이학박사 학위논문

Rational torsion on optimal curves and rank 1 elliptic curves

(최적곡선의 유리 비틀림점과 계수 1 타원곡선)

2012 년 8 월

서울대학교 대학원

수리과학부

이 동 건

Rational torsion on optimal curves and rank 1 elliptic curves

(최적곡선의 유리 비틀림점과 계수 1 타원곡선)

지도교수 변 동 호

이 논문을 이학박사 학위논문으로 제출함

2012 년 8 월

서울대학교 대학원

수리과학부

이 동 건

이 동 건의 이학박사 학위논문을 인준함

2012 년 8 월

위 원 장 조 영 현 (인)

부 위 원 장 변 동 호 (인)

위 원 강 석 진 (인)

위 원 김 현 광 (인)

위 원 오 병 권 (인)

Rational torsion on optimal curves and rank 1 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

Donggeon Yhee

Dissertation Director : Professor Dongho Byeon

Department of Mathematical Sciences
Seoul National University

August 2012

Abstract

In this thesis, three problems on arithmetic of elliptic curves are considered ; Goldfeld conjecture, Stein's conjecture about optimal curves differing by 3-isogeny, and Gross-Zagier conjecture.

At first, we find an infinite family of elliptic curves satisfying Goldfeld conjecture. To do that, we use Dummigan's construction [Du] which explicitly constructed a rational point of order l on the optimal curve. We will generalize his construction and applying it to Heegner points. Consequently we find a family of elliptic curves such that a positive proportion of quadratic twists has (analytic) rank 1.

Second conjecture is given by W. Stein and M. Watkins [SW]. They conjectured when $X_0(N)$-optimal curve and the $X_1(N)$-optimal curve of an isogeny class differ by a 3-isogeny. We claim that torsion points on each optimal curves has different image in Jacobians of modular curves so that we prove the optimal curves differ.

Finally we study Gross and Zagier conjecture. Gross and Zagier conjectured that if a Heegner point on elliptic curve has infinite order, then the product of the Manin constant, Tamagawa numbers, and the square root of the order of Shafarevich-Tate group is divisible by the order of torsion subgroup of $E(\mathbb{Q})$. In this thesis, we show that this conjecture is true if $E(\mathbb{Q})_{\text{tor}}$ has a point of odd order.

Key words: Torsion subgroups, Goldfeld conjecture, Gross and Zagier conjecture, Optimal curves, Selmer groups
Student Number: 2008-30085

Contents

Chapter 1

Introduction

Let $E/\mathbb{Q} : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{Q}$ of conductor N and let $L(s, E) = \sum_{n=1}^{\infty} a(n)n^{-s}$ be its Hasse-Weil L-function defined for $\Re(s) > \frac{3}{2}$. The work of Breuil, Conrad, Diamond, Taylor and Wiles [B-C-D-T] [T-W] [Wi] implies that $L(s, E)$ has an analytic continuation to $\mathbb{C}$ and satisfies a functional equation relating the values at s and $2-s$. Let ϵ be the sign of the functional equation of $L(s, E)$ and f be the newform associated with E. For each positive $d \mid N$ let $w_d = \pm 1$ be such that $W_d f = w_d f$, where W_d is the Atkin-Lehner involution. Then we have that $\epsilon = -\prod_{p|N} w_p$. Let D be the fundamental discriminant of the quadratic field $\mathbb{Q}(\sqrt{D})$, and let $\chi_D = (\frac{D}{\cdot})$ denote the usual Kronecker character. For D coprime to the conductor of E, the Hasse-Weil L-function of the quadratic twist $E_D : Dy^2 = x^3 + a'x + b'$ of E is the twisted L-function $L(s, E_D) = \sum_{n=1}^{\infty} \chi_D(n)a(n)n^{-s}$. Goldfeld [Go] conjectured that

$$\sum_{|D|<X} \mathrm{Ord}_{s=1} L(s, E_D) \sim \frac{1}{2} \sum_{|D|<X} 1.$$

A weaker version of this conjecture is that for $r = 0$ or 1,

$$\sharp\{|D| < X | \ \mathrm{Ord}_{s=1} L(s, E_D) = r\} \gg X,$$

i.e, that $\mathrm{Ord}_{s=1} L(s, E_D) = r$ for a positive proportion of D.

In [V99], Vatsal proved that if $E/\mathbb{Q}$ is a semi-stable elliptic curve with

a $\mathbb{Q}$-rational point of order 3 and good reduction at 3, then for a positive proportion of D, $\mathrm{Ord}_{s=1}L(E_D, s) = 0$. But for the case $r = 1$, less is known.

In chapter 3, we prove the following theorem.

Main Theorem 1. *Let $E/\mathbb{Q}$ be an elliptic curve of square-free conductor N with a rational point of order $3 \nmid N$. If there is only one prime $p|N$ such that $\omega_p = -1$, then*

$$\sharp\{|D| < X|\ \mathrm{Ord}_{s=1}L(s, E_D) = 1\} \gg X.$$

Let $X_1(N) = \Gamma_1(N)\backslash\mathcal{H}^*$ and $X_0(N) = \Gamma_0(N)\backslash\mathcal{H}^*$ denote the usual modular curves with Jacobian $J_1(N)$ and $J_0(N)$, respectively. There is a unique curve $E_i \in \mathcal{C}$, for $i = 0, 1$, and a parametrization $\phi_i : X_i(N) \to E_i$ such that for any $E \in \mathcal{C}$ and parametrization $\phi_i' : X_i(N) \to E$, there is an isogeny $\pi_i : E_i \to E$ such that $\pi_i \circ \phi_i = \phi_i'$. For $i = 0, 1$, the curve E_i is called the $X_i(N)$-*optimal curve* [B-C-D-T] [T-W] [Wi].

Let $\mathcal{C}$ denote an isogeny class of elliptic curves defined over $\mathbb{Q}$ of conductor N. There are examples where they differ. For example, $E_0 = X_0(11)$ and $E_1 = X_1(11)$ differ by a 5-isogeny. Stein and Watkins [SW] have made a precise conjecture about when E_0 and E_1 differ by a 3-isogeny, based on numerical observation. For the 3-isogeny case, the conjecture is the following.

Conjecture 1. (Stein and Watkins) *For $i = 0, 1$, let E_i be the $X_i(N)$-optimal curve of an isogeny class $\mathcal{C}$ of elliptic curves defined over $\mathbb{Q}$ of conductor N. Then the following statements are equivalent.*
(A) There is an elliptic curve $E \in \mathcal{C}$ given by $E : y^2 + axy + y = x^3$ with discriminant $a^3 - 27 = (a-3)(a^2+3a+9)$, where a is an integer such that no prime factors of $a - 3$ are congruent to 1 (mod 6) and $a^2 + 3a + 9$ is a power of a prime number.
(B) E_0 and E_1 differ by a 3-isogeny.

In chapter 4, we prove the following theorem.

Main Theorem 2 *Let (A) and (B) be as in the conjecture.*
(i) (A) implies (B), except one case.

(ii) If N is square-free and $3 \nmid N$, then (B) implies (A).

Let c be the Manin constant of E and $m = \prod_{p|N} m_p$, where m_p is the Tamagawa number of E at a prime divisor p of N. Let K be an imaginary quadratic field with fundamental discriminant D_K, where all prime divisors of N split in K and $\mathcal{O}_K$ be the ring of integers in K. Then there exist a Heegner point x of discriminant D_K of $X_0(N)$, which corresponds to a pair of two N-isogeneous elliptic curves by the same $\mathcal{O}_K$ of complex multiplcation. The point x is defined over the Hilbert class field H of K. Put $P_K = \sum_{\sigma \in \mathrm{Gal}(H/K)} \phi(x)^\sigma$. Then $P_K \in E(K)$.

Let $L(E/K, s)$ be the L-series of E over K and $Ш(E/K)$ be the Shafarevich-Tate group of E over K. Kolyvagin [Ko] proved that if P_K has infinite order, then $E(K)$ has rank 1 and $Ш(E/K)$ is finite. Gross and Zagier [G-Z] proves that if P_K has infinite order, then the L-function $L(E/K, s)$ has a simple zero at $s = 1$ and, consequently, the first part of Birch and Swinnerton-Dyer conjecture is true.

Gross and Zagier also obtain a formular

$$L'(E/K, 1) \;=\; \frac{||\omega||^2 \hat{h}(P_K)}{c^2 u_K^2 |D_K|^{1/2}} \tag{1.1}$$

for the derivative of $L(E/K, s)$ at $s = 1$. On the other hand, the second part of Birch and Swinnerton-Dyer conjecture predicts that

$$L'(E/K, 1) = \frac{||\omega||^2 m^2 \hat{h}(P_K) |Ш(E/K)|}{|D_K|^{1/2} [E(K) : \mathbb{Z}P_K]^2}.$$

From the formular (1.1), the prediction by BSD can be written by

Conjecture 2 [(2.3) Conjecture, p.311, G-Z] *Let K be an imaginary quadratic field and $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$. If P_K has infinite order, then the integer $c \cdot m \cdot |Ш(E/K)|^{\frac{1}{2}}$ is divisible by $|E(\mathbb{Q})_{\mathrm{tor}}|$.*

In chapter 5, we prove the following theorem.

Main Theorem 3 *Conjecture 2 is true if $E(\mathbb{Q})_{\mathrm{tor}}$ has a point of odd order.*

Chapter 2

Preliminaries

This chapter consists of preliminaries for later discussion.

2.1 Elliptic curves

An elliptic curve is a nonsingular curve of genus 1 with a fixed rational point.

Definition 2.1.1. *A nonsingular curve E in $\mathbb{P}^2_F$ is called an* elliptic curve *over a field F if E is a zero locus of an equation*

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

where $a_i \in F$. The defining equation is called a Weierstrass equation *for E.*

The nonsingularity means that

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

has nonzero gradient at any point (x, y) satisfying $f(x, y) = 0$. In convenience, we may use an embedding $E \hookrightarrow F^2 \cup \{\infty\}$ defined by $[x, y, z] \mapsto (x/z, y/z)$ for nonzero z and $[0, 1, 0] \mapsto \infty$. Thus, a point of an elliptic curve is written in (x, y) or ∞. We define a set of *L-rational point* of E by

$$E(L) = \{(x, y) \in L^2 \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\infty\},$$

for any extension L/F or any subfield $L \subset F$. If $L = F = \mathbb{Q}$, we call a point in $E(\mathbb{Q})$ as a *rational point*. As a topic of numer theory, we assume a Weierstrass equation to be Diophantine, i.e. $a_i \in \mathbb{Z}$ or a ring of integers of a number field.

To solve Diophantine equation, one may use "modulo method" to solve the equation. The method does not always give solution, but often shows many characters of the solution set. For example, $x^2 + y^2 = p$ does not have an integral solution if $p \equiv -1 \pmod 4$, because $-1 \equiv z^2 \pmod p$ has no solution if $p \equiv -1 \pmod 4$. In the process, we have applied the method on $x^2 + y^2 = p$, not on $px^2 + py^2 = p^2$, though they have same zeros. In this manner, we have to choose a good equation.

2.2 Minimal Weierstrass equations

In this section E is defined over $\mathbb{Z}$, i.e. $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$. Applying modulo method, we obtain an equation over $\mathbb{F}_p$ for a prime p.

Example.

1. Let $E : y^2z + xyz + pyz^2 = x^3$ and $F = \mathbb{F}_p$. Define a map

$$\begin{aligned} \rho_p : \quad E(\mathbb{Q}) &\to \mathbb{P}^2_F \\ (x, y, z) &\mapsto (\bar{x}, \bar{y}, \bar{z}). \end{aligned}$$

   where $x, y, z \in \mathbb{Z}$ and $\bar{a}$ denotes the residue class of a modulo p. Then $(x, y, z) \in \rho_p(E(\mathbb{Q}))$ satisfies $y^2z + xyz = x^3$, which defines a singular curve with singular point $(0, 0, 1)$.

   Let q be a prime dividing $27p - 1$. Define

$$\begin{aligned} \rho_q : \quad E(\mathbb{Q}) &\to \mathbb{P}^2_F \\ (x, y, z) &\mapsto (\bar{x}, \bar{y}, \bar{z}). \end{aligned}$$

   Then the point $(x, y, z) \in \rho_q(E(\mathbb{Q}))$ satisfies $y^2z + xyz + \bar{p}yz^2 = x^3$, which is also a singular curve. However, $(0, 0, 1)$ is not a singular point

in this case.

If r is a prime and $r \nmid p(27p-1)$, then $\rho_r(E)$ is a nonsingular curve defined by $y^2z + xyz + \bar{p}yz^2 = x^3$.

2. Let $E' : y'^2z' + mx'y'z' + pm^3y'z'^2 = x'^3$ for $(m, p(27p-1)) = 1$. Then the set of integral points in E' is isomorphic to those of E under a map $(x', y', z') = (m^2x, m^3y, z)$. However, the image $\rho_q(E'(\mathbb{Q}))$ is singular if and only if $q = p$, $q|(27p-1)$, or $q|m$, where $\rho_q(E(\mathbb{Q}))$ is nonsingular for $q|m$.

Thus we have to choose a *good* equation, before applying reduction modulo p. We want an equation such that the $\rho_p(E)$ is nonsingular as many p as possible.

2.2.1 Minimality

Definition 2.2.1 (Discriminant)**.** *Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. We define the following terms depending on E,*

$$\begin{cases} b_2 &= a_1^2 + 4a_2 \\ b_4 &= a_1a_3 + 2a_4 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2 \\ \Delta_E &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \end{cases} \tag{2.1}$$

Δ_E is called the discriminant *of E.*

If the characteristic of base field is not $2, 3$, then the discriminant can be written as $\Delta_E = -16(4A^3 + 27B^2)$ where $E : y^2 = x^3 + Ax + B$.

In one variable equation $f(x) = 0$, the discriminant of f determines whether the equation has multiple roots or not. Similarly, the discriminant of E determines whether E is singular or not.

Proposition 2.2.2. *E is singular if and only if $\Delta_E = 0$.*

Definition 2.2.3 (Minimal Weierstrass equations)**.** *Let S be the set of ellipitic curves which are isomorphic to E over a number field F and whose*

Weierstrass equations have $\mathcal{O}_F$-integral coefficients. For a prime $\mathfrak{p}$ of F, we say E' is a $\mathfrak{p}$-minimal model *and its Weierstrass equation is a* $\mathfrak{p}$-minimal Weierstrass equation *for E, if* $\mathrm{ord}_{\mathfrak{p}}\Delta_{E'} = \min\{\mathrm{ord}_{\mathfrak{p}}\Delta_E \mid E \in S\}$.

If E' is minimal at all prime $\mathfrak{p}$, then E' is called a (global) minimal model *of E, or just* (globally) minimal*, and the defining equation of E' is called a* (global) minimal Weierstrass equation *for E.*

The $\mathfrak{p}$-minimal model is the best one on which we use reduction mod $\mathfrak{p}$. It is known that

Proposition 2.2.4. *If the base field F has class number 1, i.e the ring of integers $\mathcal{O}_F$ is PID, then E has a minimal model.*

Over $\mathbb{Q}$, therefore, we can choose a minimal equation for any elliptic curve E. Let $f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ be the minimal equation, with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$.

Definition 2.2.5 (Reduction)**.** *Let p be a prime. The* reduction *of E* at p *is a curve defined by $f(x,y) = 0$ over $\mathbb{F}_p$. We denote the set of $\mathbb{F}_p$-rational point of the reduction by*

$$\widetilde{E_p} = \{(x,y) \in \mathbb{F}_p^2 \mid f(x,y) = 0\} \cup \{\infty\}.$$

Note. E can be viewed as a *scheme over* $\mathbb{Z}$ in the sense of $E(\infty) = E(\mathbb{Q})$ and $E(p) = \widetilde{E_p}$, where ∞ is the infinite place (0) and p is the finite prime of $\mathbb{Z}$. This paper, however, is written in a variety language, not in scheme language.

2.2.2 Singularity

Let F be a base field and $f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 \in F[x,y]$ such that $E = \{(x,y) \in \overline{F} \mid f(x,y) = 0\} \cup \{\infty\}$ is a singular curve. It is known that C has only one singular point, say (x_0, y_0), and ∞ is not the singular point. There are two kinds of singularities.

Definition 2.2.6. *Let*

$$f(x,y) - f(x_0,y_0) = \{(y-y_0) - \alpha(x-x_0)\}\{(y-y_0) - \beta(x-x_0)\} - (x-x_0)^3$$

for $\alpha, \beta \in \overline{K}$.

