Mazur-Tate Type Conjectures for Elliptic Curves Defined over Quadratic Imaginary Fields

Dominic Lemelin

Department of Mathematics and Statistics

McGill University, Montreal

October, 2001

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfilment of the requirements of the degree of Doctor of Philosophy (Ph.D.)

Affectueusement dédié à
ce que j'ai de plus cher au monde,

Irène, Friedrich et Bruno.

Je perçois la science mathématique comme une représentation (non injective) de la raison humaine. Elle est un langage permettant la contemplation de la logique du raisonnement humain. Cette thèse m'a permi pendant quelques années de vivre d'un peu de poésie.

Contents

Abstract

Elliptic curves defined over quadratic imaginary fields $\mathbb{K}$ have been studied less than those defined over $\mathbb{Q}$. They are nevertheless conjecturally modular and Birch and Swinnerton-Dyer conjectures have been stated for them as well.

For elliptic curves over $\mathbb{Q}$, Mazur and Tate have formulated some refined conjectures of Birch and Swinnerton-Dyer type. They define an element θ belonging to a group ring $Z[G]$ where G is the Galois group of a finite abelian extension of $\mathbb{Q}$, and conjecture that it belongs to a power of the augmentation ideal $I \subseteq Z[G]$ that is at least the rank of $E(\mathbb{Q})$. The behavior of θ is similar to the order of vanishing at 1 of p-adic L-functions: for example, primes of split multiplicative reduction for the curve appear in the conjectures.

In this thesis, we use modular symbols computed on some hyperbolic upper-half space to construct theta elements associated to elliptic curves defined over quadratic imaginary fields of class number 1. We state conjectures similar to those of Mazur and Tate for such curves and experimentally test many cases of the conjectures. The tests include situations in which we use prime ideals of $\mathcal{O}_{\mathbb{K}}$ where the elliptic curves have split multiplicative reduction.

Résumé

Les courbes elliptiques définies sur les corps quadratiques imaginaires $\mathbb{K}$ ont jusqu'à présent fait l'objet de moins de recherche que celles définies sur $\mathbb{Q}$. Elles sont néanmoins supposément modulaires et les conjectures de Birch et Swinnerton-Dyer ont été énoncées pour ces dernières aussi.

Pour les courbes elliptiques sur $\mathbb{Q}$, Mazur et Tate ont formulé des conjectures raffinées analogues à celles de Birch et Swinnerton-Dyer. Ils définissent un élément θ appartenant à un anneau de groupe $Z[G]$, où G est le groupe de Galois d'une extension abélienne finie de $\mathbb{Q}$. Ils conjecturent ensuite que cet élément appartient à une puissance I^ρ de l'idéal d'augmentation $I \subseteq Z[G]$ où ρ doit être plus grand ou égal au rang de $E(\mathbb{Q})$. Le comportement de θ est similaire à ce que l'on a avec l'ordre du zéro en 1 des fonctions L p-adiques: par exemple, les premiers de réduction multiplicative déployée de la courbe apparaissent dans les conjectures.

Dans cette thèse, nous utilisons des symboles modulaires calculés sur un demi-espace supérieur hyperbolique afin de construire des éléments thêta associés aux courbes elliptiques définies sur les corps quadratiques imaginaires de nombre de classe 1. Nous énonçons des conjectures similaires à celles de Mazur et Tate pour de telles courbes et vérifions expérimentallement plusieurs cas de ces conjectures. Les tests incluent des situations où nous utilisons des idéaux premiers de $\mathcal{O}_{\mathbb{K}}$ pour lesquels les courbes elliptiques ont une réduction multiplicative déployée.

Acknowledgements

I would first like to thank professor Henri Darmon, my thesis supervisor, for his suggestion of this very interesting research topic. His inspiration and intuitions in this mystifying field of research are absolutely astonishing. I also want to express my sincere thanks to fellow students of number theory, who have been of valuable help in my general number theoretic formation, and to Cuco Trujillo-Cortez for making these years at McGill so pleasant.

I am also grateful to John Cremona, who kindly accepted to send me a copy of his own thesis. This has turned out to be an essential ingredient for my work.

Financial help was received during my graduate studies mainly from the *Natural Science and Engineering Research Council* (NSERC), *Fonds pour la formation de chercheurs et l'aide à la recherche* (FCAR) and the *Centre interuniversitaire en calcul mathématique et algébrique* (CICMA). I thank these organizations for their financial support towards my research activities. I also wish to thank heartily members of my close family who have financially as well as psychologically supported my studies. Further funding came from diverse teaching positions in the Department of Mathematics and Statistics of McGill University.

I owe the most to my wife, Irène, for her strong support during the whole of my graduate studies. I recognize that Irène and my sons, Friedrich and Bruno, showed patience and kind understanding during these hard working years. I must admit that it is them, not me, who really suffered the most. This thesis is dedicated to them.

Introduction

It is very well known that the points on an elliptic curve E defined over a number field $\mathbb{F}$ satisfy a group law defined over $\mathbb{F}$. The set $E(\mathbb{F})$ of $\mathbb{F}$-rational points forms an abelian group whose structure is partially known. The Mordell-Weil theorem states that

$$E(\mathbb{F}) \cong \mathbb{Z}^r \oplus E(\mathbb{F})_{\text{tors}},$$

where the torsion part and r are both finite. The problem is that the proof is not effective and does not give an actual value for r.

This is where the Birch and Swinnerton-Dyer conjecture comes to the rescue. A complex analytic function $L(E, s)$ is defined from the elliptic curve's local data in such a way that it is tempting to believe that its order of vanishing at $s = 1$ increases with the number of $\mathbb{F}$-rational points on E. The heuristic argument is very far from a proof though. It is even unclear a priori that $L(E, s)$ is *defined* at $s = 1$. The Birch and Swinnerton-Dyer conjecture states that $L(E, s)$ is indeed defined at $s = 1$ and that its order of vanishing at that point is precisely equal to r, the rank of $E(\mathbb{F})$. This beautiful conjecture states a relationship between algebraic or arithmetic properties and analytic properties, and can be viewed as an instance of a local-global principle. At present it is still far from being completely understood.

Elliptic curves in general, and more particularly their modularity and the Birch and Swinnerton-Dyer conjecture for them, have been studied much more thoroughly when the field of definition is $\mathbb{Q}$. This is most striking when we realize that the modularity of elliptic curves defined over $\mathbb{Q}$ has by now been proved completely, whereas few theoretical results are available for the modularity of general elliptic curves defined over quadratic imaginary fields $\mathbb{K}$. In the case where $\mathbb{K}$ has class number 1, the modularity of some particular elliptic curves has been established. Still, even for elliptic curves defined over $\mathbb{Q}$, the Birch and Swinnerton-Dyer conjecture remains bewildering.

Some very partial results are available for the Birch and Swinnerton-Dyer conjecture in the case where elliptic curves are defined over $\mathbb{Q}$. We will mention some in the thesis. Even though the partial results available consist in major mathematical achievements, the results nevertheless remain scarce. It is therefore quite interesting to get some insight into the conjecture by studying other ones, analogous in some ways to the Birch and Swinnerton-Dyer conjecture. The most notable of these is a p-adic version of the Birch and Swinnerton-Dyer conjecture. Assuming (at the time) the modularity of an elliptic curve E defined over $\mathbb{Q}$, Mazur and Swinnerton-Dyer used modular symbols associated to the curve in order to construct p-adic measures for the elliptic curve and thus dually define a p-adic L-function for E. At first, it was believed that this p-adic L-function should behave like its complex counterpart and have order of vanishing at $s = 1$, where s lives in some p-adic domain $\mathbb{Z}_{p,d}^*$, equal to r. Further investigations by Mazur, Tate and Teitelbaum have shown that the situation is more subtle than that. It has been further conjectured that if p is a prime of split multiplicative reduction for E, and only in that case, then the order of vanishing of the p-adic L-function at $s = 1$ is increased by exactly 1.

The p-adic version of the Birch and Swinnerton-Dyer conjecture was eventually refined by Mazur and Tate to $(\mathbb{Z}/m\mathbb{Z})^*$-valued conjectures, where m is not necessarily prime. They constructed, again using modular symbols for modular elliptic curves defined over $\mathbb{Q}$, a theta element θ_m belonging to a group ring $Z[G_m]$, where $G_m = (\mathbb{Z}/m\mathbb{Z})^*$ and Z is $\mathbb{Z}$ together with some inverted primes and G is the Galois group of a ray class field extension $\mathbb{T}$ of $\mathbb{Q}$ with conductor m. It is then conjectured that θ_m belongs to I^r, where I is the augmentation ideal of $Z[G]$ and r is the rank of E as before. Taking into account the p-adic flavor of the construction, Mazur and Tate actually conjectured and tested experimentally in a few cases that $\theta_m \in I^{r+s}$, where s is the number of primes of split multiplicative reduction for E dividing m.

The original contribution of this thesis consists in generalizing the work of Mazur and Tate to elliptic curves E defined over quadratic imaginary fields $\mathbb{K}$ of class number 1. Using modular symbols computed from geodesic cycles on a hyperbolic upper half space, we construct theta elements $\theta_{\mathcal{M}}$ belonging to a group ring $Z[G]$, where G is the Galois group of the ray class field extension $\mathbb{T}$ of $\mathbb{K}$ with conductor $\mathcal{M}$, an integral ideal of $\mathcal{O}_{\mathbb{K}}$. We conjecture that $\theta_{\mathcal{M}}$ belongs to I^{r+s}, where r is the rank of E and s is the number of prime ideals of $\mathcal{O}_{\mathbb{K}}$ dividing $\mathcal{M}$ where E has split multiplicative reduction. We then experimentally test many cases of the conjectures, including cases in which s is not trivial.

The above procedure requires the modularity of the elliptic curves E defined over $\mathbb{K}$. The thesis includes a discussion of the notion of modularity for these elliptic curves and stresses some important differences with elliptic curves over $\mathbb{Q}$. In particular, it has not been proved yet that general elliptic curves over $\mathbb{K}$ are indeed modular. There are some limited results for particular curves though. In his Oxford Ph.D. thesis, John Cremona gave numerical evidence for the modularity of some elliptic curves defined over Euclidean quadratic imaginary fields.

Assuming the modularity of the elliptic curves studied, we may then use associated modular symbols to compute theta elements for them. According to the description of modularity for such elliptic curves, modular symbols may be computed through the integration of a harmonic differential form on a real 3-manifold $X_0(\mathcal{N})$, where the level $\mathcal{N}$ of the form, an integral ideal of $\mathcal{O}_{\mathbb{K}}$, is taken to be the conductor $\mathcal{N}_E$ of the elliptic curve. The group ring $Z[G]$ in which theta elements live must have some integrality properties, for if Z were $\mathbb{Q}$ say, then all our conjectures become trivial. Kurčanov is one of the early investigators of these harmonic differential forms. He argues in [Kur78] that the above integrations do satisfy some integrality properties, but very few details appear. As this is critical to our work, we have improved on his statement and given a detailed proof of that fact. Our proof is also constructive, in that precise optimal conditions are given on Hecke operators to know when they can be used to “close paths”. The precise understanding of integrality properties of the modular symbols for elliptic curves defined over imaginary quadratic fields of class number 1 is also one of the original contributions of this thesis.

Chapter 1

Preliminaries on Elliptic Curves, their Rank, and Modularity.

The theory of elliptic curves is central in modern number theory. It is thus well known and we will be rather brief here. The reader will find the basic facts about elliptic curves in many available books, for example in [Kna92] or [Kob93], which are elementary enough and also contain an introduction to modular forms. Some classical references include [Cas91] and [Tat74]. A more comprehensive introduction to elliptic curves is the standard book of Silverman [Sil86] together with its continuation [Sil94]. The statement of the Birch and Swinnerton-Dyer conjecture over number fields or global fields can be found in [Lan91], [Tat66] or the most recent version of Ireland and Rosen [IR90].

1.1 Basic Definitions

In this chapter, we will consider our global field of definition to be a number field. Many of the statements could be generalized to arbitrary global fields, or even to any field, but we will not bother making the distinctions. An **elliptic curve** E over $\mathbb{F}$, which we denote $E_{/\mathbb{F}}$, is a projective non-singular curve of genus one, together with a distinguished $\mathbb{F}$-rational point on it, called the **origin** and denoted $\mathcal{O}$.

Up to an isomorphism of algebraic curves over $\mathbb{F}$, the affine part $E\setminus\{\mathcal{O}\}$ of an elliptic curve can be given by an equation in Weierstraß form:

$$E_{/\mathbb{F}}:\ y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \tag{1.1}$$

where a_1, a_2, a_3, a_4, a_5 and a_6 are elements of $\mathbb{F}$. There is only one point at infinity, and it is precisely the origin $\mathcal{O}$ of the elliptic curve. In the case where $\mathbb{F}$ has characteristic different from 2 or 3, it is useful to simplify this equation. If $\mathrm{char}(\mathbb{F})\neq 2$, we may find an $\mathbb{F}$-isomorphic copy of the form

$$E_{/\mathbb{F}}:\ y^2=4x^3+b_2x^2+2b_4x+b_6 \tag{1.2}$$

where $b_2=a_1^2+4a_2, b_4=2a_4^2+a_1a_3$ and $b_6=a_3^2+4a_6$. When the characteristic of $\mathbb{F}$ is not 3 either, we may further simplify to

$$E_{/\mathbb{F}}:\ y^2=x^3-27c_4x-54c_6 \tag{1.3}$$

where $c_4=b_2^2-24b_4$ and $c_6=-b_2^3+36b_2b_4-216b_6$.

An elliptic curve, up to isomorphism, can be given by an equation of the form (1.1), (1.2) or (1.3). We also have a simple criterion to know when such equations do determine elliptic curves. Essentially, we only have to check the non-singularity of the curve that these equations determine. Indeed, the genus can then be computed using Hurwitz formula to be precisely 1, and the point at infinity is rational. For this, we further define

$$b_8=a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2.$$

It is then proved that equations (1.1) or (1.2) yield a non-singular curve if and only if the **discriminant**

$$\Delta=-b_2^2b_8-8b_4^3-27b_6^2+9b_2b_4b_6$$

is not zero. We may define Δ this way whenever the elliptic curve is given by equations (1.1) or (1.2), irrespective of the characteristic of $\mathbb{F}$. In case the elliptic curve is given by (1.3), we use

$$\Delta=\frac{c_4^3-c_6^2}{1728}.$$

There are many other invariants associated to elliptic curves. One that will be very important to us is the **conductor** $\mathcal{N}_E$ of the elliptic curve. It is a non-zero integral ideal of $\mathbb{F}$, which is naturally identified with a positive integer when $\mathbb{F} = \mathbb{Q}$. It is given by

$$\mathcal{N}_E = \prod_{\mathcal{P}} \mathcal{P}^{f_{\mathcal{P}}}$$

where the product is taken over the prime ideals of $\mathbb{F}$ and $f_{\mathcal{P}}$ depends only on the reduction type of E at $\mathcal{P}$. When $\mathcal{P}$ does not lie over 2 or 3, then

$$f_{\mathcal{P}} = \begin{cases} 0 & \text{when } E \text{ has good reduction at } \mathcal{P}, \\ 1 & \text{when } E \text{ has multiplicative reduction at } \mathcal{P}, \\ 2 & \text{when } E \text{ has additive reduction at } \mathcal{P}. \end{cases}$$

The definitions of the reduction types can be found in [Sil86], and the definition of $f_{\mathcal{P}}$ when $\mathcal{P}$ divides 6 is rather technical. It can be found for instance in [Sil94], or in [Tat75].

Remark 1.1 $\mathcal{N}_E$ precisely tells us where E has bad reduction. $\mathcal{N}_E$ always divides the minimal discriminant $\mathcal{D}$ of E (see [Sil86] for the definition) and these two values actually have the same support, meaning that a prime $\mathcal{P}$ divides $\mathcal{N}_E$ if and only if it also divides $\mathcal{D}$. When the ring of integers $\mathcal{O}_{\mathbb{F}}$ of $\mathbb{F}$ is a principal ideal domain, then there is an equation for E for which $\mathcal{D} = (\Delta)$. □

1.2 The Mordell-Weil Theorem and the Birch and Swinnerton-Dyer Conjecture

An elliptic curve over $\mathbb{F}$ is an algebraic group over $\mathbb{F}$. That is, the data defining an elliptic curve as above determines a group law that is defined over $\mathbb{F}$. The elliptic curve being projective, it follows that the algebraic group is commutative. We thus call the group operation **addition** and denote it by $+$. This group law is given explicitly in terms of the coefficients in equations (1.1), (1.2) or (1.3), the formulas can be found in any of the books mentioned at the beginning of this chapter. The group law being defined over $\mathbb{F}$, it follows that the points of the elliptic curve defined over any fixed extension field of $\mathbb{F}$ form a group.

The following fundamental result in the theory of elliptic curves is called the **Mordell-Weil Theorem**.

Theorem 1.1 Let $E_{/\mathbb{F}}$ be an elliptic curve, and let $\mathbb{L}$ be any finite extension field of $\mathbb{F}$. Then the group $E(\mathbb{L})$ of $\mathbb{L}$-rational points of E is finitely generated. ∎

The Mordell-Weil theorem can be written symbolically as

$$E(\mathbb{L}) \cong \mathbb{Z}^r \oplus E(\mathbb{L})_{\text{tors}}$$

with r, the $\mathbb{L}$-**rank** of the elliptic curve, finite. Thus r depends on $\mathbb{L}$. When no extension field $\mathbb{L}$ is mentioned, the **rank** of $E_{/\mathbb{F}}$ means its $\mathbb{F}$-rank. The torsion part is finite. We will not be very interested in its structure in this thesis.

Theorem 1.1 seems wonderful as stated here, but there is a problem: its proof is not effective. That is, the proof does not yield an actual value for r, and neither does it yield generators for the free part of $E(\mathbb{L})$. In this spirit, the beautiful conjecture of Birch and Swinnerton-Dyer that we will shortly describe is of interest. As we will see, it gives a partial answer to this problem, for it conjectures an exact value for r.

We proceed towards the statement and motivation of the Birch and Swinnerton-Dyer conjecture, but we first need to introduce substantial preliminary notions.

Consider an elliptic curve E defined over $\mathbb{F}$. For any prime ideal $\mathcal{P}$ of the ring of integers $\mathcal{O}_{\mathbb{F}}$ of $\mathbb{F}$, we may consider the reduced curve $\tilde{E}$ of E defined over the residue field $k_{\mathcal{P}}$ (see [Sil86] for the definition) and count the number of rational points (points of $\mathbb{P}^2(k_{\mathcal{P}})$) on $\tilde{E}$. Denote this number by $N_{\mathcal{P}}$.

Remark 1.2 To be well-defined, the above procedure actually requires a *minimal model* for the elliptic curve. In the cases of most interest in this thesis, namely $\mathbb{F} = \mathbb{Q}$ or a quadratic imaginary field $\mathbb{K}$ of class number 1, we may find a global minimal model for E, that is, a model which is minimal at all finite places of $\mathbb{F}$. Otherwise, one needs to work with models that vary with the primes of $\mathbb{F}$, being minimal for the prime under consideration. We then have that the reduced curve is also an elliptic curve if and only if $\mathcal{P} \nmid \mathcal{N}_E$, the conductor of E, or equivalently, if and only if $\mathcal{P} \nmid \mathcal{D}$, the minimal discriminant of E. $\square$

We expect $N_{\mathcal{P}}$ to be close to $\mathrm{N}_{\mathbb{F}/\mathbb{Q}}(\mathcal{P})+1$. Indeed, an important result of Hasse says:

Proposition 1.2 (Hasse's Inequality)

$$|\mathrm{N}_{\mathbb{F}/\mathbb{Q}}(\mathcal{P}) + 1 - N_{\mathcal{P}}| \;\leq\; 2\sqrt{\mathrm{N}_{\mathbb{F}/\mathbb{Q}}(\mathcal{P})}.$$

$\blacksquare$

Denote by $a_{\mathcal{P}}$ the "error term" $\mathrm{N}_{\mathbb{F}/\mathbb{Q}}(\mathcal{P}) + 1 - N_{\mathcal{P}}$. Using these, at each prime $\mathcal{P}$ we define a **local Euler factor** $L_{(\mathcal{P})}(E,s)$, a complex valued function of a complex variable, as:

$$L_{(\mathcal{P})}(E,s) = \begin{cases} \left[1 - a_{\mathcal{P}}\mathrm{N}_{\mathbb{F}/\mathbb{Q}}(\mathcal{P})^{-s}\right]^{-1} & \text{if } \mathcal{P} \mid \mathcal{N}_E, \\ \left[1 - a_{\mathcal{P}}\mathrm{N}_{\mathbb{F}/\mathbb{Q}}(\mathcal{P})^{-s} + \mathrm{N}_{\mathbb{F}/\mathbb{Q}}(\mathcal{P})^{1-2s}\right]^{-1} & \text{otherwise.} \end{cases}$$

We may now form the formal **Euler product**

$$L(E_{/\mathbb{F}},s) = \prod_{\mathcal{P}} L_{(\mathcal{P})}(E,s)$$

where the product is taken on all the finite places of $\mathbb{F}$. This is called the L**-function** associated to $E_{/\mathbb{F}}$. It is also sometimes called the L**-series** associated to $E_{/\mathbb{F}}$, for it can formally be rewritten as

$$L(E_{/\mathbb{F}},s) = \sum_{\mathcal{N}} \frac{a_{\mathcal{N}}}{\mathrm{N}_{\mathbb{F}/\mathbb{Q}}(\mathcal{N})^s} \tag{1.4}$$

for some integer Fourier coefficients $a_{\mathcal{N}}$, and the sum is taken over all non-zero ideals of $\mathcal{O}_{\mathbb{F}}$.

