then we must have that $x([2]P) = (x'^4 - 8ax')/(4x'^3 + 4a) = x' = x([-1]P)$, so we get $x(x^3 + 4a) = 0$. Thus

$$E[3] = \{O, (0, \pm\sqrt{a}), (\sqrt[3]{-4a}, \pm\sqrt{-3a}), (\sqrt[3]{-4a}\omega, \pm\sqrt{-3a}), (\sqrt[3]{-4a}\omega^2, \pm\sqrt{-3a})\}.$$

Similarly, we get

$$E_D[3] = \{O, (0, \pm\sqrt{a}D), (\sqrt[3]{-4aD^2}, \pm\sqrt{-3a}D), (\sqrt[3]{-4aD^2}\omega, \pm\sqrt{-3a}D), (\sqrt[3]{-4aD^2}\omega^2, \pm\sqrt{-3a}D)\},$$

and comparing $E_D[3]$ with $E[3]$ gives the lemma. □

Proposition 5.35. *If* $E(K)[3] = 0$, *then* $\dim_{\mathbb{F}_3}\mathrm{Sel}_3(E/K) = 2\cdot\dim_{\mathbb{F}_3}\mathrm{Sel}_{\mathfrak{p}_L}(E/K)$.

Proof. From the exact sequence

$$0 \to E[\mathfrak{p}_L] \to E[3] \to E[\mathfrak{p}_L] \to 0,$$

we can have the exact sequence

$$0 \to \mathrm{Sel}_{\mathfrak{p}_L}(E/K) \to \mathrm{Sel}_3(E/K) \to \mathrm{Sel}_{\mathfrak{p}_L}(E/K).$$

By the similar argument to Proposition 2.2 and Corollary 2.3 of [Ch], we have that the cokernel of the map $\mathrm{Sel}_3(E/K) \to \mathrm{Sel}_{\mathfrak{p}_L}(E/K)$ is less than or equal to 1. So $\dim_{\mathbb{F}_3}\mathrm{Sel}_3(E/K) = 2\cdot\dim_{\mathbb{F}_3}\mathrm{Sel}_{\mathfrak{p}_L}(E/K)$ or $\dim_{\mathbb{F}_3}\mathrm{Sel}_3(E/K) = 2\cdot\dim_{\mathbb{F}_3}\mathrm{Sel}_{\mathfrak{p}_L}(E/K)+1$. But Proposition 5.1 and 5.2 imply that $\dim_{\mathbb{F}_3}\mathrm{Sel}_3(E/K)$ should be even, so we have $\dim_{\mathbb{F}_3}\mathrm{Sel}_3(E/K) = 2\cdot\dim_{\mathbb{F}_3}\mathrm{Sel}_{\mathfrak{p}_L}(E/K)$. □

Now we can prove Theorem 5.36 which is a cubic twist analogue to the work [MR2] of Mazur and Rubin on quadratic twists of elliptic curves.

Theorem 5.36. ([BK3], in preparation) *Suppose* E/K *is an elliptic curve such that* $\mathrm{Gal}(M/K) \cong \mathbb{Z}_6$. *Then for every* $n \geq 0$, E *has many cubic twists* E_D/K *with* $\dim_{\mathbb{F}_3}\mathrm{Sel}_3(E_D/K) = 2n$.

Proof. First, we assume that $d_3(E/K) = 2n$. By Theorem 5.31, E has many cubic twists A_L/K with $d_3(A_L/K) = 2n$. Since $A_L = E_D \times E_{D^2}$ for some $D \in K^*$, we have $d_3(A_L/K) = \dim_{\mathbb{F}_3}\mathrm{Sel}_{\mathfrak{p}_L}(E_D/K) + \dim_{\mathbb{F}_3}\mathrm{Sel}_{\mathfrak{p}_L}(E_{D^2}/K)$. Hence by

Proposition 5.33 and Proposition 5.35, $d_3(A_L/K) = \dim_{\mathbb{F}_3}\mathrm{Sel}_3(E_D/K) = 2n$ for many cubic twists E_D/K.

