Computations on the Birch and Swinnerton-Dyer conjecture for elliptic curves over pure cubic extensions

Céline Maistret

A Thesis in

The Department of Mathematics

and Statistics

Presented in Partial Fulfillment of the Requirements for the Degree of Master of Science (Mathematics) at Concordia University

Montreal, Quebec, Canada

August 2012

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By: Céline Maistret

Entitled: Computations on the Birch and Swinnerton-Dyer conjecture for elliptic curves over pure cubic extensions

and submitted in partial fulfillment of the requirements for the degree of

Master of Science (Mathematics)

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final Examining Committee:

Professor Chantal David	Chair
Professor Chantal David	Examiner
Professor Chris Cummins	Examiner
Professor Francisco Thaine	Examiner
Professor Hershy Kisilevsky	Supervisor

Approved by _____

Chair of Department or Graduate Program Director

_____

Dean of Faculty

Date _____

Abstract

Computations on the Birch and Swinnerton-Dyer conjecture for elliptic curves over pure cubic extensions

Céline Maistret

The Birch and Swinnerton-Dyer conjecture remains an open problem. In this thesis, we propose to give numerical evidence toward this conjecture when restricted to elliptic curves over pure cubic extensions.

We present the general conjecture for elliptic curves over number fields and detail each arithmetic invariants involved. Assuming the conjecture holds, for given elliptic curves E over specific number fields K, we compute the order of the Shafarevich-Tate group of $E(K)$.

Acknowledgements

I would like to thank my supervisor, Professor Hershy Kisilevsky, for presenting me with this problem, patiently guiding me through it and always being available for my questions.

I also thank Jack Fearney for his help with SAGE, Tim Dokchitser and Andrew Granville for their help with MAGMA.

I am grateful to the department of mathematics of Concordia University for giving me the opportunity to teach and tutor during my studies and particularly to its staff for their kindness and availability.

Lastly, I thank my family and friends for their encouragement and support at all time.

Contents

List of Tables

Introduction

In the article *Notes on elliptic curves II* ([BSD65]), Birch and Swinnerton-Dyer presented their conjecture concerning the rank of the Mordell-Weil group $E(\mathbb{Q})$ of an elliptic curve $E/\mathbb{Q}$. Along with prediction on the rank, they proposed a refined version of this conjecture, predicting the form of the leading term in the Taylor expansion of $L(E/\mathbb{Q}, s)|_{s=1}$, where $L(E/\mathbb{Q}, s)$ is the L-function attached to E.
Later on, John Tate presented a generalization of their conjecture to abelian varieties over number fields in his article *On the conjecture of Birch and Swinnerton-Dyer and a geometric analog* ([Bou66]). This generalization to number fields restricted to elliptic curves is the object of our study. It can be stated as follows (see [DD05])

Conjecture 1. *(Birch and Swinnerton-Dyer for a number field K)*

(a) The L-function $L(E/K, s)$ has an analytic continuation to $s = 1$, and

$$ord_{s=1}L(E/K, s) = rk(E(K)). \tag{1}$$

(b) The Shafarevich-Tate group $Ш(E/K)$ is finite, and the leading coefficient in the Taylor expansion of $L(E/K, s)$ at $s = 1$ is equal to

$$\frac{|Ш(E/K)|R_{E/K}C(E/K)\Omega}{|E(K)_{tors}|^2\sqrt{|\Delta_K|}} \tag{2}$$

We describe in detail this conjecture and then propose to verify (2) for specific elliptic curves over number fields $K = \mathbb{Q}(\sqrt[3]{m})$ for given m.

In chapter 1, we present the basic theory of elliptic curves and introduce the necessary notions for understanding their arithmetic invariants involved in the Birch and Swinnerton-Dyer conjecture.

In chapter 2, we define the notion of an L-function attached to an elliptic curve over a number field. In order to prepare for our computations, we focus on the specific case of $L(E/K, s)$ where $K = \mathbb{Q}(\sqrt[3]{m})$ and give a factorization of $L(E/K, s)$ in terms of $L(E/\mathbb{Q}, s)$ twisted by Artin representations.

Keeping the restriction to pure cubic number fields, chapter 3 introduces the Birch and Swinnerton-Dyer conjecture for this particular case. Each feature of this conjecture is detailed in this context and a way of computing that feature is given .

In chapter 4, we present numerical results obtained for specific elliptic curves. We used the mathematical software SAGE and the computational algebra system MAGMA to numerically compute invariants of elliptic curves. These results provide numerical evidence for the conjecture.

In the conclusions, we discuss our computations and their limits.

Chapter 1

Elliptic Curves

1.1 Introduction

This chapter presents the basic theory of elliptic curves.

First, we give definitions and properties. Then, we introduce the notion of group of rational points and we define some arithmetic invariants of an elliptic curve via the survey of the Mordell-Weil theorem's proof.

Finally, by looking successively at elliptic curves over the complex numbers and over non-Archimedean local fields, we introduce all invariants involved in the right hand side of conjecture 1.b. above.

The main references for this chapter are [Sil09] and [ST92].

1.2 Generalities

Definition 1.2.1. *Let K be a field. An elliptic curve over K, denoted E/K, is a pair (E, O), where E is a nonsingular projective curve of genus one over K and O is a K-rational point on E.*

Every such curve can be described as a projective plane cubic curve, given by the generalized Weierstrass normal form (see Chapter III, Proposition 3.1 in [Sil09])

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{1.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$.

However, it is more common to consider affine coordinates $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ in order to write the Weierstrass equation for E/K

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.2}$$

and to add the extra point at infinity $O = [0, 1, 0]$.

Given an elliptic curve, we can define constants attached to its Weierstrass form. These constants are called the *Tate values* and are defined as follows.

Definition 1.2.2. *The Tate Values are*

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6, \end{aligned}$$

where a_1, a_2, a_3, a_4, a_6 refer to the coefficients of the Weierstrass form (1.2).

From these values, we define the discriminant and the J-invariant of the curve.

Definition 1.2.3. *The discriminant and the J-invariant are*

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \quad \textit{and} \quad j := \frac{c_4^3}{\Delta}, \quad \textit{respectively.}$$

In particular, two elliptic curves are isomorphic over $\bar{K}$, where $\bar{K}$ denotes the algebraic closure of K, if and only if they both have the same j-invariant (see Chapter III, proposition 1.4 in [Sil09]).

Our goal being mainly computational, we use the Weierstrass normal form (1.2) to input an elliptic curve into mathematical softwares SAGE and MAGMA. Nonetheless, working over number fields, we have $Char(K) = 0$, which allows us to simplify (1.2) into

$$E : y^2 = x^3 + Ax + B, \quad \Delta \neq 0, \tag{1.3}$$

where we retrieve the discriminant of E being $\Delta = -16(4A^3 + 27B^2) \neq 0$ and its non-vanishing ensures the non-singularity of E/K (see [Kna92], III,2).

1.2.1 Mordell-Weil group

If E/K is an elliptic curve given by a Weierstrass equation, we can consider

$$E(\bar{K}) = \{(x, y) \in \bar{K}^2 \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}. \tag{1.4}$$

A particular property of elliptic curves is that $E(\bar{K}) \subset \mathbb{P}^2$ can be equipped with a group stucture, where the addition law is described geometrically via the chord and tangent law. This makes $E(\bar{K})$ into an abelian group with identity element O (see [ST92], Chapter I).

As a consequence of the addition law involving lines between two points, for each subfield $K \subseteq F \subseteq \bar{K}$, the next proposition defines the corresponding subgroup of F-rational points on E.

Proposition 1.2.1. *Suppose that E is defined over K and consider the field F such that $K \subseteq F \subseteq \bar{K}$. Then*

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

is a subgroup of $E(\bar{K})$. It is the group of F-rational points on E, called the Mordell-Weil group over F.

In order to elaborate on the structure of $E(\bar{K})$ and $E(K)$ we introduce the notion of isogeny.

Definition 1.2.4. *Let (E_1, O_1) and (E_2, O_2) be elliptic curves over K.*

(a) A morphism from (E_1, O_1) to (E_2, O_2) is a rational map which is regular at every point of (E_1, O_1).

(b) An isogeny from (E_1, O_1) to (E_2, O_2) is a morphism

$$\phi : E_1 \mapsto E_2 \quad satisfying \quad \phi(O_1) = O_2.$$

As an example, we define the multiplication by m isogeny.

Definition 1.2.5. *For each $m \in \mathbb{Z}$, the multiplication by m isogeny is the map*

$$[m] : E(\bar{K}) \mapsto E(\bar{K}),$$

$$where\ [m](P) = \begin{cases} P + P + ... + P \quad if\ m > 0; \\ [m](-P) \quad if \quad m < 0; \\ O \quad if \quad m = 0. \end{cases}$$

This isogeny yields the notion of points of finite order.

Definition 1.2.6. *Let E/K be an elliptic curve and $m \in \mathbb{Z}$ with $m \geq 1$.*
The m-torsion subgroup of $E(\bar{K})$, denoted $E(\bar{K})[m]$, is the set of points of $E(\bar{K})$ of order m

$$E(\bar{K})[m] = \{P \in E(\bar{K}) \mid [m](P) = O\}. \tag{1.5}$$

We then define the torsion subgroup of $E(\bar{K})$, denoted $E(\bar{K})_{tors}$, to be the set of points of finite order :

$$E(\bar{K})_{tors} = \{P \in E(\bar{K}) \mid [m](P) = O \ for\ some\ m \in \mathbb{Z}\}. \tag{1.6}$$

By proposition 1.2.1., $E(K)$ has the following subgroup

$$E(K)_{tors} = \{P \in E(K) \mid [m](P) = O \ for \ some \ m \in \mathbb{Z}\}. \tag{1.7}$$

The structure of $E(K)_{tors}$ depends on the field upon which the points are considered. When working with $K = \mathbb{Q}$, Mazur's theorem provides a characterization of $E(\mathbb{Q})_{tors}$ (see [Maz]).

Theorem 1.2.1. *(Mazur) Let $E/\mathbb{Q}$ be an elliptic curve. The torsion subgroup $E(\mathbb{Q})_{tors}$ of $E(\mathbb{Q})$ is isomorphic to one of the following fifteen groups :*

$$\mathbb{Z}/N\mathbb{Z} \ \ with \ \ 1 \leq N \leq 10 \ \ or \ \ N = 12, \tag{1.8}$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \ \ with \ \ 1 \leq N \leq 4. \tag{1.9}$$

For the more general case of K being a number field, the boundedness of $E(K)_{tors}$, as $[K : \mathbb{Q}]$ is fixed, was proven by Merel (see [Mer]).

Theorem 1.2.2. *(Merel) Let $d \geq 1$ be an integer. There exists a real number $B(d)$ such that for all elliptic curves E defined over a number field K of degree d over $\mathbb{Q}$, every torsion point of $E(K)$ is of order $< B(d)$, where $B(d)$ depends only on d.*

Merel's theorem provides an upper bound for m in (1.7). The boundedness of $E(K)_{tors}$ follows from the structure of $E(\bar{K})[m]$ given by the next proposition (see Chapter III, Corollary 6.4 in [Sil09]).

Proposition 1.2.2. *Let E be an elliptic curve defined over a number field K, and let $m \in \mathbb{Z}$ with $m \neq 0$, we have*

$$E(\bar{K})[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

1.3 The Mordell-Weil Theorem

We consider the structure of $E(K)$, given by the Mordell-Weil Theorem.

Theorem 1.3.1. *(Mordell-Weil) Let E/K be an elliptic curve, the Mordell-Weil group $E(K)$ is finitely generated, i.e.,*

$$E(K) \simeq \mathbb{Z}^r \oplus E(K)_{tors},$$

where $r \geq 0$.

Definition 1.3.1. *The number r of copies of $\mathbb{Z}$ in the Mordell-Weil group $E(K)$ is called the rank of $E(K)$, denoted $rk(E(K))$.*

In particular, the rank of $E(K)$ is predicted in the first part of the Birch and Swinnerton-Dyer conjecture.

The proof of the Mordell-Weil theorem consists of proving the two main theorems listed below. Both theorems are important since their proofs yield definitions of invariants involved in the Birch and Swinnerton-Dyer conjecture.

Theorem 1.3.2. *There exists a function*

$$h : E(K) \to \mathbb{R},$$

satisfying

(a) For all points $Q \in E(K)$, there is a constant C_Q depending only on Q, and an absolute constant C depending only on E, such that

$$h(P + Q) \leq 2h(P) + C_Q,$$

$$h([m]P) \geq m^2 h(P) + C, \quad for\ all\ P \in E(K).$$

(b) For all $B > 0$,

$$\{P \in E(K) \mid h(P) < B\} \ \ is finite.$$

Theorem 1.3.3. *(The weak Mordell-Weil Theorem) For any integer $n \geq 1$, the group $E(K)/nE(K)$ is finite.*

Mordell-Weil's theorem is then a consequence of the descent lemma.

Lemma 1.3.1. *Let G be an abelian group equipped with a height function as described in theorem 1.3.2., and assume that G/nG is finite for some $n > 1$ then G is finitely generated.*

1.3.1 The Weak Mordell-Weil Theorem

Before studying the existence of the height function presented in theorem 1.3.2., we present a survey of the Weak Mordell-Weil theorem's proof. The survey of this proof matters for our study as it leads to the definition of the Shafarevich-Tate group, whose order appears in conjecture 1.b.
The details for the entire proof can be found in Chapter VIII.1. of [Sil09].

Considering the multiplication by n isogeny defined above, applied to $E(\bar{K})$ equipped with the discrete topology, we have the following exact sequence of modules equipped with their natural continuous action of the profinite group $G := Gal(\bar{K}/K)$ (see [Dar04])

$$0 \longrightarrow E(\bar{K})[n] \longrightarrow E(\bar{K}) \xrightarrow{n} E(\bar{K}) \longrightarrow 0\,. \tag{1.10}$$

Galois cohomology of (1.10) yields the long exact cohomology sequence

$$0 \longrightarrow E(K)[n] \longrightarrow E(K) \xrightarrow{n} E(K) \tag{1.11}$$
$$H^1(G, E(\bar{K})[n]) \longrightarrow H^1(G, E(\bar{K})) \xrightarrow{n} H^1(G, E(\bar{K})),$$

where $H^1(G, E(\bar{K}))$ is the first cohomology group of the G-Module $E(\bar{K})$ defined by

$$H^1(G, E(\bar{K})) = \frac{Z^1_{cont}(G, E(\bar{K}))}{B^1(G, E(\bar{K}))}, \tag{1.12}$$

$Z^1_{cont}(G, E(\bar{K}))$ is the group of continuous 1-cocycles from G to $E(\bar{K})$,
$B^1(G, E(\bar{K}))$ is the group of 1-coboundaries from G to $E(\bar{K})$.