There is a quite general theory of series defined by Euler products of any degree, whereby one computes a right half plane of convergence for the Euler product and expressions for the $a_{\mathcal{N}}$ in terms of the $a_{\mathcal{P}}$. We will see some of these expressions in the context of cusp forms later. In this general context of the theory of Euler products, one shows using Hasse's inequality that the expression defining the above L-function converges in the right half plane $\mathrm{Re}(s) > 3/2$.

Let us now discuss the heuristics that lead to the Birch and Swinnerton-Dyer conjecture. One may show that whether $\mathcal{P}$ divides $\mathcal{N}_E$ or not, we always have that the local Euler factors evaluated at 1 are given by:

$$L_{(\mathcal{P})}(E, 1) = \mathrm{N}(\mathcal{P})/\#E_{ns}(k_{\mathcal{P}}),$$

where $E_{ns}(k_{\mathcal{P}})$ means the non-singular points on the reduced curve. To be consistent, we should have used the notation $\tilde{E}$ here, but the reader will be indulgent, for this is a very standard abuse of notation. Now Hasse's inequality says that each local Euler factor evaluated at $s = 1$ should be close to 1. So formally, $L(E_{/\mathbb{F}}, s = 1)$ is roughly an infinite product of ones, which is the first requirement if one is to hope that it should indeed be defined at $s = 1$. Of course, we just said that the Euler product possibly does not converge on the left of $\Re(s) = 3/2$, but the first statement in the Birch and Swinnerton-Dyer conjecture below will assert that an analytic continuation exists for the L-function.

The most important part of this conjecture though comes from the following reasoning. If the rank of the elliptic curve is high, then there are lots of rational points to furnish points on the reduced curve, i.e., $\#E_{ns}(k_{\mathcal{P}})$ should tend to be on the high side permitted by Hasse's inequality. Then the local Euler factors evaluated at $s = 1$ should tend to be smaller than one, and the product will tend to vanish there with order increasing with the rank of the elliptic curve. This leads to the belief that perhaps the order of vanishing of the L-function at $s = 1$ is the same as the rank of the group of rational points on the curve. Experimental tests, as originally presented in [BSD65] tend to confirm this, and also permit to actually predict a value for the r^{th} derivative of $L(E, s)$ at $s = 1$. We are led to this statement of the Birch and Swinnerton-Dyer conjecture.

Conjecture 1.3 (Birch, Swinnerton-Dyer)

Let $E_{/\mathbb{F}}$ be an elliptic curve, $L(E_{/\mathbb{F}}, s)$ its complex L-function, and let r be the rank of $E(\mathbb{F})$.

0) The complex L-function a priori defined for $\Re(s) > \frac{3}{2}$ has an analytic continuation to an entire function on the complex plane;

1) $\operatorname{ord}_{s=1} L(E_{/\mathbb{F}}, s) = r$;

2) The value of the first non-zero Taylor coefficient is:

$$\lim_{s\to 1} \frac{L(E_{/\mathbb{F}}, s)}{(s-1)^r} = \frac{2^t\ \Omega\ |\text{Ш}(E_{/\mathbb{F}})|\ R(E_{/\mathbb{F}})\ \prod c_{\mathcal{P}}}{\sqrt{|D_{\mathbb{F}}|}\ |T|^2}\ ;$$

where the product is taken over all the prime ideals $\mathcal{P}$ of $\mathcal{O}_{\mathbb{F}}$, $D_{\mathbb{F}}$ is the absolute discriminant of the number field, T is the torsion part of the $\mathbb{F}$-rational points, t is the number of complex places of $\mathbb{F}$, $\text{Ш}(E_{/\mathbb{F}})$ is the Shafarevich-Tate group of the elliptic curve, Ω is the complex period of $E_{/\mathbb{C}}$, $R(E_{/\mathbb{F}})$ is the canonical height regulator, and the $c_{\mathcal{P}}$ are local reduction factors as defined in [Sil94]. ■

This thesis will deal with part 1) of this conjecture. Part 0) was dealt with in John Cremona's thesis [Cre81] where he experimentally shows a Shimura-Taniyama type of correspondence between elliptic curves defined over quadratic imaginary fields $\mathbb{K}$ and cusp forms for $\mathrm{GL}_2(\mathbb{A}_{\mathbb{K}})$. We will come back to this in chapter 3. A natural extension to this thesis would be to make up a Mazur-Tate type conjecture that would also deal with the third part above, giving a value for the first non-vanishing Taylor coefficient. This requires a good theory of p-adic heights and regulators, as developed for example in [MT83] and [MT91].

Now recall that the Hasse-Minkowski principle, or local-global principle, asserting that there should be a global rational point on the curve if and only if there are local rational points everywhere *fails* for curves of genus one in general. Of course, this principle is vacuous for elliptic curves, for these *start* their lives with an $\mathbb{F}$-rational point by definition. However, the Birch and Swinnerton-Dyer conjecture is quite wonderful, for it gives another type of local-global principle for elliptic curves. It says roughly *how many* global rational points there should be on the elliptic curve starting with local data only. Note that from this point of view, the appearance of the Shafarevich-Tate group in the conjecture is of no surprise, for this group is precisely what measures the failure of the usual local-global principle for the forms of the corresponding curve of genus one.

The Birch and Swinnerton-Dyer conjecture is very beautiful, for it brings in analytic tools to study the fundamentally algebraic question of the determination of r. In the author's opinion, such interrelationships between the different branches of mathematics are amongst the most amazing insights of the discipline. However, one should honestly also remark that the Birch and Swinnerton-Dyer conjecture still encompasses weak points. In particular, it does not yield generators for the group of rational points. Even worse, it is even unclear whether the value of r, that is, the order of vanishing of the L-function, can be computed, both in practice and in theory. For example, it is an open problem to prove that there exists an elliptic curve E defined over $\mathbb{Q}$ with $\operatorname{ord}_{s=1} L(E, s) = 4$.

Finally let us mention that this conjecture is still very mysterious, for the relationship conjectured is very deep and not well understood. Even the partial results that we have at our disposal so far, as discussed in the next chapter, tend to be rather technical and not very illuminating.

1.3 Modular Elliptic Curves

The modularity of elliptic curves will be required for the statement, in the following chapters, of conjectures analogous to the Birch and Swinnerton-Dyer conjecture. Some interesting references for the theory of classical modular forms are [Kna92], [Kob93], [Lan76] and [Miy89]. The classical book [Shi71] by Goro Shimura is more advanced.

Consider $\mathcal{H}$, the Poincaré upper half plane $\{z = x + iy \in \mathbb{C} \mid y > 0\}$. It is equipped with the hyperbolic metric

$$ds^2 = \frac{dx^2 + dy^2}{y^2} \ .$$

We also consider $\mathcal{H}^*$, the union of $\mathcal{H}$ and the cusps $\mathbb{P}^1(\mathbb{Q})$ with its usual topology.

An action of $\mathrm{GL}_2^+(\mathbb{R})$ on $\mathcal{H}$, easily extended to $\mathcal{H}^*$ is given by linear fractional transformations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (z) = \frac{az + b}{cz + d} \ .$$

These are Möbius transformations and are known to preserve the hyperbolic geometry of $\mathcal{H}$. They naturally induce an action on functions $f : \mathcal{H} \to \mathbb{C}$, that we linearly extend to the group ring $\mathbb{C}(\mathrm{GL}_2^+(\mathbb{R}))$. For $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{R})$, it is convenient to define a **stroke operator**, operating on the right, as

$$f|_\sigma(z) = \det(\sigma)\, f(\sigma(z))\, j(\sigma, z)^{-2}$$

where $j(\sigma, z) = cz + d$ is the **automorphy factor**.

Remark 1.3 The diagonal matrices act trivially on $\mathcal{H}$, thus the action of $\mathrm{GL}_2^+(\mathbb{R})$ descends to one of $\mathrm{PSL}_2(\mathbb{R})$. $\square$

Let N be a positive integer and let $\Gamma_0(N)$ be the following *congruence subgroup* of $\mathrm{SL}_2(\mathbb{Z})$:

$$\Gamma_0(N) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \ \mid \ N \text{ divides } c\}.$$

We may then consider the quotient topological space $\Gamma_0(N)\backslash\mathcal{H}^*$. This can be given the structure of a Riemann surface, and we denote it by $X_0(N)$. According to general principles this is also an algebraic curve over $\mathbb{C}$.

A **cusp form** of **weight** $k = 2$ and **level** N is a function $f : \mathcal{H} \to \mathbb{C}$ such that $f(z)\, dz$ descends to a holomorphic differential on $X_0(N)$. Such functions are invariant under the action of the stroke operator:

$$f|_\sigma = f, \quad \forall \sigma \in \Gamma_0(N).$$

They have a Fourier expansion at infinity of the form

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z},$$

or more simply, a ***q*-expansion**

$$f = \sum_{n=1}^{\infty} a_n q^n \tag{1.5}$$

where $q = e^{2\pi i z}$. The $\mathbb{C}$-vector space generated by all cusp forms at level N is denoted $S_2(\Gamma_0(N))$, and has finite dimension g, the genus of $X_0(N)$.

Important elements of $\mathbb{C}(\mathrm{GL}_2^+(\mathbb{R}))$ acting on $S_2(\Gamma_0(N))$, called **Hecke operators**, are indexed by the positive integers n and denoted T_n. For prime $n = p$ not dividing the level N, these are

$$T_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} + \sum_{k=0}^{p-1} \begin{pmatrix} 1 & k \\ 0 & p \end{pmatrix}$$

When p divides N, we drop the matrix $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ from the definition. Hecke operators indexed by integers n may be defined recursively by (non-strict) multiplicativity.

A cusp form $f \in S_2(\Gamma_0(N))$ that is also an eigenfunction for the Hecke operators T_p, for all primes p is called an **eigenform**. We know that eigenforms necessarily have $a_1 \neq 0$, and when $a_1 = 1$, we say that the cusp form f is **normalized**. When f is normalized, we have that the eigenvalue of T_p on f is precisely the p^{th} Fourier coefficient a_p of the q-expansion (1.5). The other Fourier coefficients a_n are thus obtained from the recursive definition of the Hecke operators.

An eigenform $f(z) \in S_2(\Gamma_0(N))$ that is induced from one at a lower level M dividing N is called an **oldform**. This means that either $f(z)$ is also in $S_2(\Gamma_0(M))$, or is of the form $g(rz)$ with $g \in S_2(\Gamma_0(M))$ and r divides N/M. The subspace of $S_2(\Gamma_0(N))$ spanned by the oldforms is denoted $S_2^{\text{old}}(\Gamma_0(N))$ and its orthogonal complement with respect to some inner product, called the Petersson inner product, is $S_2^{\text{new}}(\Gamma_0(N))$. Eigenforms in $S_2^{\text{new}}(\Gamma_0(N))$ are called **newforms**.

To an eigenform $f = \sum_{n=1}^{\infty} a_n q^n$, we associate its ***L*-series**, or ***L*-function**

$$L(f,s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s} \ ,$$

a complex function of the complex variable s. Using the multiplicativity of the a_n, one shows that this function is defined for $\Re(s) > \frac{3}{2}$. The association

$$f = \sum_{n=1}^{\infty} a_n q^n \quad \rightsquigarrow \quad L(f,s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

is more than just formal. Indeed, it is gotten by an analytic transformation using a **Mellin integral**:

$$L(f,s) = \frac{(-2\pi i)^s}{\Gamma(s)} \int_0^{i\infty} f(z) z^{s-1} \, dz \ = \frac{(2\pi)^s}{\Gamma(s)} \int_0^{\infty} f(it) t^s \, \frac{dt}{t} \, .$$

With this, we may show that $L(f,s)$ actually has an analytic continuation to the entire complex plane and satisfies a functional equation.

Now consider an elliptic curve E defined over $\mathbb{Q}$. The conductor of E, an integral ideal of $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, may be identified with a positive integer N. In chapter 1, we associated an L-series to E also. We say that $E_{/\mathbb{Q}}$ is **modular**, or is a **Weil curve**, provided that

$$L(E_{/\mathbb{Q}}, s) = L(f_E, s)$$

for some normalized eigenform $f_E \in S_2(\Gamma_0(N))$. An equivalent definition that is more geometric in nature says that $E_{/\mathbb{Q}}$ is modular provided there exists a non-constant rational map

$$\phi : X_0(N) \to E_{/\mathbb{Q}} \ .$$

Then the elliptic curve's invariant differential ω (see [Sil86] for the definition) pulls back to $\phi^*(\omega) = c 2\pi i f_E(z) \ dz$, where $c \in \mathbb{Q}$ is called the **Manin constant**. When $c = \pm 1$, we say that E is a **strong** Weil curve, or that the parameterization ϕ is **strong**. Unfortunately, this geometric characterization of modularity will be lost when we consider elliptic curves defined over quadratic imaginary fields.

It is by now proved that indeed, all elliptic curves defined over $\mathbb{Q}$ are modular. The essential ingredients for a proof of that were supplied by Andrew Wiles and Richard Taylor in [Wil95] and [TW95], when they showed that semistable elliptic curves (curves of square free conductor) are always modular. This result is famous for it implied a proof of Fermat's Last Theorem. Conrad, Diamond and Taylor have extended these results to all curves whose conductor is not divisible by 27, and with the help of C. Breuil, they finally showed in the summer of 1999 that any elliptic curve defined over $\mathbb{Q}$ is indeed modular. See [Dar99] for an account of this.

Chapter 2

Conjectures of Birch and Swinnerton-Dyer Type in the Rational Case

Researchers so far have mostly concentrated their attention on the case of elliptic curves defined over $\mathbb{Q}$. Although a complete proof of the Birch and Swinnerton-Dyer conjecture still seems out of reach even in this case, there are nevertheless quite a few partial results and analogous conjectures that have been worked out. The first section of this chapter is mostly of historical nature, but the following sections form our main inspiration for the work to be done in chapter 3.

2.1 Partial Results on the Birch and Swinnerton-Dyer Conjecture

Papers about numerical and theoretical evidence for the conjecture are numerous, especially for elliptic curves defined over $\mathbb{Q}$, which is our interest in this section. Some results come from particular cases, although sometimes valid for infinite families of curves, and some results of theoretical nature apply to large classes of curves or prove a weaker statement. We will only mention some of the main evidences.

The Birch and Swinnerton-Dyer conjecture has been experimentally tested on many elliptic curves defined over $\mathbb{Q}$ already, and this supplies lots of evidence for it. One may look for instance at the original paper [BSD65] from Birch and Swinnerton-Dyer themselves. Of interest to us, some tests have also been done for elliptic curves defined over quadratic imaginary fields by Cremona and Whitley [CW94]. Note though that often in these tests, the order of the Shafarevich-Tate group Ш is not known. The verification then consists in saying that indeed, the Birch and Swinnerton-Dyer conjecture would be true provided that the order of Ш is some hypothetical value. In all cases, the value predicted for $|Ш|$ turns out to be a square number, in agreement with Cassels' result [Cas62].

Theorem 2.1 (Cassels' Pairing)
There exists an alternating bilinear pairing

$$Ш \times Ш \to \mathbb{Q}/\mathbb{Z}$$

whose kernel is precisely the group of divisible elements of Ш. In particular, the order of Ш or of any of its p-primary parts is a square, whenever finite. ■

Whether Ш is indeed finite or not is a still a deep question and we will not delve into that.

On the theoretical side, a first result that tends to confirm the validity of the Birch and Swinnerton-Dyer conjecture comes from the observation that isogenous elliptic curves have the same number of points modulo any prime p, so that they have identical L-functions. (The converse to this, the **isogeny theorem** of Serre is harder, see [Ser68].) So the first non-zero term of the L-series is an isogeny invariant, and conjecturally, the quantity

$$\Omega\,|Ш|\,R\prod_p c_p\,|T|^{-2}$$

appearing in the Birch and Swinnerton-Dyer conjecture should be an isogeny invariant. Although none of the individual terms here need be the same for isogenous curves, Cassels did prove this meaningful property in [Cas65].

The next main theoretical advance came from Coates and Wiles. For elliptic curves defined over $\mathbb{Q}$ that have complex multiplication (see [Sil86] for the definition), they prove in [CW77]:

Theorem 2.2 If $E_{/\mathbb{Q}}$ has complex multiplication and if $E(\mathbb{Q})$ is infinite, then $L(E_{/\mathbb{Q}}, 1) = 0$. ∎

Still for curves with complex multiplication, we also have Rubin's results [Rub87]:

Theorem 2.3 Let $E_{/\mathbb{Q}}$ be a curve with complex multiplication.

1. If $L(E_{/\mathbb{Q}}, 1) \neq 0$, then $Ш(E_{/\mathbb{Q}})$ is finite.
2. If the rank of $E_{/\mathbb{Q}}$ is at least 2, then $L(E_{/\mathbb{Q}}, s)$ vanishes at $s = 1$ with order at least 2. ∎

The year before that, Gross and Zagier came with striking theoretical evidence. In [GZ86], it is shown:

Theorem 2.4 Let $E_{/\mathbb{Q}}$ be a modular elliptic curve. A *simple* zero of $L(E_{/\mathbb{Q}}, s)$ at $s = 1$ implies that $E(\mathbb{Q})$ is infinite. ∎

The modularity of elliptic curves was discussed in section 1.3. We now know that this result applies to all elliptic curves E defined over $\mathbb{Q}$. Together with the results of Coates and Wiles and of Rubin, we obtain the following for curves $E_{/\mathbb{Q}}$ with complex multiplication.

Theorem 2.5 Let E be an elliptic curve defined over $\mathbb{Q}$ that has complex multiplication. If the order of vanishing of $L(E_{/\mathbb{Q}}, s)$ at $s = 1$ is less than or equal to 1, then it equals the rank of $E_{/\mathbb{Q}}$. ∎

In 1988, Kolyvagin [Kol89] significantly improved on the results of Coates-Wiles, Gross-Zagier and Rubin. He essentially proved the latter result for modular (hence all) elliptic curves $E_{/\mathbb{Q}}$, and proved also in these cases the finiteness of Ш.

Theorem 2.6 (Gross-Zagier, Kolyvagin)

If the order of vanishing ρ_E of $L(E_{/\mathbb{Q}}, s)$ at $s = 1$ satisfies $\rho_E \leq 1$, then $E(\mathbb{Q})$ has rank ρ_E and Ш is finite. ■

Kolyvagin essentially showed that the existence of a point of infinite order y_K on $E(\mathbb{K})$, for some chosen quadratic imaginary field $\mathbb{K}$, implies that the rank of $E(\mathbb{K})$ is 1 and that Ш$(E/\mathbb{K})$ is finite. The point y_K is called a **Heegner point** and is constructed using the theory of complex multiplication. To get the above theorem, we need to descend Kolyvagin's result to $E(\mathbb{Q})$ and make a connection with the L-functions. This latter task is still quite difficult. It is accomplished with some further analytic results and the work of Gross and Zagier, connecting the height of Heegner points with derivatives of L-functions.

2.2 Modular Symbols

In order to present some other conjectures that are analogous to that of Birch and Swinnerton-Dyer, we need to introduce the theory of modular symbols.

Consider f an eigenform in $S_2(\Gamma_0(N))$. We define the **modular symbol** λ_f associated to the cusp form f as a function $\lambda_f : \mathbb{P}^1(\mathbb{Q}) \to \mathbb{C}$ by

$$\begin{aligned} \lambda_f(x) = & \; 2\pi \textstyle\int_0^\infty f(x+it)\, dt \\ = & \; -2\pi i \textstyle\int_x^{i\infty} f(z)\, dz \end{aligned}$$

The second equality holds since the fundamental group of the upper half plane is trivial.

Modular symbols permit us to interpolate special values of L-functions. For example, the definition of the L-function associated to a cusp form as a Mellin transform immediately yields

$$L(f,1) = \frac{(2\pi)^1}{\Gamma(1)} \int_0^\infty f(it) t^1 \frac{dt}{t} = 2\pi \int_0^\infty f(it)\, dt = \lambda_f(0).$$

Modular symbols were really born in a small paper of Birch [Bir71] in which he uses them to compute special values of twists of complex L-functions. This result, theorem 2.9 below, is actually fundamental to this thesis, so we will prove it.

Consider the cusp form $f = \sum_{n=1}^{\infty} a_n q^n$ and a Dirichlet character modulo m

$$\chi : \ (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^* .$$

We define the **twist** of f by χ as

$$f_\chi = \sum_{n=1}^{\infty} \chi(n) a_n q^n ,$$

and a twisted L-function by

$$L(f, \chi, s) = L(f_\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n) a_n}{n^s}$$

This latter is derived from the Mellin transform

$$L(f, \chi, s) = \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty f_\chi(it) t^s \frac{dt}{t} = \frac{(-2\pi i)^s}{\Gamma(s)} \int_0^{i\infty} f_\chi(z) z^{s-1} \, dz \, .$$

Remark 2.1 A twist of a cusp form is also a cusp form, but for another congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. See [Kob93, chapter III] for the details. □

For a primitive Dirichlet character χ of conductor m, we define its **Gauss sum**:

$$\tau(\chi) = \sum_{a=0}^{m-1} \chi(a) e^{2\pi i a/m} \ .$$

Lemma 2.7 Let χ be a primitive Dirichlet character modulo m, and let $\tau(\chi)$ be its Gauss sum. For any integer b, we have

$$\sum_{a=0}^{m-1} \chi(a) e^{2\pi i ab/m} = \overline{\chi(b)} \tau(\chi).$$

Proof. [Miy89, pp.80-81] ■

Lemma 2.8 Let $\xi_m = e^{2\pi i/m}$. Define $\delta_m(n,l) = \frac{1}{m}\sum_{b=0}^{m-1} \xi_m^{b(n-l)}$.
Then $\delta_m(n,l) = \begin{cases} 1 & \text{if } n \equiv l \pmod{m}, \\ 0 & \text{otherwise.} \end{cases}$
$\delta_m(n,l)$ is thus some kind of "modular" Kronecker delta.