Next, we consider the remaining cases $d_3(E/K) \neq 2n$. Note that if E satisfies the hypotheses of this theorem, then so does every cubic twist E_D of E by Lemma 5.34. Also by Lemma 5.34 the hypotheses of Proposition 5.32 remain valid for E_D, so E has a cubic twist A_L/K such that $d_3(A_L/K) = 2n$. Similarly, we get $\dim_{\mathbb{F}_3}\mathrm{Sel}_3(E_D/K) = 2n$ for a cubic twist E_D/K. Note that every cubic twist $(E_D)_{D'}$ of E_D is also a cubic twist $E_{D''}$ of E. Hence the first argument shows that E has many such cubic twists. □

Remark 5.37. Recall that the Tate-Shafarevich conjecture predicts that $Ш(E/K)$ is finite. So under the conjecture, the p-primary subgroup $Ш(E/K)[p^\infty]$ is finite for any prime number p. Then the Cassels pairing which gives an alternating bilinear pairing on $Ш(E/K)$ shows that $\dim_{\mathbb{F}_p} Ш(E/K)[p]$ is even (see for example, Appendix C, §17 of [Sm]). Thus from the Kummer short exact sequence

$$0 \longrightarrow E(K)/pE(K) \longrightarrow \mathrm{Sel}_p(E/K) \longrightarrow Ш(E/K)[p] \longrightarrow 0,$$

we obtain that $\mathrm{rank}\, E/K \equiv \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/K) \pmod 2$ if $E(K)[p] = 0$. Since $K \ni \zeta_3$, the rank of E_D/K is even for all cubic twists E_D by Remark 4.11. Therefore, $\dim_{\mathbb{F}_3} \mathrm{Sel}_3(E_D/K)$ should be even if $E(K)[3] = 0$.

Bibliography

[ABF] J. A. Antoniadis, M. Bungert and G. Frey, *Properties of twists of elliptic curves*, J. Reine Angew. Math. **405** (1990) 1-28.

[BCDT] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curve over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001) 843-939.

[BJK] D. Byeon, D. Jeon and C.H. Kim, *Rank-one quadratic twists of an infinite family of elliptic curves*, J. Reine Angew. Math. **633** (2009) 67-76.

[BKW] J. Brüdern, K. Kawada and T. D. Wooley, *Additive representation in thin sequence II: The binary Goldbach problem*, Mathematica **47** (2000) 117-125.

[BK] D. Byeon, N. Kim, *Elliptic curves of rank zero satisfying the p-part of the Birch and Swinnerton-Dyer conjecture*, Manuscripta Math. **142** (2013) 383-390.

[BK2] D. Byeon, N. Kim, *Elliptic curves with all cubic twists of the same root number*, Journal of Number Theory, **136** (2014) 22-27.

BIBLIOGRAPHY

[BK3] D. Byeon, N. Kim, *Selmer ranks of cubic twists of elliptic curves*, in preparation.

[C] J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966) 193-291.

[CCH] B. Conrad, K. Conrad and H. Helfgott, *Root numbers and ranks in positive characteristic*, Adv. Math. **198** (2005) 684-731.

[Ch] Y-M. J. Chen, *The Selmer groups and the ambigious ideal class groups of cubic fields*, Bull. Austral. Math. Soc. 54 (1996), 267-274.

[D] T. Dokchitser, *Notes on the parity conjecture*, In: Elliptic Curves, Hilbert Modular Forms and Galois Deformations, CRM Barcelona Advanced Courses in Math. Birkhauser (2013) 201-249.

[DD] T. Dokchitser, V. Dokchitser, *Elliptic curves with all quadratic twists of positive rank*, Acta Arith. **137** (2009) 193-197.

[DD2] T. Dokchitser, V. Dokchitser, *Root numbers of elliptic curves in residue characteristic 2*, Bull. Lond. Math. Soc. **40** (2008) 516-524.

[DH] H. Davenport and H. Heilbronn, *On the density of disciminants of cubic fields ii*, Proc. Roy. Soc. London Ser. A **322** (1971) 405-420.

[Du] N. Dummigan, *Rational torsion on optimal curves,* Int. J. Number Theory **513** (2005) 513-531.

[F] G. Frey, *On the Selmer group of twists of elliptic curves with $\mathbb{Q}$-rational torsion points*, Canad. J. Math. **40** (1988) 649-665.

BIBLIOGRAPHY

[G] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, In: Number theory, Carbondale 1979, Lecture Notes in Math. **751**, Springer-Verlag, Berlin, 1979.

[GV] R. Greenberg and V. Vatsal, *On the Iwasawa invariants of elliptic curves*, Invent. Math. **142** (2000) 17-63.

[H] T. Hadano, *Elliptic curves with a torsion point,* Nagoya Math. J. **66**(1977) 99-108.

[HHW] D. E. Haile, I. Han, and A. R. Wadsworth, *Curves C that are cyclic twists of* $Y^2 = X^3 + c$ *and the relative Brauer groups Br(k(C)/k)*, Trans. Amer. Math. Soc., 364 (2012), 4875-4908.