From (1.11) we obtain the following short exact sequence

$$0 \to E(K)/nE(K) \to H^1(G, E(\bar{K})[n]) \to H^1(G, E(\bar{K}))[n] \to 0, \tag{1.13}$$

where $H^1(G, E(\bar{K}))[n] = \{c \in H^1(G, E(\bar{K})) \mid nc = 0\}$.

In order to conclude that $E(K)/nE(K)$ is finite, we would need to specify an embedding into a finite group. In the case of number fields, the sequence (1.13) does not provide a solution as $H^1(G, E(\bar{K})[n])$ is never finite (see [Dar04]).
We then approach this sequence from a local point of view.

For any place v of K, the embedding of K into the completion K_v, extended to an embedding of $\bar{K}$ into $\bar{K}_v$, induces an inclusion $G_v := Gal(\bar{K}_v/K_v) \subset G$, leading to the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/nE(K) & \xrightarrow{\delta} & H^1(G, E(\bar{K})[n]) & \longrightarrow & H^1(G, E(\bar{K}))[n] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle res_v} & & \downarrow{\scriptstyle res_v} & \searrow^{\gamma_v} & \downarrow{\scriptstyle res_v} & & \\ 0 & \longrightarrow & E(K_v)/nE(K_v) & \xrightarrow{\delta} & H^1(G_v, E(\bar{K})[n]) & \longrightarrow & H^1(G_v, E(\bar{K}))[n] & \longrightarrow & 0 \end{array}$$

where res_v denotes the restriction homomorphism relative to the inclusion $G_v \subset G$.

This diagram yields the definition of two groups, the second of which is the Shafarevich-Tate group.

Definition 1.3.2. *The n-Selmer group of E over K , denoted $Sel_n(E/K)$, is the set of classes $c \in H^1(G, E(\bar{K})[n])$ such that $\gamma_v(c) = 0$ for all places v of K.*

Definition 1.3.3. *The Shafarevich-Tate group of E/K, denoted $Ш(E/K)$, is the set of classes $c \in H^1(G, E(\bar{K}))$ such that $res_v(c) = 0$, for all places v of K.*

In particular, the n-Selmer group of E over K has been proved to be finite.

Proposition 1.3.1. *$Sel_n(E/K)$ is finite (see Chapter X.4, Theorem 4.2(b) in [Sil09]).*

We conclude that $E(K)/nE(K)$ is finite by applying the following lemma to (1.13) (see lemma 2.2 in [Mil06]).

Lemma 1.3.2. *For any pairs of maps of modules*

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C \tag{1.14}$$

there is an exact kernel-cokernel sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & ker(\alpha) & \longrightarrow & ker(\beta \circ \alpha) & \xrightarrow{\alpha} & ker(\beta) & \longrightarrow & coker(\beta) \\ & & & & & \searrow & & & \\ & & coker(\alpha) & \longrightarrow & coker(\beta \circ \alpha) & \xrightarrow{\alpha} & coker(\beta) & \longrightarrow & 0 \end{array}$$

From (1.13) we obtain the exact sequence

$$0 \longrightarrow E(K)/nE(K) \xrightarrow{\delta} Sel_n(E/K) \longrightarrow Ш(E/K)[n] \longrightarrow 0\,, \tag{1.15}$$

which implies that $E(K)/nE(K)$ is finite.

By looking at the exact sequence (1.15), one is led to ask the question of finiteness of $Ш(E/K)$. This group has been conjectured to be finite by Shafarevich and Tate. Moreover, Cassels showed that if $Ш(E/K)$ is finite then it is of square order (see p. 420 in [Bou66]).

In particular, we assume that $Ш(E/K)$ is finite as we compute and provide some numerical results in chapter 4 on its order.

1.4 Height function

The notion of height, to be defined later on, plays a role in the proof of the Mordell-Weil theorem via theorem 1.3.2.
In addition, it provides an invariant attached to E/K : the elliptic regulator, denoted by $R_{E/K}$.

Definition 1.4.1. *The set of standard absolute values on a number field K, denoted M_K, is the set of absolute values on K whose restriction to $\mathbb{Q}$ is one of the absolute values in $M_{\mathbb{Q}}$, where $M_{\mathbb{Q}}$ consists of*

(a) One archimedean absolute value

$$|x|_\infty = max\{x, -x\}, \tag{1.16}$$

(b) For each prime $p \in \mathbb{Z}$, one non-archimedean absolute value

$$|p^n \frac{a}{b}|_p = p^{-n}, \qquad where\ a, b \in \mathbb{Z}\ and\ p \nmid ab. \tag{1.17}$$

Definition 1.4.2. *Let $v \in M_K$. We define the local degree at v, denoted n_v to be*

$$n_v = [K_v : \mathbb{Q}_v], \tag{1.18}$$

where K_v and $\mathbb{Q}_v$ represent the completions of K and $\mathbb{Q}$ with respect to v.

We consider the notion of height of a point $P \in \mathbb{P}^2(K)$. We use the following product formula to justify that the height function to be defined later on, does not depend on the choice of homogeneous coordinates (see Chapter VIII, prop 5.4 in [Sil09]).

Proposition 1.4.1. *Let $x \in K^*$. Then*

$$\prod_{v \in M_K} |x|_v^{n_v} = 1 \tag{1.19}$$

We note that homogeneous coordinates for a point $P \in \mathbb{P}^2(K)$ have the form $[\lambda X : \lambda Y : \lambda Z]$ for any $\lambda \in K^*$. By the product formula, the following definition does not depend on the choice of homogeneous coordinates for P.

We define the height of $P \in \mathbb{P}^2(K)$ relative to K, denoted by $H_K(P)$.

Definition 1.4.3. *Let $P \in \mathbb{P}^2(K)$ be such that $P = [X : Y : Z]$ with $(X, Y, Z) \in \mathcal{O}_K^3$.*

$$H_K(P) = \prod_{v \in M_K} max\{|X|_v, |Y|_v, |Z|_v\}^{n_v} \tag{1.20}$$

We then restrict this definition to points $P \in E(K)$ by letting

$$H_K(P) = \begin{cases} 1 \ if \ \ P = O = [0 : 1 : 0]; \\ H_K([X : 1 : Z]) \ otherwise. \end{cases} \tag{1.21}$$

Remark 1.4.1. *By definition, we have $H_K(P) \geq 1$ for all $P \in E(K)$.*

From definition 1.4.3. we derive the following:

Definition 1.4.4. *The logarithmic height on $E(K)$ is the function*

$$h_K : E(K) \to \mathbb{R} \quad such \ that \qquad h_K(P) = logH_K(P). \tag{1.22}$$

We extend definition 1.4.3. to any $P \in \bar{K}$ by defining the absolute height of P, denoted $H(P)$ and its corresponding absolute logarithmic height, denoted $h(P)$.

Definition 1.4.5. *Choose a number field F such that $P \in \mathbb{P}^2(F)$. The absolute height of P is defined as follows*

$$H(P) = H_F(P)^{1/[F:\mathbb{Q}]}$$

Definition 1.4.6. *The absolute logarithmic height on $E(\bar{K})$ is the function*

$$h : E(\bar{K}) \to \mathbb{R} \quad such\ that \qquad h(P) = logH(P). \tag{1.23}$$

Remark 1.4.2. *By remark 1.4.1., we have $h(P) \geq 0$ for all $P \in E(\bar{K})$.*

1.4.1 Properties of the height function

We justify the existence of a height function on $E(K)$ satisfying conditions of theorem 1.3.2. by deriving some properties of the absolute logarithmic height.

Since the set $\{P \in \mathbb{P}^2(K) \mid H(P) < C\}$ is finite, by definition of the absolute logarithmic height, we have the following lemma.

Lemma 1.4.1. *For any constant C, the set of $P \in E(K)$ such that $h(P) < C$ is finite.*

Working through the algebra of the addition law for two points P and Q on $E(\bar{K})$, one can prove the following theorem (see Chapter VIII.6, Theorem 6.2 in [Sil09]).

Theorem 1.4.1. *Let E/K be an elliptic curve. For all $P, Q \in E(\bar{K})$ we have*

$$h(P+Q) + h(P-Q) = 2h(P) + 2h(Q) + O(1), \tag{1.24}$$

where $O(1)$ refers to the "big O" notation and depends only on E.

By remark 1.4.2. we have $h(P-Q) \geq 0$, which yields the following:

Corollary 1.4.1. *Let E/K be an elliptic curve,*

$$h(P+Q) \leq 2h(P) + O(1) \quad for\ all\ P \in E(\bar{K}), \tag{1.25}$$

where $O(1)$ depends on E and Q.

Finally, we complete the set of conditions needed in theorem 1.3.2. by proving the following corollary.

Corollary 1.4.2. *Let E/K be an elliptic curve, $m \in \mathbb{Z}$,*

$$h([m]P) = m^2 h(P) + O(1) \quad for\ all\ P \in E(\bar{K}) \tag{1.26}$$

Proof : By induction on m.

Clearly, for $m = 0, 1$ the result holds.

Assume that it holds for $m-1$ and m.

From theorem 1.4.1. with $[m]P$ and P instead of P and Q respectively, we have

$$\begin{aligned} h([m+1]P) &= -h([m-1]P) + 2h([m]P) + 2h(P) + O(1) \\ &= (-(m-1)^2 + 2m^2 + 2)h(P) + O(1) \\ &= (m+1)^2 h(P) + O(1). \end{aligned}$$

□

1.4.2 Canonical height

We further extend the notion of height for a point on an elliptic curve by defining the canonical height of this point.

First we remark that if it exists, the canonical height is unique by the following proposition.

Proposition 1.4.2. *There exists at most one function* $\hat{h} : E(\bar{K}) \to \mathbb{R}$ *satisfying*

(a) $\hat{h}(P) - h(P)$ *is bounded on* $E(\bar{K})$,

(b) $\hat{h}(2P) = 4\hat{h}(P)$.

Proof : If $\hat{h}$ satisfies (a) with bound B, then

$$|\hat{h}([2^n]P) - h([2^n]P)| \leq B \tag{1.27}$$

If it also satisfies (b) then

$$|\hat{h}(P) - \frac{h([2^n]P)}{4^n}| \leq \frac{B}{4^n} \tag{1.28}$$

therefore $h([2^n]P)/4^n$ converges to $\hat{h}(P)$.

□

The sequence $h([2^n]P)/4^n$ is Cauchy in $\mathbb{R}$. Indeed, since by corollary 1.4.2, we can find a constant A such that $|h(2P) - 4h(P)| \leq A$ for all $P \in E(\bar{K})$, one can show that for $N \geq M \geq 0$ we have $|\frac{h(2^N P)}{4^N} - \frac{h(2^M P)}{4^M}| \leq \frac{A}{3.4^M}$ (see Lemma 4.6 in [Mil06]). Therefore the following definition is consistent.

Definition 1.4.7. *Let E/K be an elliptic curve. The canonical height or Néron-Tate height, denoted by $\hat{h}$, is the function*

$$\hat{h} : E(\bar{K}) \to \mathbb{R},$$

such that

$$\hat{h}(P) = \lim_{N\to\infty} \frac{1}{4^N} h([2^N]P).$$

Remark 1.4.3. *We defined $\hat{h}(P)$ as a limit involving $h(P)$. In the same way, we can define the canonical height associated to $h_K(P)$, denoted by $\hat{h}_K(P)$, by letting*

$$\hat{h}_K(P) = \lim_{N\to\infty} \frac{1}{4^N} h_K([2^N]P)$$

We note that by definition 1.4.5. we have $h(P) = \frac{1}{[K:\mathbb{Q}]} h_K(P)$ hence

$$\hat{h}(P) = \frac{1}{[K:\mathbb{Q}]} \hat{h}_K(P). \tag{1.29}$$

The next theorem follows from the properties of the height function listed above and leads to the definition of the elliptic regulator.

Theorem 1.4.2. *(Néron-Tate) Let E/K be an elliptic curve, and let $\hat{h}$ be the canonical height on $E(\bar{K})$*

(a) For all $P, Q \in E(\bar{K})$

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q). \tag{1.30}$$

(b) For all $P \in E(\bar{K})$ and all $m \in \mathbb{Z}$

$$\hat{h}([m]P) = m^2 \hat{h}(P). \tag{1.31}$$

(c) The canonical height $\hat{h}$ is a quadratic form on $E(\bar{K})$ and the pairing

$$<,>: E(\bar{K}) \times E(\bar{K}) \to \mathbb{R}$$

$$< P, Q >= \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)), \tag{1.32}$$

is bilinear.

(d) Let $P \in E(\bar{K})$, $\hat{h}(P) = 0 \iff$ P is a torsion point.

We can therefore define a pairing associated to the canonical height.

Definition 1.4.8. *The canonical height pairing or Néron-Tate pairing on E/K is the bilinear form*

$$<,>: E(\bar{K}) \times E(\bar{K}) \to \mathbb{R}$$

such that

$$< P, Q >= \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)). \tag{1.33}$$

Remark 1.4.4. *In reference to remark 1.4.3, we denote by $<,>_K$ the canonical height pairing associated to $\hat{h}_K$.*

Finally, we define the elliptic regulator of E/K.

Definition 1.4.9. *The elliptic regulator of E/K, denoted $R_{E/K}$, is defined as follows*

$$R_{E/K} = det(< P_i, P_j >)_{1 \le i \le r \ , \ 1 \le j \le r}, \tag{1.34}$$

where $P_1, P_2, ..., P_r \in E(K)$ generates $E(K)/E(K)_{tors}$.

Remark 1.4.5. *Conventions and computability of the regulator.*

(a) When $r = 0$, by convention we let $R_{E/K} = 1$.

(b) It is possible to define $R_{E/K}$ using the canonical height pairing associated to $\hat{h}_K$. By remark 1.4.3, both regulators differ by a power of $[K : \mathbb{Q}]$. This choice in the definition of $R_{E/K}$ is important in regard to the Birch and Swinnerton-Dyer conjecture. We will discuss it in chapter 3, section 3.3.1.