Proof. If m divides $n-l$, then

$$\sum_{b=0}^{m-1} (\xi_m^{n-l})^b = \sum_{b=0}^{m-1} 1^b = m.$$

Otherwise $\xi_m^{n-l} \neq 1$ and we may write

$$\sum_{b=0}^{m-1} (\xi_m^{n-l})^b = \frac{1-(\xi_m^{n-l})^m}{1-\xi_m^{n-l}} = \frac{1-1^{n-l}}{1-\xi_m^{n-l}} = 0.$$

■

Theorem 2.9 (Birch-Manin)

Let χ be an even primitive Dirichlet character mod m with Gauss sum $\tau(\chi)$. Then

$$L(f,\chi,1) = \frac{\tau(\chi)}{m} \sum_{b \bmod m} \bar{\chi}(b)\lambda_f(\frac{b}{m}).$$

Proof.

$$L(f,\chi,1) = \frac{(-2\pi i)^1}{\Gamma(1)} \int_0^{i\infty} \left(\sum_{n=1}^{\infty} \chi(n) a_n e^{2\pi i n z} \right) z^{1-1}\, dz$$

We do not write the details, but standard convergence arguments as in the proof of the analytic continuation of the modular L-function, using the Atkin-Lehner involution to split the integral and avoid integrating close to $z=0$, permit rearrangements of the terms, so

$$L(f,\chi,1) = -2\pi i \int_0^{i\infty} \sum_{l=0}^{m-1} \chi(l) \sum_{n \equiv l \mod m} a_n e^{2\pi i n z}\, dz.$$

The clever trick is to introduce the above $\delta_m(n,l)$ in the formula:

$$\begin{aligned} L(f,\chi,1) &= -2\pi i \int_0^{i\infty} \sum_{l=0}^{m-1} \chi(l) \sum_{n=1}^{\infty} \left(\frac{1}{m} \sum_{b=0}^{m-1} \xi_m^{b(n-l)} \right) a_n e^{2\pi i n z}\, dz \\ &= \frac{1}{m} \sum_{b=0}^{m-1} \left(\sum_{l=0}^{m-1} \chi(l) \xi_m^{-bl} \right) \left(-2\pi i \int_0^{i\infty} \sum_{n=1}^{\infty} a_n \xi_m^{bn} e^{2\pi i n z}\, dz \right) \end{aligned}$$

Using lemma 2.7, we get

$$L(f,\chi,1)=\frac{1}{m}\sum_{b \mod m}\bar{\chi}(b)\tau(\chi)\left(-2\pi i\int_0^{i\infty}\sum_{n=1}^{\infty}a_n e^{2\pi i n(z+b/m)}\,dz\right)$$

and the result follows. ■

$f\in S_2(\Gamma_0(N))$ being fixed, λ_f essentially just associates to $x\in\mathbb{P}^1(\mathbb{Q})$ a path from x to $i\infty$. The invariance of $f(z)dz$ under $\Gamma_0(N)$ descends this path to one on $X_0(N)$. We therefore often extend the definition of modular symbols and view them as formal elements of the homology of this curve:

$$\lambda_f:\mathbb{P}^1(\mathbb{Q})\to H_1(X_0(N),\mathbb{R}).$$

We then denote the homology class of a path from a to b in $\mathcal{H}^*$ projected to $X_0(N)$ by $\{a,b\}$.

Remarks 2.2

1. This new notion of modular symbol is a strict extension of the previous definition for the obvious reason that paths in $\mathcal{H}^*$ are no more restricted to be from cusps to infinity.

2. The original f does not appear explicitly in $H_1(X_0(N),\mathbb{R})$. The dimension of $S_2(\Gamma_0(N))$ may be greater than 1. This will cause no confusion, for f is fixed by the context. More precisely, a modular symbol would be a pair $(\delta,f)\in H_1(X_0(N),\mathbb{R})\times S_2(\Gamma_0(N))$, and for a path from a to b in $\mathcal{H}^*$ we would write $\{a,b\}_f$. □

$\mathcal{H}$ being simply connected, the following formal properties of modular symbols are evident.

Proposition 2.10 Let $a,b,c\in\mathcal{H}^*$, and let $\sigma\in\Gamma_0(N)$. Then

1. $\{a,a\}=0$;

2. $\{a,b\}=-\{b,a\}$;

3. $\{a, b\} + \{b, c\} = \{a, c\}$;

4. $\{\sigma a, \sigma b\} = \{a, b\}$;

5. $\{a, \sigma a\} \in H_1(X_0(N), \mathbb{Z})$. ■

We also have

Corollary 2.11 With γ also in $\Gamma_0(N)$,

1. $\{a, \sigma a\} = \{b, \sigma b\}$;

2. $\{a, \sigma\gamma a\} = \{a, \sigma a\} + \{a, \gamma a\}$.

Proof.

1. $\{a, \sigma a\} = \{a, b\} + \{b, \sigma a\} = \{a, b\} + \{b, \sigma b\} + \{\sigma b, \sigma a\}$
   $= \{a, b\} + \{b, \sigma b\} + \{b, a\} = \{b, \sigma b\}$.

2. $\{a, \sigma\gamma a\} = \{a, \sigma a\} + \{\sigma a, \sigma\gamma a\} = \{a, \sigma a\} + \{a, \gamma a\}$. ■

According to corollary 2.11, the following notation is well defined: $\{\sigma\} = \{a, \sigma a\}$ for any $a \in \mathcal{H}^*$. Also, for $\alpha \in \mathcal{H}^*$ we will let $\{\alpha\}$ denote $\{\alpha, i\infty\}$. When α is a cusp equivalent to $i\infty$ under $\Gamma_0(N)$, then any representative path for $\{\alpha\}$ on $X_0(N)$ is closed, so that $\{\alpha\} \in H_1(X_0(N), \mathbb{Z})$. More generally, we have the important **Manin-Drinfeld Theorem** stating that for any cusp α not necessarily equivalent to $i\infty$, $\{\alpha\}$ is in the *rational* homology. We proceed to prove this theorem.

Lemma 2.12 Let $\alpha_1 = p_1/q_1$ and $\alpha_2 = p_2/q_2$ be any two rational numbers written in lowest terms. Then α_1 is equivalent to α_2 modulo $\Gamma_0(N)$ iff multiplicative inverses s_i of p_i modulo q_i, $(i = 1, 2)$, can be found such that $s_1 q_2 \equiv s_2 q_1 \mod (q_1 q_2, N)$.

Proof. [Cre97, p. 16]. ■

The action of Hecke operators on $S_2(\Gamma_0(N))$ may be dualized to an action on modular symbols. Let $\sigma \in \mathrm{GL}_2^+(\mathbb{R})$. If $\delta = \{a, b\}$, then $\sigma\delta$ is defined as $\sigma\delta = \{\sigma a, \sigma b\}$. This makes sense, since $\mathcal{H}$ is simply connected, so that $\{a, b\}$ and $\{\sigma a, \sigma b\}$ are completely determined by their endpoints only. Moreover, this respects the duality between $H_1(X_0(N))$ (the modular symbols) and $H^1(X_0(N)) \cong S_2(\Gamma_0(N))$:

$$\langle \delta, f|_{T_p} \rangle \;=\; \langle T_p\delta, f \rangle.$$

For $p \nmid N$, we then have

$$\begin{aligned} T_p\{\alpha, i\infty\} &= \left(\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} + \sum_{k=0}^{p-1} \begin{pmatrix} 1 & k \\ 0 & p \end{pmatrix} \right) \{\alpha, i\infty\} \\ &= \{p\alpha, i\infty\} + \sum_{k=0}^{p-1} \{\frac{\alpha+k}{p}, i\infty\}. \end{aligned}$$

Theorem 2.13 (Manin-Drinfeld)
For any cusp $\alpha \in \mathbb{P}^1(\mathbb{Q})$, $\{\alpha\}_f \in H_1(X_0(N), \mathbb{Q})$.

The essential ingredients of the proof are shown in [Maz72], although there is a mistake there in the characterization of the equivalence classes of cusps. A more thorough version of this proof can be found in Manin's original article [Man72].

Proof. This proof is a corrected and more detailed version of Mazur's presentation. It uses the action of Hecke operators to "close the path".

From the above formula, for $p \nmid N$, we have

$$T_p\{\alpha, i\infty\} = \{p\alpha, \alpha\} + \{\alpha, i\infty\} + \sum_{k=0}^{p-1} \left(\{\frac{\alpha+k}{p}, \alpha\} + \{\alpha, i\infty\} \right). \tag{2.1}$$

For f a Hecke eigenform attached to an elliptic curve $E_{/\mathbb{Q}}$, we have that $T_pf = a_pf$ for some integer a_p. Let $\{a, b\}_f$ be the natural image of $\{a, b\} \in H_1(X_0(N), \mathbb{Q})$ in $H_1(E, \mathbb{Q})$ induced by the modular parameterization ϕ. Since the map induced by ϕ factors through $H_1(X_0(N), \mathbb{Q})/I_f$ where I_f is the ideal generated by $\langle T_p - a_p \mid p \text{ prime}, \; p \nmid N \rangle$, it follows that the image of $T_p\{\alpha, i\infty\}_f$ in $H_1(E, \mathbb{Q})$ is equal to $a_p\{\alpha, i\infty\}_f$. Hence by (2.1), we have

$$(a_p - 1 - p)\{\alpha, i\infty\}_f = \{p\alpha, \alpha\}_f + \sum_{k=0}^{p-1} \{\frac{\alpha+k}{p}, \alpha\}_f.$$

Note that $a_p - 1 - p$ is not zero as explained in remark 2.3 below. We need to find some p for which the right hand side will be in the integral homology. The claim, suggested by Mazur, is that any $p \equiv 1 \pmod{N}$ will do. Indeed, let $\alpha_1 = p_1/q_1$ be α and $\alpha_2 = p_2/q_2$ be any of $p\alpha$ or $(\alpha + k)/p$ written in lowest terms. One must verify that lemma 2.12 can be solved for s_1 and s_2 in all cases.

- Consider the case $\alpha_2 = p\alpha$ and suppose $p \nmid q_1$. Then $\frac{p_2}{q_2} = \frac{pp_1}{q_1}$ are in lowest terms, and with the right choices of signs, $p_2 = pp_1$ and $q_2 = q_1$. Lemma 2.12 then requires a solution to the system of congruences

$$\begin{aligned} s_1 p_1 &\equiv 1 && \mod q_1, \\ s_2 p p_1 &\equiv 1 && \mod q_1, \\ s_1 q_1 &\equiv s_2 q_1 && \mod (q_1^2, N). \end{aligned}$$

  Since both p and p_1 are coprime to q_1, the first two equations are solvable for s_1 and s_2 mod q_1, and even mod q_1^2, in which case any solution to these will satisfy

$$s_1 \equiv s_2 p \mod q_1^2,$$

  hence also mod (q_1^2, N). But this also satisfies the third equation,

$$s_2 p q_1 \equiv s_2 q_1 \mod (q_1^2, N),$$

  since $p \equiv 1 \bmod N$, thus also mod (q_1^2, N).

- The cases $\alpha_2 = \frac{p_1}{q_1/p}$, $\alpha_2 = \frac{p_1 + q_1 k}{q_1 p}$ and $\alpha_2 = \frac{(p_1+q_1k)/p}{q_1}$ are treated in similar fashions. ■

Remarks 2.3

1. There is another way to look at this result, whose underlying idea is very beautiful. It consists in looking at the projection of the path on the Jacobian $J_0(N)$. Cusps correspond to points of finite order under the group law of this abelian variety. The path can thus be stretched by an integral factor and be closed. This is quite elegant, but unfortunately this will not generalize to modular symbols and cusp forms for imaginary quadratic fields.

2. The above proof requires $a_p - 1 - p \neq 0$. Given that we consider cusp forms f associated to elliptic curves, we then notice that $a_p - 1 - p = -\mathcal{N}_p$. This is is never zero since $\mathcal{N}_p$ always counts at least an origin on the reduction at p of E_f. $\square$

The use of modular symbols in the context of the Birch and Swinnerton-Dyer conjecture requires us to use modular symbols associated to modular elliptic curves $E_{/\mathbb{Q}}$. This is done through the modular parameterization

$$\phi : X_0(N) \to E$$

which induces a map

$$\tilde{\phi} : H_1(X_0(N)) \to H_1(E)\,.$$

Although $X_0(N)$ is defined as a complex manifold $\Gamma_0(N)\backslash\mathcal{H}^*$, it may be shown that it is actually an algebraic variety defined over $\mathbb{Q}$, and that ϕ is a rational map.

The modular symbol $\{\alpha\} = \{\alpha, i\infty\}$ associated to a cusp α being in the rational homology $H_1(X_0(N), \mathbb{Q})$, $\tilde{\phi}$ permits us to view it as an element of the rational homology $H_1(E, \mathbb{Q})$ of $E_{/\mathbb{Q}}$.

We may simplify our point of view further. Indeed, we have that the dimension of $H_1(E, \mathbb{R})$ is twice the genus of $E_{/\mathbb{C}}$, this latter being one by definition. Complex conjugation acts as an involution on $H_1(E, \mathbb{R})$, and splits it into real and pure imaginary parts:

$$H_1(E, \mathbb{R}) \cong H_1^+(E, \mathbb{R}) \oplus H_1^-(E, \mathbb{R}),$$

where complex conjugation has eigenvalue $+1$ on the 1-dimensional real part $H_1^+(E, \mathbb{R})$ and -1 on the 1-dimensional pure imaginary part $H_1^-(E, \mathbb{R})$.

We will consider the projection to the real part $H_1^+(E, \mathbb{R})$ only. According to Manin-Drinfeld (theorem 2.13), we are then led to identify the modular symbol $\{\alpha\}$ associated to a cusp α with an element $[\alpha] \in H_1^+(E, \mathbb{Q}) \cong \mathbb{Q}$.

The factor of conversion between $[\alpha]$ and the real part of $\lambda_f(\alpha)$ is the **real period** Ω^+ of $E_{/\mathbb{Q}}$, that is, $\mathrm{Re}(\lambda_f(\alpha)) = \Omega^+[\alpha]$. The real period can be computed directly as

$$\Omega^+ = \frac{1}{2}\int_{E(\mathbb{R})} |\omega|$$

where ω is the invariant differential of E mentioned in chapter 1.

Nowadays, modular symbols have become famous for many applications. They are used for computing special values of complex L-functions, to define p-adic L-functions associated to cusp forms, to study analogous (p-adic and Mazur-Tate) versions of the Birch and Swinnerton-Dyer conjecture, and Henri Darmon has recently used them to compute rational points on elliptic curves [Dar].

2.3 p-Adic Birch and Swinnerton-Dyer Conjectures

So far, we have been concerned with the behaviour and special values of the L-function $L(E_{/\mathbb{Q}}, s)$ associated to an elliptic curve. This is a *complex* valued function of a *complex* variable s. In [MSD74], Mazur and Swinnerton-Dyer figured out that one could use modular symbols to attach to elliptic curves $E_{/\mathbb{Q}}$ a *p-adic* L-function $L_p(E_{/\mathbb{Q}}, s)$ of a *p-adic* variable s. They proved a functional equation and naïvely stated a conjecture of Birch and Swinnerton-Dyer type. In 1986, Mazur, Tate and Teitelbaum pushed the analysis of this p-adic L-function further. They made experimental tests, gave precise Birch and Swinnerton-Dyer type conjectures, and stated relationships between the p-adic and the complex L-functions. We give a short description of this work. Refer to the article [MTT86] for the details.

The elliptic curve $E_{/\mathbb{Q}}$ being modular, we define a p-adic L-function $L_p(f_E, s)$ for the cusp form f_E attached to $E_{/\mathbb{Q}}$ (see section 1.3), and transform it very slightly into a p-adic L-function $L_p(E_{/\mathbb{Q}}, s)$ associated to $E_{/\mathbb{Q}}$. Our definition of $L_p(f, s)$ for a cusp form f should be analogous to that of the usual complex L-function $L(f, s)$, replacing only archimedean analysis by p-adic analysis as much as possible. To this end, we use the definition of $L(f,s)$ in terms of a Mellin transform.

$$L(f,s) = \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty f(it)t^{s-1}\,dt = \frac{(2\pi)^s}{\Gamma(s)} \int_{\mathbb{R}^*_{>0}} t^s \left(f(it)\frac{dt}{t} \right).$$

This regrouping is suggestive of the following modifications.

1. We should integrate over a p-adic group. This will be some

$$\mathbb{Z}^*_{p,d} := \varprojlim_n (\mathbb{Z}/dp^n\mathbb{Z})^* \cong \mathbb{Z}_p^* \times (\mathbb{Z}/d\mathbb{Z})^*,$$

   for d coprime to p.

2. $f(it)\frac{dt}{t}$ should be seen as a "complex measure associated to f", and it requires to be changed for some "p-adic measure associated to f", $d\mu_f(x)$, yet to be defined. This is where modular symbols associated to f will come into play.

3. $t^s = e^{s\log t}$ is not well defined in the p-adic context. We need to take the roots of unity out of t. It is then natural to replace it by the p-adic exponential $\langle x\rangle^s$. See for example, [Was97, Section 5.1] where the structure of $\mathbb{Z}_p^*$ and $\mathbb{C}_p^*$ are described. Roughly, put $q = p$ except for $p = 2$ in which case we put $q = 4$. Then any $a \in \mathbb{Z}_p^*$ can be written uniquely as $a = \omega(a)\langle a\rangle$, where $\langle a\rangle \in 1 + q\mathbb{Z}_p$ and $\omega(a)$, the Teichmüller character of a, is the unique $\phi(q)^{\text{th}}$ root of unity in $\mathbb{Z}_p$ satisfying $a \equiv \omega(a) \pmod q$.

Thus up to some fudge factors, we should have

$$L_p(f,s) \text{ ``}=\text{'' } \int_{\mathbb{Z}^*_{p,d}} \langle x\rangle^s d\mu_f(x)\,.$$

We proceed to the construction of the p-adic measure μ_f.

We suppose f is an eigenform for T_p with eigenvalue a_p, for some p coprime to its level N. Suppose further that a_p is a unit in $\mathbb{Z}_p$. This is no major restriction, since we will consider forms f_E associated to an elliptic curve E, so that we only have to use one of the infinitely many primes p of ordinary reduction for E (see [Sil86, chapter V]).

Let α be the unique unit root of $X^2 - a_pX + p$, the characteristic polynomial of T_p. For a coprime to pd, Mazur, Tate and Teitelbaum define in section I.10 of [MTT86]

$$\mu_f(a + p^r d\mathbb{Z}_{p,d}) := \frac{1}{\alpha^r}\lambda_f(\frac{a}{p^r d}) - \frac{1}{\alpha^{r+1}}\lambda_f(\frac{a}{p^{r-1}d})\,. \tag{2.2}$$

Using the action of the Hecke operator T_p on f, one shows that μ_f is a distribution:

$$\sum_{\substack{b \equiv a \pmod{p^r d} \\ b \mod p^{r+1}d}} \mu_f(b + p^{r+1}d\mathbb{Z}_{p,d}) \;=\; \mu_f(a + p^r d\mathbb{Z}_{p,d})$$

Remark 2.4 The fact that this distribution is actually a measure follows from the fact that the modular symbols entering the definition of μ_f have bounded denominators. This can be seen from the proof of the Manin-Drinfeld theorem. We will come back to this later, as this is important in conjectures of Mazur-Tate type as well. □

To give some meaning to the coming definition of the p-adic L-function, we really need to give a general version including twists by Dirichlet characters. Let χ be a Dirichlet character of conductor m, coprime to the level N. We define

$$L_p(f, \chi, s) := \int_{\mathbb{Z}_{p,d}^*} \langle x\rangle^s \chi(x) d\mu_f(x)$$

where $m = p^r d$, d coprime to p. Of course in the p-adic context, a Dirichlet character mod m of $\mathbb{Z}_{p,d}^*$ is a character of $\mathbb{Z}_{p,d}^*$ which is defined modulo $m\mathbb{Z}_{p,d}^*$ for some integer m. In particular, it is a character of finite order. Then we may define $L_p(f, s)$ using the principal character, that is, the primitive trivial character (conductor 1).

$$L_p(f, s) := L_p(f, \chi = \mathbf{1}, s) = \int_{\mathbb{Z}_p^*} \langle x\rangle^s d\mu_f(x)$$

We hope that $L_p(f, s)$ has interesting special values. However, we will only be interested in the special values at $s = 0$. To remedy this weakness, we look at them for infinitely many characters. For this, we define the ***p*-adic multiplier**

$$e_p(\chi) := \frac{1}{\alpha^r}(1 - \frac{\chi(p)}{\alpha})(1 - \frac{\chi^{-1}(p)}{\alpha})\,.$$

χ^{-1} is the inverse character to χ. Thus $\chi^{-1}(p) = \chi(p)^{-1}$ except when $\chi(p) = 0$, in which case $\chi^{-1}(p) = 0$ also. Note that we have $e_p(\chi) = 1/\alpha^r$ if p divides m. Mazur, Tate and Teitelbaum then claim

Proposition 2.14 For even primitive Dirichlet characters χ of conductor m coprime to the level N,

$$L_p(f, \chi, 0) = e_p(\chi)\tau(\chi)L(f_{\chi^{-1}}, s = 1) \tag{2.3}$$

where $\tau(\chi)$ is the Gauss sum associated to χ.