[I] H. Iwaniec, *Primes represented by quadratic polynomials in two variables*, Collection of articles dedicated to Carl Ludwig Siegel on the occasion of his seventy-fifth birthday, V. Acta Arith. **24** (1973/74) 435-459.

[J] K. James, *Elliptic curves satisfying the Birch and Swinnerton-Dyer conjecture mod* 3, J. Number Theory **76** (1999) 16-21.

[JO] K. James and K. Ono, *Selmer groups of quadratic twists of elliptic curves*, Math. Ann. **314** (1999) 1-17.

[K] S. Kobayashi, *The local root number of elliptic curves with wild ramification*, Math. Ann. **323** (2002) 609-623.

[Ma] L. Mai, *The analytic rank of a family of elliptic curves*, Canad. J. Math. **45** (1993) 847-862.

[Mi] J. S. Milne, *Elliptic curves*, Book Surge Publishers, Charleston, SC, 2006.

BIBLIOGRAPHY

[MR] B. Mazur, K. Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Annals of Math. **166** (2007) 579-612.

[MR2] B. Mazur, K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010) 541-575.

[MRS] B. Mazur, K. Rubin, A. Silverberg, *Twisting commutative algebraic groups*, Journal of Algebra **314**(2007) 419-438.

[NH] J. Nakagawa and K. Horie, *Elliptic curves with no torsion points*, Proc. Amer. Math. Soc. **104** (1988) 20-25.

[Pa] V. Pal, *Periods of quadratic twists of elliptic curves*, Proc. Amer. Math. Soc. **140** (2012) 1513-1525.

[Pe] A. Perelli. *Goldbach numbers represented by polynomials*, Rev. Mat. Iberoamericana **12** (1996) 477-490.

[R] D. Rohrlich, *Variation of the root number in families of elliptic curves*, Compositio Math. **87** (1993) 119-151.

[R2] D. Rohlich, *Elliptic curves and the Weil-Deligne group*, In: Elliptic Curves and Related Topics, CRM Proceedings and Lecture Notes **4**, Amer. Math. Soc.(1994), 125 – 157.

[Sb] A. Silverberg, *Applications to cryptography of twisting commutative algebraic groups*, Discrete Appl. Math. **156** (2008) 3122-3138.

[Sm] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, New York : Springer-Verlag, 1985.

[St] A. Sato, *The behavior of Mordell-Weil groups under field extensions*, preprint.

BIBLIOGRAPHY

[T] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, In: Modular functions of one variable IV, Lecture Notes in Math. **476**, New York: Springer-Verlag (1975) 33-52.

[TW] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. **141** (1995) 553-572.

[V] V. Vatsal, *Canonical periods and congruence formulae*, Duke Math. J. **98** (1999) 397-419.

[W] A. Weil, *Adeles and Algebraic Groups*, Progress in Math., vol. **23**, Birkhäuser, Boston, 1982.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995) 443-551.

[ZK] D. Zagier, G. Kramarz, *Numerical investigations related to the L-series of certain elliptic curves*, J. Indian Math. Soc. **52** (1987) 51-69.

국문초록

이 학위논문에서는 타원곡선의 비틀림 곡선의 다양한 성질에 대해 연구하였다.

우선, 유리수체위의 타원곡선에 대하여 생각하자. 그러면 양의 비율의 이차 비틀림 곡선에 대하여, 계수가 0이고 Birch 와 Swinnerton-Dyer 추측의 3-부분이 성립함을 증명하였다. 이전에는 그러한 곡선이 유한개 존재함을 알았다.

두번째로, 임의의 수체위에 정의된 j-불변수가 0인 타원곡선을 생각하자. 이 수체의 간단한 조건으로 이 타원곡선의 모든 삼차 비틀림 곡선이 같은 근 숫자를 갖는지 안갖는지를 판별하였다. 이 정리는 Dokchitser 와 Dokchitser 가 타원곡선의 이차 비틀림 곡선에 대한 정리를 삼차 비틀림 곡선으로 확장한 것이다.

마지막으로, 1의 3승근을 포함한 수체를 생각하자. 적당히 약한 조건을 만족하는 j-불변수가 0인 이 수체위의 타원곡선에 대하여, 3-Selmer 군의 차원이 임의의 양의 짝수가 되는 삼차 비틀림 곡선이 무한히 많이 존재하면 보였다. 이 정리는 Mazur 와 Rubin의 타원곡선의 이차 비틀림 곡선에 대한 정리의 대응이다.

주요어휘: 타원곡선, 삼차 비틀림곡선, 이차 비틀림곡선, Selmer 군, 근 숫자, Birch 와 Swinnerton-Dyer 추측

학번: 2009-30844