- *If* $\alpha \neq \beta$, *the singular point is called a* node. *In addition, if* $\alpha, \beta \in K$ *it is said to be* splitting. *If* $\alpha, \beta \notin K$ *it is said to be* nonsplitting.
- *If* $\alpha = \beta$, *the singular point is called a* cusp.

Now let E be an elliptic curve and $\widetilde{E_p}$ be a reduction of E modulo p, where the reduction is taken on the minimal Weierstrass equation for E.

Definition 2.2.7. *E has* multiplicative reduction(resp., additive reduction) *at p if $\widetilde{E_p}$ has a node(resp., cusp). The reduction is said to be* splitting (resp., nonsplitting) *if $\widetilde{E_p}$ has a splitting(resp., nonsplitting) node.*

The following fact is well known (Appendix C, [Sil1]).

Proposition 2.2.8. *Let E be an elliptic curve over a number field $\mathbb{F}$ and $\mathfrak{p}$ be a prime in $\mathbb{F}$. Let $E^0_{\mathfrak{p}} := \{P \in E(\mathbb{F}) \mid \tilde{P}$ is nonsingular$\}$. Then $E^0_{\mathfrak{p}}$ is a subgroup of $E(\mathbb{F})$ and a quotient $E(\mathbb{F})/E^0_{\mathfrak{p}}$ is a finite abelian group.*

Definition 2.2.9 (Tamagawa number)**.** *Let $\mathbb{F} = \mathbb{Q}$ in proposition 2.2.8. $m_p := |E(\mathbb{Q})/E^0_p|$ is called The* local Tamagawa number. *Their product*

$$m = \prod_{p:prime} m_p$$

over all primes is called (global) Tamagawa number.

2.3 Mordell-Weil groups

An elliptic curve E is an abelian group.

2.3.1 Complex elliptic curves

Over $\mathbb{C}$, with $X = x + \frac{1}{12}(a_1^2 + 4a_2)$ and $Y = 2y + a_1x + a_3$, we have new equation for E,

$$E \ : \ Y^2 = 4X^3 - g_2X - g_3.$$

Definition 2.3.1 (Weierstrass $\mathcal{P}$-function)**.** *Let $z_1, z_2 \in \mathbb{C}$ be a pair of $\mathbb{R}$-linearly independent complex numbers and $\Lambda = \{m_1 z_1 + m_2 z_2 \mid m_1, m_2 \in \mathbb{Z}\}$ be a lattice on $\mathbb{C}$. A function*

$$\mathcal{P}_\Lambda(z) = \frac{1}{z^2} + \sum_{w \in \Lambda - \{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right)$$

is called a Weierstrass $\mathcal{P}$-function*. In particular, we define a meromorphic function $\mathcal{P}_\tau := \mathcal{P}_\Lambda$ for $\Lambda = \{m_1 + m_2\tau \mid m_1, m_2 \in \mathbb{Z}\}$.*

Definition 2.3.2 (Eisenstein series of weight k)**.**

$$G_k(\tau) = \sum_{(c,d) \in Z^2 - \{(0,0)\}} \frac{1}{(c\tau + d)^k}$$

for an even integer $k > 2$.

Let $g_2 = 60G_4$ and $g_3 = 140G_6$. A meromorphic function $\mathcal{P}$ satisfies a functional equation

$$\mathcal{P}_\tau'^2 = 4\mathcal{P}_\tau^3 - g_2(\tau)\mathcal{P}_\tau - g_3(\tau),$$

which defines an elliptic curve $E_\tau(\mathbb{C}) = \{(\mathcal{P}_\tau(z), \mathcal{P}_\tau'(z) \mid z \in \mathcal{H}\} \cup \{\infty\}$.

Proposition 2.3.3. *Every elliptic curve E over $\mathbb{C}$ can be written as E_τ, i.e. E is isomorphic to E_τ for some $\tau \in \mathcal{H}$.*

An *isomorphism* refers a holomorphic map which has a holomorphic inverse.

With the proposition, we have a bijection between $E(\mathbb{C})$ and a complex torus $\mathbb{C}/\Lambda$. Since $\mathbb{C}/\Lambda$ is an abelian group, E can be equipped with a group structure induced from $\mathbb{C}/\Lambda$. In other word, $E(\mathbb{C})$ is a Lie group T^2.

In this way, however, we have to choose another $\mathcal{P}$-function for each finite field $\mathbb{F}_q$ where E is defined. In addition, it is not easy to know which point $R \in E(\mathbb{C})$ is $P + Q$ for $P, Q \in E$ using $\mathcal{P}$. Thus, we will define the group structure on E in other way.

2.3.2 Picard groups

Let E be a (or an elliptic) curve. The *Picard group* $\mathrm{Pic}^0(E)$ is an abelian group which is equipped with a natual map $E \to \mathrm{Pic}^0(E)$ via $P \mapsto (P)-(O)$, where $O = \infty$ is the identity of group E as a torus.

Definition 2.3.4 (Picard group)**.** *Let* $\mathrm{Div}^0(E)$ *be the group*

$$\Big\{ \sum_{P\in E} \nu_P \cdot (P) \mid \sum_{P\in E} \nu_P = 0 \Big\}$$

of divisors on E*.* $\mathrm{Div}^0(E)$ *has a subgroup consisting of* principal divisors*,*

$$\mathrm{Princ}(E) = \{ \mathrm{div} f \mid f : E \to \mathbb{C}, \textit{homolmorphic}\},$$

where $\mathrm{div} f = \sum n_P \cdot (P)$ *if* f *has a zero at* P *with multiplicity* n_P*.*

A Picard group *is a factor group*

$$\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\mathrm{Princ}(E).$$

Consider a map

$$\begin{aligned} \iota : E &\to \mathrm{Pic}^0(E) \\ P &\mapsto (P) - (O) \end{aligned}$$

By Bezout's theorem, for any $P \in E$, there is unique $P' \in E$ such that P, O, and P' lie on a line $x + c = 0$. Let $f(x, y) = x + c$ be a function on E. Then $\mathrm{div} f = (P) + (P') - 2(O)$. Thus we can choose unique $P' \in E$ for each $P \in E$ such that $(P') - (O) = -((P) - (O))$ in $\mathrm{Pic}^0(E)$. Similary, for any $P, Q \in E$, there is unique $R \in E$ such that P, Q, and R lie on same line $ax + by + c = 0$. For $f(x, y) = ax + by + c$, $\mathrm{div} f = (P) + (Q) + (R) - 3(O)$ and we know $((P) - (O)) + ((Q) - (O)) = (R') - (O)$ in $\mathrm{Pic}^0(E)$. Now define a binary operation $+ : E \times E \to E$ via $P + Q = R'$ where $R \in E$ is the third point on the line through P and Q. Our claim is that the binary operation $+$ is the addition on torus.

Theorem 2.3.5. *Let* $E = E_\tau$*. Then* $(E, +)$ *is a group and is isomorphic to* $(\mathbb{C}/\Lambda_\tau, +)$*.*

We use two aspects of the group structures to study elliptic curves. They provide different merit to understand the groups. Assume E is defined over $\mathbb{Q}$. Let $P_i = (x_i, y_i) \in E(\mathbb{C})$ for $i = 1, 2, 3$ and $P_3 = P_1 + P_2$. Then a line L passing through P_1 and P_2 is defined by

$$(x_2 - x_1)(y - y_1) = (y_2 - y_1)(x - x_1).$$

Then the third point of $L \cap E$ is $-P_3$.

Proposition 2.3.6. *Let $y = \lambda x + \nu$ be the line through P_1 and P_2, or tangent to E when $P_1 = P_2$. Then*

$$P_3 = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -(\lambda + a_1)x_3 - \nu - a_3).$$

For an elliptic curve over a field of characteristic $p < \infty$, we can take a group structure induced from line relations, i.e $P + Q + R = O$ if P, Q, R are on a same line.

Fix $\overline{\mathbb{Q}_p} \hookrightarrow \mathbb{C}$. For an elliptic curve E defined over $\mathbb{F}_q$, where q is a power of p, and $P, Q \in E$, we obtain an elliptic curve E' over $\overline{\mathbb{Q}_p}$ by lifting : Choose a_i' for $E' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$ such that $a_i' \equiv a_i \pmod{p}$ for $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Then $P', Q' \in E'(\overline{\mathbb{Q}_p})$ exist such that $P' \equiv P, Q' \equiv Q \pmod{p}$. Then reduce the group structures on $E'(\mathbb{C})$ to $E'(\overline{\mathbb{Q}_p})$ and $E(\mathbb{F}_q)$.

As a torus, the set of torsion points are obvious. Let n be any positive integer and $E[n] = \{P \in E(\mathbb{C}) \mid n \cdot P = 0\}$. Then $E[n]$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ as an abelian group. If E is defined over $\overline{\mathbb{F}_p}$, we have similar argument.

Proposition 2.3.7. *Let K be a base field of characteristic p. Then*

1. *$E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ if $(p, n) = 1$.*
2. *$E[l] \cong \mathbb{Z}/l\mathbb{Z}$ or $\{O\}$ if l is a power of p.*

We say E is ordinary if $E[p] \cong \mathbb{Z}/p\mathbb{Z}$ and supersingular if $E[p] \cong \{O\}$.

We can define the same binary operation on the reduction. In the case, $(\tilde{E}, +)$ may not be a group. If the reduction is bad, then it has a different property.

Proposition 2.3.8. *Let E be a singular curve as above and E_{ns} denote $E - \{(x_0, y_0)\}$. Then*

1. *If E has a node, then $(E_{ns}, +)$ is isomorphic to a multiplicative group $(K^*, \cdot)$.*
2. *If E has a cusp, then $(E_{ns}, +)$ is isomorphic to an additive group $(K, +)$.*

$(E_{ns}, +)$ is defined as the way on an elliptic curve by line relation.

2.4 Isogenies and dual isogenies

Let E and E' be elliptic curves over $\mathbb{C}$.

Definition 2.4.1 (Isogeny)**.** *Let $f : E \to E'$ be a holomorphic map between Riemann surfaces and a group homomorphism. Then f is called an* isogeny*. If f is nonconstant, we say E' is isogenous to E.*

From now on, a map between elliptic curves denotes an isogeny.

Let $f : E \to E'$ be an isogeny. In general, f induces its dual f^* on a set of functions via $f^*(g) = g \circ f$. For example, we have $f^* : \mathrm{Pic}^0(E') \to \mathrm{Pic}^0(E)$. Note that $\mathrm{Div}^0(E) = \{n : E \to \mathbb{Z} \mid \ | \{P \mid n(P) \neq 0\} | < \infty, \ \sum n(P) = 0 \ \}$ is a set of functions and $g \circ f$ is a function on E for any function g on E'. Since $E \cong \mathrm{Pic}^0(E)$, we can define an isogeny $f^* : E' \to E$.

Definition 2.4.2 (Dual isogeny)**.** *Let $f : E \to E'$ be an isogeny. Then*

$$\begin{aligned} f^* : \ E' &\to E \\ P &\mapsto \sum_{Q \in f^{-1}(P)} Q \end{aligned}$$

is called the dual isogeny *of f.*

For an isogeny $f : E \to E'$ of degree n, $f^* \circ f = [n]$ on E. $[n]$ is the multiplication by n map. Moreover, E is isogenous to E' under f^*. Thus the isogenous relation on elliptic curves is an equivalence relation.

2.5 Modular curves and modular forms

"Modularity" is a keyword to understand elliptic curves. There are many interesting results for studying ellipitic curves described in modular method.

2.5.1 Modular curves

From now on, for any 2×2 matrix γ, we denote $\gamma = \begin{pmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{pmatrix}$.

Let $\tau, \tau' \in \mathcal{H}$ be conjugate, i.e. $\gamma\tau = \tau'$ for some $\gamma \in SL_2(\mathbb{Z})$. Then two elliptic curves

$$\begin{aligned} E_\tau &: y^2 = 4x^3 - g_2(\tau)x - g_3(\tau) \\ E_{\tau'} &: y'^2 = 4x'^3 - g_2(\tau')x' - g_3(\tau') \end{aligned}$$

are isomorphic under $x' \mapsto u^2 x,\ y' \mapsto u^3 y$ for $u = (c_\gamma \tau + d_\gamma)^{k/2}$

Thus two lattice Λ and Λ' define isomorphic elliptic curves if they are conjugate. In other words, $SL_2(\mathbb{Z})\backslash\mathcal{H} := \{SL_2(\mathbb{Z}) \cdot \tau \mid \tau \in \mathcal{H}\}$ is a family of elliptic curves.

Proposition 2.5.1. *There is one-to-one correspondence between $SL_2(\mathbb{Z})\backslash\mathcal{H}$ and the set of isomorphic classes of elliptic curves.*

By proposition 2.5.1, elliptic curves over $\mathbb{C}$ can be parametrized by the points in $SL_2(\mathbb{Z})\backslash\mathcal{H}$. As this observation, for some special subgroup Γ of $SL_2(\mathbb{Z})$, $\Gamma\backslash\mathcal{H}$ presents another parametrization on elliptic curve. They are called *enhanced elliptic curves*.

Let $\mathcal{H}$ be the upper half plane and $\widehat{\mathcal{H}} = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. $SL_2(\mathbb{Z})$ acts on $\widehat{\mathcal{H}}$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}.$$

Let N be a positive integer. $SL_2(\mathbb{Z})$ contains subgroups, called congruence subgroups of level N,

$$\begin{aligned}\Gamma(N) &= \{\gamma \in SL_2(\mathbb{Z}) \mid \gamma \equiv I \pmod N\} \\ \Gamma_1(N) &= \{\gamma \in SL_2(\mathbb{Z}) \mid a_\gamma \equiv d_\gamma \equiv 1, c_\gamma \equiv 0 \pmod N\} \\ \Gamma_0(N) &= \{\gamma \in SL_2(\mathbb{Z}) \mid c_\gamma \equiv 0 \pmod N\}.\end{aligned}$$

These groups act on $\mathcal{H}$ and $\widehat{\mathcal{H}}$. With the action, define new curves.

$$\begin{aligned}Y(N) = \Gamma(N)\backslash\mathcal{H}, \quad Y_0(N) = \Gamma_0(N)\backslash\mathcal{H}, \quad Y_1(N) = \Gamma_1(N)\backslash\mathcal{H} \\ X(N) = \Gamma(N)\backslash\widehat{\mathcal{H}}, \quad X_0(N) = \Gamma_0(N)\backslash\widehat{\mathcal{H}}, \quad X_1(N) = \Gamma_1(N)\backslash\widehat{\mathcal{H}}\end{aligned}$$

Such curves are called *modular curves*. $X(N)$(respecitvely, $X_0(N)$ and $X_1(N)$) is a compactification of $Y(N)$(resp, $Y_0(N)$ and $Y_1(N)$) with the induced topology.

Proposition 2.5.2. *Modular curves are moduli of elliptic curves defined over* $\mathbb{C}$. *In particular,*

- $Y(N) = \{(E, P, Q) \mid E \text{ is an elliptic curve}\}/\cong$
  where $P, Q \in E$ *are points of order* N *such that* $e(P, Q) = e^{2\pi i/N}$ *and* $(E, P, Q) \cong (E', P', Q')$ *if and only if there is an isomorphism* $\phi : E \to E'$ *such that* $\phi(P) = P', \phi(Q) = Q'$.

- $Y_1(N) = \{(E, P) \mid E \text{ is an elliptic curve}\}/\cong_1$
  where $P \in E$ *is a point of order* N *and* $(E, P) \cong_1 (E', P')$ *if and only if there is an isomorphism* $\phi : E \to E'$ *such that* $\phi(P) = P'$.

- $Y_0(N) = \{(E, C) \mid E \text{ is an elliptic curve}\}/\cong_0$
  where C *is a cyclic subgroup of* E *of order* N *and* $(E, < P >) \cong_0 (E', < P' >)$ *if and only if there is an isomorphism* $\phi : E \to E'$ *such that* $\phi(C) = C'$.

The proposition for $N = 1$ implies proposition 2.5.1. In addition, cusps in $X(N) - Y(N)$, $X_1(N) - Y_1(N)$, and $X_0(N) - Y_0(N)$ are corresponded to singular cubic curves.

Remark.(isogeny) Using $Y_0(N)$, we can describe a kind of isogeny. Let $E_\tau = \mathbb{C}/\langle 1, \tau\rangle$ be an elliptic curve and $C = \left\langle \frac{1}{N} \right\rangle$ be a cyclic subgroup of E_τ. Then E/C is isomorphic to an elliptic curve $E' = \langle 1, N\tau\rangle$. E_τ and E' are isogenous. For the natural projection $\pi : E \to E/C$, we have $[N] = \pi \circ \pi^* : E' \to E/C$.