(c) There exist algorithms to compute the canonical height of a point on an elliptic curve (see for example [EW00], [Sil97]). In particular, SAGE and MAGMA provide height functions. The limitation in the computability of $R_{E/K}$, given an elliptic curve E/K, arises from finding generators of $E(K)/E(K)_{tors}$. For most cases, methods to find generators are unknown. We address this issue in Chapter 3, section 3.3.1.

1.5 Elliptic curves over $\mathbb{C}$

The aim of this section is to define the notion of periods associated to an elliptic curve. We start by defining doubly periodic functions and we introduce the periods of an elliptic curve by exploring its isomorphism with a torus.

Definition 1.5.1. *Let ω_1, ω_2 be complex numbers that are linearly independant over $\mathbb{R}$. Then*

$$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{n_1\omega_1 + n_2\omega_2 \mid n_1, n_2 \in \mathbb{Z}\}$$

is called a lattice and

$$F = \{a_1\omega_1 + a_2\omega_2 \mid 0 \leq a_i < 1, i = 1, 2\}$$

is a fundamental parallelogram for L.

Definition 1.5.2. *A doubly periodic function is a meromorphic function*

$$f : \mathbb{C} \to \mathbb{C} \cup \infty$$

such that

$$f(z + \omega) = f(z),$$

for all $z \in \mathbb{C}$ *and all* $\omega \in L$.

In particular, if $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, *then*

$$f(z + \omega_i) = f(z) \quad i = 1, 2.$$

The numbers $\omega_i \in L$ *are called the periods of* f.

In addition to being an example of a doubly periodic function, the Weierstrass $\wp$-function defined below yields an isomorphism between an elliptic curve over $\mathbb{C}$ and a lattice.

Definition 1.5.3. *Given a lattice* L, *we define the Weierstrass* $\wp$*-function as*

$$\wp(z) = \wp(z; L) = \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right).$$

The definition of the Weierstrass $\wp$-function is justified by the next theorem. Moreover, we see that every such doubly periodic function is a rational function of $\wp$ and $\wp'$ (see section 9.2 in [Was03]).

Theorem 1.5.1. *(a) The sum defining* $\wp(z)$ *converges absolutely and uniformly on compact sets not containing elements of* L.

(b) $\wp(z)$ *is meromorphic on* $\mathbb{C}$ *and has a double pole at each* $\omega \in L$.

(c) $\wp(-z) = \wp(z)$ *for all* $z \in \mathbb{C}$.

(d) $\wp(z+\omega) = \wp(z)$ *for all* $\omega \in L$.

(e) The set of doubly periodic rational functions for L *is* $\mathbb{C}(\wp, \wp')$.

We can give a specific expression for $\wp'$ by introducing the Eisenstein series.

Definition 1.5.4. *For integers* $k \geq 3$*, we define the Eisenstein series by*

$$G_k = G_k(L) = \sum_{\substack{\omega \in L \\ \omega \neq 0}} \omega^{-k}$$

The sum is indeed convergent. Moreover, we note that $G_k = 0$ *if* k *is odd (see lemma 9.4 in [Was03]).*

Theorem 1.5.2. *(a) Let* $\wp(z)$ *be the Weierstrass* $\wp$*-function for a lattice* L*. Then*

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6 \tag{1.35}$$

(b) $\Delta = (60G_4)^3 - 27(140G_6)^2 \neq 0$

In particular, theorem 1.5.2. implies that (1.35) defines an elliptic curve. An element $z \in \mathbb{C}$ is thus mapped to the point with complex coordinate $(\wp(z), \wp'(z))$. By L-periodicity of $\wp(z)$ and $\wp'(z)$, we have a function from $\mathbb{C}/L$ to $E(\mathbb{C})$. This function is an isomorphism of groups as the next theorem shows (see theorem 9.10 in [Was03]).

Theorem 1.5.3. *Let L be a lattice and let E be the elliptic curve $y^2 = 4x^3 - 60G_4x - 140G_6$. The map*

$$\begin{aligned} \phi :& \mathbb{C}/L \to E(\mathbb{C}) \\ & z \mapsto (\wp(z), \wp'(z)) \\ & 0 \mapsto \infty \end{aligned}$$

is an isomorphism of groups.

Therefore, by this isomorphism, to each elliptic curve over $\mathbb{C}$ corresponds a lattice $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.
From this correspondence, we define the periods of an elliptic curve isomorphic to $\mathbb{C}/L$ to be the periods of the Weierstrass $\wp$-function for the lattice L.

Remark 1.5.1. *Since we are considering elliptic curves defined over $\mathbb{Q}$, we can apply the following result for our further computations (see p. 274 in [Was03]).*

Proposition 1.5.1. *Given an elliptic curve defined over $\mathbb{R}$, the lattice L associated to E is given by*

(a) $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ *with* $\omega_1 \in \mathbb{R}$ *and* $\omega_2 \in i\mathbb{R}$

or

(b) $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ *with* $\omega_1 \in \mathbb{R}$ *and* $\Re(\omega_2) = \frac{1}{2}(\omega_1)$

Therefore we can fix notations by letting $\omega_+ = \omega_1$ and $\omega_- = \Im(\omega_2)$.
We note that this proposition holds for elliptic curves E isomorphic to an elliptic curve defined over $\mathbb{R}$.

1.6 Elliptic curves over non-Archimedean Local fields

The present section gives an overview of local properties of elliptic curves and introduces local invariants.

Let K be a local field with respect to the discrete additive valuation ord corresponding to the prime ideal $\mathfrak{p}$. If $M = \{x \in K \mid ord(x) > 0\}$ is the maximal ideal in $\mathcal{O}_K$, we let $\pi\mathcal{O}_K = M$ and we consider the normalized valuation ord by setting $ord(\pi) = 1$.

1.6.1 Reduction modulo $\mathfrak{p}$

Let E/K be an elliptic curve given by a Weierstrass equation such that $ord(a_i) \geq 0$ for $i = 1, 2, 3, 4, 6$.
For computational purposes, it is important to consider a minimal model for our elliptic curve. The notion of minimality is defined as follows:

Definition 1.6.1. *The equation of E/K is called minimal if $ord(\Delta)$ is minimal among all curves in the same isomorphism class.*

Minimality of a Weierstrass equation can be verified by applying the following theorem (see Chapter 4, Theorem 4.2. in [SZ03]).

Theorem 1.6.1. *(a) For every elliptic curve E/K over a local field K, there exists a minimal Weierstrass equation.*

(b) Let E/K be an elliptic curve given by a Weierstrass equation with integral coefficients. If $ord(\Delta) < 12$, then the equation is minimal.

Remark 1.6.1. *For elliptic curves over $\mathbb{Q}$, there is an equation which is minimal at all primes dividing its discriminant, as $\mathbb{Z}$ is a Principal Ideal Domain. This is called a globally minimal Weierstrass equation of $E/\mathbb{Q}$.*

By considering a minimal equation, one can observe the local behavior of E/K by reducing it modulo $\mathfrak{p}$.

Definition 1.6.2. *Let E be an elliptic curve over a local field K with minimal equation*

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

The reduced curve $\tilde{E}$ is the curve

$$\tilde{E} : y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6}, \tag{1.36}$$

where $\tilde{a_i} \in \mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ for $i = 1, 2, 3, 4, 6$.

Then at $\mathfrak{p}$, E/K is said to have:

(a) good reduction if $\tilde{E}$ is an elliptic curve.

(b) bad reduction otherwise. This case can be further reduced as:

   i. split multiplicative reduction if $\tilde{E}$ has a node and the slopes of its tangents lie in $\mathbb{F}_\mathfrak{p}$.

   ii. non-split multiplicative reduction if $\tilde{E}$ has a node but the slopes of its tangents lie in $\mathbb{F}_{\mathfrak{p}^2} \setminus \mathbb{F}_\mathfrak{p}$.

   iii. additive reduction if $\tilde{E}$ has a cusp.

The following proposition allows the characterization of E/K based on its minimal Weierstrass equation (see Chapter 4, Prop 4.4 in [SZ03]).

Proposition 1.6.1. *Let E/K be an elliptic curve over a local field K with minimal Weierstrass equation.*

(a) The curve has good reduction $\iff$ $ord(\Delta) = 0$.

(b) The curve has multiplicative reduction $\iff$ $ord(\Delta) > 0$ and $ord(c_4) = 0$.

The reduction is split multiplicative when

i. at $char(\mathbb{F}_\mathfrak{p}) \neq 2, 3$: $-c_4c_6$ is a square in $\mathbb{F}_\mathfrak{p}$.

ii. at $char(\mathbb{F}_\mathfrak{p}) = 3$: b_2 is a square in $\mathbb{F}_\mathfrak{p}$.

iii. at $char(\mathbb{F}_\mathfrak{p}) = 2$: $x^2 + a_1x + (a_3a_1^{-1} + a_2)$ has a root in $\mathbb{F}_\mathfrak{p}$.

otherwise the reduction is non-split multiplicative.

(c) The curve has additive reduction if and only if $ord(\Delta) > 0$ and $ord(c_4) > 0$.

1.6.2 Tamagawa Numbers

We are now interested by the behavior of each point $P \in E(K)$ when reducing E/K at a prime $\mathfrak{p}$ of $\mathcal{O}_K$.

Definition 1.6.3. *Let E/K be an elliptic curve given by a minimal Weierstrass equation over the local field K. For $n \in \mathbb{Z}$ we define*

$$E_n(K) = \{P = (x, y) \in E(K) \mid ord(x) \leq -2n\} \cup \{O\}. \tag{1.37}$$

When fixing an upper bound μ for $-2n$ as defined below, the next proposition proves that $E_n(K)$ is a group using addition formulas on x-coordinates of points $P, Q \in E(K)$ (see Chapter 4, Prop 4.9 in [SZ03]).

Definition 1.6.4. *The upper bound μ is defined to be the quantity*

$$\mu := min\{ord(b_2), \frac{1}{2}ord(b_4), \frac{1}{3}ord(b_6), \frac{1}{4}ord(b_8)\}. \tag{1.38}$$

Proposition 1.6.2. *(Lutz' lemma)*
Let $n \in \mathbb{Z}$ with $-2n < \mu$. For $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ we have

(a) if $P \in E_n(K)$ then $2P \in E_n(K)$.

(b) if $P, Q \in E_n(K)$ then $ord(x_{P\pm Q}) \leq max\{ord(x_P), ord(x_Q)\}$.

By considering the group of non-singular points on the reduced curve mod $\mathfrak{p}$, we introduce the Tamagawa number at $\mathfrak{p}$.

Proposition 1.6.3. *(see Chapter 4, Prop 4.10 in [SZ03])*
Let E/K be an elliptic curve over the local field K.

(a) We have the following inclusion of subgroups

$$E(K) \supseteq E_0(K) \supseteq E_1(K) \supseteq ... \supseteq E_{n-1}(K) \supseteq E_n(K) \supseteq ... \supseteq \{O\}. \tag{1.39}$$

(b) There is an exact sequence of abelian groups

$$0 \to E_1(K) \to E_0(K) \to \tilde{E}_{ns}(\mathbb{F}_\mathfrak{p}) \to 0, \tag{1.40}$$

where $\tilde{E}_{ns}(\mathbb{F}_\mathfrak{p})$ denotes the group of non-singular points on the curve reduced mod $\mathfrak{p}$.

In particular, for $n = 0, 1$, this gives an alternative definition to $E_n(K)$ (see p. 188 in [Sil09]).

$$E_0(K) = \{P \in E(K) \mid \tilde{P} \in \tilde{E}_{ns}(\mathbb{F}_\mathfrak{p})\}. \tag{1.41}$$

$$E_1(K) = \{P \in E(K) \mid \tilde{P} = \tilde{O}\}. \tag{1.42}$$

Definition 1.6.5. *The Tamagawa number at* $\mathfrak{p}$ *is defined to be*

$$c_{\mathfrak{p}} := [E(K) : E_0(K)]. \tag{1.43}$$

One can compute it using the following theorem (Tate algorithm).

Theorem 1.6.2. *Let* E/K *be an elliptic curve over the local field* K*.*

$$c_{\mathfrak{p}} = \begin{cases} 1 \quad if\ E\ has\ good\ reduction\ at\ \mathfrak{p}; \\ -ord(j) \quad if\ E\ has\ multiplicative\ reduction\ at\ \mathfrak{p}; \\ \leq 4 \quad if\ E\ has\ additive\ reduction\ at\ \mathfrak{p}. \end{cases} \tag{1.44}$$

Remark 1.6.2. *If* E *has additive reduction at* $\mathfrak{p}$*, we refer to Table 15.1 p. 448 in [Sil09], which lists the nature of* $E(K)/E_0(K)$ *with respect to* $ord_{\mathfrak{p}}(j)$ *and hence provide* $c_{\mathfrak{p}}$*.*

Chapter 2

L-functions of elliptic curves

2.1 Introduction

This second chapter introduces the notion of L-function of elliptic curves.

We first define this notion for elliptic curves over $\mathbb{Q}$. Later, we extend the definition to elliptic curves over number fields.

Concentrating on the general case of number fields, we note that such L-functions can be expressed as a product of L-functions over $\mathbb{Q}$ twisted by Artin representations. In order to produce such a factorization for our computations, we explore the specific case of $K = \mathbb{Q}(\sqrt[3]{m})$ by looking at its Galois closure $M = \mathbb{Q}(\sqrt[3]{m}, \sqrt{-3})$ and work with the representations of $Gal(M/\mathbb{Q})$ acting on the roots of $x^3 - m$.