These are the nice interpolation properties that we desire of $L_p(f, s)$. The proof is a consequence of the Birch-Manin theorem (theorem 2.9). We write a proof in the particular case where p divides m, for the reader to see its use. This case of the proof does not appear in [MTT86], but a discussion on the case where p does not divide m is included there, thus yielding the complete picture.

Sketch of proof. By definition,

$$L_p(f, \chi, 0) = \int_{\mathbb{Z}^*_{p,d}} \langle x\rangle^0 \chi(x)\ d\mu_f(x)$$

χ is a Dirichlet character modulo m, so $\chi(x) = \chi(b)$ is constant on $x \in b + m\mathbb{Z}_{p,d}$. Therefore

$$\begin{aligned} L_p(f, \chi, 0) &= \sum_{b\in(\mathbb{Z}/m\mathbb{Z})^*} \chi(b) \int_{b+m\mathbb{Z}_{p,d}} d\mu_f(x) \\ &= \sum_{b\in(\mathbb{Z}/m\mathbb{Z})^*} \chi(b)\mu_f(b + m\mathbb{Z}_{p,d}) \end{aligned}$$

We assumed that p divides m, in which case b is coprime to pd, and we use equation (2.2) to compute the measure of $b + p^r d\mathbb{Z}_{p,d}$.

$$\begin{aligned} L_p(f, \chi, 0) &= \sum_{b\in\mathbb{Z}/m\mathbb{Z}} \chi(b)[\frac{1}{\alpha^r}\lambda_f(\frac{b}{m}) - \frac{1}{\alpha^{r+1}}\lambda_f(\frac{b}{m/p})] \\ &= \frac{1}{\alpha^r}\sum_{b\in\mathbb{Z}/m\mathbb{Z}} \chi(b)\lambda_f(\frac{b}{m}) - \frac{1}{\alpha^{r+1}}\sum_{b\in\mathbb{Z}/m\mathbb{Z}} \chi(b)\lambda_f(\frac{pb}{m}) \end{aligned}$$

We use Birch-Manin (theorem 2.9) on the first sum to get

$$L_p(f,\chi,0) = e_p(\chi)\frac{m}{\tau(\bar{\chi})}L(f,\bar{\chi},1) - \frac{1}{\alpha^{r+1}}\sum_{b\in\mathbb{Z}/m\mathbb{Z}}\chi(b)\lambda_f(\frac{pb}{m})$$

We need now show that the remaining sum vanishes. The proof is similar to that of Birch-Manin.

$$\begin{aligned}
\sum_{b\in\mathbb{Z}/m\mathbb{Z}}\chi(b)\lambda_f(\frac{pb}{m}) &= \sum_{b\in\mathbb{Z}/m\mathbb{Z}}\chi(b)\left(-2\pi i\int_0^{i\infty}\sum_{n=1}^{\infty}a_n e^{2\pi i n(z+pb/m)}\,dz\right)\\
&= -2\pi i\sum_{b\in\mathbb{Z}/m\mathbb{Z}}\left(\frac{1}{\tau(\bar{\chi})}\sum_{l=0}^{m-1}\bar{\chi}(l)\xi_m^{-bl}\right)\cdot\int_0^{i\infty}\sum_{n=1}^{\infty}a_n e^{2\pi i n z}\xi_m^{bpn}\,dz\\
&= \frac{-2\pi i}{\tau(\bar{\chi})}\int_0^{i\infty}\sum_{l=0}^{m-1}\bar{\chi}(l)\sum_{n=1}^{\infty}\left(\sum_{b\in\mathbb{Z}/m\mathbb{Z}}\xi_m^{-bl}\xi_m^{bpn}\right)a_n e^{2\pi i n z}\,dz\\
&= \frac{-2\pi i}{\tau(\bar{\chi})}\int_0^{i\infty}\sum_{l=0}^{m-1}\bar{\chi}(l)\sum_{n=1}^{\infty}m\delta_m(pn,l)a_n e^{2\pi i n z}\,dz
\end{aligned}$$

For $\delta_m(pn,l)$ to be non-zero, we require l to be a multiple of p, since we assumed that p divides m. But in that case, it is $\bar{\chi}(l)$ which is zero. Thus $\sum_{b\in\mathbb{Z}/m\mathbb{Z}}\chi(b)\lambda_f(\frac{pb}{m}) = 0$ as desired. ■

For primitive Dirichlet characters χ, we may now define twisted p-adic L-functions associated to modular elliptic curves. Let f_E be the cusp form associated to $E_{/\mathbb{Q}}$. Then

$$L_p(E,\chi,s) := L_p(f_E,\chi,s-1) \quad\text{and}\quad L_p(E,s) := L_p(E,\chi=\mathbf{1},s)\,.$$

Here, $\chi = \mathbf{1}$ must be primitive, so it is the principal character, that is, the trivial character of conductor 1.

The naïve statement of a p-adic version of the Birch and Swinnerton-Dyer conjecture given in [MSD74] essentially says that the order of vanishing of $L_p(f_E,s)$ at $s=1$ is equal to the rank of $E(\mathbb{Q})$. According to proposition 2.14, this would be equivalent to the usual Birch and Swinnerton-Dyer conjecture if the p-adic multiplier were never to vanish. However, it does sometimes vanish. This happens for the principal character χ when p is a prime of split multiplicative reduction for E. According to experimental tests that have been performed by Mazur, Tate and Teitelbaum, it has been conjectured that

Conjecture 2.15 (The Exceptional Zero Conjecture)
For primes p of split multiplicative reduction for E, the order of vanishing of $L_p(E,s)$ at $s=1$ is exactly 1 more than that of the classical complex L-function $L(E,s)$ at $s=1$. ■

This conjecture leads us to the following p-adic version of the weak Birch and Swinnerton-Dyer conjecture.

Conjecture 2.16 (p-adic weak Birch and Swinnerton-Dyer conjecture)
Let $E_{/\mathbb{Q}}$ be a (modular) elliptic curve. Let $L_p(E,s)$ be the p-adic L-function associated to E as above. Let ρ be the order of vanishing of $L_p(E,s)$ at $s=1$, and let r be the rank of $E(\mathbb{Q})$. Then

$$\rho = \begin{cases} r+1 & \text{if } E \text{ has split multiplicative reduction at } p, \\ r & \text{otherwise.} \end{cases}$$

■

Complete statements of the usual Birch and Swinnerton-Dyer conjecture also give a conjectural value for the first non vanishing Taylor coefficient. Mazur, Tate and Teitelbaum also conjecture such a value in the p-adic case.

Conjecture 2.17 (p-adic strong Birch and Swinnerton-Dyer conjecture)
Conjecture 2.16 holds and

$$L_p^{(\rho)}(E, s=1) = |\text{Ш}(E_{/\mathbb{Q}})|\mathcal{S}_p(E_{/\mathbb{Q}})\left(\prod c_l\right)\Omega^+$$

where $\mathcal{S}$ is called the p-adic sparsity and is defined using the Tate period $q_p(E)$:

$$\mathcal{S}_p(E_{/\mathbb{Q}}) = \begin{cases} R_p(E_{/\mathbb{Q}})/|T|^2 & \text{when } \rho = r, \\ \frac{\log_p(q_p(E))}{\mathrm{ord}_p(q_p(E))}\frac{R_p^{\mathrm{Sch}}(E_{/\mathbb{Q}})}{|T|^2} & \text{when } \rho = r+1. \end{cases}$$

■

The quantity $\frac{\log_{p(q_p(E))}}{\mathrm{ord}_{p(q_p(E))}}$ is usually denoted $\mathcal{L}_p(E)$ and called the $\mathcal{L}$-invariant of $E_{/\mathbb{Q}}$. $R_p(E_{/\mathbb{Q}})$ and $R_p^{\mathrm{Sch}}(E_{/\mathbb{Q}})$ are p-adic regulators for E, the most complex objects in here. As usual regulators, they measure the hyper-volume of a fundamental domain for the lattice of rational points of infinite order. Their definition in the p-adic context requires a theory of p-adic heights. Mazur and Tate in [MT83] and [MT91] develop a theory of canonical p-adic height pairings, which they use in [MTT86] for the definition of p-adic regulators.

2.4 Mazur-Tate Conjectures

Mazur-Tate conjectures were introduced as refinements of the p-adic Birch and Swinnerton-Dyer conjecture during a seminar held at Harvard around 1986. The essential remnants of this seminar consist in a paper by Gross [Gro88] as well as a paper by Mazur and Tate [MT87]. In this latter, theta elements for elliptic curves over the rationals are defined, and conjectures analogous to those of Birch and Swinnerton-Dyer are stated about them. In this thesis, we wish to generalize this latter work to elliptic curves defined over quadratic imaginary fields.

To bring in the Mazur-Tate conjectures for elliptic curves defined over $\mathbb{Q}$, we first restate the usual Birch and Swinnerton-Dyer conjecture for such elliptic curves in a suggestive way, as done in [Dar94].

Conjecture 2.18 (Birch and Swinnerton-Dyer, usual**)**
Let $E/\mathbb{Q}$ be an elliptic curve, $L(E,s)$ its usual complex L-function, and let r be the rank of $E/\mathbb{Q}$.

0) The complex L-function a priori defined for $\Re(s) > \frac{3}{2}$ has an analytic continuation to an entire function of the complex plane.

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

2) The value of the first non-zero Taylor coefficient is:

$$\lim_{s\to 1}\frac{L(E,s)}{(s-1)^r}=\frac{\Omega\,|Ш|\,R\prod_p c_p}{|T|^2}\ .$$

■

We give another formulation of this using theta-elements. Let S be the ring of germs of analytic functions of a complex variable s in neighborhoods of $s=1$. Let I be the ideal of germs that vanish at $s=1$. Then $S/I\cong\mathbb{C}$, the equivalence classes being given by the value of the germ at $s=1$. Similarly, $I^r/I^{r+1}\cong\mathbb{C}$, the equivalence classes being given by the value of the r-th Taylor coefficient, the preceding ones all vanish.

Conjecture 2.19 (Birch and Swinnerton-Dyer, restated)
Let $E/\mathbb{Q}$ be an elliptic curve, $L(E,s)$ its usual complex L-function, and let r be the $\mathbb{Z}$-rank of $E/\mathbb{Q}$.

0) $L(E,s)$ has an analytic continuation to an entire function.
   Let θ_E be its germ at $s=1$.

1) $\theta_E\in I^r\setminus I^{r+1}$.
   Let $\tilde\theta_E$ denote its projection to $I^r/I^{r+1}\cong\mathbb{C}$.

2) $\tilde\theta_E=\dfrac{\Omega\,|Ш|\,R\prod_p c_p}{|T|^2}$. ■

This θ_E is a *complex* theta-element. We will try to replace it with a more *algebraic* theta-element, belonging to a group ring $Z[G]$. However, analysis will still enter its definition. This is unavoidable: after all, the Birch and Swinnerton-Dyer conjecture is precisely an intrusion of analysis in the understanding of the algebraic problem of determining the rank, and analogous conjectures ultimately do the same.

We would like the theta-element to be closely related to the expression

$$\sum_{b\mod m}\chi(b)\lambda_f\left(\frac{b}{m}\right)\tag{2.4}$$

where χ is a Dirichlet character of conductor m. By Birch-Manin (theorem 2.9), this expression contains information about twisted complex L-functions at 1. Recall that such interpolation properties were at the heart of our satisfaction with the definition of the p-adic L-functions $L_p(E_{/\mathbb{Q}}, \chi, s)$, and that Birch-Manin is the main ingredient in the proof of the relationship between the p-adic and complex L-functions (2.3). We would thus like to transform (2.4) into an element of some group ring $Z[G]$. Note that even though we will be interested in having strong integrality properties for Z, this latter need not, a priori, be $Z = \mathbb{Z}$.

Recall from section 2.2 that for cusps $x = \frac{b}{m}$, the Manin-Drinfeld Theorem (theorem 2.13) told us that $\lambda_f(x)$ is an element of the rational homology $H_1(X_0(N), \mathbb{Q})$. We further identified $\{x\} = \lambda_f(x)$ as an element of $\mathbb{Q}$ itself through the projection on the real part of the decomposition $H_1(X_0(N), \mathbb{Q}) \cong H_1^+(X_0(N), \mathbb{Q}) \bigoplus H_1^-(X_0(N), \mathbb{Q})$. In this way, $\lambda_f(\frac{b}{m})$ is associated to an element $[\frac{b}{m}] \in \mathbb{Q}$.

We have just mentioned that we desire strong integrality properties of Z. So it is not sufficient to put $Z = \mathbb{Q}$ and to claim that $\lambda_f(x)$ is identified with $[x] \in Z = \mathbb{Q}$. However, a short look at the proof of the Manin-Drinfeld theorem permits us to realize that the denominator of $[x] \in \mathbb{Q}$ is actually bounded independently of the cusp x. Indeed, the denominators are of the form $p + 1 - a_p$ where p is any prime such that T_p can be used to close the path, that is, $p \equiv 1 \mod N$. Thus the denominators appearing in the modular symbol computations must divide

$$S := \gcd_{p \equiv 1 \mod N} (p + 1 - a_p),$$

independently of the cusp x. We let $Z = \mathbb{Z}[\frac{1}{S}]$ and identify the modular symbols $\lambda_f(\frac{b}{m})$ appearing in (2.4) with $[\frac{b}{m}] \in Z$.

Remark 2.5 The condition required on T_p, that $p \equiv 1 \mod N$, could actually be improved to get a better value for S. Moreover, the denominators appearing in $\lambda_f(x) = \lambda_f(\frac{b}{m}) \in \mathbb{Q}$ can be shown to be dependent on the denominator of x, which divides the conductor m of χ. Thus better bounds than S can also be found for particular cusps x or conductors m. Such improvements will actually be dealt with carefully later, when we work with modular symbols for the quadratic imaginary case $\mathrm{GL}_2(\mathbb{A}_{\mathbb{K}})$. $\square$

We still need a group G to play the role of the character values in (2.4). We use some abelian class field theory. Consider the abelian extension $\mathbb{Q}(\mu_m)^+/\mathbb{Q}$. This is the ray class field extension of $\mathbb{Q}$ of conductor m. This extension is unramified outside of m. We want m finite, which is the reason for taking a real extension. Let G be the Galois group of this extension. Then $G \cong (\mathbb{Z}/m\mathbb{Z})^*/\pm 1$. The Artin map associates to any prime ideal $(p) \subset \mathbb{Q}$ unramified in $\mathbb{Q}(\mu_m)^+$ a Frobenius element $\sigma_p \in G$. This is independent of the choice of generator p that is naturally chosen positive, and the map is extended to all unramified ideals by multiplicativity.

We define the **theta element** $\theta_m \in Z[G]$ as

$$\theta_m = \sum_{b \bmod m} \left[\frac{b}{m}\right] \sigma_b \tag{2.5}$$

where the sum is actually taken on representatives b of $(\mathbb{Z}/m\mathbb{Z})^*/\pm 1$.

This theta element is well-defined. First, because b is taken coprime to m so that (b) is unramified in $\mathbb{Q}(\mu_m)^+/\mathbb{Q}$ and σ_b exists. Second, by reciprocity, σ_b does not depend on the choice of representative for b. Third, $[\frac{b}{m}]$ is also well defined for b modulo m, since it is easily checked that cusp forms are periodic of period 1: $f(z+1) = f(z)$, $\forall z \in \mathcal{H}$. Finally, we require to have that $[\frac{b}{m}] = [\frac{-b}{m}]$, and this follows from the real part of the following lemma.

Lemma 2.20 $\overline{\lambda_f(b/m)} = \lambda_f(-b/m)$.

Proof.

$$\begin{aligned}
\overline{\lambda_f(b/m)} &= \overline{2\pi \int_0^\infty f(b/m + it)\, dt} \\
&= 2\pi \int_0^\infty \overline{f(b/m + it)}\, dt
\end{aligned}$$

$$
\begin{aligned}
\overline{\lambda_f(b/m)} &= 2\pi \int_0^\infty \overline{\textstyle\sum_{n=1}^\infty a_n e^{2\pi i n(b/m+it)}} \quad dt \\
&= 2\pi \int_0^\infty \textstyle\sum_{n=1}^\infty a_n e^{2\pi i n(-b/m+it)} \quad dt \qquad (a_n \in \mathbb{Z}) \\
&= 2\pi \int_0^\infty f(-b/m+it)\; dt \\
&= \lambda_f(-b/m).
\end{aligned}
$$

■

$\theta_m \in Z[G]$ is an algebraic object, but of course, analysis is hidden in the definition for the $[\frac{b}{m}]$ are defined using complex line integrals.

There will be some interplay in the coming pages between $\mathbb{Z}/m\mathbb{Z}$, $(\mathbb{Z}/m\mathbb{Z})^*$ and $(\mathbb{Z}/m\mathbb{Z})^*/\pm 1$, so we introduce the notations $\mathbb{Z}/m$, $\mathbb{Z}/m^*$ and $\mathbb{Z}/m^{*+}$ respectively. For example, having that $[\frac{b}{m}] = [\frac{-b}{m}]$ and $\sigma_b = \sigma_{-b}$, we may also rewrite θ_m as

$$
\theta_m = \sum_{b \in \mathbb{Z}/m^{*+}} \left[\frac{b}{m}\right] \sigma_b = \frac{1}{2} \sum_{b \in \mathbb{Z}/m^*} \left[\frac{b}{m}\right] \sigma_b \ ,
$$

which is actually the way Mazur and Tate define the theta element without giving the details.

For any even Dirichlet character $\chi : \mathbb{Z} \to \mathbb{C}$ of conductor m, we abuse notation and define $\chi : G \to \mathbb{C}^*$ by $\chi(\sigma_b) := \chi(b)$. This is well-defined precisely since $G = (\mathbb{Z}/m\mathbb{Z})^*/\pm 1$. We then extend χ linearly to $Z[G]$ with trivial action on Z:

$$
\begin{aligned}
\chi : \quad Z[G] &\to \quad \mathbb{C} \\
\sum z_\sigma \sigma &\mapsto \sum z_\sigma \chi(\sigma)
\end{aligned}
$$

Proposition 2.21 Let χ be a *primitive*, even Dirichlet character of conductor m. Then

$$
\chi(\theta_m) = \frac{\tau(\chi)}{2\Omega^+} L(f, \bar{\chi}, 1).
$$

Proof.

$$\begin{aligned}
\chi(\theta_m) &= \chi\left(\sum_{b\in\mathbb{Z}/m^{*+}}\left[\frac{b}{m}\right]\sigma_b\right)\\
&= \frac{1}{2}\sum_{b\in\mathbb{Z}/m^*}\left[\frac{b}{m}\right]\chi(\sigma_b)\\
&= \frac{1}{2}\sum_{b\in\mathbb{Z}/m^*}\frac{\lambda_f(b/m)}{\Omega^+}\chi(b)\\
&= \frac{1}{2\Omega^+}\left(\frac{\tau(\chi)\overline{\tau(\chi)}}{f_\chi}\right)\sum_{b\in\mathbb{Z}/m^*}\chi(b)\lambda_f(b/m)
\end{aligned}$$

χ is primitive, so its conductor f_χ is m. χ is even, so $\overline{\tau(\chi)} = \chi(-1)\tau(\overline{\chi}) = \tau(\overline{\chi})$, and χ being a Dirichlet character, we may "add zeroes" and change the summation.

$$\begin{aligned}
\chi(\theta_m) &= \frac{\tau(\chi)}{2\Omega^+}\frac{\tau(\overline{\chi})}{m}\sum_{b\in\mathbb{Z}/m}\chi(b)\lambda_f(b/m)\\
&= \frac{\tau(\chi)}{2\Omega^+}\,L(f,\bar{\chi},s=1)
\end{aligned}$$

by Birch-Manin, theorem 2.9. ■

This proposition gives us desired interpolation properties of θ_m. In particular,

Corollary 2.22 For a primitive, even Dirichlet character χ of conductor m,

$$\chi(\theta_m) = 0 \quad \text{if and only if} \quad L(f,\bar{\chi},1) = 0.$$

■

We would like to have such a relationship with non-twisted f. For this, we need to use a trivial character. The problem is that we need a character defined modulo m. The trivial character mod m, $\chi = \mathbf{1} : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$, is not the principal character, it is not primitive. However, for χ trivial, $\chi(\theta_m)$ is canonically identified with the natural projection of $\theta_m \in Z[G]$ into $Z[G/G] = Z[\langle e\rangle] \cong Z$. Fortunately, the behavior of θ_m under projections is known.

We define the **layer** of θ_m to be m. We have different theta elements at different layers m. Denote $(\mathbb{Z}/m\mathbb{Z})^*/\pm 1$ by G_m, so that $\theta_m \in Z[G_m]$, and let m' be an integral multiple of m. Define

$$z_m : \ Z[G_{m'}] \to Z[G_m]$$

as the map induced from the natural projection $G_{m'} \to G_m$, and define

$$\nu_{m'} : \ Z[G_m] \to Z[G_{m'}]$$

as the trace map. $\nu_{m'}$ is the map induced from $g \in Z[G_m] \mapsto \sum_{g'} g' \in Z[G_{m'}]$, where the sum is over all $g' \in G_{m'}$ projecting to $g \in G_m$. Then we have the following compatibility formulas for theta elements at different layers (c.f. [MT87, p.717]). These are a consequence of the action of Hecke operators T_l when $l \nmid N$ or the analogous U_l when $l \mid N$ on the theta elements. A sketch of proof of analogous properties in the quadratic imaginary case will be given in section 3.4

Lemma 2.23 Let N be the level of the cusp form f from which the following theta elements are computed. Let l be a prime number and a_l be the corresponding Fourier coefficient in the expansion of f.