2.5.2 Modular parametrizations

By definition, a modular curve is a set of equivalence classes of elliptic curves. By the way, there is an interesting result on the relation between modular curves and elliptic curves : an elliptic curve itself is similar to a modular curves.

Theorem 2.5.3 (Modularity theorem)**.** *Let E be an elliptic curve over $\mathbb{Q}$. There is an integer N and a $\mathbb{Q}$-rational surjective map*

$$X_0(N) \to E$$

such that $(\infty) \mapsto O$.

This big theorem is conjectured by Taniyama and Shimura. The conjecture is very famous for non-mathmatician because it implies *Fermat's Last Theorem*. A. Wiles proves Theorem 2.5.3 for squarefree integer N in , and for general N with Brunil, Conrad, Diamond, and Tayler [B-C-D-T][T-W][Wi].

Example. Let $E : y^2 - 10xy - 11y = x^3 - 11x^2$. Then there is a holomorphic map $X_0(11) \to E$. In fact, $X_0(11) \cong E = \mathbf{11a1}$.

The minimal $N = N_E$ in theorem 2.5.3 is called an *(analytic) conductor* of E.

Let E and E' be isogenous elliptic curves. Then $X_0(N) \to E \to E'$ makes $N'_E \leq N_E$. Since isogenous relation is an equivalence relation, $N'_E = N_E$. Thus the conductor N is an invariant under isogenies.

Remark. E and E' have same conductor if they are isogenous, but the converse is false. For example, let $E = \mathbf{158c1}$ and $E' = \mathbf{158d1}$ in Cremona's Table. E contains a rational point of order 5 and E' has a rational

point of order 3. According to proposition 3.2.1 in next chapter, there is an elliptic curve with a rational point of order 15 if E and E' are isogenous. From Mazur's classification, we know that no elliptic curve contains a rational point of order 15.

The modular parametrization factors through the Jacobian $J_0(N)$.

$$\phi : J_0(N) \to E$$

Proposition 2.5.4. *The followings are equivalent.*

1. *The dual map $\phi^* : E \to J_0(N)$ is injective.*
2. $\ker \phi$ *is connected.*
3. *ϕ is universal, i.e. if there is another modular map $\phi' : J_0(N) \to E'$, then there is an isogeny $\pi : E \to E'$ such that $\phi' = \pi \circ \phi$*

Such (E, ϕ), or E, is called an *optimal curve* or X_0-optimal curve. Similarly, E is called an X_1-optimal curve if $J_1(N) \to E$ is universal.

2.5.3 Modular forms

This section refers to Diamond-Shurman [D-S].

Definition 2.5.5. *A holomorphic function $f : \mathcal{H} \to \mathbb{C}$ is called a* modular form of weight k at level N *if*

1. *f is holomorphic at cusps of $X_1(N)$ and*
2. *$f(\gamma\tau) = (c_\gamma \tau + d_\gamma)^k f(\tau)$ for any $\gamma \in \Gamma_1(N)$.*

If f is 0 at cusps, then f is called a cusp form.

Example. For even $k > 2$, the Eisenstein series (see definition 2.3.2) of weight k is a modular form of weigth k at level 1.

Note that f is a modular form (resp, a cusp form) at level N if $M|N$ and f is a modular form (resp, a cusp form) at level M. In this manner, we say

a form f at level N is *old* if it is induced from a form g at level M for some $M|N, M < N$.

Let $\pi_a : \widehat{\mathcal{H}} \to \widehat{\mathcal{H}}$ be a multiple by a, i.e. an action by $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ and f be a modular form at level M. Then $\pi_a^* f \ : \ \tau \mapsto f(a\tau)$ is a modular form at level Ma. For fixed N, a multiple of M, we say f is a modular form at lavel N with $a = 1$.

Definition 2.5.6. *Let $S_k(N)$ be the $\mathbb{C}$-space of all cusp forms of weight k at level N.* Petersson inner product *is defined on $S_k(N)$:*

$$< f, g >= \frac{1}{V(N)} \int_{X_0(N)} f(\tau)\overline{g(\tau)}(\mathrm{Im}(\tau))^k d\mu(\tau),$$

where $\mu(\tau) = dxdy/y^2$ for $\tau = x + iy$, $V(N) = \int_{X_0(N)} d\mu(\tau)$.

In general, the integration converges if one of f and g is a cusp form of weight k and the other is a modular form of weight k, $\phi(\tau) = f(\tau)\overline{g(\tau)}(\mathrm{Im}(\tau))^k$ is invariant under $\Gamma_0(N)$ action, and $< f, g >$ does not depend on N. In this manner, when $k = 2$, f can be viewed as a differential 1-form

$$\omega_f = f(\tau)d\mu(\tau).$$

Definition 2.5.7 (Old and new forms)**.** *Let $S_k(N)$ be the $\mathbb{C}$-space of all cusp forms at level N and of weight k. The subspace of old forms is defined by*

$$S_k(N)^{old} = \sum_{d|N} \pi_d^* S_k(Nd^{-1}).$$

The subspace of new forms $S_k(N)^{new}$ is defined by orthogonal complement with respect to the Petersson inner product. In particular, a new form *refers to a normalized (i.e. $a_1(f) = 1$) element in $S_k(N)^{new}$.*

2.6 Hecke operators

In this section, we want to define two type of Hecke operators on the space of modular forms.

2.6.1 Double coset operators

Definition 2.6.1. *Let $\alpha \in SL_2(\mathbb{Z})$ and $\Gamma_1(M)\alpha\Gamma_1(N)$ be a double coset of $SL_2(\mathbb{Z})$. Choose any representatives $\{\beta_j\}_j$ such that $\Gamma_1(M)\alpha\Gamma_1(N) = \cup_j \Gamma_1(M)\beta_j$. The* weight k $\Gamma_1(M)\alpha\Gamma_1(N)$ operator *takes a modular form f at level N of weight k to*

$$< \alpha > f := \sum_j f[\beta]_k,$$

where $(f[\beta]_k)(\tau) := (\det \beta)^{k-1}(c_\beta \tau + d_\beta)^{-k} f(\beta(\tau)), \tau \in \mathcal{H}$.

The first type of Hecke operators is $< \alpha >$ for $M = N$ and $\alpha \in \Gamma_0(N)$. Since

$$\begin{aligned} \Gamma_0(N) &\to \mathbb{Z}/N\mathbb{Z} \\ \gamma &\mapsto d_\gamma \end{aligned}$$

is a surjective group homomorphism with kernel $\Gamma_1(N)$, $< \alpha >$ is determined by d_α. Thus for any integer d,

$$< d > f :=< \alpha > f$$

is well defined for any $\alpha \in \Gamma_0(N), d_\alpha \equiv d \pmod N$.

Since $\alpha^N \in \Gamma_1(N)$ for all $\alpha \in \Gamma_0(N)$, $< d >^N = 1$. In fact, $< d > f/f$ defines a character $\chi_f : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}$ for $(d, N) = 1$.

The second type of Hecke operator is $< \alpha >$ for α_p, where

$$\alpha_p = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$$

for a prime p. Write

$$T_p(f) =< \alpha_p > f.$$

Proposition 2.6.2. *Let p and q be primes and d and e be integers such that $(d, N) = (e, N) = 1$.*

1. *Let f be a modular form at level N of weight k. Then*

$$T_p f = \begin{cases} \sum_{j=0}^{p-1} f[\left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right)]_k & \text{if } p|N, \\ \sum_{j=0}^{q-1} f[\left(\begin{smallmatrix} 1 & j \\ 0 & q \end{smallmatrix}\right)]_k + f[\left(\begin{smallmatrix} m & n \\ N & q \end{smallmatrix}\right)\left(\begin{smallmatrix} q & 0 \\ 0 & 1 \end{smallmatrix}\right)] & \text{if } q \nmid N \end{cases}, \text{ where } mq - nN = 1.$$

2. *$< d >, < e >, T_p$, and T_q commute each other, as actions on the space of modular forms at level N of weight k.*

Now note that $< d >$ and T_p are determined by matrix actions. In other words, $< d >$ and T_p act on a modular curve $X_1(N)$ via

$$< d >: \Gamma_1(N)\tau \mapsto \Gamma_1(N)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\tau, \ \left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right) \in \Gamma_0$$

and

$$T_p : \Gamma_1(N)\tau \mapsto \sum_j \Gamma_1(N)\beta_j\tau,$$

where β_j are given in proposition 2.6.2. In particular, $< d >$ induces an endomorphism $[d]$, a multiplication by d, on elliptic curves.

Let E be an elliptic curve and define $a_E(p) = p + 1 - |\widetilde{E_p}|$ for each prime p and $a(n)$ for $n \in \mathbb{N}$ by

- $a(1) = 1$,
- $a(mn) = a(m)a(n)$ if m and n are relatively prime, and
- $a(p^r) = a(p^{r-1})a(p) - p$

For the sequence $a(n)$, define

$$f_E(z) = \sum_{n=1}^{\infty} a(n)q^n,$$

where $q = \exp(2\pi iz)$. Such f_E is called the *associated newform*, associated to E. The Hecke operator T_p on $\mathrm{Div}^0(Y_1(N))$ acts on the set of $\{f_E \mid E \ : \text{ elliptic curve}\}$, in particular, on $a(q)$ for all prime q.

Proposition 2.6.3. *Let $f_E(z) = \sum a_f(n)q^n$. Then for any prime p and $f' = T_p f$,*

$$a_{f'}(1) = a_f(p).$$

The Modularity theorem, *every elliptic curve is modular*, can be written by :

Theorem 2.6.4. *Let E be an elliptic curve of conductor N. Then f_E is a newform at level N of weight 2.*

2.6.2 The Atkin-Lehner involution

Define W_N on $S_k(N)$ by $W_N f = -f[\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)]_2$, i.e.

$$(W_N f)(\tau) = -\frac{1}{N\tau^2} f(-\frac{1}{N\tau}).$$

Proposition 2.6.5. *Let f_E be an associated new form.*

- *W_N is self-adjoint with respect to the Petersson inner product*

$$< \ , \ >: S_2(\Gamma_0(N)) \times S_2(\Gamma_0(N)) \to \mathbb{C}.$$

- *$W_N^2 =$*id *and f_E is an eigenvector, i.e. $W_N f = \omega_N f$ for $\omega_N \in \{1, -1\}$.*

The eigenvalue w_N is called the root number of E. The following proposition on w_p and reduction type of E is an important idea for Dummigan's results, introduced in the next chapter.

Proposition 2.6.6. *Suppose $E/\mathbb{Q}$ has a multiplicative reduction at p. Then*

$$w_p = 1 \Leftrightarrow E \text{ has nonsplitting multiplicative reduction.}$$

2.7 Hasse-Weil L-function

Let E be an elliptic curve with associated newform $f = \sum a(n)q^n$. Then an analytic continuation of

$$s \mapsto \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$$

is called the *L-function of* E, denoted by $L(E, s)$.

Let $\Lambda(s, E)$ be the modified L-function of E and $\Lambda(s, E) = \epsilon\Lambda(2 - s, E)$. Then $\epsilon = -w_N$. For a prime $p|N$, we can also define w_p via W_p. Applying W_p on $f_E = \sum a(n)q^n$, we have $w_p = -a(p)$, for any prime $p||N$.

Chapter 3

Rational torsion and quadratic twists

When an elliptic curve $E/\mathbb{Q}$ of square-free conductor N has a rational point of odd prime order $l \nmid N$, Dummigan [Du] explicitly constructed a rational point of order l on the optimal curve E_0, isogenous over $\mathbb{Q}$ to E, under some conditions. In this chapter, we show that his construction also works unconditionally. And applying it to Heegner points on elliptic curves, we find a family of elliptic curves $E/\mathbb{Q}$ such that a positive proportion of quadratic twists of E has (analytic) rank 1.

3.1 Construction of rational torsion points

We will find a point in $J_0(N)$ rather than one in elliptic curves.

Let N be a positive integer, and let δ denote a positive divisor of N. For a family $\mathbf{r} = (r_\delta)$ of rational numbers $r_\delta \in \mathbb{Q}$ indexed by all the positive divisors δ of N, define

$$g_{\mathbf{r}} = \prod_{\delta|N} \eta_\delta^{r_\delta}.$$

Such $g_{\mathbf{r}}$ is called a Dedekind η-product, where $\eta_\delta(z) = \eta(\delta z)$. We will use a propsition (cf. Proposition 3.2.1, [Li]) without proof.

Proposition 3.1.1 (Ligozat)**.** *The Dedekind η-product $g_{\mathbf{r}}$ is a modular func-*

tion on the modular curve $X_0(N)$ if and only if the following conditions are satisfied:

1. $\sum_{\delta|N} r_\delta \delta \equiv 0 \pmod{24}$;
2. $\sum_{\delta|N} r_\delta \frac{N}{\delta} \equiv 0 \pmod{24}$;
3. $\sum_{\delta|N} r_\delta = 0$;
4. $\prod_{\delta|N} \delta^{r_\delta}$ *is a the square of a rational number.*

The $\Gamma_0(N)$-equivalent classes of cusps on $X_0(N)$ are

$$\begin{aligned}(P_1) &= \{c \mid c \in \mathbb{Z}\},\\ (P_N) &= \{\frac{a}{cN} \mid a, c \in \mathbb{Z}, (a, cN) = 1\} \cup \{\infty\}, \text{ and}\\ (P_r) &= \{\frac{a}{cr} \mid a, c, r \in \mathbb{Z}, (a, cr) = 1, r = (cr, N), r \neq 1, N\}.\end{aligned}$$

Given $E/\mathbb{Q}$ of level N, let f be the associated newform for E and w_d be eigenvalues such that $W_d f = w_d f$, for positive $d|N$. Let G be the product of those primes suth that $w_p = 1$. Define a (cuspidal) divisor of $X_0(N)$:

$$Q = \sum_{\delta|N/G} w_\delta (P_{\delta G}).$$

Q is a divisor of degree 0 if there is a prime p such that $w_p = -1$.

3.2 Rational torsion and optimal curves

3.2.1 Known facts

Let $\eta(z) = q^{1/24} \prod_{n=1}^{\infty}(1 - q^n)$ be Dedekind's eta function, a 24^{th} root of Δ, and define $\eta_d(z) = \eta(dz)$ for $d|N$ and

$$r := \prod_{p|G}(p^2 - 1) \prod_{p|N/G} (p - 1), \; h := (r, 24)$$

where p runs through primes. Now there is a function

$$F = \left(\prod_{g|G} \prod_{d|N/G} \eta_{dg}^{w_d \mu(g) g} \right)^{24/h}$$

where μ is the Möbius function.

In [Du], Dummigan proves the following theorem.

Theorem 3.2.1. *Let $E/\mathbb{Q}$ be an elliptic curve of square-free conductor N with a rational point of odd prime order $l \nmid N$ and E_0 be the $X_0(N)$-optimal curve, isogenous over $\mathbb{Q}$ to E. If $w_p = -1$ for at lest one prime $p|N$ and $l|n$, where $n = r/h$, then*

1. *Q is a $\mathbb{Q}$-rational cuspidal divisor of degree 0,*
2. *$g_r^2 \in \mathbb{Q}(X_0(N))$ and $\mathrm{div}(g_r^2) = (-1)^t w_N(2n)Q$, where t is the number of prime divisors of N,*
3. *the exact order of the rational point $[Q]$ in $J_0(N)$ is either n or $2n$,*
4. *E_0 has a $\mathbb{Q}$-rational l-torsion point P such that $\pi^*(P) = \frac{2n}{l}[Q]$.*

In particular, for E_0 and E in proposition 3.2.1, there is a rational point of l in E_0.

3.2.2 Generalization of Dummigan's result

Theorem 3.2.1 assume $l \nmid N$ and $l \mid n$. The assumption, in fact, is relevant.

Theorem 3.2.2. *Let $E/\mathbb{Q}$ be an elliptic curve of square-free conductor N with a rational point of odd prime order $l \nmid N$. Then $w_p = -1$ for at least one prime $p \mid N$, and $l|n$.*

The key tools for the proof of proposition 3.2.2 are

- parametrizations for elliptic curves with torsion structures and
- the image of torsion under reduction.

See Table 3, [Ku] for the paramerization. From the image of torsion under reduction maps, we know two facts.