2.2 Definitions

Definition 2.2.1. *Let E be an elliptic curve over $\mathbb{Q}$ given by a globally minimal Weierstrass equation and consider its associated discriminant Δ. Let $p \in \mathbb{Z}$ be prime. When E has good reduction at p, define $a_p = p + 1 - N_p$, where N_p is the number of points of E over $\mathbb{F}_p$.*
If E has bad reduction at p, define

$$\epsilon(p) = \begin{cases} 1 & if\ E \text{ has split multiplicative reduction at } p; \\ -1 & if\ E \text{ has non split multiplicative reduction at } p; \\ 0 & if\ E \text{ has additive reductive at } p. \end{cases}$$

By Hasse's theorem we have that $a_p \leq 2\sqrt{p}$ (see Chapter V, Theorem 1.1 in [Sil09]). This upper-bound allows the definition of the L-function of $E/\mathbb{Q}$ for $\Re(s) > 3/2$

$$L(E, s) = \prod_{p|\Delta} \frac{1}{1 - \epsilon(p)p^{-s}} \prod_{p\nmid\Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \tag{2.1}$$

For elliptic curves over $\mathbb{Q}$, it has been proved (Taylor, Wiles) that $L(E/\mathbb{Q}, s)$ has an analytic continuation to the complex plane with a functional equation.

We use the following definition and theorem to provide a reformulation of (2.1) where we factor $1 - a_p p^{-s} + p^{1-2s}$. For an elliptic curve over $\mathbb{Q}$, we use this reformulation to construct its L-function over a number field K as shown in (2.9) below.

Definition 2.2.2. *Let $p \in \mathbb{Z}$ be a prime. Consider $E/\mathbb{F}_p$, an elliptic curve over the finite field of p elements $\mathbb{F}_p$.*

The p-Frobenius endormorphism $\phi_p : E \to E$ is given by

$$\phi_p(x, y) = (x^p, y^p)$$

and

$$\phi_p(O) = O$$

Theorem 2.2.1. *(see Chapter 3, Theorem 3.2. in [SZ03])*

Let $E/\mathbb{F}_p$ be an elliptic curve and ϕ_p the p-Frobenius endomorphism.

(a) Let $P \in E(\bar{\mathbb{F}}_p)$. Then $P \in E(\mathbb{F}_p) \iff \phi_p(P) = P$.

(b) For all $P \in E(\bar{\mathbb{F}}_p)$, ϕ_p satisfies the following equation

$$\phi_p^2(P) - a_p\phi_p(P) + pP = O, \tag{2.2}$$

where a_p is called the trace of the p-Frobenius endomorphism, and

$$a_p = 1 + p - N_p, \tag{2.3}$$

with $N_p = \#E(\mathbb{F}_p)$.

Moreover, let $n \in \mathbb{N}$ and let $\alpha_p, \beta_p \in \mathbb{C}$ be the roots of $T^2 - a_pT + p$, we have (see Chapter V, Theorem 2.3.1. in [Sil09])

$$\#E(\mathbb{F}_{p^n}) = p^n + 1 - (\alpha_p^n + \beta_p^n) \ \text{ and } \ p^n = \alpha_p^n\beta_p^n. \tag{2.4}$$

Remark 2.2.1. *We can also re-write (2.1) as*

$$L(E,s) = \prod_{p|\Delta} \frac{1}{1-\epsilon(p)p^{-s}} \prod_{p\nmid\Delta} \frac{1}{(1-\frac{\alpha_p}{p^s})(1-\frac{\beta_p}{p^s})} \tag{2.5}$$

We now extend the definition of L-functions to elliptic curves over number fields.

Definition 2.2.3. *Let $E/\mathbb{Q}$ be an elliptic curve.*

Consider a number field K, and let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$ above p with norm $N(\mathfrak{p}) = p^f$, where $f = [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p]$.

Let $N_\mathfrak{p}$ be the number of points of $E(\mathbb{F}_\mathfrak{p})$.

For $\Re(s) > 3/2$, the L-function of E/K is defined as

$$L(E/K,s) = \prod_{\mathfrak{p}\subset\mathcal{O}_K} L_\mathfrak{p}(E,s)^{-1}, \tag{2.6}$$

where

$$L_\mathfrak{p}(E,s) = \begin{cases} 1 - a_\mathfrak{p} N(\mathfrak{p})^{-s} + N(\mathfrak{p})^{1-2s} & if\ E\ has\ good\ reduction\ at\ \mathfrak{p}; \\ 1 - \epsilon_\mathfrak{p} N(\mathfrak{p})^{-s} & otherwise. \end{cases} \tag{2.7}$$

and

$a_\mathfrak{p} = N(\mathfrak{p}) + 1 - N_\mathfrak{p} = p^f + 1 - \#E(\mathbb{F}_{p^f})$.

$$\epsilon(\mathfrak{p}) = \begin{cases} 1 & if\ E\ has\ split\ multiplicative\ reduction\ at\ \mathfrak{p}; \\ -1 & if\ E\ has\ non\ split\ multiplicative\ reduction\ at\ \mathfrak{p}; \\ 0 & if\ E\ has\ additive\ reductive\ at\ \mathfrak{p}. \end{cases}$$

Recall that from (2.4) we have the following expression of $a_\mathfrak{p}$ in terms of α_p and β_p as in (2.5)

$$a_\mathfrak{p} = \alpha_p^f + \beta_p^f. \tag{2.8}$$

Therefore (2.7) becomes

$$L_{\mathfrak{p}}(E,s) = \begin{cases} \big(1-\frac{\alpha_p^f}{p^{fs}}\big)\big(1-\frac{\beta_p^f}{p^{fs}}\big) & if\ E\ has\ good\ reduction\ at\ \mathfrak{p}; \\ \big(1-\frac{\epsilon_{\mathfrak{p}}}{p^{fs}}\big) & otherwise. \end{cases} \tag{2.9}$$

which provide a construction of $L(E/K,s)$ from $L(E/\mathbb{Q},s)$.

The L-function of E/K has been conjectured to have an analytic continuation to the entire complex plane and to satisfy a functional equation (see Conjecture 16.1 in [Sil09]).

2.3 Dedekind Zeta-functions, Artin L-functions and representations

In our computations using the Birch and Swinnerton-Dyer conjecture, we are interested in expressing $L(E/K,s)$ as a product of twisted L-functions of $E/\mathbb{Q}$.

In this section, we recall some theory on Dedekind Zeta-functions of number fields, Artin L-functions and representations in order to provide such factorization.

First we define the Dedekind zeta-function of a number field K.

Let K be a number field and $\mathfrak{a}$ an integral ideal with prime decomposition

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}}, v_{\mathfrak{p}} \geq 0, v_{\mathfrak{p}} = 0 \quad for\ almost\ all\ \mathfrak{p}. \tag{2.10}$$

Let $N(\mathfrak{a}) = N_{K/\mathbb{Q}}(\mathfrak{a})$.

Definition 2.3.1. *The Dedekind zeta-function $\zeta_K(s)$ is defined as*

$$\zeta_K(s) = \sum_{\mathfrak{a}\neq 0} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \big(1 - \frac{1}{N(\mathfrak{p})^s}\big)^{-1}, \tag{2.11}$$

where $s \in \mathbb{C}, \Re(s) > 1$.

In a more general sense, we introduce the notion of L-function of normal extensions of $\mathbb{Q}$ associated to a representation of their Galois group. Such L-functions are called Artin L-functions.

Suppose that M is a finite, normal extension of $\mathbb{Q}$ of degree n.
Let G be its Galois group, i.e. $G = Gal(M/\mathbb{Q})$, and let $\{\rho_M\} : G \to GL_d(\mathbb{C})$ be a representation of G.
Let $\alpha \in G$, we define the character $\chi(\alpha)$ of degree d attached to ρ_M to be the trace of $\rho_M(\alpha)$. In particular, $\chi(\alpha)$ depends only on the conjugacy class of α.

Let $\mathfrak{p}$ be a prime in $\mathcal{O}_M$ lying above $p \in \mathbb{Z}$. Let $Frob_{\mathfrak{p}/p} \in G$ denote the Frobenius automorphism of $M/\mathbb{Q}$ relative to $\mathfrak{p}$ and denote by $I_{\mathfrak{p}}$ the inertia group at $\mathfrak{p}$.

Definition 2.3.2. *Let $\rho_M : G \to GL(V)$, where V is a complex vector space of dimension d, be a representation of G with associated character χ. We define the Artin L-function of $M/\mathbb{Q}$ relative to χ to be*

$$L(s,\chi) = L(s,\chi,M/\mathbb{Q}) = \prod_{p\in\mathbb{Z}} det\big(I - \rho_M(Frob_{\mathfrak{p}/p})|_{V^{I_{\mathfrak{p}}}} p^{-s}\big)^{-1} \tag{2.12}$$

Hence each local factor of $L(s,\chi)$ is defined by the characteristic polynomial of $\rho_M(Frob_{\mathfrak{p}/p})$ evaluated at p^{-s}, where ρ_M is restricted to the subspace of V on which $\rho_M(I_{\mathfrak{p}})$ acts as the identity, denoted $V^{I_{\mathfrak{p}}}$.

As it will be used later for the factorization of $L(E/K, s)$, we introduce the notion of Artin L-function twisted by a representation:

Proposition 2.3.1. *Let ρ_1, ρ_2 be two representations of G as above with respective characters χ_1,χ_2. Then $\rho_1 \otimes \rho_2$ is another representation of G with character ψ say. Let $\alpha \in G$, we have (see Chapter 4, Theorem 4.1 in [Isa76]):*

$$\psi(\alpha) = \chi_1(\alpha)\chi_2(\alpha)$$

Definition 2.3.3. *The Rankin L-function or Rankin convolution L-function attached to two representations ρ_1, ρ_2 with respective characters χ_1, χ_2 is $L(s, \rho_1 \otimes \rho_2)$. By proposition 2.3.1. above we have : $L(s, \rho_1 \otimes \rho_2) = L(s, \chi_1\chi_2)$.*
The literature sometimes refers to this convolution as a twist of $L(s, \chi_1)$ by the character χ_2.

2.3.1 Properties of Artin L-functions and representations

We present some properties of Artin L-functions and representations to be used later on.

Definition 2.3.4. *(a) Let $\{\rho_M(\alpha)\}_{\alpha\in G}$ and $\{\rho'_M(\alpha)\}_{\alpha\in G}$ be two representations.*

If there exists a non-singular matrix P such that

$$P\rho_M(\alpha)P^{-1} = \rho'_M(\alpha) \quad \forall\alpha \in G,$$

then these representations are equivalent

.

(b) If $\{\rho_M(\alpha)\}_{\alpha\in G}$ *is equivalent to* $\{\rho'_M(\alpha)\}_{\alpha\in G}$ *such that*

$$\{\rho'_M(\alpha)\}_{\alpha\in G} = \begin{pmatrix} \rho^1_M(\alpha) & 0 \\ 0 & \rho^2_M(\alpha) \end{pmatrix} \forall \alpha \in G,$$

where $\{\rho^1_M(\alpha)\}_{\alpha\in G}$ *and* $\{\rho^2_M(\alpha)\}_{\alpha\in G}$ *are representations of* G*, then* $\{\rho_M(\alpha)\}_{\alpha\in G}$ *is reducible.*

If χ *is the character of an irreducible representation, it is said to be simple.*

Proposition 2.3.2. *(see Chapter 8.3 in [CF10]).*

Recall that M *is a finite, normal extension of* $\mathbb{Q}$ *of degree* n*.*

(a) The character associated to the trivial representation

$$\mathbb{I} : G \to \mathbb{C}^* \quad s.t. \quad g \mapsto 1 \quad for\ all\ g \in G, \tag{2.13}$$

is called principal and the following holds

$$\sum_{\alpha\in G} \chi(\alpha) = \begin{cases} n & if\ \chi\ is\ principal; \\ 0 & otherwise. \end{cases} \tag{2.14}$$

(b) The number g *of simple characters is equal to the number of conjugacy classes in* G *and if* $\chi_1, \chi_2, ..., \chi_g$ *are the simple characters of* G *then*

$$\sum_{i=1}^{g} \chi_i(\alpha)\overline{\chi_i}(\alpha') = \begin{cases} n/l_\alpha & if\ \alpha' \in <\alpha>; \\ 0 & otherwise. \end{cases} \tag{2.15}$$

where l_α *is the number of elements in the conjugacy class* $<\alpha>$ *of* α*.*

In particular, if we take $\alpha' = \alpha = 1$ we have

$$\sum_{i=1}^{g} d_i^2 = n \tag{2.16}$$

where d_i is the degree of χ_i.

When $M/\mathbb{Q}$ has intermediate fields, their Artin L-functions have the following properties.

Proposition 2.3.3. *(see Chapter 8.3 in [CF10]).*

(a) Let $\mathbb{Q} \subset K \subset M$ be a tower of finite extensions. Let $H = Gal(M/K)$ and suppose that $G = \sum_i H\alpha_i$ is a partition of G into cosets of H.

To each character χ of H corresponds an induced character χ^* of G, given by

$$\chi^*(\alpha) = \sum_{\substack{i \\ \alpha_i \alpha \alpha_i^{-1} \in H}} \chi(\alpha_i \alpha \alpha_i^{-1}), \quad \alpha \in G \tag{2.17}$$

and

$$L(s, \chi^*, M/\mathbb{Q}) = L(s, \chi, M/K). \tag{2.18}$$

(b) Suppose that $\mathbb{Q} \subset F \subset M$ is a tower of finite extensions such that F is normal over $\mathbb{Q}$. Let $H = Gal(M/F)$, then $G/H = Gal(F/\mathbb{Q})$.

If χ is a character of G/H, it can also be consider as a character of G and

$$L(s, \chi, M/\mathbb{Q}) = L(s, \chi, F/\mathbb{Q}) \tag{2.19}$$

(c) Suppose that $\chi = \chi_1 + \chi_2$ is not simple. Then $L(s, \chi) = L(s, \chi_1)L(s, \chi_2)$.

We summarize these properties by the following example for $M/\mathbb{Q}$, a finite, normal extension of $\mathbb{Q}$ of degree n.

Consider a general character χ and its associated Artin L-function, $L(s, \chi, M/\mathbb{Q})$. By proposition 2.3.2.c. above, if we let

$$\chi = \sum_{i=1}^{g} m_i \chi_i \quad with\ m_i \in \mathbb{Z}, \tag{2.20}$$

where χ_i are simple characters, it suffices to work with $L(s, \chi_i, M/\mathbb{Q})$ and form a product.

Moreover, by propositions 2.3.2.a. and 2.3.2.b., one can express $L(s, \chi, M/\mathbb{Q})$ as a product of Artin L-function corresponding to subfields of M fixed by subgoups of G. More precisely, if we let H be any subgroup of G and $\psi_{j,1\leq j\leq g}$ be its simple characters, we can consider ψ_j^*, their induced characters of G as defined in (2.17).