1. If l divides both m and N, then $\quad z_m(\theta_{ml}) = a_l \theta_m$.
2. If l is coprime to both m and N, then $\quad z_m(\theta_{ml}) = (a_l - \sigma_l - \sigma_l^{-1})\theta_m$.
3. If l divides N but not m, then $\quad z_m(\theta_{ml}) = (a_l - \sigma_l^{-1})\theta_m$.
4. If l divides m but not N, then $\quad z_m(\theta_{ml}) = a_l\theta_m - \nu_m(\theta_{m/l})$. ■

Under these compatibilities, we may take an inverse limit of theta elements, and this leads to an interesting interpretation. Define $\Theta_p \in Z[[\mathbb{Z}_p^*]]$ by

$$\Theta_p := \varprojlim_n \theta_{p^n} \ .$$

Of course, if χ is a finite character of conductor p^k, then $\chi(\Theta_p) = \chi(\theta_{p^k})$. Now Θ_p is essentially the same as the p-adic L-function $L_p(E, s)$ studied in [MTT86] since both interpolate values of the classical complex L-function of E for infinitely many finite characters.

We now state the desired interpolation property for non twisted f.

Proposition 2.24 Let I be the augmentation ideal of the group ring $Z[G]$, that is, the kernel of the trivial character:

$$0 \longrightarrow I \longrightarrow Z[G] \xrightarrow{\chi=\mathbf{1}} \mathbb{C} \longrightarrow 0 \ .$$

If $L(f,1)=0$, then θ_m belongs to I.

Proof. As mentioned above, for trivial χ, $\chi(\theta_m)$ is canonically identified with the natural projection of $\theta_m \in Z[G]$ to $Z[G/G] = Z[\langle e\rangle] \cong Z$. Decompose m into distinct primes as $m = l_1^{e_1} l_2^{e_2} \dots l_k^{e_k}$. Applying lemma 2.23 $e_1+e_2+\ldots+e_k$ times, we obtain that $\chi(\theta_m)$ is a multiple of θ_1 which is zero when $L(f,1)=0$. ■

Note we do not claim that $\theta_m \in I$ iff $L(f,1)=0$. One of the interesting reasons for this appears in the next proposition. In the following, whenever we construct a theta element for an elliptic curve E, we always mean that we construct it from the cusp form f associated to E.

Proposition 2.25 Let l be a prime of split multiplicative reduction for an elliptic curve $E_{/\mathbb{Q}}$ and let m be a multiple of l. Then θ_m belongs to I, irrespective of the value of $L(f,1) = L(E,1)$.

Proof. As in the proof of proposition 2.24, we apply lemma 2.23 $e_1+e_2+\ldots+e_k$ times. We obtain that θ_m projects to $(a_l - \sigma_l^{-1})$ times some multiple of θ_1. The factor $(a_l - \sigma_l^{-1})$ must appear since l divides N. Moreover, since we project to θ_1, σ_l is trivial, and $a_l = 1$ for primes of split multiplicative reduction. Thus θ_m projects to 0 as desired. ■

Remark 2.6 In the context of elliptic curves defined over $\mathbb{K}$, the above proposition will remain a conjecture, but only for the reason that the modularity of $E_{/\mathbb{K}}$ is conjectural. □

In the situation where θ_m is constructed for a given elliptic curve $E_{/\mathbb{Q}}$, proposition 2.24 together with the Birch and Swinnerton-Dyer conjecture yields

Conjecture 2.26

Let $E_{/\mathbb{Q}}$ be a modular elliptic curve of rank r. If $r \geq 1$, then θ_m belongs to I. ■

We now try to refine the conjectures in order to take into account higher ranks. Inspired by the Birch and Swinnerton-Dyer conjecture as well as by the work of Mazur, Tate and Teitelbaum on the p-adic L-function in which exceptional zeroes appear, Mazur and Tate conjecture the following.

Conjecture 2.27 (Mazur, Tate)

Let $E_{/\mathbb{Q}}$ be a given modular elliptic curve and fix a layer m. Denote by s the number of primes of split multiplicative reduction for E dividing m. Let r be the $\mathbb{Z}$-rank of the Mordell-Weil group of $E_{/\mathbb{Q}}$. Then $\theta_m \in I^{r+s}$. ■

Barry Mazur and John Tate, with the help of Glenn Stevens who supplied computer algorithms for the computation of modular symbols, did test the above conjecture in many instances [MT87, section 3.2]. In particular, they verified the conjecture in cases where as many as two primes of split multiplicative reduction were involved.

Still, conjecture 2.27 does not claim that the order of vanishing of θ_m is *exactly* $r+s$. It may be that θ_m belongs to I^{r+s+1} as well, or to even higher powers of I. The reason comes from the structure of the powers of $I \subset Z[G]$ itself. This will be seen in section 3.5.6. For example, if $Z = \mathbb{Q}$ or simply if the exponent of G is invertible in Z, then $I^k = I$ for all $k \geq 1$. We will usually try to avoid this by taking $Z = \mathbb{Z}$.

In any case, I^{r+s}/I^{r+s+1} is always a torsion group. Indeed, the natural map

$$\begin{aligned} G &\to Z[G] \\ g &\mapsto g-1 \end{aligned}$$

induces a homomorphism

$$\mathrm{Sym}_k(G) \to I^k/I^{k+1}. \tag{2.6}$$

In the case where $Z = \mathbb{Z}$, it is known that (2.6) is an epimorphism, and that it is an isomorphism if and only if G is cyclic [BG72]. It may thus be that $\theta_m \in I^{r+s}$ non trivially projects to zero in I^{r+s}/I^{r+s+1}. It is not an easy task, but one may actually conjecture a value for this projection of θ_m. We will discuss this type of behaviour in section 3.6.

Chapter 3

Modular Elliptic Curves over a Quadratic Imaginary Field $\mathbb{K}$

We are nowadays familiar with the notion of modular elliptic curves, provided these are defined over $\mathbb{Q}$. However, the case of elliptic curves defined over an arbitrary global field $\mathbb{F}$ has been less studied. The Langlands philosophy permits us to believe that such elliptic curves are also modular. This is explained, for example, in [Gel76]. This means there exists a cusp form for $\mathrm{GL}_2(\mathbb{A}_\mathbb{F})$ whose associated L-function is the same as that of the elliptic curve, or equivalently, whose Fourier coefficients of prime index are given by the trace of the corresponding Frobenius operators on Tate modules of the elliptic curve. Unfortunately, these cusp forms and L-functions are not always easy to describe in classical language. In the case of interest to us though, when the field of definition is a quadratic imaginary field $\mathbb{K}$ of class number 1, we do have a quite nice description, but it is not as well known as in the case $\mathbb{F} = \mathbb{Q}$.

3.1 Cusp Forms for $\mathrm{GL}_2(\mathbb{A}_\mathbb{K})$

Cusp forms for $\mathrm{GL}_2(\mathbb{A}_\mathbb{F})$ are in general quite hard to describe in an elementary way, and one needs to keep the defining adelic formulation for them. However, we certainly do know instances where these forms are more easily described. The first is the case of the classical cusp forms for $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$, that are described as holomorphic functions on the upper half plane $\mathcal{H}$ satisfying some automorphy and cuspidality conditions. Another instance which is reasonably well known is the case where $\mathbb{F}$ is a totally real number field. In this case, the cusp forms are defined as an h^+-tuple of holomorphic functions in r_1 complex variables, where r_1 is the number of real places of $\mathbb{F}$, hence the degree of the extension $\mathbb{F}/\mathbb{Q}$, and h^+ is the narrow class number. The domain of definition actually consists in h^+ connected components $\mathcal{H}^{r_1}$, a product of r_1 usual upper half planes, and the cusp forms must satisfy some automorphy and cuspidal conditions. This is the theory of Hilbert modular forms.

A less well known example where cusp forms can be described by classical (non-adelic) means is our case of interest. Kurčanov in [Kur78] has shown that cusp forms for $\mathrm{GL}_2(\mathbb{A}_\mathbb{K})$ with $\mathbb{K}$ quadratic imaginary can be interpreted as harmonic differential forms on a real three-manifold. This is much in the same spirit as cusp forms for $\Gamma_0(N)$ that are interpreted as holomorphic differentials on the compactified Riemann surface $X_0(N) = \overline{\Gamma_0(N)\backslash\mathcal{H}}$. A down-to-earth elementary description of these functions can be found in John Cremona's thesis [Cre81]. Cremona follows the approach of Weil in [Wei71] for the particular case of quadratic imaginary fields of class number one. This permits a non-adelic description of cusp forms. We give a summary of Cremona's exposition, details of which can be found in his thesis [op. cit.]. A good description is also available in the comprehensive book by Elstrodt, Grunewald and Mennicke [EGM98].

Remark 3.1 In his thesis [op. cit.], Cremona has used this description to exhibit modular elliptic curves defined over $\mathbb{K}$. He gave numerical evidence for a Shimura-Taniyama type of correspondence in the case of elliptic curves defined over $\mathbb{K}$. $\square$

Cusp forms for $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ can be seen as certain functions on the upper half plane $\mathcal{H}$ through the well-known identification

$$\mathcal{H} \cong \mathrm{PSL}_2(\mathbb{R})/\mathrm{PSO}_2(\mathbb{R}).$$

When considering $\mathrm{GL}_2(\mathbb{A}_\mathbb{K})$, the place at infinity is complex. In this case, $\mathrm{PSL}_2(\mathbb{C})/\mathrm{PSU}_2(\mathbb{C})$ can be identified with hyperbolic upper half space $\mathcal{H}_3$, which is defined as

$$\mathcal{H}_3 := \{(z,t) \in \mathbb{C} \times \mathbb{R} \mid t > 0\}.$$

Indeed, any element $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{C})$ can be written as the product

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \begin{pmatrix} t & z \\ 0 & 1 \end{pmatrix} \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}$$

with $\alpha \in \mathbb{C}^*$, $|u|^2 + |v|^2 = 1$, and where z and t are given by

$$z = \frac{a\bar{c} + b\bar{d}}{|c|^2 + |d|^2} \in \mathbb{C} \ , \quad \text{and} \quad t = \frac{ad - bc}{|c|^2 + |d|^2} \in \mathbb{R}_{>0} \ .$$

In short,

$$\mathrm{GL}_2(\mathbb{C}) = Z \cdot B \cdot \mathrm{SU}_2(\mathbb{C}) \ ,$$

where Z is the center of $\mathrm{GL}_2(\mathbb{C})$ and

$$B = \left\{ \begin{pmatrix} t & z \\ 0 & 1 \end{pmatrix} \ \middle| \ z \in \mathbb{C}, \ t \in \mathbb{R}_{>0} \right\} \ .$$

We deduce $B = \mathrm{PSL}_2(\mathbb{C})/\mathrm{PSU}_2(\mathbb{C})$, and note that the map

$$\begin{array}{ccc} B & \longrightarrow & \mathcal{H}_3 \\ \left(\begin{smallmatrix} t & z \\ 0 & 1 \end{smallmatrix}\right) & \mapsto & (z,t) \end{array}$$

is a bijection. We thus obtain the desired identification

$$\mathcal{H}_3 \cong \mathrm{PSL}_2(\mathbb{C})/\mathrm{PSU}_2(\mathbb{C}) \ .$$

This identification induces an action of $\mathrm{GL}_2(\mathbb{C})$ on $\mathcal{H}_3$ given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} z \\ t \end{pmatrix} = \begin{pmatrix} \frac{(az+b)\overline{(cz+d)} + (at)\overline{(ct)}}{|cz+d|^2 + |ct|^2} \\ \frac{|ad-bc|t}{|cz+d|^2+|ct|^2} \end{pmatrix} \ . \tag{3.1}$$

Under this action, a basis of invariant differentials on this space is given by

$$\boldsymbol{\beta} = (\beta_0, \beta_1, \beta_2) = \left(\frac{-dz}{t}, \frac{dt}{t}, \frac{d\bar{z}}{t} \right) .$$

Note that if we restrict the action to $\mathrm{SL}_2(\mathbb{C})$ and identify (z,t) with Hamilton's quaternion $h = z + t\hat{\jmath}$, then the above action is reminiscent of Möbius linear fractional transformations, for it can be expressed as (see [EGM98, section 1.1])

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : h \mapsto (ah+b)(ch+d)^{-1}$$

where the last additions and division are of course performed in the non-commutative quaternion division ring.

Just like $\mathrm{GL}_2^+(\mathbb{R})$, acting as Möbius linear fractional transformations, preserves the hyperbolic geometry of the upper half plane, the action of $\mathrm{GL}_2(\mathbb{C})$ preserves the hyperbolic structure of $\mathcal{H}_3$. This latter is given by the metric

$$ds^2 = \frac{dx^2 + dy^2 + dt^2}{t^2} ,$$

where $x + iy = z$. Geodesics are then given by vertical lines and semicircles perpendicular to the **floor** of $\mathcal{H}_3$, that is, the set $\{(z,0) \in \mathbb{C} \times \mathbb{R}\}$.

The special case where $c = 0$ is of interest, for it corresponds to matrices appearing in the definition of Hecke operators to be seen below. We rewrite the action explicitly in this case.

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} z \\ t \end{pmatrix} = \begin{pmatrix} \frac{az+b}{d} \\ |\frac{a}{d}|t \end{pmatrix} . \tag{3.2}$$

We define **extended upper half space** $\mathcal{H}_3^*$ as the union of $\mathcal{H}_3$ and the **cusps** $\mathbb{P}^1(\mathbb{K})$, that is, the $\mathbb{K}$-rational floor points $\{(z,0) \in \mathbb{C} \times \mathbb{R} \mid z \in \mathbb{K}\}$ together with a point at infinity. The point at infinity is denoted $j\infty$, and should be thought of as "infinitely far up", i.e., as a limit as t approaches infinity of (z, t), for any fixed z. Note that $\mathcal{H}_3^*$ depends on the contextual quadratic imaginary field $\mathbb{K}$. We extend the action of $\mathrm{GL}_2(\mathbb{C})$ to $\mathcal{H}_3^*$ in the natural way. In particular, for the floor cusps, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} z \\ 0 \end{pmatrix} = \begin{cases} j\infty & \text{if } z = -\frac{d}{c}, \\ \begin{pmatrix} \frac{az+b}{cz+d} \\ 0 \end{pmatrix} & \text{otherwise.} \end{cases} \tag{3.3}$$

When it is clear from the context that the action is on cusps, then we will drop the second component and simply write

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d} \qquad (\text{or } j\infty) \tag{3.4}$$

This notation is advantageous for it is concise and very similar to the action of $\Gamma_0(N)$ on rational cusps $x \in \mathbb{P}^1(\mathbb{Q})$.

In the topology on $\mathcal{H}_3^*$, sets of the form $\{(z, t) \mid t > r\} \cup \{j\infty\}$ for any $r > 0$ are declared to be open. This gives us a basis $\mathcal{B}$ of open sets around $j\infty$, and bases of open sets around the other cusps are the union of some floor cusp with "open spheres" tangent to the floor at the cusp. By open spheres, we mean the intuitive notion of an open sphere using the Euclidean metric in $\mathbb{R}^3$, see Figure 1. In this way the bases of open sets around $j\infty$ and the floor cusps are compatible with the action of $\mathrm{GL}_2(\mathbb{C})$.

Figure 1: Basis Open Sets Around Cusps

We will shortly see that cusp forms for $\mathrm{GL}_2(\mathbb{A}_{\mathbb{K}})$ are vector valued functions $\mathbf{F} : \mathcal{H}_3 \to \mathbb{C}^3$ satisfying some automorphy and cuspidality conditions. On these, we define an action of $\mathrm{GL}_2(\mathbb{C})$ through the use of a **stroke operator**

$$\mathbf{F}|_\sigma(z,t) = \mathbf{F}(\sigma(z,t))J(\sigma;(z,t))$$

where the **automorphy factor** J is defined the following way:

For $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we set $\Delta = \det(\sigma)$, $r = \overline{cz+d}$, $s = \bar{c}t$ and

$$J(\sigma;(z,t)) = \frac{1}{|r|^2+|s|^2}\begin{pmatrix} r^2\Delta & -2rs\Delta & s^2\Delta \\ r\bar{s} & |r|^2-|s|^2 & -\bar{r}s \\ \overline{s^2\Delta} & \overline{2rs\Delta} & \overline{r^2\Delta} \end{pmatrix}.$$

Now fix a quadratic imaginary field $\mathbb{K}$ of class number one and discriminant D, let $\mathcal{N}$ be any non-zero integral ideal of $\mathcal{O}_{\mathbb{K}}$ and consider the discrete subgroup of $\mathrm{GL}_2(\mathbb{C})$ given by

$$\Gamma_0(\mathcal{N}) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}_{\mathbb{K}}) \mid c \in \mathcal{N}\}.$$

A **cusp form** of weight 2 for $\Gamma_0(\mathcal{N})$ is a vector-valued function

$$\mathbf{F} = (F_0, F_1, F_2) : \mathcal{H}_3 \to \mathbb{C}^3$$

such that

1. $\mathbf{F}\cdot\boldsymbol{\beta}$ is a $\Gamma_0(\mathcal{N})$-invariant harmonic differential form on $\mathcal{H}_3$,
2. $\int_{\mathbb{C}/\mathcal{O}_{\mathbb{K}}} \mathbf{F}|_\sigma(z,t)\,dz = 0, \quad \forall\sigma\in\mathrm{SL}_2(\mathcal{O}_{\mathbb{K}})$.

Remark 3.2 Since $\mathbb{K}$ is a principal ideal domain, all cusps are equivalent under $\mathrm{SL}_2(\mathcal{O}_{\mathbb{K}})$, and part 2 is a cuspidality condition at all cusps. □

We call $\mathcal{N}$ the **level** of $\mathbf{F}$. These cusp forms are invariant under the action of the stroke operator:

$$\mathbf{F}|_\sigma = \mathbf{F}, \quad \forall \sigma \in \Gamma_0(\mathcal{N}).$$

It is derived in sections 3.1 and 3.2 of [Cre81] that such cusp forms $\mathbf{F}$ a Fourier-Bessel expansion of the form

$$\mathbf{F}(z,t) = \sum_{0 \neq \alpha \in \mathcal{O}_{\mathbb{K}}} c(\alpha) t^2 \mathbf{K}\left(\frac{4\pi\,|\alpha|\,t}{\sqrt{|D|}}\right) \psi\left(\frac{\alpha z}{\sqrt{D}}\right), \tag{3.5}$$

where $\psi(z) = \exp(4\pi i \Re(z))$, and

$$\mathbf{K}(t) = \left(-\frac{i}{2}K_1(t),\ K_0(t),\ \frac{i}{2}K_1(t)\right),$$

K_0 and K_1 being *modified* or *hyperbolic* Bessel functions [Arf85, section 11.5].

Let us denote by $S_2(\Gamma_0(\mathcal{N}))$ the $\mathbb{C}$-vector space of cusp forms of weight 2 for $\Gamma_0(\mathcal{N})$. It is finite-dimensional for any $\mathcal{N}$.

We may now extend the action of $\mathrm{GL}_2(\mathbb{C})$ on the vector-valued functions of $\mathcal{H}_3$ considered to the group ring $\mathbb{C}[\mathrm{GL}_2(\mathbb{C})]$ by linearity. Let $\mathcal{P}$ be a prime ideal with generator π. We define the **Hecke operator** T_π acting on $S_2(\Gamma_0(\mathcal{N}))$ for $\mathcal{P}$ coprime to the level $\mathcal{N}$ by

$$T_\pi = \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix} + \sum_{\alpha \bmod \pi} \begin{pmatrix} 1 & \alpha \\ 0 & \pi \end{pmatrix}. \tag{3.6}$$

When $\mathcal{P}$ divides $\mathcal{N}$, we drop the matrix $\left(\begin{smallmatrix} \pi & 0 \\ 0 & 1 \end{smallmatrix}\right)$ from the definition. In this case, there are also "Atkin-Lehner" involutions acting on $S_2(\Gamma_0(\mathcal{N}))$ given by

$$W_\pi = \begin{pmatrix} \pi^k x & y \\ \nu z & \pi^k w \end{pmatrix},$$

where k is the valuation of $\mathcal{N}$ at $\mathcal{P}$, ν is a generator of $\mathcal{N}$ and x, y, z, w are any elements of $\mathcal{O}_{\mathbb{K}}$ such that $|W_\pi| = \pi^k$. The **Fricke involution**

$$W_\nu = \begin{pmatrix} 0 & -1 \\ \nu & 0 \end{pmatrix}$$

is the product of all Atkin-Lehner involutions: $W_\nu = \prod_{\mathcal{P}|\mathcal{N}} W_\pi$.

Hecke operators T_π also act on $S_2(\Gamma_0(\mathcal{N}))$, for fixed $\mathcal{N}$ coprime to (π). Their effect on a cusp form $\mathbf{F}$ defined by (3.5) is to give a new cusp form $\mathbf{F}' = \mathbf{F} \mid T_\pi$ whose Fourier coefficients $c'(\alpha)$ are given by

$$c'(\alpha) = N(\pi)c(\alpha\pi) + c(\alpha/\pi).$$

A **Hecke eigenform** is an element of $S_2(\Gamma_0(\mathcal{N}))$ that is an eigenfunction for all the Hecke operators T_π such that (π) does not divide $\mathcal{N}$. Hecke operators and Atkin-Lehner involutions acting on a fixed $S_2(\Gamma_0(\mathcal{N}))$ actually all commute. Eigenforms are thus also eigenfunctions for the Atkin-Lehner and Fricke involutions. As in chapter 2, eigenforms $f \in S_2(\Gamma_0(\mathcal{N}))$ are **oldforms** when they are induced from lower levels $\mathcal{M}$ dividing $\mathcal{N}$. Their span is denoted $S_2^{\text{old}}(\Gamma_0(\mathcal{N}))$. The orthogonal complement of $S_2^{\text{old}}(\Gamma_0(\mathcal{N}))$ in $S_2(\Gamma_0(\mathcal{N}))$ is denoted $S_2^{\text{new}}(\Gamma_0(\mathcal{N}))$, and eigenforms in there are called **newforms**.