Lemma 3.2.3. *Let E be an elliptic curve in proposition* 3.2.2 *and $p \mid \Delta$, i.e. E' has bad reduction at p. Assume that E has no additive reduction.*

1. *If an l-torsion point become a singular point under reduction modulo p, then $w_p = -1$ and $l \mid \mathrm{ord}_p(\Delta)$.*

2. *Assume that an l-torsion point become a nonsingular point under reduction modulo p. Then l divide the order of $\tilde{E}(\mathbb{F}_p)_{ns}$. In particular, $w_p = -1$ if and only if $l \mid p-1$ and $w_p = 1$ if and only if $l \mid p+1$.*

To prove this lemma, we may assume $(0,0)$ is a rational torsion point of order l. If it is necessary, we can translate E' by $(x,y) \mapsto (x-\alpha, y-\beta)$. If $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x$ is a singular curve and $(0,0)$ is the singular point, then we can easily know $a_2 = a_3 = a_4 = 0$ and the curve is the zero locus of $F(x,y) = y^2+a_1xy-x^3$. Since $F(x,y)-F(0,0) = y(y+a_1x)-x^3$, the curve has split multiplicative singularity. This proves the first part of the lemma. The second part comes from the order of nonsingular group $\tilde{E}_p$.

From lemma 3.2.3, we know that $l \mid n$ holds if there is a prime $p \mid \Delta$ such that $l \nmid \mathrm{ord}_p(\Delta)$ and $l \neq 3$, and there is a prime p such that $w_p = -1$ if a torsion point has singular image in the reduction.

Proof of Theorem 3.2.2

$l = 3, 5$, or 7. We prove the theorem for each case.

Case I. $l = 3$.

In this case as a minimal Weierstrass equation for E, we can take

$$E : y^2+axy+by = x^3, \quad a,b \in \mathbb{Z},\ b > 0.$$

Since the conductor N of E is square-free, we can assume that $\gcd(a,b) = 1$. $(0,0)$ is a point of order 3.

Let $\Delta = b^3(a^3-27b)$ be the minimal discriminant of E. For a prime $p \mid \Delta$ $(p \neq 3)$, we have, by lemma 3.2.3,

(1) If $p \mid b$, then $w_p = -1$,
(2) For each $p \mid a^3 - 27b$, $w_p = -1$ if $p \equiv 1$ (mod 3) and $w_p = 1$ if $p \equiv -1$ (mod 3).

Thus if $a^3 - 27b$ has two or more prime factors, then $9|r$, so $3|n$.

Now we consider the case that $a^3 - 27b$ has only one or no prime factor. Let $b = ts$, $t, s \in \mathbb{N}$, where for each prime $p \mid b$, $p \mid t$ if $p \equiv 1 \pmod 3$ and $p \mid s$ if $p \equiv -1 \pmod 3$.

Lemma 3.2.4.
(i) If $a^3 - 27b = m^3$ for an integer m, then there is at least one prime $p|t$.
(ii) If $a^3 - 27b = \pm 1$ and $t = p^k$ for a prime p, then $p \equiv 1$ (mod 9).

Proof:
(i) If $a^3 - 27b = m^3$, then $a \equiv m \pmod s$ because for all $p \mid s$, $p \equiv -1 (\text{ mod } 3)$ and $3 \nmid |(\mathbb{Z}/s\mathbb{Z})^*|$. Let $a = \alpha s + m$, $\alpha \in \mathbb{Z}$. Then

$$a^3 = (\alpha^3 s^2 + 3\alpha^2 sm + 3\alpha m^2)s + m^3 = (27t)s + m^3.$$

This implies α is a multiple of 3, moreover, a multiple of 9, so $a = 9\beta s + m$, $\beta \in \mathbb{Z}$. Thus

$$\beta(27\beta^2 s^2 + 9\beta sm + m^2) \quad = \quad t.$$

By completing the square in the second factor, we see that $t > 1$ and there is at least one prime $p|t$.
(ii) Suppose that $a^3 - 27b = \pm 1$ and $t = p^k$ for a prime p. By the same way in (i), we have that

$$\beta(27\beta^2 s^2 \pm 9\beta s + 1) \quad = \quad t.$$

Since $(\beta, t/\beta) = 1$ and $(t/\beta) > 1$, $\beta = 1$. Thus $27s^2 \pm 9s + 1 = p^k$. Euler's case $n = 3$ of Fermat's Last Theorem and the equation $(\pm 3s)^3 + (27s^2 \pm 9s + 1) = (\pm 3s + 1)^3$ imply that 3 cannot divide k. So $p \equiv \pm 1 \pmod 9$ and by the choice of t, we have that $p \equiv 1 \pmod 9$. □

If there are at least two primes $p|t$, then $9|r$, so $3|n$. Suppose that there is only one prime $p|t$. If $a^3 - 27b$ has a prime factor q, then $q - 1$ or $q^2 - 1$

is divisible by 3 and $p-1$ is divisible by 3, so $9|r$ and $3|n$. If $a^3-27b=\pm 1$, then $p-1$ is divisible by 9 by Lemma 3.2.4, so $9|r$ and $3|n$. If there is no prime $p|t$, then $a^3-27b=q^k$ for a prime q and $3 \nmid k$ by Lemma 3.2.4. This implies that $q=\pm 1 \pmod 9$. So $9|r$ and $3|n$.

On the other hand, if $b \neq 1$, then there is a prime $p \,|\, b$ such that $\omega_p=-1$. If $b=1$, then $\Delta=a^3-27=(a-3)(a^2+3a+9)$. $a-3$ and a^2+3a+9 are relatively prime. Suppose $\omega_p=1$ for a prime $p \,|\, a^3-27$. Since $p \equiv -1 \pmod 3$ and $a^3 \equiv 27 \pmod p$, we have that $p \,|\, a-3$. Thus there should be another prime $q \,|\, a^2+3a+9$ such that $\omega_q=-1$. This completes the proof of $l|n$ for the case $l=3$.

Case II. $l=5$.

In this case, we need the following lemma, which follows from the proof of Proposition 5.3, [V05].

Lemma 3.2.5. *Let l be an odd prime. Let $E_0/\mathbb{Q}$ be an optimal elliptic curve of the minimal discriminant Δ and of square-free conductor N. Suppose that $l \nmid N$ and Δ be the l^{th}-power of a rational number. Then there is a prime divisor $p \,|\, N$ such that $p \equiv 1 \pmod l$.*

Proof: For an odd prime l, if Δ is an l^{th} power, then we know that $E_0[l] \cong (\mathbb{Z}/l\mathbb{Z}) \bigoplus \mu_l$ is a decomposable $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$-module (see Proposition 4.2, [Du]). From Theorem 1.1 [V05], we have $\mu_l \subset E \subset J_0(N)$ and $\mu_l \subset E[l]$ is contained in the Shimura subgroup V of $J_0(N)$. Since the order of V divides $\phi(N)$ by Corollary 1, [L-O], there is a prime $p \,|\, N,\ p \equiv 1 \pmod l$ if $l^2 \nmid N$. □

Let E be an elliptic curve with a point of order 5. As a minimal Weierstrass equation for E, we can take

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

with $u, v \in \mathbb{Z}$, $(u,v)=1$ and the minimal discriminant is

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

For $p \mid \Delta$, we know that,

(1) If $p \mid uv$*, then* $w_p = -1$.
(2) For each $p \mid v^2 - 11uv - u^2$*,* $w_p = -1$ *if* $p \equiv 1 \pmod 5$ *and* $w_p = 1$ *if* $p \equiv -1 \pmod 5$.

If $|uv| > 1$ and $p \mid uv$, then $w_p = -1$. If $|uv| = 1$, then the elliptic curve is isomorphic to $y^2 + y = x^3 - x^2$, $\Delta = -11$, $N = 11$, and $w_{11} = -1$. So there is at least one prime $p \mid N$ such that $w_p = -1$.

Let E_0 be the optimal elliptic curve, isogenous over $\mathbb{Q}$ to E, of the minimal discriminant Δ_0. We note that E_0 and E have the same n. If Δ_0 is not the 5th-power of a rational number, then Dummigan [Du] proved that $5 \mid n$. If Δ is the 5th-power of a rational number, then by Lemma 3.2.5, there is a prime divisor $p \mid N$ such that $p \equiv 1 \pmod 5$. So $5 \mid n$.

This completes the proof of the case $l = 5$.

Case III. $l = 7$. As a minimal Weierstrass equation for E, we can take

$$E : y^2 + (u^2 + uv - v^2)xy - u^3v^2(v - u)y = x^3 - uv^2(v - u)x^3$$

with $u, v \in \mathbb{Z}$, $(u, v) = 1$ and the minimal discriminant is

$$\Delta = v^7(v - u)^7u^7(v^3 - 8uv^2 + 5u^2v + u^3).$$

Proposition 4.3. in [Du] shows that $7 \mid n$. And if $p \mid uv(v - u)$, then $w_p = -1$ and there is at least one p such that $w_p = -1$. This completes the proof of the case $l = 7$.

Now we complete the proof of Theorem 3.2.2.

□

Example.(Proposition 5.1, [B-J-K]) There are infinitely many m such that

$$(9(2m + 1) - 1)^3 = 27p + q \tag{3.1}$$

for some prime p, q. For such triple (m, p, q), define a family of elliptic curves $\{E_m \mid (m, p, q) \text{ satisfies (3.1)}\}$ where

$$E_m \ : \ y^2 + (9(2m + 1) - 1)xy + py = x^3.$$

Then the discriminant Δ_m of E_m is p^3q and the conductor N_m is pq. E_m has splitting multiplicative reduction at p and nonsplitting multiplicative reduction at q. The sign of Atkin-Lehner involutions are $w_p = -1$ and $w_q = 1$. In this case $q \equiv -1 \pmod{27}$ so the constructed point $[R]$ is of order 3. In fact, E_m is $X_0(pq)$-optimal in the 3-isogeny class.

3.3 Rank one quadratic twists

Let $E/\mathbb{Q} : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{Q}$ of conductor N and let $L(s, E) = \sum_{n=1}^{\infty} a(n)n^{-s}$ be its Hasse-Weil L-function defined for $\Re(s) > \frac{3}{2}$. The work of Breuil, Conrad, Diamond, Taylor and Wiles [B-C-D-T] [T-W] [Wi] implies that $L(s, E)$ has an analytic continuation to $\mathbb{C}$ and satisfies a functional equation relating the values at s and $2-s$. Let ϵ be the sign of the functional equation of $L(s, E)$. Then we have that $\epsilon = -\prod_{p|N} w_p$. Let D be the fundamental discriminant of the quadratic field $\mathbb{Q}(\sqrt{D})$, and let $\chi_D = (\frac{D}{\cdot})$ denote the usual Kronecker character. For D coprime to the conductor of E, the Hasse-Weil L-function of the quadratic twist $E_D : Dy^2 = x^3 + ax + b$ of E is the twisted L-function $L(s, E_D) = \sum_{n=1}^{\infty} \chi_D(n)a(n)n^{-s}$. Goldfeld [Go] conjectured that

$$\sum_{|D|<X} \mathrm{Ord}_{s=1} L(s, E_D) \sim \frac{1}{2} \sum_{|D|<X} 1.$$

A weaker version of this conjecture is that for $r = 0$ or 1,

$$\sharp\{|D| < X | \ \mathrm{Ord}_{s=1} L(s, E_D) = r\} \gg X,$$

i.e, that $\mathrm{Ord}_{s=1} L(s, E_D) = r$ for a positive proportion of D.

In [V99], Vatsal proved that if $E/\mathbb{Q}$ is a semi-stable elliptic curve with a $\mathbb{Q}$-rational point of order 3 and good reduction at 3, then for a positive proportion of D, $\mathrm{Ord}_{s=1} L(E_D, s) = 0$. But for the case $r = 1$, less is known. In [B-J-K], it is proved that if $E_0/\mathbb{Q}$ is an optimal elliptic curve of square-free conductor N satisfying the following two conditions;

(i) $N = pq$, where p, q are different primes such that $\omega_p = -1$, $\omega_q = 1$ and $p \neq 3$, $q \equiv -1$ (mod 9),
(ii) there is an elliptic curve E, isogenous over $\mathbb{Q}$ to E_0 and having a $\mathbb{Q}$-rational 3-torsion point,

then $\mathrm{Ord}_{s=1}L(s, E_{0D}) = 1$, for a positive proportion of fundamental discriminants D. And using a variant of the binary Goldbach problem for polynomials, we proved that there are infinitely many elliptic curves satisfying the conditions. Using Theorem 3.2.2, we will prove the following theorem.

Main Theorem 1 *Let $E/\mathbb{Q}$ be an elliptic curve of square-free conductor N with a rational point of order $3 \nmid N$. If there is only one prime $p|N$ such that $\omega_p = -1$, then*

$$\sharp\{|D| < X|\ \mathrm{Ord}_{s=1}L(s, E_D) = 1\} \gg X.$$

Examples. The elliptic curves satisfying the condition in Theorem **??** whose conductor is less than 100 are following; **14A1, 14A2, 14A4, 14A6, 19A1, 19A3, 26A1, 26A3, 35A1, 35A3, 37B1, 37B3, 38A1, 38A3, 77B1, 77B3** in [CreT]. This list includes Vatsal's example **19A1** in [V98] and Byeon's example **37B1** in [B04].

3.4 Proof of Main Theorem 1

A Dedekind eta-product $g_{\mathbf{r}} = \prod_{d|N} \eta_d^{r_d}$ is said to be *l-power like* if $\widetilde{g_{\mathbf{r}}} := \prod_{d|N} d^{r_d}$ is the l^{th}-power of a rational number.

Proposition 3.4.1. *Let $E/\mathbb{Q}$ be an elliptic curve of square-free conductor N with a rational point of odd prime order $l \nmid N$ and E_0 be the optimal elliptic curve, isogenous over $\mathbb{Q}$ to E. Let P be the rational point of order l in Theorem 3.2.1. Then the Dedekind eta-product $g_{\mathbf{r}}$ corresponding to $\pi^*(P)$ is not l-power like if and only if there is only one prime p such that $w_p = -1$.*

Proof: Let $N = p_1 \cdots p_s q_1 \cdots q_t$ for primes p_i, q_j $(i = 1, \cdots, s, j = 1, \cdots, t)$ with Atkin-Lehner involution sign $w_{p_i} = -1, w_{q_j} = 1$. Let $G = q_1 \cdots q_t$. We have proven $s \geq 1$ in the previous section. The g_{r} corresponding to $\pi^*(P)$ is given by [Du]

$$g_{\mathbf{r}} := (\prod_{g|G} \prod_{d|(N/G)} \eta_{dg}^{w_d \mu(g) g})^{24/h},$$

where $h := (r, 24)$, $r := \prod_{q_j}(q_j^2 - 1) \prod_{p_i}(p_i - 1)$, and μ is the Möbius function.

If $s \geq 2$, then

$$\prod_{d|p_1 \cdots p_s} dg^{w_d \mu(g) g} = \prod_{d|p_3 \cdots p_s} \left(\frac{dp_2 g}{dp_1 p_2 g} \right)^{-w_d \mu(g) g} \left(\frac{dg}{dp_1 g} \right)^{w_d \mu(g) g} = 1,$$

so $\widetilde{g_{\mathbf{r}}} = (\prod_{g|q_1 \cdots q_t} \prod_{d|p_1 \cdots p_s} (dg)^{w_d \mu(g) g})^{\frac{24}{h}} = 1$ and $g_{\mathbf{r}}$ is l-power like.

If $s = 1$, then we have

$$\widetilde{g_{\mathbf{r}}} = \left(\prod_{g|\frac{N}{p_1}} \left(\frac{g}{p_1 g} \right)^{\mu(g) g} \right)^{\frac{24}{h}} = \left(\prod_{g|\frac{N}{p_1}} \left(\frac{1}{p_1} \right)^{\mu(g) g} \right)^{\frac{24}{h}} = (p^{-(1-q_1)\cdots(1-q_s)})^{\frac{24}{h}}.$$

If $l = 3$, then we know that r is always divisible by 9, in particular, by 3, so $l \nmid \frac{24}{h}$ and if $l = 5, 7$, then $l \nmid \frac{24}{h}$. Since $l \,|\, (q_j + 1)$, $\widetilde{g_{\mathrm{r}}}$ is not the l^{th}-power of a rational number and $g_{\mathbf{r}}$ is not l-power like. $\square$

In [B-J-K], it is proved that if an elliptic curve $E/\mathbb{Q}$ of conductor N satisfies the following four conditions;

(i) the sign ϵ of the functional equation of $L(s, E)$ is equal to +1,
(ii) E has a $\mathbb{Q}$-rational 3-torsion point P,
(iii) $\pi^*(P)$ is a $\mathbb{Q}$-rational cuspidal divisor of order 3 in $J_0(N)$,
(iv) the Dedekind eta-product $g_{\mathbf{r}}$ such that $\operatorname{div} g_{\mathbf{r}} = 3\pi^*(P)$ *is not 3-power like,*

then $\operatorname{Ord}_{s=1} L(s, E_D) = 1$, for a positive proportion of fundamental discriminants D. So from Theorem 3.2.1, Theorem 3.2.2, and Proposition 3.4.1, we have the following proposition.