Keeping notations used in (2.20), there exist $r_i \in \mathbb{Z}$ such that (see Chapter VIII,3,V(ii) in [CF10])

$$\psi_j^*(\alpha) = \sum_{i=1}^{g} r_i \chi_i(\alpha) \quad \forall \alpha \in G \tag{2.21}$$

and if $F \subseteq M$ is the subfield of M fixed by H, by proposition 2.3.2.a. we have

$$L(s, \psi_j^*, M/\mathbb{Q}) = L(s, \psi_j, M/F). \tag{2.22}$$

2.3.2 Factorization of $L(E/K, s)$

We wish to provide a factorization for $L(E/K, s)$ as a product of twisted L-functions of $E/\mathbb{Q}$ as above. This can be achieved using Artin's formalism as presented on p. 3 in [Dok05] as follows:

Suppose that $K/\mathbb{Q}$ is a finite Galois extension. Then the Dedekind zeta-function of K can be factored as the following product

$$\zeta_K(s) = \prod_{\sigma} L(\sigma, s)^{dim(\sigma)} \tag{2.23}$$

where $L(\sigma, s)$ are Artin L-functions and the product ranges over irreducible representations of $Gal(K/\mathbb{Q})$.
Similarly, if $E/\mathbb{Q}$ is an elliptic curve, one has the product formula for L-functions

$$L(E/K, s) = \prod_{\sigma} L(E, \sigma, s)^{dim(\sigma)} \tag{2.24}$$

where the product ranges over irreducible representations of $Gal(K/\mathbb{Q})$ and $L(E, \sigma, s)$ is the L-function of E twisted by the Artin representation σ.

In particular, for our specific case of $K = \mathbb{Q}(\sqrt[3]{m})$ with galois closure $M = \mathbb{Q}(\sqrt[3]{m}, \sqrt{-3})$ we have (see p. 308 in [Dok05])

$$L(E/K, s) = L(E, \sigma, s), \tag{2.25}$$

where σ is the representation obtained by inducing the trivial representation of $Gal(\bar{\mathbb{Q}}/\mathbb{Q}(\sqrt[3]{m}))$ to $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$. This is a permutation representation of degree 3 which factors through $Gal(M/\mathbb{Q})$. It coincides with the representation of $Gal(M/\mathbb{Q})$ acting on the roots of $x^3 - m$.

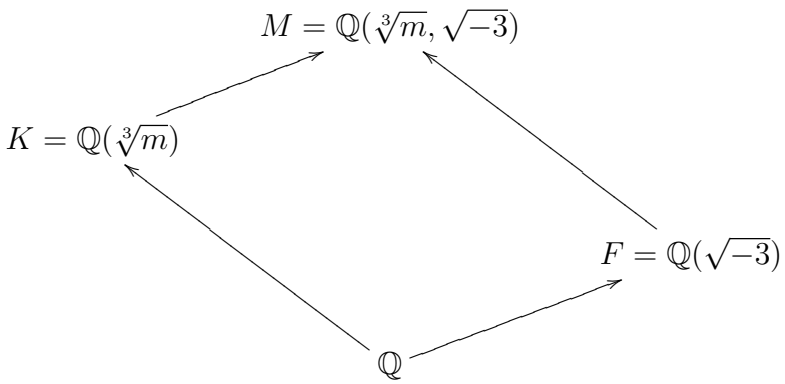
2.3.3 Non-abelian cubic extensions

Let $K = \mathbb{Q}(\sqrt[3]{m})$ with Galois closure $M = \mathbb{Q}(\sqrt[3]{m}, \sqrt{-3})$.

In order to provide a factorization of $L(E/K, s)$, this section will study the representation of $Gal(M/\mathbb{Q})$ acting on the roots of $x^3 - m$.

We conclude by looking at the intermediate fields of $M/\mathbb{Q}$ and use the properties of Artin L-functions developed above.

Consider our setup :



We let $\rho = \frac{-1+\sqrt{-3}}{2}$ be the primitive third root of unity and denote $\alpha_1 = \rho\sqrt[3]{m}$, $\alpha_2 = \rho^2\sqrt[3]{m}$ and $\alpha_3 = \sqrt[3]{m}$ the roots of $x^3 - m$. $Gal(M/\mathbb{Q})$ is then isomorphic to the permutation group S_3 with complex conjugation corresponding to the permutation (1,2) which permutes α_1 and α_2 and fixes α_3 and with multiplication by ρ corresponding to (1,2,3) sending α_1 to α_2, α_2 to α_3 and α_3 to α_1.

Using this isomorphism, we express $Gal(M/\mathbb{Q})$ as follows

$$Gal(M/\mathbb{Q}) \simeq S_3 = \{e, (1,2,3), (3,2,1), (1,2), (2,3), (3,1)\},$$

where e is the identity element of the group.

S_3 has 3 conjugacy classes : $< e >, < (1,2,3,) >= \{(1,2,3), (3,2,1)\}$,

$< (1,2) >= \{(1,2), (2,3), (3,1)\}$.

By proposition 2.3.1.b., we have 3 simple characters

(a) χ_0 of degree d_0

(b) χ_1 of degree d_1

(c) χ_2 of degree d_2

By (2.16) we have $d_0^2 + d_1^2 + d_2^2 = 6$. Moreover $d_0 = 1$ as χ_0 is the trivial character and $d_1 = 1$ as $\chi_1(m) = \left(\frac{-3}{m}\right)$ is a Dirichlet character. Therefore we must have $d_2 = 2$. We have the following character's table:

Table 2.1: Character's table for $Gal(M/\mathbb{Q})$

	χ_0	χ_1	χ_2
$< e >$	1	1	2
$< (1,2,3) >$	1	1	-1
$< (1,2) >$	1	-1	0

As K is fixed by H_1, we consider its induced characters on G. It has 2 conjugacy classes, hence 2 simple characters ψ_3, ψ_4, where ψ_3 is the trivial character. Using (2.17) we produce the following induced characters of G:

Table 2.2: Induced character's table for $Gal(M/\mathbb{Q})$

	ψ_3^*	ψ_4^*
$< e >$	3	3
$< (1,2,3) >$	0	0
$< (1,2) >$	1	-1

From table 2.1. we conclude that $\psi_3^* = \chi_0 + \chi_2$.

Moreover by (2.18) we have

$$\zeta_K(s) = L(s, \psi_3, M/K) = L(s, \psi_3^*, M/\mathbb{Q}) \tag{2.26}$$

Hence by proposition 2.3.2.c. we obtain

$$\zeta_K(s) = L(s, \psi_3^*, M/\mathbb{Q}) = L(s, \chi_0, M/\mathbb{Q})L(s, \chi_2, M/\mathbb{Q}) \tag{2.27}$$

From which we conclude on the factorization of $L(E/K, s)$

$$L(E/K, s) = L(E/\mathbb{Q}, s)L(E/\mathbb{Q}, \chi_2, s), \tag{2.28}$$

We use this factorization of $L(E/K, s)$ for the computations shown in chapter 4.

Chapter 3

The Birch and Swinnerton-Dyer Conjecture

3.1 Introduction

First, we state the Birch and Swinnerton-Dyer conjecture for elliptic curves in its general version and deduce its consequences for elliptic curves $E/\mathbb{Q}$ and E/K where K is a pure cubic extension.

Then, we develop the necessary theory to numerically compute features involved in the conjecture and present the quotient that will be computed in chapter 4.

3.2 Presentation of the conjecture

Let K be a number field and let E/K be an elliptic curve.

So far we have presented invariants relative to E/K and $E/\mathbb{C}$ in addition to the L-functions associated to E/K. The following conjecture supports the idea that $L(E/K, s)$ encodes information on E/K in a most precise way.

Conjecture 2. *(Birch and Swinnerton-Dyer)*

(a) The L-function $L(E/K, s)$ has an analytic continuation to $s = 1$, and

$$ord_{s=1} L(E/K, s) = rank\ of\ E(K). \tag{3.1}$$

(b) The leading coefficient in the Taylor expansion of $L(E/K, s)$ at $s = 1$ is equal to

$$\frac{|Ш(E/K)| R_{E/K} C(E/K) \Omega}{|E(K)_{tors}|^2 \sqrt{|\Delta_K|}}, \tag{3.2}$$

where

- $Ш(E/K)$ *is the Shafarevich-Tate group of* E/K.
- $R_{E/K}$ *is the regulator of* E/K.
- $C(E/K) = \prod_{\mathfrak{p} \subset \mathcal{O}_K} c_{\mathfrak{p}}$ *is the product of Tamagawa Numbers.*
- Ω *represents a product involving periods of* E, ω_+, ω_-
- $E(K)_{tors}$ *is the subgroup of torsion points of* $E(K)$.
- Δ_K *is the discriminant of the field* K.

Remark 3.2.1. *From section 2.3.3., we were able to conclude that* $L(E/K,s) = L(E/\mathbb{Q},s)L(E/\mathbb{Q},\chi_2,s)$. *Therefore, as developed precisely in 3.3.4. below, the leading term of* $L(E/K,s)$ *in the Taylor expansion at* $s=1$, *has the leading term of* $L(E/\mathbb{Q},s)$ *at* $s=1$ *as a factor.*

Conjecture 2.a. has been proved in the case where $K=\mathbb{Q}$ *and the rank of* $E(\mathbb{Q})=0,1$ *(more details on the status of the conjecture can be found p. 452 in [Sil09]). In the case where* $rk(E(\mathbb{Q}))\neq 0,1$, *the conjecture is as follows*

Conjecture 3. *(Birch and Swinnerton-Dyer)*

(a) The L-function $L(E/\mathbb{Q},s)$ *has a zero at* $s=1$ *of order equal to the rank of* $E(\mathbb{Q})$.

(b) The leading coefficient in the Taylor expansion of $L(E/K,s)$ *at* $s=1$ *is equal to*

$$\frac{|Ш(E/\mathbb{Q})|R_{E/\mathbb{Q}}C(E/\mathbb{Q})\omega}{|E(\mathbb{Q})_{tors}|^2}, \tag{3.3}$$

where $\omega=\omega_+$ if $\Delta_E>0$ and $\omega=2\omega_+$ otherwise (see p 30 in [Cre97]).

3.3 Computations over pure cubic extensions of $\mathbb{Q}$

We are interested to analyse numerically Conjecture 2.b. in the context of $K=\mathbb{Q}(\sqrt[3]{m})$.

The next sections will detail the computations of several features needed to proceed with our computations.

3.3.1 Computing the Regulator $R_{E/K}$

Let us recall that by definition, for a given elliptic curve E/K, we have

$$R_{E/K} = det(< P_i, P_j >)_{1 \leq i \leq r \ , \ 1 \leq j \leq r},$$

where $P_1, P_2, ..., P_r \in E(K)$ generates $E(K)/E(K)_{tors}$.

Case 1 : $E(K)$ is of rank 1, generated by a point P, we have

$$\begin{aligned} R_{E/K} &= det(< P, P >) \\ &= det(\frac{1}{2}(\hat{h}(P+P) - \hat{h}(P) - \hat{h}(P)) \\ &= det(\frac{1}{2}(\hat{h}(2P) - 2\hat{h}(P)) \\ &= det(\frac{1}{2}(4\hat{h}(P) - 2\hat{h}(P)) \\ &= det(\hat{h}(P)) \\ &= \hat{h}(P) \end{aligned}$$

Case 2 : $E(K)$ is of rank 2, generated by points P and Q, we have

$$R_{E/K} = det \begin{pmatrix} < P, P > & < P, Q > \\ < Q, P > & < Q, Q > \end{pmatrix},$$

where $< P, Q >= \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q))$.

Therefore, the regulator can be computed given the canonical height of the generators of $E(K)$. It is computable using tools such as SAGE or MAGMA provided that these generators are given.

In order for this to happen, we followed the work of Kisilevsky (see p13 in [Kis12]). Indeed, for specific elliptic curves $E/\mathbb{Q}$, this paper provides a way of producing a pair consisting on a pure cubic extension K and a point on $E(K)$. This process is described below.

Let $E/\mathbb{Q}$ be an elliptic curve. If E has a 3-torsion point rational over $\mathbb{Q}$, then E can be given by the following Weierstrass equation

$$E : y^2 + 3uxy + ty = x^3 \tag{3.4}$$

with $u, t \in \mathbb{Q}$.
Moreover, for each $r \in \mathbb{Q}$, $E(K_r)$ admits a point P of infinite order over $K_r = \mathbb{Q}(\sqrt[3]{m})$ where m and $P = (x, y)$ are parametrized by r in the following way

$$m = \frac{2(r+1)(r-1)^2}{tr - t + 2u^3} \tag{3.5}$$

$$x = -\frac{2(r - 1 - um^{1/3})}{m^{2/3}} \tag{3.6}$$

$$y = \frac{4u^3 - t(r-1)^2}{r^2 - 1} - 3ux \tag{3.7}$$

Given an elliptic curve $E/\mathbb{Q}$ satisfying the conditions above, we use the height function of MAGMA to compute R_{E/K_r} for each given r, u and t.

Remark 3.3.1. *MAGMA's height function computes the canonical height $\hat{h}(P)$ of a point P.*

As mentioned p. 106 in [Kna92] and p. 419 in [Bou66], the regulator involved in the Birch and Swinnerton-Dyer conjecture is computed from of the height relative to the field over which the Mordell-Weil group is considered.

Recall that by (1.29) we have

$$h(P) = \frac{1}{[K:\mathbb{Q}]} h_K(P)$$

Therefore we need to consider the following inner product to compute the regulator.

$$\begin{aligned} < P, Q >_K &= \frac{1}{2}(\hat{h}_K(P+Q) - \hat{h}_K(P) - \hat{h}_K(Q)) \\ &= \frac{1}{2}([K:\mathbb{Q}]\hat{h}(P+Q) - [K:\mathbb{Q}]\hat{h}(P) - [K:\mathbb{Q}]\hat{h}(Q)). \end{aligned}$$

3.3.2 Computing the Tamagawa product $C(E/K)$

For a given elliptic curve $E/\mathbb{Q}$, we wish to compute

$$C(E/K) = \prod_{\mathfrak{p} \subset \mathcal{O}_K} c_{\mathfrak{p}} \tag{3.8}$$

for $K = \mathbb{Q}(\sqrt[3]{m})$.