Modulo the units of $\mathcal{O}_{\mathbb{K}}$, we have unique factorization of the elements of the principal ideal domain $\mathcal{O}_{\mathbb{K}}$. Elements of $\mathcal{O}_{\mathbb{K}}$ may be declared primes or composites according to the ideal they generate. We use this terminology in the following.

An eigenform $\mathbf{F}$ can be normalized such that $c(1) = 1$, in which case all its Fourier coefficients can be read off from the eigenvalues of the above operators. For the Fourier coefficients indexed by primes, we have

$$c(\pi)F = \begin{cases} T_\pi F & \text{when } \pi \nmid \mathcal{N}, \\ -W_\pi F & \text{when } \pi || \mathcal{N}, \\ 0 & \text{when } \pi^2 \mid \mathcal{N}. \end{cases}$$

For the prime power indices :

$$c(\pi^r) = \begin{cases} c(\pi)c(\pi^{r-1}) - N(\pi)c(\pi^{r-2}) & \text{for primes of good reduction,} \\ c(\pi)^r & \text{otherwise.} \end{cases} \tag{3.7}$$

For composite indices, the Fourier coefficients are multiplicative. Finally, the missing case of $c(\alpha)$ when α is a unit follows from the following discussion.

Let ϵ_0 be a generator of the group of units $\mathcal{O}_{\mathbb{K}}^*$. Consider the action of the matrix $\left(\begin{smallmatrix}\epsilon_0 & 0\\ 0 & 1\end{smallmatrix}\right)$ on $\mathcal{H}_3$. It induces an involution J on $S_2(\Gamma_0(\mathcal{N}))$ for $\left(\begin{smallmatrix}\epsilon_0 & 0\\ 0 & 1\end{smallmatrix}\right)^2$ is equivalent to $\left(\begin{smallmatrix}\epsilon_0 & 0\\ 0 & \epsilon_0^{-1}\end{smallmatrix}\right) \in \Gamma_0(\mathcal{N})$ modulo scalar matrices. This splits the space of cusp forms as

$$S_2(\Gamma_0(\mathcal{N})) = S_2^+(\Gamma_0(\mathcal{N})) \bigoplus S_2^-(\Gamma_0(\mathcal{N})).$$

The cusp forms in $S_2^+(\Gamma_0(\mathcal{N}))$ have J-eigenvalue $+1$ and satisfy $c(\epsilon\alpha) = c(\alpha)$ for all $\alpha \in \mathcal{O}_{\mathbb{K}}$ and all $\epsilon \in \mathcal{O}_{\mathbb{K}}^*$. Those in $S_2^-(\Gamma_0(\mathcal{N}))$, have J-eigenvalue -1 and satisfy $c(\epsilon_0\alpha) = -c(\alpha)$ for all $\alpha \in \mathcal{O}_{\mathbb{K}}$. The newforms in $S_2^+(\Gamma_0(\mathcal{N}))$ are called **plusforms** whereas those in $S_2^-(\Gamma_0(\mathcal{N}))$ are called **minusforms**.

Remark 3.3 One checks easily that $T_{\epsilon_0\pi} = JT_\pi$. Thus we may not in general define $T_{\mathcal{P}}$. However, we will exclusively apply Hecke operators on (conjectural) plusforms, in which case we do have that $T_{\mathcal{P}}$ is well defined. A similar remark also holds for involutions $W_{\mathcal{P}}$ and $W_{\mathcal{N}}$, which depend on choices of π and ν. □

3.2 Modular Symbols Attached to Cusp Forms for $\mathbf{GL}_2(\mathbb{A}_{\mathbb{K}})$

We define modular symbols in this new setting very similarly to the rational case discussed in Chapter 2. However, we will see that there are some limits to the analogy.

Consider $\mathbf{F}$, a *rational* eigenform in $S_2(\Gamma_0(\mathcal{N}))$, that is, the coefficients of its Fourier-Bessel expansion are in $\mathbb{Q}$. We define the **modular symbol** $\lambda_{\mathbf{F}}$ associated to the cusp form $\mathbf{F}$ as a map $\lambda_{\mathbf{F}} : \mathbb{P}^1(\mathbb{K}) \to \mathbb{C}$ by

$$\lambda_{\mathbf{F}}(A) = \alpha_{\mathbb{K}} \int_A^{j\infty} \mathbf{F} \cdot \boldsymbol{\beta}$$

where $\alpha_{\mathbb{K}} = -16\pi^2/\omega D$, D being the (negative) fundamental discriminant of $\mathbb{K}$, and ω the order of $\mathcal{O}_{\mathbb{K}}^*$. This integral is well defined since $\mathcal{H}_3^*$ is simply connected. In particular, we may choose a convenient vertical path of integration. Write

$A = (z_A, 0) \in \mathcal{H}_3^*$. The defining integral then reduces to

$$\begin{aligned}\lambda_{\mathbf{F}}(A) &= \alpha_{\mathbb{K}} \int_0^\infty F_1(z_A, t)\, \frac{dt}{t} \\ &= \alpha_{\mathbb{K}} \int_0^\infty \sum_{0 \neq \alpha \in \mathcal{O}_{\mathbb{K}}} c(\alpha) t^2 K_0 \left(\frac{4\pi\, |\alpha|\, t}{\sqrt{|D|}} \right) \psi \left(\frac{\alpha z_A}{\sqrt{D}} \right) \frac{dt}{t}\ .\end{aligned}$$

Since we consider fields $\mathbb{K}$ that have class number 1, the sum on the non-zero elements α of $\mathcal{O}_{\mathbb{K}}$ may be split into a sum on the non-zero ideals (α) of $\mathcal{O}_{\mathbb{K}}$ and a sum on its units ϵ. For a plusform $\mathbf{F}$, we further have that $c(\epsilon\alpha) = c(\alpha)$. We can therefore rewrite $\lambda_{\mathbf{F}}(A)$ for plusforms as

$$\lambda_{\mathbf{F}}(A) = \alpha_{\mathbb{K}} \int_0^\infty \sum_{(\alpha) \neq (0)} c(\alpha) t K_0 \left(\frac{4\pi\, |\alpha|\, t}{\sqrt{|D|}} \right) \sum_{\epsilon \in \mathcal{O}_{\mathbb{K}}^*} \psi \left(\frac{\epsilon \alpha z_A}{\sqrt{D}} \right) dt \tag{3.8}$$

which makes it clear that $\lambda_{\mathbf{F}}$ actually has *real* range.

Remark 3.4 The real range of $\lambda_{\mathbf{F}}$ is actually a very significant difference from the rational case, in which the periods of the cusp form can be used as a lattice in $\mathbb{C}$ to create an elliptic curve. $\square$

We continue as in chapter 2. $\mathbf{F}$ being fixed, $\lambda_{\mathbf{F}}$ associates to $A \in \mathbb{P}^1(\mathbb{K})$ a path from A to $j\infty$. The invariance of $\mathbf{F} \cdot \boldsymbol{\beta}$ under $\Gamma_0(\mathcal{N})$ descends this path to one on $X_0(\mathcal{N})$, defined as the compact real 3-manifold $\Gamma_0(\mathcal{N}) \backslash \mathcal{H}_3^*$. We extend the definition of modular symbols and view them as formal elements of the homology of this curve:

$$\lambda_{\mathbf{F}} : \mathbb{P}^1(\mathbb{K}) \to H_1(X_0(\mathcal{N}), \mathbb{R}). \tag{3.9}$$

We then denote the homology class of a path from a to b in $\mathcal{H}_3^*$ projected to $X_0(\mathcal{N})$ by $\{a, b\}$. Again, the extension (3.9) of the modular symbol notion is non-trivial since paths in $\mathcal{H}_3^*$ are no more restricted to be from cusps to infinity. Also to be more precise one should, as mentioned in Remarks 2.2 as well, write $\{a, b\}_{\mathbf{F}}$. We will consider $\mathbf{F}$ to be fixed from the context.

We have the following properties for the modular symbols as well.

Proposition 3.1 Let $a, b, c \in \mathcal{H}_3^*$, and let $\sigma, \gamma \in \Gamma_0(\mathcal{N})$. Then

1. $\{a, a\} = 0$;

2. $\{a, b\} = -\{b, a\}$;

3. $\{a, b\} + \{b, c\} = \{a, c\}$;

4. $\{\sigma a, \sigma b\} = \{a, b\}$;

5. $\{a, \sigma a\} \in H_1(X_0(\mathcal{N}), \mathbb{Z})$.

6. $\{a, \sigma a\} = \{b, \sigma b\}$;

7. $\{a, \sigma\gamma a\} = \{a, \sigma a\} + \{a, \gamma a\}$. ■

Accordingly, the notation $\{\sigma\} = \{a, \sigma a\}$ for any $a \in \mathcal{H}_3^*$ is well-defined, and we also let $\{A\}$ denote $\{A, j\infty\}$. When A is a cusp equivalent to $j\infty$ under $\Gamma_0(\mathcal{N})$, then any representative path for $\{A\}$ on $X_0(\mathcal{N})$ is closed, so that $\{A\} \in H_1(X_0(\mathcal{N}), \mathbb{Z})$. It is essential for our applications that the modular symbols $\{A\}$ for *all* cusps A be in the *rational* homology. We thus need some kind of Manin-Drinfeld theorem in our setting too.

Lemma 3.2 Let $\alpha_1 = p_1/q_1$ and $\alpha_2 = p_2/q_2$ be any two elements of $\mathbb{K}$ written in lowest terms, that is, $p_i, q_i \in \mathcal{O}_{\mathbb{K}}$, and $(p_i, q_i) = \mathcal{O}_{\mathbb{K}}$. Then α_1 is equivalent to α_2 modulo $\Gamma_0(\mathcal{N})$ iff multiplicative inverses s_i of p_i modulo the ideal (q_i), (i=1,2), can be found such that $s_1 q_2 \equiv u^2 s_2 q_1 \pmod{(q_1 q_2) + \mathcal{N}}$ for some unit $u \in \mathcal{O}_{\mathbb{K}}^*$.

Proof. [Cre84, Lemma 2.2.7] ■

The action of the Hecke operators on $S_2(\Gamma_0(\mathcal{N}))$ may be dualized to the modular symbols as was done in chapter 2. Then for (π) coprime to $\mathcal{N}$, using the definition (3.6) and equation (3.4), we have

$$\begin{aligned} T_\pi\{\alpha, j\infty\} &= \left(\begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix} + \sum_{\gamma \bmod \pi} \begin{pmatrix} 1 & \gamma \\ 0 & \pi \end{pmatrix} \right) \{\alpha, j\infty\} \\ &= \{\pi\alpha, j\infty\} + \sum_{\gamma \bmod \pi} \{\frac{\alpha+\gamma}{\pi}, j\infty\}. \end{aligned} \tag{3.10}$$

Theorem 3.3 For any cusp $\alpha \in \mathbb{P}^1(\mathbb{K})$, $\{\alpha\}_{\mathbf{F}} \in H_1(X_0(\mathcal{N}), \mathbb{Q})$.

Remark 3.5 The following is an adaptation of the corresponding proof of theorem 2.13. However, computational efficiency is a concern here as explained in Chapter 3. We will thus improve on the congruence conditions used to choose the Hecke operator closing the path. We have not found such details of the proof in the literature. Kurčanov in [Kur78] says: "It is readily seen that there exist infinitely many principal prime ideals (p) such that ... (paths can be closed)", but all details are missing. Shai Haran has some very general adelic argument in this direction in [Har86]. It seems that these results are not very well known, or perhaps unsatisfactory. For example, rationality of modular symbols is essential in the work of Tan [Tan95] and he mentions cases where the rationality is known. He does not refer to Kurčanov's or Haran's results. We give here a detailed, constructive and non-adelic proof. Note also that Cremona and Whitley in [CW94] give some details for the special case $\{0\}$, thus yielding a rationality property for L-functions at 1. □

Proof of theorem 3.3. From equation (3.10), for π coprime to $\mathcal{N}$, we have

$$T_\pi\{\alpha, j\infty\} = \{\pi\alpha, \alpha\} + \{\alpha, j\infty\} + \sum_{\gamma \bmod \pi} \left(\{\frac{\alpha+\gamma}{\pi}, \alpha\} + \{\alpha, j\infty\} \right).$$

Modular symbols $\{a, b\}_{\mathbf{F}}$ associated to a rational Hecke eigenform $\mathbf{F}$ corresponding to an elliptic curve $E_{/\mathbb{K}}$ are in the $\mathbf{F}$-isotypic part of the homology $H_1(X_0(\mathcal{N}))^{\mathbf{F}}$. Since $T_\pi \mathbf{F} = c(\pi)\mathbf{F}$ for some integer $c(\pi)$, we obtain by duality

$$(c(\pi) - 1 - \mathrm{N}(\pi))\{\alpha, j\infty\}_{\mathbf{F}} = \{\pi\alpha, \alpha\}_{\mathbf{F}} + \sum_{\gamma \bmod \pi} \{\frac{\alpha+\gamma}{\pi}, \alpha\}_{\mathbf{F}}. \tag{3.11}$$

$c(\pi) - 1 - \mathrm{N}(\pi)$ is not zero. In our case of interest, namely when $\mathbf{F}$ is attached to an elliptic curve $E_{/\mathbb{K}}$, this follows for reasons similar to those explained in remark 2.3. We need to find some π for which the right hand side will be in the integral homology. Let $\alpha_1 = p_1/q_1$ be α and $\alpha_2 = p_2/q_2$ be any of $\pi\alpha$ or $(\alpha+\gamma)/\pi$ written in lowest terms. We let ν be a generator of $\mathcal{N}$ and δ be a generator of (q_1, ν). We also factor q_1 as $q_1 = q\delta$.

Claim 3.4 : Any π coprime to $\mathcal{N}$ satisfying the following condition will do:

$$\pi \equiv u^2 \mod (\delta, \nu/\delta), \quad \text{for some unit } u \in \mathcal{O}_{\mathbb{K}}^*.$$

We verify that lemma 3.2 can be solved for s_1 and s_2 in any case.

- Consider the case $\alpha_2 = \pi\alpha$ and suppose $(\pi, q_1) = \mathcal{O}_{\mathbb{K}}$. Then $\frac{p_2}{q_2} = \frac{\pi p_1}{q_1}$ are in lowest terms, and with the right choices of units, $p_2 = \pi p_1$ and $q_2 = q_1$. Lemma 3.2 then requires a solution to the system of congruences

$$\begin{aligned} s_1 p_1 &\equiv 1 & \mod (q_1), \\ s_2 \pi p_1 &\equiv 1 & \mod (q_1), \\ s_1 q_1 &\equiv u^2 s_2 q_1 & \mod (q_1^2, \nu). \end{aligned}$$

p_1 and π are both coprime to q_1, thus the first two equations are solvable for s_1 and s_2 mod (q_1), and even mod (q_1^2), in which case any solution to these will satisfy

$$s_1 \equiv s_2 \pi \mod (q_1^2),$$

hence also mod (q_1^2, ν). There remains to simultaneously satisfy the third equation:

$$\pi s_2 q \delta \equiv u^2 s_2 q \delta \mod (q_1^2, \nu).$$

But $(q_1^2, \nu) = (\delta^2, \nu)$ and the last equation rewrites:

$$\pi s_2 q \equiv u^2 s_2 q \mod (\delta, \nu/\delta).$$

This equation can be satisfied when π is as in the above claim.

- Consider again $\alpha_2 = \pi\alpha$, but suppose now that $(\pi, q_1) = (\pi)$. Then $\frac{p_2}{q_2} = \frac{p_1}{q_1/\pi}$ are in lowest terms, and with the right choices of units, $p_2 = p_1$ and $q_2 = q_1/\pi$. Lemma 3.2 then requires to solve

$$\begin{aligned} s_1 p_1 &\equiv 1 & \mod (q_1), \\ s_2 p_1 &\equiv 1 & \mod (q_1/\pi), \\ s_1 \frac{q_1}{\pi} &\equiv u^2 s_2 q_1 & \mod (q_1^2/\pi, \nu). \end{aligned}$$

Now π is coprime to ν, so $(q_1^2/\pi, \nu) = (q_1^2, \nu) = (\delta^2, \nu)$, and using $q_1 = q\delta$, the last equation becomes

$$s_1 \frac{q}{\pi} \equiv u^2 s_2 q \mod (\delta, \nu/\delta).$$

p_1 is coprime to q_1, so the first equation is solvable for s_1. The same solution ($s_2 = s_1$) can be used for the second equation as well and also fits in the last equation provided only that π is chosen to further satisfy $\pi \equiv u^{-2} \bmod (\delta, \nu/\delta)$.

- Now consider $\alpha_2 = (\alpha+\gamma)/\pi$ and $(\pi, p_1 + \gamma q_1) = \mathcal{O}_{\mathbb{K}}$, that is, $\frac{p_2}{q_2} = \frac{p_1+\gamma q_1}{\pi q_1}$ are in lowest terms, and we may choose $q_2 = \pi q_1$ and $p_2 = p_1 + \gamma q_1$. The system of equations to be considered is

$$\begin{aligned} s_1 p_1 &\equiv 1 && \mod (q_1), \\ s_2(p_1+\gamma q_1) &\equiv 1 && \mod (\pi q_1), \\ s_1 \pi q_1 &\equiv u^2 s_2 q_1 && \mod (\pi q_1^2, \nu). \end{aligned}$$

Again, π is coprime to ν so that $(\pi q_1^2, \nu) = (q_1^2, \nu) = (\delta^2, \nu)$. Using also $q_1 = q\delta$ in the third equation, we modify the system to

$$\begin{aligned} s_1(p_1+\gamma q_1) &\equiv 1 && \mod (q_1), \\ s_2(p_1+\gamma q_1) &\equiv 1 && \mod (\pi q_1), \\ s_1 \pi q &\equiv u^2 s_2 q && \mod (\delta, \nu/\delta). \end{aligned}$$

Similarly to the previous case, the second equation is solvable for s_2, and the same solution $s_1 = s_2$ can be used for the first equation. This also satisfies the last equation when π matches claim 3.4.

- Finally consider the case $\alpha_2 = (\alpha+\gamma)/\pi$ with $\pi \mid (p_1 + \gamma q_1)$, that is, $\frac{p_2}{q_2} = \frac{(p_1+\gamma q_1)/\pi}{q_1}$ are in lowest terms, and we choose the units so that $q_2 = q_1$ and $p_2 = (p_1 + q_1\gamma)/\pi$. The system of equations from lemma 3.2 rewrites

$$\begin{aligned} s_1(\pi p_2 - q_2\gamma) &\equiv 1 && \mod (q_2), \\ s_2 p_2 &\equiv 1 && \mod (q_2), \\ s_1 q_2 &\equiv u^2 s_2 q_2 && \mod (q_2^2, \nu). \end{aligned}$$

We slightly simplify these equations to

$$\begin{aligned} s_1 \pi p_2 &\equiv 1 && \mod (q_2), \\ s_2 p_2 &\equiv 1 && \mod (q_2), \\ s_1 q_2 &\equiv u^2 s_2 q_2 && \mod (q_2^2, \nu), \end{aligned}$$

and note that since $q_1 = q_2$ here, this is equivalent to the first case. ■

Remarks 3.6

1. In chapter 3, we will implement the choice of T_π with $\pi \equiv 1 \mod (\delta, \nu/\delta)$. It is easy to see that $(\delta, \nu/\delta) \neq \mathcal{N}$, so this is always an improvement over $\pi \equiv 1 \mod \mathcal{N}$. Oftentimes we even have that $(\delta, \nu/\delta) = \mathcal{O}_{\mathbb{K}}$, in which case any T_π with (π) coprime to $\mathcal{N}$ will do. This will happen for example whenever N is squarefree, that is, whenever we work with semistable elliptic curves in chapter 3. This improvement will turn out to be crucial for the implementation of modular symbols calculations.

2. In remark 2.3, we had noted that there was another way to view the Manin-Drinfeld theorem in the rational case which is very beautiful for it is geometric in nature. It looks at projections of paths on a Jacobian and uses the group law to stretch it by an integral factor and close it. Unfortunately, such a point of view is not available here. In the quadratic imaginary case, we simply do not have a Jacobian $J_0(\mathcal{N})$ of $X_0(\mathcal{N})$ at our disposal. The real range of $\lambda_{\mathbf{F}}$ (see remark 3.4) prevents the periods of $\mathbf{F}$ to furnish a (full rank) lattice Λ in $\mathbb{C}^g$ for any complex dimension g. There is thus no hope to have an Eichler-Shimura type of construction to associate some $J = \mathbb{C}^g/\Lambda$ to $\mathbf{F}$.

   A related question is whether $X_0(\mathcal{N})$ can be used to uniformize elliptic curves defined over $\mathbb{K}$. This cannot be an easy task, since $X_0(\mathcal{N})$ has no complex structure, it is only a real 3-manifold. We will come back to this in the next section. □

Denote by $\mathbb{P}^1_\infty(\mathbb{K})$ the set of cusps $\alpha \in \mathbb{P}^1(\mathbb{K})$ that are equivalent to $j\infty$ modulo $\Gamma_0(\mathcal{N})$. We have already seen from equation (3.8) that $\lambda_{\mathbf{F}} : \mathbb{P}^1(\mathbb{K}) \to \mathbb{C}$ has real range. Kurčanov [Kur78] has shown that $\lambda_{\mathbf{F}}$ restricted to $\mathbb{P}^1_\infty(\mathbb{K})$ forms a rank 1 real lattice. However, his proof is existential and does not yield an actual value for a generator of the lattice. We denote by $\Omega(\mathbf{F})$ the smallest positive value in the range of $\lambda_{\mathbf{F}} : \mathbb{P}^1_\infty(\mathbb{K}) \to \mathbb{R}$, and call it the **period** of $\mathbf{F}$. For $\alpha \in \mathbb{P}^1(\mathbb{K})$, we define

$$[\alpha] := \lambda_{\mathbf{F}}(\alpha)/\Omega(\mathbf{F}),$$

and according to theorem 3.3, $[\alpha] \in \mathbb{Q}$.