Proposition 3.4.2. *Let $l = 3$. Let $E/\mathbb{Q}$ and $E_0/\mathbb{Q}$ be as in Proposition 3.4.1. If there is only one prime $p \mid N$ such that $\omega_p = -1$, then*

$$\sharp\{|D| < X| \ \mathrm{Ord}_{s=1} L(s, E_{0D}) = 1\} \gg X.$$

Proof of Main Theorem 1 :

Let $E/\mathbb{Q}$ be an elliptic curve of square-free conductor N with a rational point of order $3 \nmid N$. Suppose that there is only one prime $p|N$ such that $\omega_p = -1$. Let E_0 be the optimal elliptic curve which is isogenous over $\mathbb{Q}$ to E. Then by Proposition 3.4.2, we have that

$$\sharp\{|D| < X| \ \mathrm{Ord}_{s=1} L(s, E_{0D}) = 1\} \gg X.$$

Since the two elliptic curves E and E_0 are in the same isogeny class,

$$L(E, s) = L(E_0, s) = \sum_{n=1}^{\infty} a(n) n^{-s}.$$

So if D is coprime to the conductor of E, then

$$L(E_D, s) = L(E_{0D}, s) = \sum_{n=1}^{\infty} \chi_D(n) a(n) n^{-s}.$$

Thus we also have that

$$\sharp\{|D| < X| \ \mathrm{Ord}_{s=1} L(s, E_D) = 1\} \gg X,$$

and this completes the proof.

Chapter 4

Optimal curves differing by a 3-isogeny

Stein and Watkins [SW] conjectured that for a certain family of elliptic curves E, the $X_0(N)$-optimal curve and the $X_1(N)$-optimal curve of the isogeny class $\mathcal{C}$ containing E of conductor N differ by a 3-isogeny. In this chapter, we prove that this conjecture is true.

4.1 A 3-Isogenous class over rational field

Let E be an elliptic curve and C be a cyclic subgroup consisting of rational points. Then a quotient map $E \to E/C$ defines an isogeny over $\mathbb{Q}$. More precisely, choose $\tau \in \mathcal{H}$ such that $\tau \in Y_0(N)$ is an enhanced elliptic curve (E, C), where $N = |C|$. Then E/C is an elliptic curve defined by $\tau' = N\tau$, i.e. $E/C = \mathbb{C}/\Lambda_{\tau'}$. Hadano [H] parametrizes the isogeny classes.

Theorem 4.1.1 (Hadano)**.** *Let E, E' be elliptic curves over $\mathbb{Q}$ and $E \to E'$ be a 3-isogeny over $\mathbb{Q}$, whose kernel consists of rational points. E' has a rational point of order 3 if and only if E has a Weierstrass equation of form $y^2 + axy + t^3y = x^3$. In the case, E' is defined by*

$$y^2 + (a + 6t)xy + t(a^2 + 3at + 9t^2)y = x^3.$$

Assume $b = t^3$, i.e. E' has a rational cyclic subgroup C' of order 3.

From Euler's case for Fermat's last theorem and an equation $(a+6t)^3 - (a-3t)^3 = 27t(a^2+3at+9t^2)$, we know that $t(a^2+3at+9t^2)$ cannot be a cube and E'/C' has no rational point of order 3, except when $a = -6, t = 1$. Note that if $a = -6t$ and $t \neq 1$, then we may take $x = t^2X, y = t^3Y$ and $E : Y^2 - 6XY + Y = X^3$. Thus, a 3-isogeny class is one of three cases :

1. $E \to E'$, where E' has no rational torsion point of order 3, or
2. $E \to E' \to E''$,
3. $a = -6$, $E =$ **27a4** : $y^2 - 6xy + y = x^3$, and

$$\textbf{27a4} \to \textbf{27a3} \to \textbf{27a1} \to \textbf{27a2}$$

where all $\to$ is an isogeny with kernel consisting of rational porints of order 3 and $O = \infty$.

Assume N is not divisible by 3^2. In the case 1, E is the optimal curve up to 3-isogenies and is also $X_1(N)$-optimal. Case 2 is more complicate. E is $X_1(N)$-optimal, but need not be optimal.

Examples

1. Let $E =$ **26a3** : $y^2+xy+y = x^3$. Then $E' =$ **26a1** : $y^2+7xy+13y = x^3$ is optimal.
2. Let $E =$ **2170c1** : $y^2+13xy+y = x^3$. E is optimal, and the isogenous curves are $E' =$ **2170c3** and $E'' =$ **2170c2**.
3. $E =$ **182b1** : $y^2 - 5xy + 8y = x^3$ is optimal, where $E' =$ **182b2** and $E'' =$ **182b3**.

Example 1 is an isogeny class in which X_0-optimal curve differ from X_1-optimal curve. A conjecture in [SW] suggests a criterion to determine whether two kinds of optimal curves differ or not.

Conjecture 1. *For $i = 0, 1$, let E_i be the $X_i(N)$-optimal curve of an isongeny class $\mathcal{C}$ of elliptic curves defined over $\mathbb{Q}$ of conductor N. Then the following statements are equivalent.*

(A) There is an elliptic curve $E \in \mathcal{C}$ given by $E : y^2 + axy + y = x^3$ with discriminant $a^3 - 27 = (a-3)(a^2+3a+9)$, where a is an integer such that no prime facotrs of $a-3$ are congruent to $1 \pmod 6$ and a^2+3a+9 is a power of a prime number.

(B) E_0 and E_1 differ by a 3-isogeny.

Using Dummigan's construction and Mazur's result ; theorem **I** and **III** [Mz], we have the following theorem.

Main Theorem 2. *Let (A) and (B) be as in the Conjecture 1.*

*(i) (A) implies (B), except one case : $\mathcal{C} =$ **27a**.*

(ii) If N is square-free and $3 \nmid N$, then (B) implies (A).

4.2 Proof of Main Theorem 2

We need following two theorems, one from [V05] and another from [Ed][Appendix, Mz], to prove Main Theorem 2.

Theorem 4.2.1 (Vatsal)**.** *Suppose that the isogeny class $\mathcal{C}$ consists of semistable curves. The étale isogeny $\pi : E_{\min} \to E_1$ has degree a power of two.*

Theorem 4.2.2 (Mazur and Rapoport)**.** *Let $N = Mp = pq_1 \cdots q_s$ be a positive square-free integer, where $p \geq 5$ and q_i's are different prime integers. Then the order of $(0) - (\infty)$ in $\Phi_{Mp,p}$ is*

$$\frac{p-1}{\alpha} \prod_{i=1}^{s} (q_i + 1),$$

where $\alpha = 2, 4, 6,$ or 12.

Moreover, we prove two lemmas.

Lemma 4.2.3. *Let E be an elliptic curve given by $E : y^2 + axy + by = x^3$, where a, b are integers such that $(a, b) = 1$. Let $p \nmid 3$ be a prime number such that $p \,|\, \Delta = b^3(a^3 - 27b)$. Then we have*

(i) If $p \mid b$, then $w_p = -1$,
(ii) If $p \mid a^3 - 27b$ and $p \equiv 1 \pmod 3$, then $w_p = -1$,
(iii) If $p \mid a^3 - 27b$ and $p \equiv -1 \pmod 3$, then $w_p = 1$.

Proof: Since $c_4 := b(a^3 - 24b)$, E has multiplicative reduction at p for every prime factor p of Δ. For every prime factor p of b, E has a split multiplicative reduction at p, so $w_p = -1$. For every prime factor $p \equiv -1 \pmod 3$ of $a^3 - 27b$ has a non-split multiplicative reduction at p, so $w_p = 1$ and for every prime factor $p \equiv 1 \pmod 3$ of $a^3 - 27b$ has a split multiplicative reduction at p, so $w_p = -1$ because the slopes of the tangent lines at the node $(-a^2/9, a^3/27) \in E(\mathbb{F}_p)$ are $(-3a \pm a\sqrt{-3})/6$ when $p \neq 2$. Similarly we can show that $w_2 = 1$ if $2 | a^3 - 27b$. □

Lemma 4.2.4. *If an elliptic curve E is given by $E : y^2 + axy + y = x^3$ with discriminant $a^3 - 27 = (a-3)(a^2 + 3a + 9)$, where a is an integer such that no prime factors of $a - 3$ are congruent to 1 (mod 6) and $a^2 + 3a + 9$ is a power of a prime number, then one of the followings holds.*

- *$a = -6, -3, 0$ and $w_3 = -1$, or*
- *the conductor N of E is a square-free integer such that $3 \nmid N$.*

There is only one prime divisor p of N such that $w_p = -1$, and $w_3 = -1$ when $a = -6, -3, 0$.

Proof: $a^2 + 3a + 9$ is a power of 3 if and only if $a \in \{-6, -3, 0, 3\}$. Since $a^3 - 27 \neq 0$, $a \in \{-6, -3, 0\}$ or $3 \nmid a$. If $3 \mid N$, then E is as in the following table.

a	E	Conductor	Atkin-Lehner w_p
-6	**27a4**	$27 = 3^3$	$w_3 = -1$
-3	**54a3**	$54 = 2 \cdot 3^3$	$w_2 = 1, w_3 = -1$
0	**27a3**	$27 = 3^3$	$w_3 = -1$

If $3 \nmid N$, then $c_4 = a(a^3 - 24)$ and $\Delta = a^3 - 27$ are relatively prime so N is square-free.

Now suppose that an elliptic curve E is given by $E : y^2 + axy + y = x^3$ with discriminant $a^3 - 27 = (a-3)(a^2 + 3a + 9)$, where a is an integer such

that $3 \nmid a$, no prime factors of $a-3$ are congruent to 1 (mod 6), and a^2+3a+9 is a power of a prime number p. Then $3 \nmid a^3-27$ and for any prime divisor of N, E has multiplicative reduction. So the conductor N of E is a square-free integer such that $3 \nmid N$. Suppose that $a^2+3a+9 = p^k$. Then k should be odd except when $a = 5$ and $p = 7$. So $p \equiv 1$ (mod3). By Lemma 4.2.3, $w_p = -1$ and $w_q = 1$ for every $q|a-3$. □

Now we prove Main Theorem 2.

Proof of Main Theorem 2 :

(i) Let $E \in \mathcal{C}$ be an elliptic curve given by

$$E : y^2 + axy + y = x^3$$

with discriminant $\Delta = a^3-27 = (a-3)(a^2+3a+9)$, where a is an integer such that no prime factors of $a-3$ are congruent to 1 (mod 6) and $a^2+3a+9 = p^r$ is a power of a prime integer p. If E has a rational point Q of order 6 and $[2]Q = (0,0)$, then E is given by

$$y^2 + 2(a+b)xy + 2ab^2y = x^3$$

with $a, b \in \mathbb{Z}$. This implies $2ab^2 = 1$, a contradiction. Thus

$$T = \{(0,0), (0,-1), \infty\}$$

is the torsion group of $E(\mathbb{Q})$.

By Theorem 4.1.1, the quotient curve E' of E by T has a rational point of order 3 and the equation of E' is given by

$$E' : y^2 + (a+6)xy + (a^2+3a+9)y = x^3.$$

The discriminant of Δ' of E' is $\Delta' = (a^3-27)^3$ and $T' = \{(0,0), (0,-(a^2+3a+9), \infty\}$ is the torsion group of order 3 in $E'(\mathbb{Q})$. Since E' also has a rational point of order 3, we have the following étale 3-isogenies of elliptic curves

$$E \longrightarrow E' \longrightarrow E''.$$

Assume $a \neq -6, -3, 0$. Since $(a+6)^3-(a-3)^3 = 3^3(a^2+3a+9)$, (a^2+3a+9) cannot be a cube and E'' has no rational point of order 3. So the isogeny class $\mathcal{C}$ of E is

$$E \xrightarrow{3} E' \xrightarrow{3} E'',$$

where the horizontal arrow denotes an étale 3-isogeny. Thus E is $E_{\min}$ in $\mathcal{C}$.

By Theorem 4.2.1, E is E_1 in $\mathcal{C}$. By Theorem 3.2.1, E'' cannot be E_0 in $\mathcal{C}$. To prove (i), it is enough to show that E cannot be E_0 in $\mathcal{C}$. Suppose that E is E_0 in $\mathcal{C}$. Let $\phi : X_0(N) \to E$ be the modular parametrization and $\psi : J_0(N) \to E$ be the induced homomorphism. Then the dual $\hat{\psi} : E \to J_0(N)$ is injective. Let $E(\mathbb{Q}_p)/E_{ns}(\mathbb{Q}_p)$, where $E_{ns}(\mathbb{Q}_p)$ be the subgroup of points which have nonsingular reduction modulo p, and $\Phi_{N,p}$ be the component groups of E and $J_0(N)$ respectively. Let $\lambda : E(\mathbb{Q}) \to E(\mathbb{Q}_p)/E_{ns}(\mathbb{Q}_p)$ and $\lambda' : J_0(N)(\mathbb{Q}) \to \Phi_{N,p}$ be their canonical reduction maps. Then we have the following commutative diagram.

$$\begin{array}{ccc} & \overset{\lambda}{\rightarrow} & \\ E(\mathbb{Q})_{\text{tors}} & & E(\mathbb{Q}_p)/E_{ns}(\mathbb{Q}_p) \\ \downarrow \hat{\psi} & & \downarrow \hat{\psi}' \\ & \overset{\lambda'}{\rightarrow} & \\ J_0(N)(\mathbb{Q})_{\text{tors}} & & \Phi_{N,p}, \end{array} \tag{4.1}$$

where $\hat{\psi}'$ is the injective homomorphism induced by $\hat{\psi}$.

By Lemma 4.2.4, the conductor N of E is a square-free integer such that $3 \nmid N$ and there is only one prime divisor p of N such that $w_p = -1$. Write $N = Mp$, where $M = q_1 \cdots q_s$ and q_i are different primes. Then $q_i | a-3$ and $q_i \equiv 2 \pmod 3$ for all $i = 1, \cdots, s$.

By Theorem 3.2.1, if E is E_0 in $\mathcal{C}$, then E has the point P of order 3 such that

$$\hat{\psi}(P) = \frac{2(p-1)}{3h} \prod_{i=1}^{s} (q_i^2 - 1)[(P_M) - (P_N)]$$

in $J_0(N)$, where $h = (r, 24)$ and $r = (p-1)\prod_{i=1}^{s}(q_i^2-1)(p-1)$. We note that $3|h$. Since $P_M \in C_0$ and $P_N \in C_1$, $\lambda'((P_M) - (P_N)) = (0) - (\infty)$.

Theorem 4.2.2 and $3 \nmid \prod_{i=1}^{s}(q_i - 1)$ imply that

$$\lambda'(\hat{\psi}(P)) = \frac{2(p-1)}{3h} \prod_{i=1}^{s}(q_i + 1) \prod_{i=1}^{s}(q_i - 1)[(0) - (\infty)]$$

is not trivial in $\Phi_{N,p}$. So $P \in E$ should have singular reduction mod p. But the points $(0, 0)$ and $(0, -1)$ in E have nonsingular reduction mod p. Thus E cannot be E_0 in $\mathcal{C}$.

Thus we have $E = E_1$ and $E' = E_0$ if $a \neq -6, -3, 0$. If $a = -3$, then $E_1 = E$ and $E_0 =$ **54a1**. If $a = 0$ or -6, then $\mathcal{C} =$ **27a**. It completes the proof of (i).

(ii) Suppose that E_0 and E_1 differ by a 3-isogeny and the conductor N of these curves is a square-free integer such that $3 \nmid N$. By Theorem 4.2.1, there is an etále 3-isogeny from E_1 to E_0. So E_1 has a rational point of order 3 and as a minimal model for E_1, we can take

$$E_1 : y^2 + axy + by = x^3$$

with $a, b \in \mathbb{Z}$, $b > 0$. The discriminant of Δ_1 of E_1 is

$$\Delta_1 = b^3(a^3 - 27b)$$

and $T_1 = \{(0, 0), (0, -b), \infty\}$ is the torsion group of order 3 in $E_1(\mathbb{Q})$.