We first note that for $\mathfrak{p}$ in $\mathcal{O}_K$ where E has good reduction, by definition, $c_{\mathfrak{p}} = 1$. Moreover, by proposition 1.6.1.a., we know that such primes are those $\mathfrak{p}$ in $\mathcal{O}_K$ above $p \in \mathbb{Q}$ not dividing the discriminant Δ of E.

Hence we can reduce the above product to the following :

$$C(E/K) = \prod_{\mathfrak{p} | \Delta} c_{\mathfrak{p}} \tag{3.9}$$

For each $p \in \mathbb{Q}$ dividing Δ we consider its splitting in K using the following theorem (see Theorem 6.4.3 in [Coh93]).

Theorem 3.3.1. *Let $K = \mathbb{Q}(\sqrt[3]{m})$ be a pure cubic field, where m is cube free and not equal to ± 1.*
Write $m = ab^2$ with a, b square free and coprime. Let θ be the cube root of m belonging to K. Then

(a) if $a^2 \not\equiv b^2 \pmod 9$ then

$$(1, \theta, \frac{\theta^2}{b}) \tag{3.10}$$

is an integral basis of K and the discriminant of K, $\Delta_K = -27a^2b^2$.

(b) if $a^2 \equiv b^2 \pmod 9$ then

$$(1, \theta, \frac{\theta^2 + ab^2\theta + b^2}{3b}) \tag{3.11}$$

is an integral basis of K and the discriminant of K, $\Delta_K = -3a^2b^2$.

In the case of p not dividing the index $[\mathbb{Z}_K : \mathbb{Z}[\theta]] = b$ or $3b$, which will always be our case, the decomposition of $p\mathbb{Z}_K$ follows that of $X^3 - m$ modulo p, which is detailed in the next proposition.

Proposition 3.3.1. *Let p be a prime not dividing m. The decomposition of $X^3 - m$ modulo p is as follows*

(a) if $p \equiv 2 \pmod 3$, then $X^3 - m \equiv (X - u)(X^2 - vX + w) \pmod p$.

(b) if $p \equiv 1 \pmod 3$ and $m^{(p-1)/3} \equiv 1 \pmod p$ then $X^3 - m \equiv (X - u_1)(X - u_2)(X - u_3) \pmod p$.

(c) if $p \equiv 1 \pmod 3$ and $m^{(p-1)/3} \not\equiv 1 \pmod p$ then $X^3 - m$ is irreducible (mod p).

(d) if $p = 3$, then $X^3 - m \equiv (X - a)^3 \pmod p$.

Finally, letting $p\mathbb{Z}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\mathfrak{p}_3^{e_3}$, with $e_i = 0, 1, 2$ *or* 3 for $i = 1, 2, 3$, we have the product of Tamagawa numbers:

$$C(E/K) = \prod_{p|\Delta} c_{\mathfrak{p}_1}^{e_1} c_{\mathfrak{p}_2}^{e_2} c_{\mathfrak{p}_3}^{e_3}, \tag{3.12}$$

where each $c_{\mathfrak{p}_i}$, $i = 1, 2, 3$ is given by Theorem 1.6.2. and Remark 1.6.2.

3.3.3 Computing the product of periods Ω

For elliptic curves over $\mathbb{Q}$, the Birch and Swinnerton-Dyer conjecture is stated explicitely, fixing the periods (ω as denoted earlier) involved in the leading term of the Taylor expansion of $L(E/\mathbb{Q}, s)$ at $s = 1$ (see p. 452 in [Sil09]) .

The case of number fields is more involved as the conjecture is derived from a general conjecture for abelian varieties made by Tate (see p. 6 in [Bou66]). We will follow the work of Dokchitser and Dokchitser in [DD05] who interpret precisely the general conjecture for elliptic curves.

For an elliptic curve $E/\mathbb{Q}$ and the Artin representation χ_2 presented in section 2.3.3, the following quotient is rational (see Introduction in [DD05]).

$$\frac{L(E,\chi_2,1)}{\omega_+^{d^+(\chi_2)} 2\omega_-^{d^-(\chi_2)}}, \tag{3.13}$$

where $d^{\pm}(\chi_2)$ denote the dimensions of the ± 1 eigenspaces of complex conjugation on χ_2.

In this case, χ_2 being of degree 2 and complex conjugation being represented as $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, we have $d^+ = 1$ and $d_- = 1$.
Combining with ω involved in (3.3) in the factorization of $L(E/K,s)$ in (2.28) we have the following expression for Ω

$$\Omega = \omega(\omega_+ 2\omega_-), \tag{3.14}$$

where ω_+, ω_- for specific elliptic curves can be found in Cremona's tables in [Cre97] or computed by means of MAGMA or SAGE functions for elliptic curves.

3.3.4 Computing the leading term of $L(E/K,s)$ at $s=1$

We first recall the result obtained in section 2.3.3. :

$$L(E/K,s) = L(E/\mathbb{Q},s)L(E/\mathbb{Q},\chi_2,s), \tag{3.15}$$

where χ_2 is a character of degree 2 associated to an Artin representation of $Gal(M/\mathbb{Q})$. In our specific case of $K = \mathbb{Q}(\sqrt[3]{m})$, the anaytic continuation of $L(E/K,s)$ has been proved in [Dok05] (Theorem 14). In our case, $r = 3$, $n = 1$.

Theorem 3.3.2. *Let E be an elliptic curve over $\mathbb{Q}$. Let ρ be an Artin representation over $\mathbb{Q}$ which factors through $Gal(\mathbb{Q}(\sqrt[r^n]{m}, \mu_{r^n})/\mathbb{Q})$ for some $n \geq 0$. Then $L(E, \rho, s)$ has analytic continuation to the complex plane.*

We can therefore express $L(E/K, s)$ as a power series around 1:

$$L(E/K, s) = \sum_{n=0}^{\infty} \frac{1}{n!} L^{(n)}(E/K, s)|_{s=1}(s-1)^n \tag{3.16}$$

Assuming Conjecture 2.a. holds, we must have $L(E/K, 1) = 0$ since we assume the rank of $E(K)$ to be at least one. Hence we can expand (3.16) as follows

$$\begin{aligned} L(E/K, s) &= L(E/K, 1) + L'(E/K, 1)(s-1) + \frac{1}{2}L''(E/K, 1)(s-1)^2 + O((s-1)^3) \\ &= L'(E/K, 1)(s-1) + \frac{1}{2}L''(E/K, 1)(s-1)^2 + O((s-1)^3), \end{aligned}$$

where $L'(E/K, 1)$ and $L''(E/K, 1)$ refer to $L'(E/K, s)$ and $L''(E/K, s)$ evaluated at $s = 1$.

Moreover, from the factorization of $L(E/K, s)$ we have

$$\begin{aligned} L(E/K, s) &= L(E/\mathbb{Q}, s)L(E/\mathbb{Q}, \chi_2, s) \\ &= \big[L(E/\mathbb{Q}, 1) + L'(E/\mathbb{Q}, 1)(s-1) + O((s-1)^2)\big]\big[L(E/\mathbb{Q}, \chi_2, 1) + \\ &L'(E/\mathbb{Q}, \chi_2, 1)(s-1) + O((s-1)^2)\big] \\ &= L(E/\mathbb{Q}, 1)L(E/\mathbb{Q}, \chi_2, 1) + L(E/\mathbb{Q}, 1)L'(E/\mathbb{Q}, \chi_2, 1)(s-1) + \\ &L'(E/\mathbb{Q}, 1)L(E/\mathbb{Q}, \chi_2, 1)(s-1) + O((s-1)^2). \end{aligned}$$

We need to consider two cases in order to conclude.

Case 1: $rk(E(\mathbb{Q})) = 0$.

$L(E/K, 1) = 0$ and $L(E/\mathbb{Q}, 1) \neq 0$, we must have $L(E/\mathbb{Q}, \chi_2, 1) = 0$.

The above reduces then to

$$L(E/K, s) = L(E/\mathbb{Q}, 1)L'(E/\mathbb{Q}, \chi_2, 1)(s-1) + O((s-1)^2). \tag{3.17}$$

Therefore the leading term of $L(E/K, s)$ is $L'(E/K, 1) = L(E/\mathbb{Q}, 1)L'(E/\mathbb{Q}, \chi_2, 1)$.

And assuming conjecture 3.b. holds we have

$$L(E/\mathbb{Q}, 1) = \frac{|Ш(E/\mathbb{Q})|R_{E/\mathbb{Q}}C(E/\mathbb{Q})\omega}{|E(\mathbb{Q})_{tors}|^2} \tag{3.18}$$

Case 2: $rk(E(\mathbb{Q})) = 1$ and $rk(E(K)) = 2$.

$L(E/K, 1) = L'(E/K, 1) = 0$ and $L(E/\mathbb{Q}, 1) = 0$. We have

$$L(E/K, s) = L'(E/\mathbb{Q}, 1)(s-1)L'(E/\mathbb{Q}, \chi_2, 1)(s-1) + O((s-1)^3). \tag{3.19}$$

Therefore the leading term of $L(E/K, s)$ is $\frac{1}{2}L''(E/K, 1) = L'(E/\mathbb{Q}, 1)L'(E/\mathbb{Q}, \chi_2, 1)$.

And assuming conjecture 3.b. holds we have

$$L'(E/\mathbb{Q}, 1) = \frac{|Ш(E/\mathbb{Q})|R_{E/\mathbb{Q}}C(E/\mathbb{Q})\omega}{|E(\mathbb{Q})_{tors}|^2} \tag{3.20}$$

Chapter 4

Numerical Results

4.1 Introduction

This chapter introduces numerical results for specific elliptic curves. Computations have been achieved using MAGMA, SAGE and Maple based on the work done in different contexts by Cremona, Dokchitser T, Dokchitser V and Stein, presented in [Cre97], [DD05] and [Ste91].

We detail computations concerning curves that satisfy conditions presented in section 3.2.1., E37B3, E19A3 and E189B1 as denoted in Cremona's table ([Cre97]).
By varying our parameter r we produce several pure cubic extensions associated to each curves and present numerical results in the sections to follow.

4.2 Computations with curves admitting no point of infinite order over $\mathbb{Q}$

From section 3.3.1., we recall that for elliptic curves given by Weierstrass equations as in (3.4), we get a pair (K_r, P) consisting of a pure cubic extension K_r and a point P in $E(K_r)$.

In this section, we consider elliptic curves admitting no $\mathbb{Q}$-rational point. We therefore work in case 1 as in (3.17) and have the following leading term for the Taylor expansion of $L(E/K, s)$ at $s = 1$.

$$\begin{aligned} L'(E/K_r, 1) &= \frac{|Ш(E/K_r)|R_{E/K_r}C(E/K_r)\Omega}{|E(K_r)_{tors}|^2\sqrt{|\Delta_{K_r}|}} \\ \iff L(E/\mathbb{Q}, 1)L'(E/\mathbb{Q}, \chi_2, 1) &= \frac{|Ш(E/K_r)|R_{E/K_r}C(E/K_r)\Omega}{|E(K_r)_{tors}|^2\sqrt{|\Delta_{K_r}|}} \end{aligned}$$

Now, taking into consideration Conjecture 3.b., we further have

$$L(E/\mathbb{Q}, 1)L'(E/\mathbb{Q}, \chi_2, 1) = \frac{|Ш(E/K_r)|R_{E/K_r}C(E/K_r)\Omega}{|E(K_r)_{tors}|^2\sqrt{|\Delta_{K_r}|}} \tag{4.1}$$

$$\iff L'(E/\mathbb{Q}, \chi_2, 1) = \frac{|Ш(E/K_r)|R_{E/K_r}C(E/K_r)\Omega}{L(E/\mathbb{Q}, 1)|E(K_r)_{tors}|^2\sqrt{|\Delta_{K_r}|}} \tag{4.2}$$

$$\iff L'(E/\mathbb{Q}, \chi_2, 1) = \frac{|E(\mathbb{Q})_{tors}|^2}{|Ш(E/\mathbb{Q})|R_{E/\mathbb{Q}}C(E/\mathbb{Q})\omega}\frac{|Ш(E/K_r)|R_{E/K_r}C(E/K_r)\Omega}{|E(K_r)_{tors}|^2\sqrt{|\Delta_{K_r}|}} \tag{4.3}$$

From which we get the following quotient

$$\frac{|Ш(E/K_r)|}{|Ш(E/\mathbb{Q})|} = \frac{L'(E/\mathbb{Q}, \chi_2, 1)R_{E/\mathbb{Q}}C(E/\mathbb{Q})|E(K_r)_{tors}|^2\omega\sqrt{|\Delta_{K_r}|}}{|E(\mathbb{Q})_{tors}|^2R_{E/K_r}C(E/K_r)\Omega} \tag{4.4}$$

We will use this last equality to approximate numerically the order of the Shafarevich-Tate group of $E(K_r)$.

Remark 4.2.1. *We could have chosen to compute* $|Ш(E/K)|$ *using* $L'(E/K_r, 1)$ *directly from*

$$L'(E/K_r, 1) = \frac{|Ш(E/K_r)|R_{E/K_r}C(E/K_r)\Omega}{|E(K_r)_{tors}|^2\sqrt{|\Delta_{K_r}|}} \tag{4.5}$$

The numerical results are indeed equal.

4.2.1 E37B3

In their article [FKK12], Fearnley, Kisilevsky and Kuwata studied the curve $E37B3$ which has the following Weierstrass equation

$$E_{37} : y^2 + y = x^3 + x^2 - 3x + 1. \tag{4.6}$$

In particular, they present it in a suitable model for our computations by substituing (x, y) by $(x + 1, y + 2x)$

$$E_{37} : y^2 + 4xy + y = x^3, \tag{4.7}$$

which in view of equation (3.4) corresponds to the case $u = \frac{3}{4}$ and $t = 1$.
By (3.5) we obtain the following parametrization for

$$m = \frac{2(r + 1)(r - 1)^2}{r - 1 + 2(\frac{3}{4})^3}. \tag{4.8}$$

The next sections present tables of numerical results for $E37B3$ over different number fields K_r.

4.2.2 Invariants of $E37B3$ over $\mathbb{Q}$

Table 4.1. presents invariants of $E37B3$ and features related to $E_{37}(\mathbb{Q})$.

These results were computed with MAGMA's functions for elliptic curves and compared with Cremona's table of elliptic curves.