3.3 Modularity of $E_{/\mathbb{K}}$

We have, in the previous section, treated modular symbols in the context of cusp forms for $\mathrm{GL}_2(\mathbb{A}_{\mathbb{K}})$. The use of modular symbols in the context of the Birch and Swinnerton-Dyer conjecture requires us to view them as associated to elliptic curves $E_{/\mathbb{K}}$. For elliptic curves defined over the rationals, $E_{/\mathbb{Q}}$, we could do this through the modular parameterization $\phi : X_0(N) \to E$ which induces a map $\tilde{\phi} : H_1(X_0(N)) \to H_1(E)$. Moreover, we know that all elliptic curves defined over $\mathbb{Q}$ are modular.

A major drawback of elliptic curves defined over arbitrary number fields is that we do not always have such a parameterization. In our quadratic imaginary case, $X_0(\mathcal{N})$ is not an algebraic variety, it does not have a complex structure. It is only a real manifold of odd dimension and so a fortiori it is not possible to find an algebraic map of the form $\phi : X_0(\mathcal{N}) \to E$. In the early eighties, it was hoped that one could find a related structure to replace $X_0(\mathcal{N})$ and recover a similar parameterization. However, attempts to find a complex manifold to uniformize elliptic curves defined over quadratic imaginary fields have been unsuccessful so far, and there is little hope to find such a simple description at the present moment. The lack of this geometric tool represents an important loss in the study of elliptic curves when they are defined over arbitrary extensions of $\mathbb{Q}$.

Elliptic curves over $\mathbb{K}$ may nevertheless be modular. For this, it suffices to find a plusform for $\mathrm{GL}_2(\mathbb{A}_\mathbb{K})$

$$\begin{aligned}\mathbf{F}(z,t) &= \sum_{0\neq\alpha\in\mathcal{O}_\mathbb{K}} c(\alpha)t^2\mathbf{K}\left(\frac{4\pi\,|\alpha|\,t}{\sqrt{|D|}}\right)\psi\left(\frac{\alpha z}{\sqrt{D}}\right)\\ &= \sum_{(\alpha)\neq(0)} c(\alpha)t^2\mathbf{K}\left(\frac{4\pi\,|\alpha|\,t}{\sqrt{|D|}}\right)\sum_{\epsilon\in\mathcal{O}_\mathbb{K}^*}\psi\left(\frac{\epsilon\alpha z}{\sqrt{D}}\right)\end{aligned}$$

to which we associate the L-series

$$L(\mathbf{F},s) = \sum_{(\alpha)\neq(0)} \frac{c(\alpha)}{\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\alpha)^s} \tag{3.12}$$

such that it equals that of $E_{/\mathbb{K}}$:

$$L(E_{/\mathbb{K}},s) = \sum_{(\alpha)\neq(0)} \frac{a_\alpha}{\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\alpha)^s}. \tag{3.13}$$

This is just equation (1.4), in which we have switched the summation index from $\mathcal{N}$ to (α) to make the correspondence clearer here.

It is actually conjectured, see [Gel76], that all elliptic curves defined over number fields $\mathbb{F}$ are modular. In our case, we write the conjecture as

Conjecture 3.5 (Shimura-Taniyama over $\mathbb{K}$)
Let E be an elliptic curve defined over $\mathbb{K}$ with conductor $\mathcal{N}_E$ and L-series given by (3.13). Then there exists a rational plusform for $\mathrm{GL}_2(\mathbb{A}_\mathbb{K})$ of level $\mathcal{N} = \mathcal{N}_E$ for which the L-series (3.12) equals that of $E_{/\mathbb{K}}$. ■

By *rational* plusform, we mean that the Fourier-Bessel coefficients $c(\alpha) \in \mathbb{Q}$. It is normal that we relate elliptic curves $E_{/\mathbb{K}}$ to rational plusforms rather than to arbitrary newforms, since the L-series of $E_{/\mathbb{K}}$ must have rational coefficients, actually $\mathbb{Z}$-integral coefficients, and it is indexed by ideals, not by the elements of $\mathcal{O}_\mathbb{K}$.

The above conjecture is purely an equality of analytic functions that are constructed in different ways. In equation (3.12) most of the $c(\alpha)$ are eigenvalues of Hecke Operators, whereas in equation (3.13), the a_α are traces of Frobenius operators, and may be found by counting points on reductions of $E_{/\mathbb{K}}$. We do not know of any geometric link between $E_{/\mathbb{K}}$ and $X_0(\mathcal{N})$.

John Cremona in his thesis [Cre81] investigated experimentally such a Shimura-Taniyama type of conjecture over $\mathbb{K}$. In there, he computes spaces of cusp forms for $\mathrm{GL}_2(\mathbb{A}_{\mathbb{K}})$ and exhibits elliptic curves defined over $\mathbb{K}$ with which there is an agreement of (truncated) L-series. Interestingly, it seems that in some cases, rational plusforms are related to abelian varieties of dimension 2 rather than elliptic curves, as remarked in the concluding note of [Cre84]. An analogue of the Eichler-Shimura correspondence here would seem more subtle than in the rational case.

Theoretical results concerning conjecture 3.5 are limited to particular curves only. For those curves $E_{/\mathbb{K}}$ that are actually defined over $\mathbb{Q}$, their modularity over $\mathbb{K}$ can be analyzed through the theory of base change [Lan80], given that they are known to be modular over $\mathbb{Q}$. More recently, Taylor and others in [HST93], [Tay94] and [Ram94] have constructed l-adic representations for cusp forms of $\mathrm{GL}_2(\mathbb{A}_{\mathbb{K}})$. In [Tay94], section 4 of the paper consists in applications for the case where $\mathbb{K}$ has class number one. An example is given in which an elliptic curve defined over $\mathbb{Q}(\sqrt{-3})$ is shown to have an L-series agreeing with the L-function $L(s) = \prod_{\nu} L_{\nu}(s)$ of an automorphic representation of $\mathrm{GL}_2(\mathbb{A}_{\mathbb{K}})$, for all ν outside a set of Dirichlet density zero. The elliptic curve used in the example is not one of those used later in this thesis. It might be possible to check the modularity of some of the curves we use following a similar approach, but we do not pursue this.

Now how do we compute modular symbols for $E_{/\mathbb{K}}$? We need to relate them to elements of $H_1(X_0(\mathcal{N}))$. However, we may not pull back a Néron differential ω on $E_{/\mathbb{K}}$ to a multiple c of an invariant differential $\mathbf{F} \cdot \boldsymbol{\beta}$ on $X_0(\mathcal{N})$:

$$\begin{array}{ccc} H^1(X_0(\mathcal{N})) & \not\to & H^1(E) \\ c\mathbf{F} \cdot \boldsymbol{\beta} & \xleftarrow{?} & \omega. \end{array}$$

Thus the possibility of defining c, called the Manin constant in the rational case, remains a mystery, and so it is not obvious how to define what it means for an elliptic curve to be strong in its isogeny class. It should be that a **strong** curve is one for which all closed modular symbols are computed integral, and such that the greatest common divisor of all such is 1. But this is directly dependent on the period $\Omega(\mathbf{F})$ introduced at the end of the last section. As mentioned there, Kurčanov has shown that there is a unique such real period for a plusform $\mathbf{F}$, but his proof is existential and does not give an actual value for that period.

The approach we have followed is simply to take the smallest period on any curve E and multiply or divide it by an integral factor c_E so that it comes in close agreement with a candidate value for $\Omega(\mathbf{F})$. We have thus adjusted our computations differently for the few curves in each isogeny class. Indeed, the periods computed for these curves differ only by the degree of the isogeny between them, for this changes the period $\Omega(E)$ listed in Table 2 by the same factor. Hence c_E is always some power of the degree of the isogenies appearing in the isogeny class of E. With this approach, there is no need to officially declare any curve in the isogeny class as strong.

It is nevertheless important to have a precise value for a candidate period $\Omega(\mathbf{F})$, up to integral factors due to isogenies. Indeed, the "transcendental part" of the modular symbols should be well known, so that the the accuracy of the computations can be checked. As will be explained in section 3.5.4, we only compute approximations to modular symbols. Theoretically, $[\alpha] = \{\alpha\}/\Omega(\mathbf{F})$ for α equivalent to $j\infty$ modulo $\Gamma_0(\mathcal{N})$ is an integer. We have confidence in our calculations when the floating point value we compute for $[\alpha]$ is indeed very close to an integer.

Even without a geometric link between $X_0(\mathcal{N})$ and $E_{/\mathbb{K}}$, the assumed modularity of $E_{/\mathbb{K}}$ makes one hope that $\Omega(\mathbf{F})$ should be related to the complex period $\Omega(E)$ of the elliptic curve. The computation of this latter is described in section 3.5.1. We have been using $\Omega^*(E) = \Omega(E)/\sqrt{|D|}$ as a candidate value for $\Omega(\mathbf{F})$, where D is the fundamental discriminant of $\mathbb{K}$. The appearance of $\sqrt{-D}$ may seem unusual, since in the rational case, the Manin constant corresponds to some winding of the paths on $X_0(N)$ when projected to E and is rational. However, this c here is simply dependent on the normalizations we have used for the integrals defining modular symbols.

3.4 Mazur-Tate Type Conjectures

In the next few sections, we state and motivate the definition of a theta element suitable for Mazur-Tate type conjectures, state such conjectures over quadratic imaginary fields, and perform experimental tests.

Let $\mathcal{M}$ be an integral ideal of a quadratic imaginary field $\mathbb{K}$ of class number 1. Consider the ray class field extension $\mathbb{T}$ of $\mathbb{K}$ with conductor $\mathcal{M}$. We take G to be the Galois group of this extension. Thus $G = \mathrm{Gal}(\mathbb{T}/\mathbb{K}) \cong (\mathcal{O}_{\mathbb{K}}/\mathcal{M})^*/\mathcal{O}_{\mathbb{K}}^*$. We will sometimes denote this group by $G_{\mathcal{M}}$.

Let E be an elliptic curve defined over $\mathbb{K}$ of conductor $\mathcal{N}$, a non-zero integral ideal of $\mathcal{O}_{\mathbb{K}}$. Let $\mathbf{F} \in S_2^+(\Gamma_0(\mathcal{N}))$ be the plusform at level $\mathcal{N}$ conjecturally associated to $E_{/\mathbb{K}}$. Let $m \in \mathcal{O}_{\mathbb{K}}$ be a generator of the principal ideal $\mathcal{M}$. We will compute modular symbols $[\frac{a}{m}] = \lambda_{\mathbf{F}}(\frac{a}{m})/\Omega(\mathbf{F}) \in \mathbb{Q}$ for representatives a of $(\mathcal{O}_{\mathbb{K}}/\mathcal{M})^*/\mathcal{O}_{\mathbb{K}}^*$. These modular symbols do not depend on choices of units for the representatives a or m since it is easily seen from equation (3.8) that the computation of $\lambda_{\mathbf{F}}$ for a plusform $\mathbf{F}$ is invariant if we change its argument by a unit.

Looking at the proof of theorem 3.3, we actually realize that the denominator of $[\frac{a}{m}]$ is bounded by

$$S = \gcd_{\pi \in C} \left(\mathrm{N}(\pi) + 1 - c(\pi)\right)$$

where C is the set of all primes π satisfying claim 3.4. S thus depends on $\mathbf{F}$ (hence on $\mathcal{N}$) and on $\mathcal{M}$. A weaker bound completely independent of the actual cusp is given by

$$S' = \gcd_{\pi \in C'} \left(\mathrm{N}(\pi) + 1 - c(\pi)\right)$$

where C' is a subset of C containing the primes π coprime to $\mathcal{N}$ satisfying the following condition. Write the prime decomposition of $\mathcal{N}$ as $\mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\dots\mathcal{P}_k^{e_k}$, with all $\mathcal{P}_i$ distinct. Let $f_i = \lfloor e_i/2 \rfloor$ and define $\mathcal{N}' = \mathcal{P}_1^{f_1}\mathcal{P}_2^{f_2}\dots\mathcal{P}_k^{f_k}$. Then C' contains only primes

$\pi \equiv u^2 \pmod{\mathcal{N}'}$ for some unit $u \in \mathcal{O}_{\mathbb{K}}^*$. Therefore S' depends only on $\mathcal{N}$ and some of the Fourier-Bessel coefficients of $\mathbf{F}$, not on the actual cusp or $\mathcal{M}$.

We obtain that $\left[\frac{a}{m}\right] \in Z \subsetneq \mathbb{Q}$, where $Z = \mathbb{Z}\left[\frac{1}{S}\right] \subset \mathbb{Z}\left[\frac{1}{S'}\right]$, and we may now define theta elements using that Z. For any **layer** $\mathcal{M}$, integral ideal of $\mathbb{K}$ with generator $m \in \mathcal{O}_{\mathbb{K}}$, we define the **theta element** $\theta_{\mathcal{M}} \in Z[G_{\mathcal{M}}]$ as

$$\theta_{\mathcal{M}} = \sum_{\sigma \in G_{\mathcal{M}}} \left[\frac{a_\sigma}{m}\right] \sigma,$$

where $a_\sigma \in \mathcal{O}_{\mathbb{K}}$ is a lift of $\sigma + \mathcal{M} \in G_{\mathcal{M}}$.

In practice, we will not compute S or S'. We will rather look at the theta element as living in the world of $Z[G_{\mathcal{M}}]$ where Z has just enough inverted primes to contain the modular symbols appearing in the definition of $\theta_{\mathcal{M}}$. More precisely, we let

$$S'' = \operatorname*{lcm}_{\sigma \in G_{\mathcal{M}}} \left(\text{denominator of } \left[\frac{a_\sigma}{m}\right]\right)$$

and we look at $\theta_{\mathcal{M}}$ as an element of $Z[G_{\mathcal{M}}]$ with $Z = \mathbb{Z}\left[\frac{1}{S''}\right]$.

We will actually even go further than that. Given $\theta_{\mathcal{M}} \in Z[G_{\mathcal{M}}]$ with $Z = \mathbb{Z}\left[\frac{1}{S''}\right]$, we will consider $\tilde{\theta}_{\mathcal{M}} = S''\theta_{\mathcal{M}} \in \mathbb{Z}[G_{\mathcal{M}}]$ and test conjectures with $\tilde{\theta}_{\mathcal{M}}$ instead. By abuse of notation, we sometimes denote $\tilde{\theta}_{\mathcal{M}}$ by $\theta_{\mathcal{M}}$ only, or even simply by $\theta \in \mathbb{Z}[G]$. As seen in section 3.5.6 and explained in detail in [Tan95], this actually leads to stronger conjectures.

Our definition of theta elements satisfies interpolation properties with respect to the complex L-function since the theorem of Birch and Manin in the rational case generalizes to quadratic imaginary fields of class number 1.

Theorem 3.6 Let χ be a primitive character of conductor $\mathcal{M}$, with gauss sum $\tau(\chi)$. Then

$$L(\mathbf{F}, \chi, 1) = \frac{4\pi\, \tau(\chi)}{\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\mathcal{M})\, V_1(1)\, \alpha_{\mathbb{K}}} \sum_{b \bmod \mathcal{M}} \bar{\chi}(b) \lambda_{\mathbf{F}}(\frac{b}{m}),$$

where $V_1(s) = \frac{2}{\pi}\int_0^\infty K_0(4\pi x)\, x^{2s-1}\, dx$.

Proof. [Kur78, proposition 1]. ∎

This leads to the following vanishing properties.

Corollary 3.7 For χ primitive of conductor $\mathcal{M}$,

$$\chi(\theta_{\mathcal{M}}) = 0 \quad \text{if and only if} \quad L(\mathbf{F}, \bar{\chi}, 1) = 0.$$

∎

As in the rational case, we may project theta elements between different layers using natural projections $z_{\mathcal{M}}$ on Galois groups, or we may lift them through trace maps $\nu_{\mathcal{M}}$. We then also have the following compatibility relations between the layers.

Lemma 3.8 Let $\mathcal{N}$ be the level of the cusp form $\mathbf{F}$ from which the following theta elements are computed. Let $\mathcal{L}$ be a prime ideal of $\mathcal{O}_{\mathbb{K}}$, and let $c(\mathcal{L})$ be the corresponding Fourier-Bessel coefficient in the expansion of $\mathbf{F}$.

1. If $\mathcal{L}$ divides both $\mathcal{M}$ and $\mathcal{N}$, then $\quad z_{\mathcal{M}}(\theta_{\mathcal{M}\mathcal{L}}) = c(\mathcal{L})\theta_{\mathcal{M}}$.
2. If $\mathcal{L}$ is coprime to both $\mathcal{M}$ and $\mathcal{N}$, then $\quad z_{\mathcal{M}}(\theta_{\mathcal{M}\mathcal{L}}) = (c(\mathcal{L}) - \sigma_{\mathcal{L}} - \sigma_{\mathcal{L}}^{-1})\theta_{\mathcal{M}}$.
3. If $\mathcal{L}$ divides $\mathcal{N}$ but not $\mathcal{M}$, then $\quad z_{\mathcal{M}}(\theta_{\mathcal{M}\mathcal{L}}) = (c(\mathcal{L}) - \sigma_{\mathcal{L}}^{-1})\theta_{\mathcal{M}}$.
4. If $\mathcal{L}$ divides $\mathcal{M}$ but not $\mathcal{N}$, then $\quad z_{\mathcal{M}}(\theta_{\mathcal{M}\mathcal{L}}) = c(\mathcal{L})\theta_{\mathcal{M}} - \nu_{\mathcal{M}}(\theta_{\mathcal{M}/\mathcal{L}})$.

Sketch of proof. The proof is just an exercise in applying Hecke operators on the theta elements, thus on the modular symbols, and keeping track of the expansion of these latter.

We will sketch the proof only for cases 1 and 4 for reasons to be seen below, and we will also assume that the layers $\mathcal{J} = \mathcal{M},\ \mathcal{M}\mathcal{L}$ or $\mathcal{M}/\mathcal{L}$ under consideration are such that $\mathcal{O}_{\mathbb{K}}^*$ injects in $(\mathcal{O}_{\mathbb{K}}/\mathcal{J})^*$. This always happens for example when the layers do not lie above 2 or 3. Then we may rewrite a theta element at layer $\mathcal{J} = (j)$ as

$$\theta_{\mathcal{J}} \;=\; \sum_{a \in (\mathcal{O}_{\mathbb{K}}/\mathcal{J})^*/\mathcal{O}_{\mathbb{K}}^*} \left[\frac{a}{j}\right] \sigma_a \;=\; \frac{1}{\omega} \sum_{a \in (\mathcal{O}_{\mathbb{K}}/\mathcal{J})^*} \left[\frac{a}{j}\right] \sigma_a.$$

where $\omega = |\mathcal{O}_{\mathbb{K}}^*|$. This is possible since the modular symbols $\left[\frac{a}{j}\right]$ are unchanged if we replace a or j by unit multiples of these as we mentioned at the beginning of the section. Writing the theta elements this way makes the lifts and projections between the different layers simpler to follow. Using l for a generator of $\mathcal{L}$, we have

$$\theta_{\mathcal{ML}} = \frac{1}{\omega} \sum_{a \in (\mathcal{O}_{\mathbb{K}}/\mathcal{ML})^*} \left[\frac{a}{ml}\right] \sigma_a \implies z_{\mathcal{M}}(\theta_{\mathcal{ML}}) = \frac{1}{\omega} \sum_{a \in (\mathcal{O}_{\mathbb{K}}/\mathcal{M})^*} \left(\sum_{\tilde{a}} \left[\frac{\tilde{a}}{ml}\right]\right) \sigma_a,$$

where the $\tilde{a}$ are the lifts of $a \mod \mathcal{M}$ to $\mathcal{ML}$. We have also abused notation and denoted by σ_a the Artin symbol evaluated at (a) for both ray class field extensions of conductor $\mathcal{M}$ and $\mathcal{ML}$. The lifts $\tilde{a}$ are easier to describe when $\mathcal{L}$ divides $\mathcal{M}$, this is why we will only discuss cases 1 and 4. In these cases, we obtain

$$z_{\mathcal{M}}(\theta_{\mathcal{ML}}) = \frac{1}{\omega} \sum_{a \in (\mathcal{O}_{\mathbb{K}}/\mathcal{M})^*} \left(\sum_{k \bmod \mathcal{L}} \left[\frac{a+km}{ml}\right]\right) \sigma_a,$$

where $a + km$ is coprime to ml.

Now consider the action of the Hecke operator $T_{\mathcal{L}}$ on $\theta_{\mathcal{M}}$. In case 1, we have

$$\begin{aligned}
T_{\mathcal{L}}(\theta_{\mathcal{M}}) &= \sum_{k \bmod \mathcal{L}} \begin{pmatrix} 1 & k \\ 0 & l \end{pmatrix} \left(\frac{1}{\omega} \sum_{a \in (\mathcal{O}_{\mathbb{K}}/\mathcal{M})^*} \left[\frac{a}{m}\right] \sigma_a\right) \\
&= \frac{1}{\omega} \sum_{k \bmod \mathcal{L}} \sum_{a \in (\mathcal{O}_{\mathbb{K}}/\mathcal{M})^*} \left[\frac{\frac{a}{m}+k}{l}\right] \sigma_a \\
&= \frac{1}{\omega} \sum_{a \in (\mathcal{O}_{\mathbb{K}}/\mathcal{M})^*} \sum_{k \bmod \mathcal{L}} \left[\frac{a+mk}{ml}\right] \sigma_a \\
&= z_{\mathcal{M}}(\theta_{\mathcal{ML}}),
\end{aligned}$$

and the result follows for this case.