By Theorem 3.2.1, E_0 also has a rational point of order 3. By Theorem 4.1.1, b is a cubic number t^3 with $t > 0$ and E_0 is given by

$$E_0 : y^2 + (a + 6t)xy + (a^2 + 3at + 9t^2)ty = x^3.$$

The discriminant of Δ_0 of E_0 is

$$\Delta_0 = (a^2 + 3at + 9t^2)^3((a + 6t)^3 - 27(a^2 + 3at + 9t^2)t) = t^3(a^3 - 27t^3)^3$$

and $T_0 = \{(0, 0), (0, -(a^2 + 3at + 9t^2)t), \infty\}$ is the torsion group of order 3 in $E_0(\mathbb{Q})$.

Consider again the commutative diagram (4.1). Let $P = (0, 0)$ or $(0, -(a^2+$

$3at + 9t^2)t)$ be the point of order 3 in E_0 and p be a prime divisor of $a^2 + 3at + 9t^2$. Write $N = Mp_1 \cdots p_u p$ such that for every prime divisor $q|M$, $w_q = 1$ and for every prime number p_i, $w_{p_i} = -1$. We note that $w_p = -1$. By Theorem 3.2.1,

$$\begin{aligned} \hat{\psi}(P) &= \frac{2n}{3} \sum_{d|(N/M)} w_d(P_{dM}) \\ &= \frac{2n}{3} \sum_{p_{i_1} \cdots p_{i_v}|(N/Mp)} (-1)^v [(P_{p_{i_1} \cdots p_{i_v} M}) - (P_{pp_{i_1} \cdots p_{i_v} M})], \end{aligned}$$

where the number of summands is 2^u and if $u \geq 1$, for the half of them, $(-1)^v = 1$ and for the other half of them, $(-1)^v = -1$. Since $P_{p_{i_1} \cdots p_{i_v} M} \in C_0$ and $P_{pp_{i_1} \cdots p_{i_v} M} \in C_1$ for any $p_{i_1} \cdots p_{i_v}$, we have

$$\lambda'((P_{p_{i_1} \cdots p_{i_v} M}) - (P_{pp_{i_1} \cdots p_{i_v} M})) = (0) - (\infty)$$

for any $p_{i_1} \cdots p_{i_v}$. Thus $\lambda'(\hat{\psi}(P))$ is trivial in $\Phi_{N,p}$ if $u \geq 1$. Since the point P in E_0 has singular reduction modulo p, $\lambda'(\hat{\psi}(P))$ is non-trivial in $\Phi_{N,p}$. So the prime number p is the only one prime number such that $w_p = -1$.

By Lemma 4.2.3, the elliptic curve E_1 in $\mathcal{C}$ should be given by $E_1 : y^2 + axy + y = x^3$ with discriminant $a^3 - 27 = (a-3)(a^2 + 3a + 9)$, where a is an integer such that no prime factors of $a - 3$ are congruent to 1 (mod 6) and $a^2 + 3a + 9$ is a power of the prime number p. So we complete the proof of (ii).

□

Example. Consider the elliptic curve $E : y^2 - 20xy + y^2 = x^3$ (**8027a3** in Cremona's table) of conductor $8027 = 23 \cdot 349$ and the quotient curve $E' : y^2 - 14xy + 349y = x^3$ (**8027a1** in Cremona's table) by $T = \{(0,0), (0,-1), \infty\}$. By Main Theorem 2 and its proof, we know that $E_0 = E'$, $E_1 = E$ and they differ by a 3-isogeny. Watkins [Wa] checked this example in another way.

4.3 Application

Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve and f be an associated newform. For f, we have a differential 1-form where ω_f. In other hand, we can define a differential 1-form

$$\omega_E = \frac{dx}{2y + a_1x + a_3},$$

which is called *Néron differential* of E. A modular parametrization $\phi : X_0(N) \to E$ give a 1-form on $X_0(N)$, by push-forward ; $\phi_*(\omega_E)$.

Now we have two 1-forms on $X_0(N)$. They have integer ratio

$$c_E = \frac{\omega_f}{\phi_*(\omega_E)},$$

which is called *Manin constant*. Note that c depends, in fact, on ϕ. If ϕ is replaced by $[n] \circ \phi$, then new c_E is a multiple by n of original one. We will denote c_E is to be minimum among possible choice.

Let (E, C) a pairs of an elliptic curves and cyclic subgroup of order l. Further, assume that C consists of $\mathbb{Q}$-rational points. For an isogeny

$$\theta \ : \ E \longrightarrow E/C,$$

1. if E is $X_0(N)$-optimal, we have two modular maps

$$\phi : X_0(N) \to E \text{ and } \theta \circ \phi : X_0(N) \to E/C.$$

2. if E/C is $X_0(N)$-optimal, as above, we have

$$\phi : X_0(N) \to E/C \text{ and } \theta^* \circ \phi : X_0(N) \to E/C$$

where θ^* is the dual of θ.

Proposition 4.3.1. *If E is as in (A) of conjecture 1, then $c_{E/C} = 3c_E$ or $9c_E$.*

Chapter 5

A conjecture of Gross and Zagier

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, c the Manin constant of E, and m the product of Tamagawa numbers of E at prmie divisors of N. Let K be an imaginary quadratic field, where all prime divisors of N split in K. Gross and Zagier [G-Z] conjectured that if $E(K)$ has rank 1, then the integer

$$c \cdot m \cdot |Ш(E/K)^{\frac{1}{2}}|$$

is divisible by $|E(\mathbb{Q})|_{tor}|$. In this chapter, we show that this conjecture is true if $E(\mathbb{Q})_{tor}$ has a point of odd order.

5.1 Heegner points

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and $\phi : X_0(N) \to E$ be a modular map. Let K be an imaginary quadratic field with fundamental discriminant D_K, where all prime divisors of N split and $\mathfrak{a}$ be an ideal of the ring of integers O_K.

Definition 5.1.1. *A* Heegner point $(O_K, \mathfrak{n}, [\mathfrak{a}])$ *denotes a point on* $X_0(N)$ *with coordinates* $j(\mathfrak{a}), j(\mathfrak{n}^\tau\mathfrak{a})$*, where* τ *is the complex conjugation and* $(N) = \mathfrak{n}^\tau\mathfrak{n}$ *is a decomposition of* N *in* K*.*

Let

$$P_E^*(D_K,1,1) := \sum_{[\mathfrak{a}} \phi((O_K,\mathfrak{n},[\mathfrak{a}])) - \sum_{[\mathfrak{a}]} \phi((O_K,\mathfrak{n},[\mathfrak{a}])^\tau),$$

where $[\mathfrak{a}]$ runs through the ideal class group of K. Following Birch, Stephens [B-S], and Gross [Gr], we have $P_E^*(D_K,1,1) \in E(K)$. Kolyvagin [Ko] proves that if $P_E^*(D_K,1,1)$ has infinite order, then $E(K)$ has rank 1 and the Shafarevich-Tate group $Ш(E/K)$ of E is a finite group.

Let E be an elliptic curve of conductor N and $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field in which all prime divisors p of N split. Let O_K be the ring of integers of K and $\mathfrak{a}$ be an ideal of O_K. Such K is said to be satisfying *Heegner condition.*

Definition 5.1.2 (A Heegner point on an elliptic curve)**.** *Let P_K be a point on $X_0(N)$ with coordinates $j(\mathfrak{a}), j(\mathfrak{n}^\tau\mathfrak{a})$, where $(N) = \mathfrak{n}\mathfrak{n}^\tau$ and $\mathfrak{n}^\tau$ denotes the complex conjugation. P_K is called a* Heegner point.

Note that P_K depends on the choice of $K, \mathfrak{a}$, and the factorization $(N) = \mathfrak{n}\mathfrak{n}^\tau$. Thus we denote such P_K by $(O_K,\mathfrak{n},[\mathfrak{a}])$, where $[\mathfrak{a}]$ denotes the ideal class in the class group $Cl(K)$ of K containing $\mathfrak{a}$.

Let

$$P_E^*(D_K,1,1) := \sum_{[\mathfrak{a}]\in Cl(K)} \phi((O_K,\mathfrak{n},[\mathfrak{a}])) - \sum \phi((O_K,\mathfrak{n},[\mathfrak{a}])^\tau).$$

By Birch and Stephens [B-S] and Gross [Gr] $P_E^*(D_K,1,1) \in E(K)$, and Kolyvagin [Ko] proves that if $P_E^*(D_K,1,1)$ has infinite order, then $E(K)$ has rank 1 and the Shafarevich-Tate group $Ш(E/K)$ of E over K is finite.

Conjecture 5.1.3. *Assume that $D \neq -3,-4$. If $P_E^*(D_K,1,1)$ has infinite order, then*

$$|Ш(E/K)| = \left(\frac{|E(K) : \mathbb{Z}P_E^*(D_K,1,1)|}{c_E \cdot m_E}\right)^2,$$

where c_E is the Manin constant of E and m_E is the product of tamagawa numbers of E.

In particular, we expect the following weak conjecture.

Conjecture 5.1.4. *Assume that $D \neq -3, -4$. If $P_E^*(D_K, 1, 1)$ has infinite order, then*

$$|E_{tor}(\mathbb{Q})| \mid c_E \cdot m_E \cdot |Ш(E/K)|^{1/2}.$$

In this chapter, we prove the following theorem.

Main Theorem 3. *Conjecture 5.1.4 is true if $E(\mathbb{Q})_{\text{tor}}$ contains a point of odd order.*

5.2 Selmer groups and Shafarevich-Tate groups

Let $\theta : E \to E'$ be an isogeny with $T = \ker \theta$. There are exact sequences

$$0 \longrightarrow T \longrightarrow E \longrightarrow E' \longrightarrow 0$$

and

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E'(F)/\theta(E(F)) & \longrightarrow & H^1(G_F, T) & \xrightarrow{\beta_\theta} & H^1(G_F, E)[\theta] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \alpha_\theta} & & \\ 0 & \longrightarrow & \prod E'(F_p)/\theta(E(F_p)) & \longrightarrow & \prod H^1(G_p, T) & \longrightarrow & \prod H^1(G_p, E)[\theta] & \longrightarrow & 0 \end{array}$$

where

- F is a number field where E, E', and θ are defined,
- p denotes any place of F,
- G_p is a decomposition group of the prime p of K,
- $\alpha : H^1(G_F, E) \to \prod H^1(G_p, E)$ is the restriction map,
- F_p is the completion of F at p, and
- all products runs through all primes of K.

Definition 5.2.1 (Selmer group and Shafarevich-Tate group)**.** *From above diagram, we define two following groups ;*

1. *θ-Selmer group $S^{(\theta)}(E/F) := \ker(\alpha_\theta) \circ \beta_\theta$ of E over F and*
2. *Shafarevich-Tate group $Ш(E/F) := \ker \alpha$ of E over F.*

There is a short exact sequence

$$0 \to E'(F)/\theta(E(F)) \to S^{(\theta)}(E/F) \to Ш(E/F)[\theta] \to 0$$

where $Ш(E/F)[\theta] = \ker(Ш(E/F) \xrightarrow{\theta} Ш(E'/F))$. In particular,

$$|Ш(E/F)[\theta]| = \frac{|S^{(\theta)}(E/F)|}{|E'(F)/\theta(E(F))|}.$$

Therefore, if we know $S^{(\theta)}(E/F)$, then $Ш(E/F)[\theta]$ is controlled by a Mordell-Weil group $E'(F)/\theta(E(F))$. In general, it is not easy to understand whole $S^{(\theta)}(E/F)$. In our situation, however, the isogeny θ, defined over $\mathbb{Q}$, has a nice property to construct a subgroup $S^{(\theta)}(E/\mathbb{Q})$.

5.2.1 Galois cohomology and field extensions

Let $\xi \in H^1(G_F, E[\theta])$. ξ defines two extensions of F.

Proposition 5.2.2. *$\ker \xi$ is well defined. For each $P \in E[\theta]$, $\xi^{-1}(P)$ is a right coset of $\ker \xi$.*

Proof: Let $G_L := \{\sigma \in G_F \mid \xi_\sigma = 0 \in E[\theta]\}$. It is easy to check that G_L is a subgroup of G_F.

Suppose $\sigma, \tau \in G_F$ and $\xi_\sigma = \xi_\tau = P$ for some $P \in E$. Then we are enough to show that $\sigma\tau^{-1} \in G_L$, i.e.

$$\begin{aligned} \xi_{\sigma\tau^{-1}} &= (\xi_\sigma)^{\tau^{-1}} + \xi_{\tau^{-1}} \\ &= (\xi_\tau)^{\tau^{-1}} + \xi_{\tau^{-1}} \quad = \xi_{id} = 0 \end{aligned}$$

Therefore $(G_L)\sigma = (G_L)\tau$. □

In general, G_L is not a normal subgroup of G_F. In particular, L/F is not Galois. Let $A = \{\xi_\sigma \in E[\theta] \mid \sigma \in G_F\}$ and $G_M := \{\tau \in G_F \mid P^\tau = P \text{ for all } P \in A\}$. Then M/F is a Galois extension.

Proposition 5.2.3. *LM is a Galois extension of F.*

Proof: We are enough to prove that $G_{LM} = G_L \cap G_M$ is a normal subgroup of G_F. We can easily check that

$$\xi_{\tau\sigma\tau^{-1}} = \xi_\tau^{\sigma\tau^{-1}} + \xi_\sigma^\tau + \xi_\tau = \xi_\tau^{\tau^{-1}} + \xi_\tau = 0$$

and

$$\theta(P^{\tau\sigma\tau^{-1}}) = \theta^{\tau\sigma\tau^{-1}}(P^{\tau\sigma\tau^{-1}}) = (\theta(P))^{\tau\sigma\tau^{-1}} = 0.$$

The second equality holds because θ is defined over F. Therefore, $\tau\sigma\tau^{-1} \in G_{LM}$ for all $\sigma \in G_{LM}$ and $\tau \in G_F$. □

Assume that A consists of three F-rational points. Then we have $M = F$ and L/F is a Galois cubic extension induced by ξ.

In other words, every nontrivial $\xi \in S^{(3)}(E/F)$ is related to some Galois cubic extension L/F.

5.2.2 A subgroup of $S^{(l)}(E/F)$

Let F be a number field and $\mathfrak{q}$ be a place of F. Let E be an elliptic curve with F-rational point of odd prime order l. $\kappa_\mathfrak{q}$ denotes the residue field of F at $\mathfrak{q}$. By [Sil1], $S^{(l)}(E/F) \subset H^1(G_F, E[l]; S)$ where S is a set of primes dividing lN where N is the conductor of E. In particular, we may choose a Galois $\mathbb{Z}/l\mathbb{Z}$-extension L/K unramified outside N. For such L, we have natural projection $[\ ] : G \to \mathbb{Z}/l \cong \mathrm{Gal}(L/K)$. Define a 1-cocyle $\xi^L : \sigma \mapsto [\sigma]Q$ in $H^1(G, E)[\theta]$ where $Q \in \ker\theta$ is a rational torsion point of order l. By definition, $\xi^L \neq 0$ in $H^1(G_K, E[l])$.

Lemma 5.2.4. *Suppose that every nonzero F-rational points of E is non-singular in any reduction. Then $\xi^L \in S^{(l)}(E/F)$.*

Proof: Let $\mathfrak{q}$ be a prime of F and $L_\mathfrak{q} = F_\mathfrak{q}(L)$ be an extension of $F_\mathfrak{q}$. Let $\lambda_\mathfrak{q}$ be the residue field of $L_\mathfrak{q}$. $\tilde{E}$ and $\tilde{E}'$ are the modulo $\mathfrak{q}$ reduction image of

E and E', respectively. Now $L_\mathfrak{q}/K_\mathfrak{q}$ is one of three extensions ; $L_\mathfrak{q} = K_\mathfrak{q}$, $L_\mathfrak{q}$ is a unramified extension of degree l, or $L_\mathfrak{q}$ is a ramified extension of degree l. Each cases can be written as ; $L \subset K_\mathfrak{q}$, $\mathfrak{q}$ inerts in L, or $\mathfrak{q}$ ramifies in L, respectively.

Suppose that $L_\mathfrak{q} = F_\mathfrak{q}$, i.e. $\mathfrak{q}$ completely splits in L. Then $\mathrm{G}_\mathfrak{q} \subset \mathrm{Gal}(\overline{\mathbb{Q}}/L)$ and $\xi^L|_\mathfrak{q} = 0$, which is a coboundary determined by $O \in E'(F_\mathfrak{q})$.