Table 4.1: Invariants of $E37B3$

$\Delta_{E_{37}}$	37
j-invariant	$\frac{2^{15}5^3}{37}$
ω_+	3.26556477871268752051292493462
ω_-	1.76761067023378947588132314450
ω	$2\omega_+$
c_4	$2^5 5$
c_6	$-2^3 251$

Table 4.2. summarizes invariants related to $E_{37}(\mathbb{Q})$ needed to compute (4.4). For each prime with bad reduction, we present the information needed to compute the Tamagawa product $C(E_{37}/\mathbb{Q})$ as indicated in section 3.3.2.

Table 4.2: $E_{37}(\mathbb{Q})$ invariants

$L(E_{37}/\mathbb{Q}, 1)$	0.72568106193615278234
$rank(E_{37}(\mathbb{Q}))$	0
$R_{E_{37}/\mathbb{Q}}$	1
$\lvert E_{37}(\mathbb{Q})_{tors}\rvert$	3
$\lvert Ш(E_{37}/\mathbb{Q})\rvert$	1
Primes with bad reduction	37
$ord_{37}(c_4)$	0
$ord_{37}(\Delta_{E_{37}})$	1
$-c_4c_6 \bmod 37$	9
reduction type at 37	split multiplicative
c_{37}	$-ord_{37}(j) = 1$
$C(E_{37}/\mathbb{Q})$	1

4.2.3 Invariants of $E37B3$ over $K_r = \mathbb{Q}(\sqrt[3]{m})$

Based on section 3.3.1., we will consider the set of cubic extensions $K_r = \mathbb{Q}(\sqrt[3]{m})$, where m is given by (3.5) for each given r.

Indexed by our choices of r, Table 4.3 lists the corresponding m and its associated number field K_r based on the following remark

$$\mathbb{Q}(\sqrt[3]{\frac{a}{b}}) \simeq \mathbb{Q}(\sqrt[3]{d}) \iff \frac{db}{a} \text{ is a cube in } \mathbb{Q}. \tag{4.9}$$

Each d is then decomposed as product ab^2 and following theorem 3.3.1., we compute the discriminant of each K_r.

Table 4.3: Number Fields $K_r = \mathbb{Q}(\sqrt[3]{m})$ associated to $E37B3$

r	m	$\mathbb{Q}(\sqrt[3]{d})$	$d = ab^2$	a^2 mod 9	b^2 mod 9	Discriminant (K_r)
-3	$\frac{-432}{5}$	$\mathbb{Q}(\sqrt[3]{50})$	$2 * 5^2$	4	7	$-27 * 4 * 25$
-13	$\frac{63504}{125}$	$\mathbb{Q}(\sqrt[3]{294})$	$2 * 3 * 7^2$	0	4	$-27 * 2^2 * 3^2 * 7^2$
-11	$\frac{19440}{49}$	$\mathbb{Q}(\sqrt[3]{630})$	$7 * 2 * 5 * 3^2$	7	0	$-27 * 2^2 * 7^2 * 5^2 * 3^2$
-7	$\frac{2592}{11}$	$\mathbb{Q}(\sqrt[3]{1452})$	$3 * 2^2 * 11^2$	3	7	$-27 * 11^2 * 2^2 * 3^2$
-5	$\frac{3888}{17}$	$\mathbb{Q}(\sqrt[3]{5202})$	$2 * 3^2 * 17^2$	4	0	$-27 * 2^2 * 3^2 * 17^2$
17	$\frac{15552}{35}$	$\mathbb{Q}(\sqrt[3]{11025})$	$7 * 2 * 5^2 * 3^2$	1	0	$-27 * 7^2 * 5^2 * 3^2$
3	$\frac{432}{91}$	$\mathbb{Q}(\sqrt[3]{16562})$	$2 * 7^2 * 13^2$	4	1	$-27 * 2^2 * 7^2 * 13^2$

Table 4.4 below presents the splitting of 37 in each cubic extension produced by our choices of r.

Using (3.12) we compute $C(E_{37}/K_r)$.

Table 4.4: Tamagawa Product $C(E_{37}/K_r)$

$\mathbb{Q}(\sqrt[3]{m})$	37 mod 3	$m^{\frac{37-1}{3}}$ mod 37	$37\mathbb{Z}_{K_r}$	$c_{\mathfrak{p}}$	$C(E_{37}/K_r)$
$\mathbb{Q}(\sqrt[3]{50})$	1	10	$\mathfrak{p}$	1	1
$\mathbb{Q}(\sqrt[3]{294})$	1	26	$\mathfrak{p}$	1	1
$\mathbb{Q}(\sqrt[3]{630})$	1	1	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	1	1^3
$\mathbb{Q}(\sqrt[3]{1452})$	1	26	$\mathfrak{p}$	1	1
$\mathbb{Q}(\sqrt[3]{5202})$	1	26	$\mathfrak{p}$	1	1
$\mathbb{Q}(\sqrt[3]{11025})$	1	1	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	1	1^3
$\mathbb{Q}(\sqrt[3]{16652})$	1	1	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	1	1^3

Table 4.5. presents the leading term of the Taylor expansion of $L(E/K_r, s)$ at $s = 1$ and the regulator of $E37B3$ over each K_r.

The computations were achieved with MAGMA's function for L-series and elliptic curves.

Table 4.5: Leading term of $L(E_{37}/K_r, s)$ at $s = 1$ and Regulator

$\mathbb{Q}(\sqrt[3]{m})$	$L'(E_{37}/K_r, 1)$	R_{E_{37}/K_r}
$\mathbb{Q}(\sqrt[3]{50})$	10.711163624980424230055118950 4	7.381681854
$\mathbb{Q}(\sqrt[3]{294})$	4.923420776046117395906056904 80	14.25065788
$\mathbb{Q}(\sqrt[3]{630})$	30.344665705611733728334731760 7	12.19881994
$\mathbb{Q}(\sqrt[3]{1452})$	17.787209725921766810922774957 2	8.989342374
$\mathbb{Q}(\sqrt[3]{5202})$	1.473096003669249477571929395 23	10.35499498
$\mathbb{Q}(\sqrt[3]{11025})$	1.610870908014429685508219376 51	11.65651447
$\mathbb{Q}(\sqrt[3]{16652})$	7.600807786969550404030813135 32	10.59271526

Table 4.6 recalls the composition of Ω based on section 3.3.3. and provides the order of $E_{37}(K)_{tors}$ computed with MAGMA.

Using information provided in the precedent tables, it presents the analytic order of $Ш(E_{37}/K_r)$ from the quotient

$$\frac{|Ш(E_{37}/K_r)|}{|Ш(E_{37}/\mathbb{Q})|} = \frac{L'(E_{37}/\mathbb{Q},\chi_2,1)R_{E_{37/\mathbb{Q}}}C(E_{37}/\mathbb{Q})\omega|E_{37}(K_r)_{tors}|^2\sqrt{|\Delta_{K_r}|}}{|E_{37}(\mathbb{Q})|^2 R_{E_{37/K_r}}C(E_{37}/K_r)\Omega} \tag{4.10}$$

Table 4.6: Order of the Shafarevich-Tate group of $E_{37}(K_r)$

$\mathbb{Q}(\sqrt[3]{m})$	Ω	$\lvert E_{37}(K)_{tors}\rvert$	analytic $\frac{\lvert Ш(E_{37}/K_r)\rvert}{\lvert Ш(E_{37}/\mathbb{Q})\rvert}$
$\mathbb{Q}(\sqrt[3]{50})$	$4\omega_+^2\omega_-$	3	8.99999999531197606544571
$\mathbb{Q}(\sqrt[3]{294})$	$4\omega_+^2\omega_-$	3	9.00000000397223010329010
$\mathbb{Q}(\sqrt[3]{630})$	$4\omega_+^2\omega_-$	3	324.000000143000283718443
$\mathbb{Q}(\sqrt[3]{1452})$	$4\omega_+^2\omega_-$	3	81.000000061730833043144 0
$\mathbb{Q}(\sqrt[3]{5202})$	$4\omega_+^2\omega_-$	3	9.00000000397223010329010
$\mathbb{Q}(\sqrt[3]{11025})$	$4\omega_+^2\omega_-$	3	9.000000000508128488152 34
$\mathbb{Q}(\sqrt[3]{16652})$	$4\omega_+^2\omega_-$	3	81.000000027089816891766 5

4.2.4 E19A3

We consider the elliptic curve E19A3 as denoted in Cremona's table ([Cre97]) given by the following equation

$$E_{19} := y^2 + y = x^3 + x^2 + x. \tag{4.11}$$

By substituting (x, y) by $(x, x+y)$ we obtain a suitable model for our computations

$$E_{19} := y^2 + 2xy + y = x^3. \tag{4.12}$$

From equation (3.4) we are in the case $u = \frac{2}{3}$ and $t = 1$. This leads to the following parametrization of m

$$m = \frac{2(r+1)(r-1)^2}{r - 1 + 2(\frac{2}{3})^3}. \tag{4.13}$$

Next sections present tables of numerical results for $E19A3$ over different number fields K_r.

4.2.5 Invariants of $E19A3$ over $\mathbb{Q}$

Table 4.7 presents invariants of $E19A3$ and features related to $E_{19}(\mathbb{Q})$.

These results were computed with MAGMA's functions for elliptic curves and compared with Cremona's table of elliptic curves.

Table 4.7: Invariants of $E19A3$

$\Delta_{E_{19}}$	-19
j-invariant	$-\frac{2^{15}}{19}$
ω_+	4.079279200464932432209552683 58
ω_-	2.063546195858620232337915658 16
ω	ω_+
c_4	-2^5
c_6	8

Table 4.8 summarizes invariants related to $E_{19}(\mathbb{Q})$ needed to compute (4.4). For each prime with bad reduction, we present the information needed to compute the Tamagawa product $C(E_{19}/\mathbb{Q})$ as indicated in section 3.3.2.

Table 4.8: $E_{19}(\mathbb{Q})$ invariants

$L(E_{19}/\mathbb{Q}, 1)$	0.45325324449610360358
$rank(E_{19}(\mathbb{Q}))$	0
$R_{E_{19}/\mathbb{Q}}$	1
$\lvert E_{19}(\mathbb{Q})_{tors}\rvert$	3
Primes with bad reduction	19
$ord_{19}(c_4)$	0
$ord_{19}(\Delta_{E_{19}})$	1
$-c_4c_6 \bmod 19$	9
reduction type at 19	split multiplicative
c_{19}	$-ord_{19}(j) = 1$
$C(E_{19}/\mathbb{Q})$	1
$\lvert Ш(E_{19}/\mathbb{Q})\rvert$	1

Based on section 3.3.1., we will consider the set of cubic extensions $K_r = \mathbb{Q}(\sqrt[3]{m})$, where m is given by (3.5) for each given r.

Indexed by our choices of r, Table 4.9 lists the corresponding m and its associated number field K_r. Each corresponding d is then decomposed as product ab^2 and following theorem 3.3.1., we compute the discriminant of each K_r.

Table 4.9: Number Fields $K_r = \mathbb{Q}(\sqrt[3]{m})$ associated to $E19A3$

r	m	$\mathbb{Q}(\sqrt[3]{d})$	$d = ab^2$	a^2 mod 9	b^2 mod 9	Discriminant (K_r)
-7	$\frac{2592}{25}$	$\mathbb{Q}(\sqrt[3]{60})$	$3 * 5 * 2^2$	0	4	$-27 * 2^2 * 3^2 * 5^2$
17	$\frac{3888}{7}$	$\mathbb{Q}(\sqrt[3]{882})$	$2 * 3^2 * 7^2$	4	0	$-27 * 2^2 * 3^2 * 7^2$
3	$\frac{432}{35}$	$\mathbb{Q}(\sqrt[3]{2450})$	$2 * 5 * 7^2$	4	1	$-27 * 2^2 * 5^2 * 7^2$
18	$\frac{15606}{25}$	$\mathbb{Q}(\sqrt[3]{2890})$	$2 * 5 * 17^2$	1	1	$-3 * 2^2 * 5^2 * 17^2$

4.2.6 Invariants of $E19A3$ over $K_r = \mathbb{Q}(\sqrt[3]{m})$

Table 4.10 below presents the splitting of 19 in each cubic extension produced by our choices of r.

Using (3.12) we compute $C(E_{19}/K_r)$.

Table 4.10: Tamagawa Product $C(E_{19}/K_r)$

$\mathbb{Q}(\sqrt[3]{m})$	19 mod 3	$m^{\frac{19-1}{3}}$ mod 19	$19\mathbb{Z}_{K_r}$	$c_{\mathfrak{p}}$	$C(E_{19}/K_r)$
$\mathbb{Q}(\sqrt[3]{60})$	1	7	$\mathfrak{p}$	1	1
$\mathbb{Q}(\sqrt[3]{882})$	1	1	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	1	1^3
$\mathbb{Q}(\sqrt[3]{2450})$	1	1	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	1	1^3
$\mathbb{Q}(\sqrt[3]{2890})$	1	7	$\mathfrak{p}$	1	1

Table 4.11. presents the leading term of the Taylor expansion of $L(E/K_r, s)$ at $s = 1$ and the regulator of $E19A3$ over each K_r.

The computations were achieved with MAGMA's function for L-series and elliptic curves.

Table 4.11: Leading term of $L(E_{19}/K_r, s)$ at $s = 1$ and Regulator

$\mathbb{Q}(\sqrt[3]{m})$	$L'(E_{19}/K_r, 1)$	R_{E_{19}/K_r}
$\mathbb{Q}(\sqrt[3]{60})$	4.151610948375928452087273591 29	9.423423993
$\mathbb{Q}(\sqrt[3]{882})$	3.532398058735429323618187538 98	11.22508805
$\mathbb{Q}(\sqrt[3]{2450})$	14.967391773117168040314126997 5	8.807902242
$\mathbb{Q}(\sqrt[3]{2890})$	2.912779257595100366469202442 11	12.48837895

Table 4.12 recalls the composition of Ω based on section 3.3.3. and provides the order of $E_{19}(K)_{tors}$ computed with MAGMA.