Suppose that $L_\mathfrak{q} \neq F_\mathfrak{q}$ and $[\lambda_\mathfrak{q} : \kappa_\mathfrak{q}] = l$, i.e $\mathfrak{q}$ inerts in L. Then θ induces a morphism $\mathcal{E} \to \mathcal{E}'$, where $\mathbb{Z}$-schems $\mathcal{E}$ and $\mathcal{E}'$ are Néron Models for E and E', and consequently, θ induces a morphism on the identity component of the special fibres

$$\tilde{\theta} \ : \ \tilde{E}_{ns}(\kappa_\mathfrak{q}) \to \tilde{E'}_{ns}(\kappa_\mathfrak{q})$$

whose kernel contains $\tilde{Q}$. Note that $\tilde{Q}$ is nonsingular under condition C. Since $|\tilde{E}(\kappa_\mathfrak{q})| = |\tilde{E'}(\kappa_\mathfrak{q})|$, there is a point $R \in E(\overline{F}_\mathfrak{q})$ such that $\tilde{R} \in \tilde{E}_{ns}(\overline{\kappa}_\mathfrak{q}) \backslash \tilde{E}_{ns}(\kappa_\mathfrak{q})$ and $\tilde{\theta}(\tilde{R}) \in \tilde{E'}(\kappa_\mathfrak{q})$. Since $\theta : E \to E'$ is defined over $\mathbb{Q}$, $R \in E(\overline{F}_\mathfrak{q}) \backslash E(F_\mathfrak{q})$ has at most l conjugations $R, R+Q, \cdots, R+[l-1]Q$, under the action of $\mathrm{Gal}(\overline{F}_\mathfrak{q}/F_\mathfrak{q})$. Since $\tilde{R} \in \tilde{E}(\kappa_\mathfrak{q})$, R has l conjugations, i.e. $R \in E(L_\mathfrak{q}) \backslash E(F_\mathfrak{q})$, where $L_\mathfrak{q}$ is the unique unramified extension of $F_\mathfrak{q}$ of degree l. Now

$$\xi^L|_\mathfrak{q} = c(\sigma \mapsto R^\sigma - R),$$

where the sign $c \in (\mathbb{Z}/l\mathbb{Z})^*$ is determined by the choice of $R \in E(\overline{F}_\mathfrak{q})$.

Suppose that $L_\mathfrak{q}$ is a totally ramified extension. Then $[L_\mathfrak{q} : F_\mathfrak{q}] = l$ and $\lambda_\mathfrak{q} = \kappa_\mathfrak{q}$, i.e. $\mathfrak{q}$ ramifies in L. By the condition (i), E has splitting multiplicative reduction at $\mathfrak{q}$ and $|E(L_\mathfrak{q})/E_{ns}(\lambda_\mathfrak{q})| = l\,|E(F_\mathfrak{q})/E_{ns}(\kappa_\mathfrak{q})|$(see [Corollary 15.2.1 [Sil1]]), where $E_{ns}(\kappa_\mathfrak{q}) \subset E(F_\mathfrak{q})$ and $E_{ns}(\lambda_\mathfrak{q}) \subset E(L_\mathfrak{q})$ are the inverse images of $\tilde{E}_{ns}(\lambda_\mathfrak{q})$ in $E(F_\mathfrak{q})$ and $E(L_\mathfrak{q})$, respectively. Therefore there is a component $\{R\} = R + E_{ns}(\lambda_\mathfrak{q}) \in E(L_\mathfrak{q})/E_{ns}(\lambda_\mathfrak{q})$ such that

$$[c]\{R\} \notin E(F_\mathfrak{q})/E_{ns}(\kappa_\mathfrak{q}),\ 1 \leq c \leq l-1 \ \text{ and } \ [l]\{R\} \in E(F_\mathfrak{q})/E_{ns}(\kappa_\mathfrak{q}).$$

If E has the minimal discriminant $\Delta = I^l J$, where I is a product of places at which Q is a singular point in the reduction and J is a product of places at which Q is nonsingular in the reduction. Then $E' = E/ < Q >$ has the

minimal discriminant $\Delta' = IJ^l$. Since $E'(F_\mathfrak{q})/E'_{ns}(\kappa_\mathfrak{q})$ is a cyclic group of order l $|E(F_\mathfrak{q})/E^0(\kappa_\mathfrak{q})|$, the image of $E(L_\mathfrak{q})/E_{ns}(\lambda_\mathfrak{q})$ under a map induced from $E \to E'$ is in $E'(F_\mathfrak{q})/E'_{ns}(\kappa_\mathfrak{q})$ so there is a point $R' \in \{R\}$ whose image under the map $E \to E'$ is in $E'(F_\mathfrak{q})$. Therefore every conjugate of R' is $R' + [c]Q$ for $0 \le c \le l-1$ and we have

$$\xi^L|_\mathfrak{q} = c(\sigma \mapsto R'^\sigma - R'),$$

where $c \in (\mathbb{Z}/l\mathbb{Z})^*$ depends on the choice of $\{R\}$ and R'.

Therefore ξ^L is locally 0 at any prime so $\xi \in S^{(\theta)}(E/F) \subset S^{(l)}(E/F)$. □

If $F = \mathbb{Q}$ or K and $l = 3$, we can calculate $S^{(3)}(E/F)$ more explicitly. θ implies a short exact sequence of G_F-modules

$$0 \to T \to E[3] \xrightarrow{\theta} \mu_3 \to 0 \tag{5.1}$$

where $T = \ker\theta = \{O, Q, 2Q\}$. Then we have a Galois cohomology sequence

$$0 \to H^1(G_F, T) \to H^1(G_F, E[3]) \xrightarrow{\theta} H^1(G_F, \mu_3).$$

Theorem 5.2.5. *If the exact sequence* (5.1) *does not split,* $S^{(3)}(E/F) = S^{(\theta)}(E/F)$. *In particular, if* $F = \mathbb{Q}$ *or* K *then we have same result.*

Proof: Let $\xi \in S^{(3)}(E/F)$. We want to show that $\theta_*(\xi) = 0$.

Let L be the field determined by $\xi^{-1}(O) \subset G_F$ and $M = F(E[3])$. By assumption, $\mathrm{Gal}(M/F) \cong S_3$. Choose any $\tau \in \mathrm{Gal}(\overline{F}/F)$ whose order in $\mathrm{Gal}(M/F)$ is 2. Let $\eta = 4\eta = \xi + \xi^\tau$. Then

$$(\xi - 2\eta) + (\xi - 2\eta)^\tau = O.$$

In particular, $\xi - 2\eta$ has image on $\{O, R, 2R\}$, where $R \in E[3]$ and $R^\tau + R = O$. Thus we will assume $\xi(G_F)$ has at most 3 points, i.e. L/F is an extension whose degree is at most 3, and

$$0 = \xi_{\tau^2} = \xi_\tau^\tau + \xi_\tau.$$

1. Assume LM/M is a cubic extension. Then LM/F is a Galois extension of degree 9 and an abelian extension. In fact,

$$\mathrm{Gal}(LM/F) \cong \mathrm{Gal}(LM/L) \times \mathrm{Gal}(LM/M) \cong \mathbb{Z}/3 \times \mathbb{Z}/3.$$

   Choose generators $\alpha \in \mathrm{Gal}(LM/L)$ and $\beta \in \mathrm{Gal}(LM/M)$ such that $\alpha(R) = R + P$ and $\xi_\beta = R$. If we need, we may replace α and β to α^2 and β^2, respectively. Note that $\mathrm{Gal}(LM/L) \cong \mathrm{Gal}(M/F)$. Then $\xi_{\beta^2} = 2R$ and $\xi_{\beta\alpha} = \xi_\beta^\alpha = R + P$. It is a contradiction.

2. Therefore we have to assume $LM = M$, i.e $L \subset M$. Since $\xi(G_F) = \{O, R, 2R\}$, $\xi_\alpha = R$ and $\xi_{\alpha^2} = 2R$ for $\alpha \in \mathrm{Gal}(M/F)$ of order 3. By definition of M, however, $\xi_{\alpha^2} = R^\alpha + R = 2R + Q$. It is a contradiction.

Therefore, $\theta_*(\xi) = 0$ and $S^{(3)}(E/F) = S^{(\theta)}(E/F)$. Note that $\mathbb{Q}$ and K satisfy the condition about G_F-module $E[3]$. □

Example 1. Let $E =$ **10621c1** and $F = \mathbb{Q}$. Since $N = 10621 = 13 \cdot 19 \cdot 43$, we can know that $S^{(3)}(E/\mathbb{Q})$ has 27 elements. Since $E(\mathbb{Q})$ has rank 0 and $E(\mathbb{Q})[3]$ has 3 elements, we conclude that $Ш(E/\mathbb{Q})[3]$ has 9 elements. BSD predicts that $Ш(E/\mathbb{Q})$ has 9 elements.

Example 2. Let $E =$ **2170c1** and $F = \mathbb{Q}$. Since $E(\mathbb{Q})$ has rank 1 and $E(\mathbb{Q})_{tor}$ has 3 points, we know that $Ш(E/\mathbb{Q})[3] = \{0\}$. BSD also predicts that $Ш(E/\mathbb{Q}) = \{0\}$.

Example 3. Let $E : y^2 + axy + y = x^3$ and $3 \nmid a$. $Ш(E/\mathbb{Q})[3]$ can be computed by Lemma 5.2.4 and Theorem 5.2.5. $Ш(E/\mathbb{Q})[3] = Ш(E/\mathbb{Q})$ for small $a \leq 61$, where $Ш(E/\mathbb{Q})$ is predicted by BSD conjecture.

5.3 Proof of Main Theorem 3

We will classfy elliptic curves up to their torsion subgroups and make a proof for the theorem case by case.

Let $T = E(\mathbb{Q})_{\text{tor}}$. As the proof for the proposition 3.2.2., we will use the order of torsions in $E(\mathbb{Q})/E_p^0$ in each p whenever we estimate the Tamagawa number m. See proposition 2.2.8. To do that, we parametrize elliptic curves for a point $(0,0)$ to be a torsion point of maximum order.

Calculating $c \cdot m$ case by case, we know that $|T|$ divides $c \cdot m$ in most cases. When $T = \mathbb{Z}/3\mathbb{Z}$, we need to estimate the order of Shafarevich-Tate group. For this reason, we observe the case $T = 3$ at the end.

Case I. $T = \mathbb{Z}/6\mathbb{Z}$

The minimal equation for E is

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

with $u, v \in \mathbb{Z}, u > 0, (u,v) = 1$ and the minimal discriminant is

$$\Delta = v^6(v+u)^3u^2(9v+u).$$

When $p \mid v(v+u)u$, then the torsion point $P = (0,0)$ is a singular point in the reduction at p. More precisely, P is of order 6 in $E(\mathbb{Q})/E_p^0$ if $p \mid v$, P is of order 3 if $p \mid v+u$, and P is of order 2 if $p \mid u$. Thus $6 \mid m_E$ except when $u = v = 1, m = 3$ and $u = 2, v = -1, m = 2$. For these two exceptions, we need to know their Manin constant.

When $u = v = 1$, then the curve is labelled by **20a2** in Cremona's table and it has the Manin constant $c = 2c_{E_0}$, where $E_0 = \mathbf{20a1}$ and c_{E_0} is the Manin constant for E_0.

When $u = 2, v = -1$, then the curve is **14a4** and it has the Manin constatn $c = 3c_{E_0}$, where $E_0 = \mathbf{14a1}$.

Thus $6 \mid c \cdot m$ if $T = \mathbb{Z}/6\mathbb{Z}$.

Case II. $T = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

E has a minimal Weierstrass equation

$$E : y^2 + (u-v)xy - uv(v+u)y = x^3 - v(v+u)x^2$$

, as same as Case I, with $u, v \in \mathbb{Z}, (u, v) = 1, 2um(5s-t) = v(t-3s)(t+3s)$ for a pair of integers $(s, t) \in \mathbb{Z}^2$ and the minimal discriminant of E is

$$\Delta = v^6(v+u)^3u^2(9v+u).$$

If one of m and n is even, then the minimal discriminant is

$$\Delta = (2s(5s-t))^6(s-t)^6(t-3s)^2(t+3s)^2(9s-t)^2.$$

In this case, there are at least two primes $p, q \mid 2s(5s-t)(s-t)$. As case I, we may observe the reduction of $(0,0)$ and conclude $36 = m_p m_q \mid m_E$.

If both of s and t are odd, then Δ is minimal outside 2.

(a) Suppose that $5s - t = 2^A$ and $s - t = 2^B$. We may assume that $s > 0$ and $A > B$. Then $s = 2^{B-2}(2^{A-B} - 1)$ and $B = 2$ ($\because$ s is supposed to be odd). If $A = B + 1$, then $3s = -t$, i.e. $s = 1$ and $t = -3$ thus $\Delta = 0$. It is a contradiction. Thus $A > B + 1$ and there is an odd prime p dividing s. Since $B = 2$, $s = t + 4$ and $t - 3s = -2(t + 6)$. Since t is also odd, there is an odd prime q dividing $t + 6$. Therefore, 12 divides $m_p m_q$ and m_E.

(b) Suppose that one of $5s - t$ and $s - t$ is not a power of 2. Thus there is an odd prime p dividing $(5s - t)(s - t)$ so $6 \mid m_p$.
If $s \neq 1$, then we choose $q \mid s$ so $6 \mid m_q$.
If $s = 1$, then

$$\Delta = 2^6(t-5)^6(t-1)^6(t-3)^2(t+3)^2(t-9)^2.$$

If both of $t-3$ and $t+3$ are powers of 2, then $t = -5, -1$ ($t \neq 1, 5$ because $\Delta \neq 0$). When $t = -5$, we may choose $p = 5, q = 3$ so that $pq \mid (5s - t)(s - t)$ and 36 divides m_E. When $t = -1$, our curve is

$$E \ : \ y^2 + 5xy - 6y = x^3 + 3x^2$$

with minimal discriminant $\Delta = 2^2 3^6 5^2$ and $12 = m_3 m_5 \mid m_E$.

Therefore, $12 \mid m_E$ in this case.

Case III. $T = \mathbb{Z}/9\mathbb{Z}$.

A Weierstrass equiation for E is

$$E : y^2 + (u^3 - v^3 + uv^2)xy - u^4v^2\tilde{b}y = x^3 - uv^2\tilde{b}x^2$$

with $u, v \in \mathbb{Z}$, $(u, v) = 1$, $\tilde{b} = (v-u)(u^2-uv+v^2)$, and the discriminant is

$$\Delta \;=\; u^9v^9(v-u)^9(u^2-uv+v^2)^3(u^3+3u^2v-6uv^2+v^3),$$

which is minimal at a prime p for all $p|uv(v-u)$. Since $\Delta \neq 0$, $|uv(v-u)| > 1$ for any possible $u, v \in \mathbb{Z}$. Thus $9 \mid t = \prod_{p|uv(v-u)} 9$ and $t \mid m$.

Case IV. $T = \mathbb{Z}/12\mathbb{Z}$

A Weierstrass equation for E is

$$E : y^2 + (u(u-v)^3 - v\tilde{c})xy - uv(u-v)^5\tilde{c}\tilde{d}y = x^3 - v(u-v)^2\tilde{c}\tilde{d}x^2$$

with $u, v \in \mathbb{Z}$, $(u, v) = 1$, $\tilde{c} = (2v-u)(u^2-3uv+3v^2)$, $\tilde{d} = (u^2-2uv+2v^2)$ and the discriminant is

$$\Delta \;=\; u^2v^{12}(u-v)^{12}(2v-u)^6\tilde{d}^3(u^2-6uv+6v^2)(u^2-3uv+3v^2)^4,$$

which is minimal at odd prime p dividing $uv(u-v)(2v-u)$. If u is odd, then Δ is also minimal at 2.

(a) If u is even, then $u = 2, v \neq 1$ or $u > 2, v(u-v) > 1$. In any case, $12 \mid t = \prod'_{p|v(u-v)} 12 \cdot \prod'_{p|u} 2 \cdot \prod'_{p|2v-u} 6$ and $t \mid m$, where the product $\prod'_p$ runs through odd primes.

(b) If u is odd, then $12 \mid t = \prod_{p|v(u-v)} 12 \cdot \prod_{p|u} 2 \cdot \prod_{p|2v-u} 6$ and $t \mid m$.

Case V. $T = \mathbb{Z}/5\mathbb{Z}$ A Weierstrass equation for E is

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

with $u, v \in \mathbb{Z}$, $(u, v) = 1$ and the discriminant is

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

Thus $5 \mid m$ unless $|uv| = 1$. If $|uv| = 1$, $E =$ **11a2** and $c = 5$.