Using information provided in the precedent tables, it presents the analytic order of $Ш(E_{19}/K_r)$ from the quotient

$$\frac{|Ш(E_{19}/K_r)|}{|Ш(E_{19}/\mathbb{Q})|} = \frac{L'(E_{19}/\mathbb{Q},\chi_2,1)R_{E_{19}/\mathbb{Q}}C(E_{19}/\mathbb{Q})\omega|E_{19}(K_r)_{tors}|^2\sqrt{|\Delta_{K_r}|}}{|E_{19}(\mathbb{Q})|^2 R_{E_{19}/K_r}C(E_{19}/K_r)\Omega} \tag{4.14}$$

Table 4.12: Order of the Shafarevich-Tate group of $E_{19}(K_r)$

$\mathbb{Q}(\sqrt[3]{m})$	Ω	$\lvert E_{19}(K)_{tors}\rvert$	$C(E_{19}/K_r)$	analytic $\frac{\lvert Ш(E_{19}/K_r)\rvert}{\lvert Ш(E_{19}/\mathbb{Q})\rvert}$
$\mathbb{Q}(\sqrt[3]{60})$	$2\omega_+^2\omega_-$	3	1	8.99999999877607768058346
$\mathbb{Q}(\sqrt[3]{882})$	$2\omega_+^2\omega_-$	3	1^3	9.00000000050812848815234
$\mathbb{Q}(\sqrt[3]{2450})$	$2\omega_+^2\omega_-$	3	1^3	80.9999999924488007403889
$\mathbb{Q}(\sqrt[3]{2890})$	$2\omega_+^2\omega_-$	3	1	8.99999995311976065445 71

4.3 Computations with a curve of rank 1 over $\mathbb{Q}$ and rank 2 over K

In this section, we consider an elliptic curve admitting a $\mathbb{Q}$-rational point. We therefore work in case 2 as in (3.17) and have

$$\begin{aligned} L''(E/K_r,1) &= \frac{2|Ш(E/K_r)|R_{E/K_r}C(E/K_r)\Omega}{|E(K_r)_{tors}|^2\sqrt{|\Delta_{K_r}|}} \\ \iff L'(E/\mathbb{Q},1)L'(E/\mathbb{Q},\chi_2,1) &= \frac{2|Ш(E/K_r)|R_{E/K_r}C(E/K_r)\Omega}{|E(K_r)_{tors}|^2\sqrt{|\Delta_{K_r}|}} \end{aligned}$$

Now, taking into consideration Conjecture 3.b., we further have

$$L'(E/\mathbb{Q},1)L'(E/\mathbb{Q},\chi_2,1) = \frac{2|Ш(E/K_r)|R_{E/K_r}C(E/K_r)\Omega}{|E(K_r)_{tors}|^2\sqrt{|\Delta_{K_r}|}} \tag{4.15}$$

$$\iff L'(E/\mathbb{Q},\chi_2,1) = \frac{2|Ш(E/K_r)|R_{E/K_r}C(E/K_r)\Omega}{L'(E/\mathbb{Q},1)|E(K_r)_{tors}|^2\sqrt{|\Delta_{K_r}|}} \tag{4.16}$$

$$\iff L'(E/\mathbb{Q},\chi_2,1) = \frac{2|E(\mathbb{Q})_{tors}|^2}{|Ш(E/\mathbb{Q})|R_{E/\mathbb{Q}}C(E/\mathbb{Q})\omega}\frac{|Ш(E/K_r)|R_{E/K_r}C(E/K_r)\Omega}{|E(K_r)_{tors}|^2\sqrt{|\Delta_{K_r}|}} \tag{4.17}$$

From which we can express the following quotient

$$\frac{|Ш(E/K_r)|}{|Ш(E/\mathbb{Q})|} = \frac{L'(E/\mathbb{Q},\chi_2,1)R_{E/\mathbb{Q}}C(E/\mathbb{Q})|E(K_r)_{tors}|^2\omega\sqrt{|\Delta_{K_r}|}}{2|E(\mathbb{Q})_{tors}|^2R_{E/K_r}C(E/K_r)\Omega} \tag{4.18}$$

We will use this last equality to approximate numerically the order of the Shafarevich-Tate group of $E(K_r)$.

4.3.1 E189B1

We consider the elliptic curve $E189B1$ as denoted in Cremona's table ([Cre97]) which has the following Weierstrass equation

$$E_{189} : y^2 + 6xy + y = x^3 \tag{4.19}$$

In view of equation (3.4), it corresponds to the case $u = 2$ and $t = 1$.
By (3.5) we obtain the following parametrization for m

$$m = \frac{2(r+1)(r-1)^2}{r - 1 + 2(2)^3} \tag{4.20}$$

Next sections present tables of numerical results for $E189B1$ over different number fields K_r.

4.3.2 Invariants of $E189B1$ over $\mathbb{Q}$

Table 4.13 presents invariants of $E189A1$ and features related to $E_{189}(\mathbb{Q})$.

These results were computed with MAGMA's functions for elliptic curves and compared with Cremona's table of elliptic curves.

Table 4.13: Invariants of $E189B1$

$\Delta_{E_{189}}$	$3^3 7$
j-invariant	$\frac{2^{21}3^3}{7}$
ω_+	2.730228818689934983780693004 14
ω_-	1.078499554898541506372855502 86
ω	$2\omega_+$
c_4	$2^7 3^2$
c_6	$-2^3 3^3 181$

Table 4.14 summarizes invariants related to $E_{189}(\mathbb{Q})$ needed to compute (4.4). For each prime with bad reduction, we present the information needed to compute the Tamagawa product $C(E_{189}/\mathbb{Q})$ as indicated in section 3.3.2.

Table 4.14: $E_{189}(\mathbb{Q})$ invariants

$L'(E_{189}/\mathbb{Q}, 1)$	1.13046249833075510395213903196
$rank(E_{189}(\mathbb{Q}))$	1
$R_{E_{189}/\mathbb{Q}}$	1.86324355221236297777936214506
$\lvert E_{189}(\mathbb{Q})_{tors}\rvert$	3
Primes with bad reduction	3,7
$ord_3(\Delta_{E_{189}}), ord_7(\Delta_{E_{189}})$	3, 1
$ord_3(c_4), ord_7(c_4)$	2,0
reduction type at 3, 7	additive, split multiplicative
c_3, c_7	1, $-ord_7(j) = 1$
$C(E_{189}/\mathbb{Q})$	1
$\lvert Ш(E_{189}/\mathbb{Q})\rvert$	1

Based on section 3.3.1., we will consider the set of cubic extensions $K_r = \mathbb{Q}(\sqrt[3]{m})$, where m is given by (3.5) for each given r.

Indexed by our choices of r, Table 4.15 lists the corresponding m and its associated number field K_r. Each corresponding d is then decomposed as product ab^2 and following theorem 3.3.1., we compute the discriminant of each K_r.

Table 4.15: Number Fields $K_r = \mathbb{Q}(\sqrt[3]{m})$ associated to $E189B1$

r	m	$\mathbb{Q}(\sqrt[3]{d})$	$d = ab^2$	a^2 mod 9	b^2 mod 9	Discriminant (K_r)
3	$\frac{16}{9}$	$\mathbb{Q}(\sqrt[3]{48})$	$3 * 4^2$	0	4	$-27 * 3^2 * 4^2$
-3	$\frac{16}{3}$	$\mathbb{Q}(\sqrt[3]{144})$	$3^2 * 4^2$	1	0	$-27 * 3^2 * 4^2$

4.3.3 Invariants of $E189B1$ over $K_r = \mathbb{Q}(\sqrt[3]{m})$

Table 4.16 below presents the splitting of 3 and 7 in each cubic extension produced by our choices of r.

Using (3.12) we compute $C(E_{189}/K_r)$.

Table 4.16: Tamagawa Product $C(E_{189}/K_r)$

$\mathbb{Q}(\sqrt[3]{m})$	$p = 3$	$3\mathbb{Z}_{K_r}$	7 mod 3	$m^{\frac{7-1}{3}}$ mod 7	$7\mathbb{Z}_{K_r}$	$C(E_{189}/K_r)$
$\mathbb{Q}(\sqrt[3]{48})$	3	$\mathfrak{p}_1^3$	1	1	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	1^6
$\mathbb{Q}(\sqrt[3]{144})$	3	$\mathfrak{p}_1^3$	1	2	$\mathfrak{p}_2$	1^4

Table 4.17. presents the leading term of the Taylor expansion of $L(E/K_r, s)$ at $s = 1$ and the regulator of $E189B1$ over each K_r.

The computations were achieved with MAGMA's function for L-series and elliptic curves.

Table 4.17: Leading term of $L(E_{189}/K_r, s)$ at $s = 1$ and Regulator

$\mathbb{Q}(\sqrt[3]{m})$	$L''(E_{189}/K_r, 1)$	R_{E_{189}/K_r}
$\mathbb{Q}(\sqrt[3]{48})$	15.00424471183762058290381730 28	21.82028785
$\mathbb{Q}(\sqrt[3]{144})$	22.31141484651985195041399840 29	32.44691778

Table 4.18 recalls the composition of Ω based on section 3.3.3. and provides the order of $E_{189}(K)_{tors}$ computed with MAGMA.

Using information provided in the precedent tables, it presents the analytic order of $Ш(E_{189}/K_r)$ from the quotient

$$\frac{|Ш(E_{189}/K_r)|}{|Ш(E_{189}/\mathbb{Q})|} = \frac{L'(E_{189}/\mathbb{Q}, \chi_2, 1) R_{E_{189}/\mathbb{Q}} C(E_{189}/\mathbb{Q}) |E_{189}(K_r)_{tors}|^2 \omega \sqrt{|\Delta_{K_r}|}}{2|E_{189}(\mathbb{Q})_{tors}|^2 R_{E_{189}/K_r} C(E_{189}/K_r) \Omega} \tag{4.21}$$

Table 4.18: Order of the Shafarevich-Tate group of $E_{189}(K_r)$

$\mathbb{Q}(\sqrt[3]{m})$	Ω	$\lvert E_{189}(K)_{tors}\rvert$	$C(E_{189}/K_r)$	analytic $\frac{\lvert Ш(E_{189}/K_r)\rvert}{\lvert Ш(E_{189}/\mathbb{Q})\rvert}$
$\mathbb{Q}(\sqrt[3]{48})$	$4\omega_+^2\omega_-$	3	1^6	1.00000000053758394523050
$\mathbb{Q}(\sqrt[3]{144})$	$4\omega_+^2\omega_-$	3	1^4	1.00000000071078902598739

Conclusion

We note that all Shafarevich-Tate group's orders computed were found to be integers, within the accuracy of our computations and, moreover, squares. This provides evidence for conjecture 2 for pure cubic extensions.

In reference to Cremona's tables of elliptic curves, we could consider building a larger table including the elliptic curves over pure cubic extensions compatible with our computations above. We remark that the obstruction to providing more examples is due to the time-consuming computations of the leading term in the Taylor expansion of $L(E/K, s)$. For fixed elliptic curves, the speed of this computation is related to the discriminant of the field K. In our cases of pure cubic extensions parametrized by $r \in \mathbb{Q}$, there are not many choices of r such that m and hence Δ_K remain small. Depending on the curve and field over which the computations have been done, results were obtained in a time range from 3 days to a month.

Finally, by the non-exhaustive character of any table of elliptic curves and taking into consideration that computations are also restricted by the difficulty of finding generators for the Mordell-Weil groups, we conclude that more theoretical work is needed to provide more arguments toward the Birch and Swinnerton-Dyer conjecture for elliptic curves over number fields.

Bibliography

[Bou66] Séminaire Bourbaki. *Séminaire Bourbaki: exposé no. 301 à 306*. Number no. 301. 1966.

[BSD65] B.J.Birch and H.P.F. Swinnerton-Dyer. *Notes on elliptic curves I and II*. Number no. 212. 1963-1965.

[CF10] J.W.S. Cassels and A. Fröhlich. *Algebraic Number Theory*. London Mathematical Society, 2010.

[Coh93] H. Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics. Springer-Verlag, 1993.

[Cre97] J.E. Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, 1997.

[Dar04] H. Darmon. *Rational Points on Modular Elliptic Curves*. Number no. 101 in Regional Conference Series in Mathematics. American Mathematical Society, 2004.

[DD05] T. Dokchitser and V. Dokchitser. Computations in non-commutative Iwasawa theory. *ArXiv Mathematics e-prints*, September 2005.

[Dok05] Vladimir Dokchitser. Root numbers of non-abelian twists of elliptic curves. *Proceedings of the London Mathematical Society*, 91(2):300–324, 2005.

[EW00] G. Everest and T. Ward. The Canonical Height of an Algebraic Point on an Elliptic Curve. *New York J. Math. 6(2000) 331-342.*, 2000.

[FKK12] J. Fearnley, H. Kisilevsky, and M. Kuwata. Vanishing and Non-Vanishing Dirichlet Twists of L-Functions of Elliptic Curves. *J. London Math. Soc.*, 2012.

[Isa76] I.M. Isaacs. *Character Theory of Finite Groups*. Number v. 69 in Pure and Applied Mathematics. Academic Press, 1976.

[Kis12] H. Kisilevsky. *Ranks of elliptic curves in cubic extensions*. New York, Springer, 2012.

[Kna92] A.W. Knapp. *Elliptic curves*, volume 40. Princeton Univ Pr, 1992.

[Maz] B. Mazur. Modular curves and the eisenstein ideal. *Publication Mathématiques de l'IHÉS*.

[Mer] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps des nombres. *Documenta mathematica*.

[Mil06] J.S. Milne. *Elliptic curves*. Kea books. BookSurge Publishers, 2006.

[Sil97] J. Silverman. Computing the canonical heights with little (or no) factorization. *Mathematics of computation, Vol 66, Number 218, 787-805*, 1997.

[Sil09] J.H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Verlag, 2009.

[ST92] J.H. Silverman and J.T. Tate. *Rational points on elliptic curves*. Undergraduate texts in mathematics. Springer-Verlag, 1992.

[Ste91] W.A. Stein. *The Birch and Swinnerton-Dyer Conjecture, a Computational Approach*. Mathematics Subject Classification, 1991.

[SZ03] S. Schmitt and H.G. Zimmer. *Elliptic Curves: A Computational Approach*. De Gruyter Studies in Mathematics. Walter de Gruyter, 2003.

[Was03] L.C. Washington. *Elliptic Curves: Number Theory and Cryptography*. CRC Press Series on Discrete Mathematics and Its Applications. Chapman & Hall/CRC, 2003.