Case VI. $T = \mathbb{Z}/10\mathbb{Z}$

A Weierstrass equation for E is

$$E : y^2 + (uS - vT)xy - u^2 v^3 STy = x^3 - uv^3 Tx^2,$$

with $u, v \in \mathbb{Z}$, $(u, v) = 1$, $S = -(v^2 - 3uv + u^2)$, $T = (v - u)(2v - u)$ and the discriminant is

$$\Delta = u^5 v^{10} (u - v)^{10} (u - 2v)^5 (u^2 - 3uv + v^2)^2 (u^2 + 2uv - 4v^2),$$

which is minimal at any odd prime p dividing $uv(u - v)(u - 2v)$. If u is odd, then Δ is minimal at all prime p dividing $uv(u - v)(u - 2v)$.

(a) If u is even, then $v(u - v) > 1$, $10 \mid t = \prod'_{p|v(u-v)} 10 \cdot \prod'_{p|u(u-2v)} 5 \cdot \prod'_{p|u^2-3uv+v^2} 2$ and $t \mid m$.

(b) If u is odd, then $10 \mid t = \prod_{p|v(u-v)} 10 \cdot \prod_{p|u(u-2v)} 5 \cdot \prod_{p|u^2-3uv+v^2} 2$ and $t \mid m$.

Case VII. $T = \mathbb{Z}/7\mathbb{Z}$

A minimal Weierstrass equation for E is

$$E : y^2 + (u^2 + uv - v^2)xy - u^3 v^2 (v - u)y = x^3 - uv^2 (v - u)x^3$$

with $u, v \in \mathbb{Z}$, $(u, v) = 1$ and the minimal discriminant is

$$\Delta = v^7 (v - u)^7 u^7 (v^3 - 8uv^2 + 5u^2 v + u^3).$$

Then $7 \mid t = \prod_{p|uv(v-u)} 7$ and $t \mid m$.

Case VIII. $T = \mathbb{Z}/3\mathbb{Z}$

For $T = \mathbb{Z}/3\mathbb{Z}$, let $E : y^2 + axy + by = x^3$. If $b \neq 1$, then $3 \mid m$. Let $E_a : y^2 + axy + y = x^3$. As Theorem 2, if $a^2 + 3a + 9$ is a power of prime and $a - 3$ has no prime factor p equivalent to 1 modulo 6, then E_a is not optimal and $3 \mid c_{E_a}$.

For the case, we are enough to consider $E : y^2 + axy + y = x^3$. Note that $3 \mid a$ if and only if $l^2 | N$. Let $p \mid \Delta = (a-3)(a^2+3a+9)$. If $p \equiv -1 \pmod 3$, then $a^3 \equiv 27 \pmod p$ has exatly one root $a \in \mathbb{Z}/p\mathbb{Z}$, i.e. $p \mid a - 3$. Thus $p \equiv 1 \pmod 3$ if $p \mid a^2 + 3a + 9$.

Consequently, by theorem 2 and proposition 4.3.1, $3 \nmid c_E$ implies that there are at least two primes p_1 and p_2 such that $p_1, p_2 \neq -1 \pmod 3$ and $p_i \mid N_E$.

Suppose $p \neq 3$. Consider two extentions of K, say K_∞ and K_∞^{ac}, defined by

$$K_\infty = \cup_{n \geq 1} K(\mu_{p^n}) \text{ and } K_\infty^{ac} = K(E_{cm}(p)),$$

where μ_{p^n} is a group of all p^n-th roots of unity and E_{cm} is an elliptic curve with complex muliplication such that $\mathrm{End}_K(E_{cm}) = \mathcal{O}_K$. These two extenstions are unramified outside p and their Galois groups over K are isomorphic to $\mathbb{Z}_p^* \cong \mu_{p-1} \times \mathbb{Z}_p$. Since $p \equiv 1 \pmod 3$, we have two cubic extensions of K unramified outside p.

Suppose $p = 3$. Let $\theta : E \to E/ < Q >$ be a natural isogeny. Choose $P \in E(K)$ which is a generator of $E(K)/ < Q >$. Then $K(\theta^{-1}(P))$ is a Galois cubic extension of K unramified outside N. Note that the extension is ramified at 3.

By lemma 5.2.4, $S^{(3)}(E/K)$ has at least 81 elements if $3 \nmid N$ and at least 27 elements if $3 \mid N$. Since $E(K)/3E(K)$ consists of 9 elements, we conclude that $|Ш(E/K)[3]$ is nontrivial. Since $|Ш(E/K)[3]$ is a square, $|T|$ divides $(|Ш(E/K)[3]|)^{1/2}$.

Now we complete the proof of Main Theorem 3.

Chapter 6

Further research

6.1 Gross-Zagier conjecture

In [Lo95], Lorenzini obtained the following similar result using a little different method.

Let E be an elliptic curve defined over $\mathbb{Q}$ with a $\mathbb{Q}$ -rational point of order M. Then following statements hold with at most five explicit exceptions for each M.
(a) If $M = 4$, then $2 \mid m$.
(b) If $M = 5, 6$, or 12, then $M \mid m$.
(c) If $M = 10$, then $50 \mid m$.
(d) If $M = 7, 8$, or 9, then $M^2 \mid m$.

From (d), we can show that Conjecture 5.1.4 is also true if $E(\mathbb{Q})_{\mathrm{tor}} \simeq \mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. So the remaining cases are $E(\mathbb{Q})_{\mathrm{tor}} \simeq \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ for the complete proof of Conjecture 5.1.4. In these cases, we need optimal curves differing by 2-isogeny, which is also conjectured in [SW], and computing 2-Selmer groups. We shall treat these cases in next paper.

6.2 Full Shafarevich-Tate group

In chapter 5, we describe l-torsion part of Shafarevich-Tate group of a certain family of elliptic curves using rational torsion points on elliptic curves.

For any prime l and number field F,

$$Ш(E/F)[l^\infty] \cong (\mathbb{Q}_l/\mathbb{Z}_l)^r \times (\text{a finite } \mathbb{Q}_l/\mathbb{Z}_l - \text{module})$$

for some integer r. Lemma 5.2.4 and Theorem 5.2.5 give an upper bound for r. In particular, for some elliptic curves such as Example 3 in the end of section 5.2, Shafarevich-Tate group completely depends on rational torsion points.

As a next topic, it is interesting to generalize Lemma 5.2.4 and Theorem 5.2.5. In particular, we may assume that $E[l]$ is a simple Galois module or we may find analogous statement of Lemma 5.2.4 and Theorem 5.2.5 for $E[l^\infty]$. The generalization is focusing on calculating r, conjectured to be $r = 0$.

Bibliography

[B04] D. Byeon, *Ranks of of quadratic twists of an elliptic curve,* Acta Arith. **114** (2004), 391-396.

[B10] D. Byeon, *Elliptic curves of rank 1 satisfying the 3-part of the Birch and Swinnerton-Dyer conjecture,* J. Number Theory, **130**(2010) 2707–2714

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

[B-J-K] 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.

[B-S] B. J. Birch and N. M. Stephens, *Computation of Heegner points,* Modular forms (Durham,1983), 13–41, Ellis Horwood Ser. Math. Appl., Statist. Oper. Res., Horwood, Chichester, 1984

[B-Y1] D. Byeon and D. Yhee, *Rational torsion on optimal curves and rank-one quadratic twists,* J. Number Theory, **131** (2011), 522–560

[B-Y2] D. Byeon and D. Yhee, *Optimal curves differing by a* 3*-isogeny,* Acta Arithmetica, in revision

[B-Y3] D. Byeon and D. Yhee, *A conjecture of Gross and Zagier,* preprint

[Cr] J. E. Cremona, *Algorithms for elliptic curves,* Cambridge University Press (1992)

BIBLIOGRAPHY

[CreT] J. E. Cremona, *Cremona's table of elliptic curves,* website address : http://www.ma.utexas.edu/users/tornaria/cnt/cremona.html

[D-S] Fred Diamond and Jerry Shurman, *A First Course in Modular Forms*, Springer, 2000

[Du] N. Dummigan, *Rational torsion on optimal curves,* Int. J. Number Theory, **1** (2005), 513–531.

[Ed] B. Edixhoven, *L'action de ;'algebre de Hecke sur les groupes de composantes des jacobiennes des courbes modulaires est "Eisenstein",* Asterisque, **196-197** (1977), 99–108.

[Go] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields,* Number Theory, Carbondale, Springer Lect. Notes **751** (1979), 108–118.

[Gr] B. H. Gross, *Heegner points on $X_0(N)$,* Modular forms (Durham,1983), 87–105, Ellis Horwood Ser. Math. Appl., Statist. Oper. Res., Horwood, Chichester, 1984

[G-Z] B. H. Gross and D. Zagier, *Heegner points and defivatives of L-series,* Invent. Math. **84**(1986), 225–320

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

[Ke] M. Kenku, *On the number of $\mathbb{Q}$-isomorphism classes of elliptic curves in each $\mathbb{Q}$-isogeny class,* J. Number Theory **15** (1982), 199–202

[Kn] A. W. Knapp, *Elliptic curves,* Math. Notes **40**, Princeton Univ. Press, Prinsceton, NJ (1992)

[Ko] V. Kolyvagin, *Euler systems,* The Grothendieck Festschrift, vol. II, Birkhãuser, Boston, MA (1990), 435–483

[Ku] D.S. Kubert, *Universal bounds on the torsion of elliptic curves,* Proc. London Math. Soc., **3 (33)** (1976), 193–237

BIBLIOGRAPHY

[Li] G. Ligozat, *Courbes modulaires de genre* 1*,* Bull. Soc. Math. France Mém. **43** (1975), 5–80.

[Lo95] Dino J. Lorenzini, *Torsion points on the modular Jacobian* $J_0(N)$*,* Compositio Mathematica, **96**(1995), 149–172

[Lo11] Dino J. Lorenzini, *Torsion and Tamagawa numbers,* Ann. Inst. Fourier., **61**(2011), 1995–2037

[L-O] S. Ling and J. Oesterlé, *The Shimura subgroup of* $J_0(N)$*,* Astérisque **6**(1991), 171–203

[Mz] B. Mazur, *Modular curves and the Eisenstein ideal,* Publications Mathématiques de l'IHÉS, **47** (1977), p. 33-186

[Og] A. P. Ogg, *Hyperelliptic modular curves,* Bull. Soc. Math. France **102** (1974), 449–462

[Sil1] Joseph H. Silverman, *The arithmetic of elliptic curves,* Springer-Verlag, New York, 1986

[Sil2] Joseph H. Silverman, *Advanced topic in the arithmetic of elliptic curves,* Springer-Verlag, 1994

[SW] W. Stein and M. Watkins, *A database of elliptic curves-first report,* in: Algorithmic Number Theory (Sydney, 2002), 267–275, Lecture Notes in Comput. Sci. 2369, Springer, Berlin, 2002

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

[V98] V. Vatsal, *Rank-one twists of a certain elliptic curve,* Mathematiche Annalen **311** (1998), 791–794.

[V99] V. Vatsal, *Canonical periods and congruence formulae,* Duke Math. J. **98** (1999), 397–419.

[V05] V. Vatsal, *Multiplicative subgroups of* $J_0(N)$ *and applications to elliptic curves,* J. Inst. Math. Jussieu. **4** (2005), 281–316.

BIBLIOGRAPHY

[Wa] M. Watkins, *Comuting the modular degree of an elliptic curve,* Experiment. Math, **11** (2002), 487–502.

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

Department of Mathematics, Seoul National University, Seoul, Korea
E-mail: dgyhee@gmail.com

국문초록

이 논문에서는 타원곡선의 산술구조에 관한 세가지 문제를 다루고 있다. Goldfeld 추측, optimal 곡선들이 차수 3으로 다른 경우에 관한 Stein의 추측, 그리고 Gross와 Zagier의 추측이다.

처음에는 Goldfeld의 추측을 만족하는 타원곡선의 모음을 무한히 많이 찾는다. 이를 위해, optimal 곡선상에서 주기 l 인 유리좌표점을 구체적으로 만들어낸 Dummigan의 결과를 이용한다. 그 결과를 일반화하여 Heegner 점에 적용할 것이다. 그로부터, 이차비틂곡선중 양수 비율이 (해석학적) 계수 1을 가지는 타원곡선의 모음을 찾는다.

두번째 문제는 W. Stein과 M. Watkins가 제시한 추측이다. 두 사람은 $X_0(N)$ optimal 곡선과 $X_1(N)$ optimal 곡선이 언제 차수 3으로 다를지 추측했다. 보형곡선의 Jacobian에서 나타나는, 두 optimal 곡선의 순환점들의 상이 서로 다름을 보임으로써 두 optimal curve가 서로 다름을 증명할 것이다.

마지막으로 Gross와 Zagier의 추측을 공부한다. 두 사람은 Heegner 점의 주기가 무한할 때(주기가 없다고도 표현한다), 세 상수 - Manin 상수, Tamagawa 수, Shafarevich-Tate 군의 크기의 제곱근 - 의 곱이, 타원곡선상에서 유한 주기를 가지는 유리수점들의 집합의 크기로 나누어진다고 추측했다. 이 논문에서, 유리수점들 중 (1보다 큰) 홀수 주기를 가지는 점들이 존재할 경우 그 추측이 참임을 보일 것이다.

주요어휘 : 순환점, Goldfeld 추측, Gross-Zagier 추측, optimal 곡선, Selmer 군

학번 : 2008-30085

감사의 글

많은 분들의 도움으로 학위논문을 마무리하면서 감사의 마음 감출 수 없습니다. 누구보다 먼저, 지도교수님이신 변동호교수님께 마음 깊히 감사드립니다. 학생 시절을 끝내고 새로운 배움을 시작하려는 지금까지, 수많은 선택과 갈등에서 고민할 때 선생님께서는 그 고민들을 넘어 이끌어주시고 가르쳐주셨습니다. 부족한 부분에 의기소침할 때는 자신감을 찾을 수 있도록, 과한 자신감에 빠져있을 때에는 차분한 격려로 제 손을 늘 잡아주시며, 연구할 수 있도록 등대가 되어주신 선생님께 존경을 올립니다.

읽기 편한 글이 아님에도, 자세히 읽어주시고 평가해주신 심사위원 선생님들의 애정어린 지적과 조언이 없었으면 논문 완성이 많이 힘들었을 것입니다. 대학원 생활 동안 여러모로 도와주시고 이번에 심사까지 해주신 조영현 교수님, 강석진 교수님, 오병권 교수님 세분께 감사드립니다. 심사를 위해 포항에서 올라와 주신 김현광 교수님께 감사드립니다. 일면식도 없는 학생의 논문을 읽고 평가해주신 Dummigan 교수님께도 감사를 드립니다.

좋은 강의를 해주신 교수님들께도 많은 은혜를 입었습니다. 논문을 심사해주신 선생님들은 물론이고, 제가 학부생일 적부터 좋은 수업을 해주신 이인석 교수님, 김영훈 교수님께도 인사를 드립니다.

졸업 후에도 후배들을 자주 챙겨주신 정연이누나, 좋은 충고를 해주시는 명일이형과 상윤이형, 같이 공부하고 어려운 일을 도와준 광현이형, 재호, 나영이, 겨울이, 효진이, 지애누나, 태경이, 좋은 팀원들 덕분에 심적으로 편안하게 공부할 수 있었습니다. 자주 아이디어를 주고 받은 용욱이와 준수, 교정을 도와준 찬호형 덕분에 논문을 잘 완성할 수 있었습니다. 저를 많이 칭찬해준 세진이형과 경석이, 졸업 후 진로에 대해 많은 이야기를 한 기룡이형과 승진이형, 조교실에서 모두를 챙겨준 경동이형과 명호형과 민재형, 저와 자주 어울려 준 웅석이 및 많은 후배들 덕에 대학원 생활이 지루하지 않았습니다. 지난 10년간 같이 생활하며 도와주신 고모부와 고모님, 사촌누님과 동생이 있어서 고생스럽지 않았습니다. 모두 대학원 생활에서 알게 모르게 힘이 되어준 분들입니다. 모두 고맙습니다.

마지막으로, 여기까지 오는데 저를 뒷받침해주시고 어떤 경우에도 항상 저를 믿어주신 부모님과 동생에게 감사의 마음을 전하고 싶습니다. 당당한 아들이자 자랑스러운 형이 되기 위한 한걸음을 내딛습니다.