In case 4, the Hecke operator contains the extra matrix $\left(\begin{smallmatrix} l & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and when it acts on $\theta_{\mathcal{M}}$, we obtain an extra

$$\begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix} \left(\frac{1}{\omega} \sum_{a \in (\mathcal{O}_{\mathbb{K}}/\mathcal{M})^*} \left[\frac{a}{m}\right] \sigma_a\right) = \frac{1}{\omega} \sum_{a \in (\mathcal{O}_{\mathbb{K}}/\mathcal{M})^*} \left[\frac{al}{m}\right] \sigma_a = \frac{1}{\omega} \sum_{a \in (\mathcal{O}_{\mathbb{K}}/\mathcal{M})^*} \left[\frac{a}{m/l}\right] \sigma_a$$

since l divides m. But this is just the extra lift $\nu_{\mathcal{M}}(\theta_{\mathcal{M}/\mathcal{L}})$ appearing in case 4. ∎

The compatibility formulae yield the following two propositions.

Proposition 3.9 Let I be the augmentation ideal of the group ring $Z[G]$. If $L(\mathbf{F}, 1) = 0$, then $\theta_{\mathcal{M}}$ belongs to I.

Proof. The proof mimics that in the rational case. We consider $\chi(\theta_{\mathcal{M}})$ where χ is the trivial character. We verify that $\theta_{\mathcal{M}} \in Z[G]$ belongs to I, that is, if $\chi(\theta_{\mathcal{M}}) = 0$, by projecting $\theta_{\mathcal{M}}$ to $Z[\langle e \rangle] \cong Z$. Applying lemma 3.8 repeatedly, we obtain that $\chi(\theta_{\mathcal{M}})$ is a multiple of $\theta_{(1)}$ which is zero when $L(\mathbf{F}, 1) = 0$. ■

Proposition 3.10 Suppose $\mathcal{M}$ is divisible by a prime of split multiplicative reduction $\mathcal{L}$ for a modular elliptic curve $E_{/\mathbb{K}}$. Then $\theta_{\mathcal{M}}$ belongs to I.

Proof. The proof is again similar to that in the rational case. We apply lemma 3.8 many times and obtain that $\theta_{\mathcal{M}}$ projects to $(c(\mathcal{L}) - \sigma_{\mathcal{L}}^{-1})$ times some multiple of $\theta_{(1)}$. $\sigma_{\mathcal{L}}$ is trivial, and $c(\mathcal{L}) = 1$ for primes of split multiplicative reduction. Thus $\theta_{\mathcal{M}}$ projects to 0 as desired. ■

Proposition 3.9 together with the Birch and Swinnerton-Dyer conjecture for elliptic curves $E_{/\mathbb{K}}$ imply

Conjecture 3.11

Let $E_{/\mathbb{K}}$ be a modular elliptic curve of rank r. If $r \geq 1$, then $\theta_{\mathcal{M}}$ belongs to I. ■

This conjecture will be tested in section 3.6, but it is only equivalent to testing the usual Birch and Swinnerton-Dyer conjecture and the modularity of the curve. Some computations will also be performed that confirm proposition 3.10, and this somehow tests the conjectural modularity of the curves only. However, we will be especially interested in tests of the following more general conjecture.

Conjecture 3.12 Let $E_{/\mathbb{K}}$ be an elliptic curve and fix a layer $\mathcal{M}$. Construct $\theta_{\mathcal{M}} \in Z[G_{\mathcal{M}}]$ from the conjecturally associated plusform $\mathbf{F}$, and let I be the augmentation ideal of $Z[G_{\mathcal{M}}]$. Denote by s the number of primes of split multiplicative reduction for $E_{/\mathbb{K}}$ dividing $\mathcal{M}$, and let r be the rank of the Mordell-Weil group of $E_{/\mathbb{K}}$. Then $\theta_{\mathcal{M}}$ belongs to I^{r+s}. ■

Again, it might be that $\theta_{\mathcal{M}}$ belongs to higher powers of I. Some examples of this behavior will be discussed in section 3.6.

3.5 Implementations

We have attached in the appendix the *GP* (*PARI*) codes used for the numerical computations. These were mostly performed on two platforms. For reasonably small computations, a *Windows* versions of *PARI* on a personal 500 MHz *Intel Pentium III* with 512 Mb of RAM has been used. The calculations requiring lots of machine time for higher precision were done on a *UNIX* server of the mathematics department at McGill University. It has been found that the accuracy of the calculations were mostly dependent on the number of terms used in the truncated L-series computed for the elliptic curves, as described in section 3.5.4. *PARI* was sometimes unable to perform the computations when trying to use too many terms, especially with the *Windows* version. The *UNIX* platform was found to be more stable.

3.5.1 Computing the Complex Period of E

We lift our curve $E_{/\mathbb{K}}$ to $E_{/\mathbb{C}}$ and write an equation for this latter in the form $y^2 = (x-e_1)(x-e_2)(x-e_3)$, with $e_1, e_2, e_3 \in \mathbb{C}$. $E_{/\mathbb{C}}$ is uniformized by $\mathbb{C}/\Lambda$, where a basis $\langle \lambda_1, \lambda_2 \rangle$ for the lattice Λ is given by

$$\lambda_1 = \int_{e_1}^{e_2} \frac{dx}{\sqrt{(x-e_1)(x-e_2)(x-e_3)}} \quad \text{and} \quad \lambda_2 = \int_{e_2}^{e_3} \frac{dx}{\sqrt{(x-e_1)(x-e_2)(x-e_3)}} .$$

The area $\Omega(E)$ of a fundamental parallelogram of Λ is then easily verified to be given by $\Omega(E) = |\mathrm{Im}(\overline{\lambda_1}\lambda_2)|$. This complex period $\Omega(E)$ is thus actually a real number.

The above elliptic integrals can be numerically computed using the arithmetic geometric-mean:

$$\lambda_1 = \frac{\pi}{\mathrm{agm}(\sqrt{e_3-e_1}, \sqrt{e_3-e_2})} \quad \text{and} \quad \lambda_2 = \frac{i\pi}{\mathrm{agm}(\sqrt{e_3-e_1}, \sqrt{e_2-e_1})} .$$

The computation is actually very efficient, for it can be done using an algorithm that converges quadratically. This has been implemented in the routine *Complex Periods* provided in the appendix.

The arithmetic-geometric mean, its algorithm and its relation to the elliptic integrals above are explained in detail in [Cox84]. The following point is worth mentioning though. We actually have to compute a *complex* arithmetic-geometric mean. However, the iterative algorithm for computing this involves a choice of square root at each iteration. So there are many possible values for arithmetic-geometric means. Contrary to what is mentioned in [CW94], we found it necessary to implement our own version of the arithmetic-geometric mean in order to compute its *simplest value* (see [Cox84] for the definition). This has been done in the routine *Simplest Value of the Complex Arithmetic-Geometric Mean.* It is this one value that corresponds to the above elliptic integrals. Indeed, the algorithm used by Cremona and Whitley and the algorithm furnished by *PARI* for the computation of the arithmetic-geometric mean gave values for the periods λ_i that do not always pass the following checks,

$$c_4 = (\frac{2\pi}{\lambda_2})^4(1+240\sum_{n=1}^{\infty}\frac{n^3q^n}{1-q^n}) \quad \text{and} \quad c_6 = (\frac{2\pi}{\lambda_2})^6(1-504\sum_{n=1}^{\infty}\frac{n^5q^n}{1-q^n})$$

with $q = e^{2\pi i\lambda_1/\lambda_2}$, and sometimes gave values for the area $\Omega(E)$ that were off by a factor of 3. These checks have been systematically performed and passed for all our calculations.

3.5.2 Computing the Cusp Form Associated to $E_{/\mathbb{K}}$

We make the assumption that $E_{/\mathbb{K}}$ is modular. Thus to $E_{/\mathbb{K}}$, there is an associated rational plusform $\mathbf{F}$ for $\mathrm{GL}_2(\mathbb{A}_{\mathbb{K}})$,

$$\mathbf{F}(z,t) = \sum_{(\alpha)\neq(0)} c(\alpha)t^2\mathbf{K}\left(\frac{4\pi\,|\alpha|\,t}{\sqrt{|D|}}\right)\sum_{\epsilon\in\mathcal{O}_{\mathbb{K}}^*}\psi\left(\frac{\epsilon\alpha z}{\sqrt{D}}\right), \tag{3.14}$$

such that for all non-zero integral ideal $\alpha\subset\mathcal{O}_{\mathbb{K}}$, the Fourier-Bessel coefficients $c(\alpha)$ appearing in the expansion of $\mathbf{F}$ are the same as the a_α appearing in the L-series (3.13) for $E_{/\mathbb{K}}$:

$$L(E_{/\mathbb{K}},s) = \sum_{(\alpha)\neq(0)}\frac{a_\alpha}{\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\alpha)^s}.$$

Our goal is to compute $\mathbf{F}$ up to a very good approximation, that is, we need to compute the $c(\alpha)$ for all (α) up to some maximal norm M that we fix.

The above expansions are indexed by the non-zero ideals of $\mathbb{K}$, thus the computation of $\mathbf{F}$ requires us to have the ideals of $\mathbb{K}$ themselves, together with their factorization into prime ideals. This factorization is necessary, as it will be used to compute the coefficients $c(\alpha)$ for which (α) is not a prime ideal of $\mathcal{O}_{\mathbb{K}}$.

We start by lifting all primes $p \leq M$ of $\mathbb{Q}$ to $p\mathcal{O}_{\mathbb{K}}$ and factor to get prime ideals $\mathcal{P}$ in $\mathbb{K}$. By taking combinations of the form $\mathcal{N} = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\ldots\mathcal{P}_k^{e_k}$ of norm $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\mathcal{N}) \leq M$, we get all the desired integral ideals of $\mathbb{K}$ together with their factorization.

We will thus end up computing a truncated Fourier-Bessel expansion for $\mathbf{F}$:

$$\mathbf{F}(z,t) \approx \sum_{\substack{(\alpha) \neq (0) \\ \mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\alpha) \leq M}} c(\alpha) t^2 \mathbf{K}\left(\frac{4\pi\,|\alpha|\,t}{\sqrt{|D|}}\right) \sum_{\epsilon \in \mathcal{O}_{\mathbb{K}}^*} \psi\left(\frac{\epsilon\alpha z}{\sqrt{D}}\right) . \tag{3.15}$$

The maximal norm M for the ideals computed then determines the length of the truncated series. The accuracy of the computations of the modular symbols described in section 3.5.4 is highly dependent on the choice of M, which typically must be in the tens of thousands.

In the following, by *prime* (or *composite*) Fourier coefficients, we mean coefficients $c(\alpha)$ for which (α) is a prime (or composite) ideal of $\mathcal{O}_{\mathbb{K}}$. The actual value $c(\alpha) \in \mathbb{Z}$ may or may not be prime.

The Fourier coefficients $c(\alpha)$ required are computed the following way. First we compute traces of Frobenius $a_{\mathcal{P}}$ for $E_{/\mathbb{K}}$ by counting rational points on the reduction $\tilde{E}_{/k_{\mathcal{P}}}$ of $E_{/\mathbb{K}}$ modulo prime ideals $\mathcal{P}$ of $\mathbb{K}$. The elliptic curve is given by an equation

$$E_{/\mathbb{K}}: \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \; .$$

For primes $\mathcal{P}$ of $\mathcal{O}_{\mathbb{K}}$ lying above 2 or 3, we keep this equation. We count the number $N_{\mathcal{P}} - 1$ of affine points on $\tilde{E}_{/k_{\mathcal{P}}}$ by looping on all values of x and y in $k_{\mathcal{P}} = \mathcal{O}_{\mathbb{K}}/\mathcal{P}$, and verifying if they satisfy the equation for E modulo $\mathcal{P}$. Then $a_{\mathcal{P}} = \mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\mathcal{P}) + 1 - N_{\mathcal{P}}$. Since there are not many elements in $k_{\mathcal{P}}$ for these primes, this procedure works well. For primes $\mathcal{P}$ lying above $p \neq 2, 3$, we find an isomorphic copy of $E_{/\mathbb{K}}$ of the form

$$E_{/\mathbb{K}}: \ y^2 = x^3 - 27c_4x - 54c_6 \tag{3.16}$$

We loop on all values of x in $k_{\mathcal{P}}$, computing the right hand side of the equation, and test whether we are getting a non zero square of $\mathcal{O}_{\mathbb{K}}$ modulo $\mathcal{P}$ or not. When $k_{\mathcal{P}}$ is large, this procedure saves lots of computation time compared to nested loops on both x and y, as is performed in characteristics 2 and 3 above. When $\mathcal{P}$ is not inert, then $k_{\mathcal{P}} \cong \mathbb{Z}/p\mathbb{Z}$ and we may use the "kronecker(x, y)" function furnished by *PARI* that returns 0 for $x \equiv 0 \pmod{y}$, 1 if x is a non-zero square modulo y, and -1 otherwise. When $\mathcal{P}$ is inert, a table was made computing the number of square roots of elements of $k_{\mathcal{P}}$. This is less efficient than when $\mathcal{P}$ is not inert, but still considerably more efficient than nested loops on both x and y.

Once we have these traces of Frobenius $a_{\mathcal{P}}$, by the assumed modularity of $E_{/\mathbb{K}}$ we have the prime Fourier coefficients $c(\mathcal{P})$, and we may compute the composite Fourier coefficients by multiplicativity. The multiplicativity is non strict. To compute the Fourier coefficients indexed by prime powers $\mathcal{P}^e$, $e \geq 2$, we use the fact that $\mathbf{F}$ is an eigenform, and use equations (3.7).

The prime ideals $\mathcal{P}$ of $\mathbb{K}$ and the traces of Frobenius $a_{\mathcal{P}}$ are computed in the routine *Prime Ideals*. All the ideals $\mathcal{N}$ in $\mathcal{O}_{\mathbb{K}}$ of norm less or equal to the maximal norm M, together with the corresponding Fourier coefficients, are computed in the routine *All Ideals*. It has been found that the computation of the prime Fourier coefficients was very time consuming. We have thus implemented the storage on disk of these coefficients, which could be retrieved for any curve in the isogeny class.

3.5.3 Euclidean Algorithms

We have implemented a standard Euclidean algorithm for the principal ideal domains $\mathbb{K}$ that are norm-Euclidean. The routine *Euclidean Algorithm for the P.I.D. K* returns a greatest common divisor g of two elements a and b of $\mathbb{K}$, as well numbers c and d in $\mathbb{K}$ that give a linear combination for the gcd:

$$g = ca + db.$$

A greatest common divisor g in the context of quadratic imaginary fields $\mathbb{K}$ is only defined modulo units $\mathcal{O}_{\mathbb{K}}^*$. This causes no problems. However for chosen g, there are many possible combinations and this is a more important issue. The choices of c and d influence the convergence of the modular symbols computations that require them. In some cases, we have found necessary to use the g given by the standard algorithm but recompute a new combination minimizing the norm of c. For this, we simply loop on the elements c of $\mathcal{O}_{\mathbb{K}}$ by increasing norm and stop as soon as we find an integral $d = \frac{g-ca}{b}$. This routine is never called with $b = 0$.

For the quadratic fields that are not norm-Euclidean, we rely on the powerful features of *PARI* . To compute the greatest common divisor of a and b, we ask *PARI* to compute the ideal $(a)+(b)$, and request a generator g for the ideal. We then compute c and d for the linear combination as above.

The contribution of Elise Whitley in her thesis [Whi90] consisted in implementing a "pseudo-Euclidean" algorithm for the quadratic imaginary fields $\mathbb{K}$ of class number 1 that are not Euclidean. Unfortunately, this algorithm is not explained in the subsequent paper [CW94]. We did not try to get a copy of her thesis, but this might be of some interest eventually.

3.5.4 Computing Integral Modular Symbols

Suppose we wish to compute a modular symbol $\{a, b\}$ that we know is integral, that is, it is known to form a closed path on $X_0(\mathcal{N})$. Then there is some $\gamma \in \Gamma_0(\mathcal{N})$ such that $b = \gamma a$. Fortunately, $\{a, b\} = \{a, \gamma a\}$ does not depend on a, that is, $\{a, \gamma a\} = \{\gamma\}$, where $\{\gamma\} = \{\tau, \gamma\tau\}$ for any $\tau \in \mathcal{H}_3^*$.

The evaluation of $\{a, b\}$ thus requires us to first find γ, and then choose a τ. Theoretically, any $\tau \in \mathcal{H}_3^*$ and any $\gamma \in \Gamma_0(\mathcal{N})$ satisfying $b = \gamma a$ would do, but in practice, we must be careful about these choices.

We need to compute

$$\{\gamma\} = \alpha_{\mathbb{K}} \int_{\tau}^{\gamma\tau} \mathbf{F} \cdot \boldsymbol{\beta} \ .$$

As in section 3.2, it is preferable to use vertical paths of integration:

$$\{\tau, \gamma\tau\} = \{\tau, j\infty\} + \{j\infty, \gamma\tau\} = \alpha_{\mathbb{K}} \int_{\tau}^{j\infty} \mathbf{F} \cdot \boldsymbol{\beta} - \alpha_{\mathbb{K}} \int_{\gamma\tau}^{j\infty} \mathbf{F} \cdot \boldsymbol{\beta}.$$

Let us write $\tau = (z_1, t_1) \in \mathbb{C} \times \mathbb{R}^+$ and similarly $\gamma\tau = (z_2, t_2)$. We obtain

$$\{\gamma\} = \alpha_{\mathbb{K}} \int_{t_1}^{j\infty} F_1(z_1, t) \frac{dt}{t} - \alpha_{\mathbb{K}} \int_{t_2}^{j\infty} F_1(z_2, t) \frac{dt}{t}.$$

For $A = (z_A, t_A) \in \mathcal{H}_3^*$, we define

$$I_{\mathbf{F}}(A) = \alpha_{\mathbb{K}} \int_{t_A}^{j\infty} F_1(z_A, t_A) \frac{dt}{t}.$$

With this notation, $\{\gamma\} = I_{\mathbf{F}}(\tau) - I_{\mathbf{F}}(\gamma\tau)$. We show how to compute such an integral. We expand F_1 as a Fourier-Bessel series and use the fact that we have a PID and a plusform to split the sum on elements of $\mathcal{O}_{\mathbb{K}}$ to sums on ideals and units, as we did for equation (3.8).

$$\begin{aligned} I_{\mathbf{F}}(A) &= \alpha_{\mathbb{K}} \int_{t_A}^{j\infty} \sum_{0 \neq \alpha \in \mathcal{O}_{\mathbb{K}}} c(\alpha) t^2 K_0 \left(\frac{4\pi \left|\alpha\right| t}{\sqrt{|D|}} \right) \psi \left(\frac{\alpha z_A}{\sqrt{D}} \right) \frac{dt}{t} \\ &= \alpha_{\mathbb{K}} \int_{t_A}^{j\infty} \sum_{(\alpha) \neq (0)} c(\alpha) t K_0 \left(\frac{4\pi \left|\alpha\right| t}{\sqrt{|D|}} \right) \sum_{\epsilon \in \mathcal{O}_{\mathbb{K}}^*} \psi \left(\frac{\epsilon \alpha z_A}{\sqrt{D}} \right) \, dt \end{aligned}$$

At infinity, the modified Bessel functions $K_n(x)$ all behave like $e^{-x}/\sqrt{2\pi x}$ (c.f. [Spi74, formula 24.108]), which is very good. If $t_A > 0$, we may then switch the integral and the sum to get

$$I_{\mathbf{F}}(A) = \alpha_{\mathbb{K}} \sum_{(\alpha) \neq (0)} c(\alpha) \sum_{\epsilon \in \mathcal{O}_{\mathbb{K}}^*} \psi \left(\frac{\epsilon \alpha z_A}{\sqrt{D}} \right) \int_{t_A}^{j\infty} t K_0 \left(\frac{4\pi \left|\alpha\right| t}{\sqrt{|D|}} \right) \, dt$$

We have the following recurrence relation ([Spi74, formula 24.56]) for the modified Bessel functions of the second kind:

$$\frac{d}{dx} x^n K_n(x) = -x^n K_{n-1}(x).$$

Using this, a natural change of variable to use it and the above mentioned behavior of $K_n(x)$ at infinity, we obtain

$$I_{\mathbf{F}}(A) = \frac{|D|}{16\pi^2}\,\alpha_{\mathbb{K}} \sum_{(\alpha)\neq(0)} \frac{c(\alpha)}{|\alpha|} \sum_{\epsilon\in\mathcal{O}_{\mathbb{K}}^*} \psi\left(\frac{\epsilon\alpha z_A}{\sqrt{D}}\right) t'_A K_1(|\alpha| t'_A) \qquad (t_A > 0)$$

where $t'_A = \frac{4\pi t_A}{\sqrt{|D|}}$. Recall that $\alpha_{\mathbb{K}} = \frac{-16\pi^2}{\omega D}$ with ω being the number of roots of unity in $\mathcal{O}_{\mathbb{K}}$. Thus for $t_A > 0$, we finalize as

$$I_{\mathbf{F}}(A) = \frac{t'_A}{\omega} \sum_{(\alpha)\neq(0)} \frac{c(\alpha)}{|\alpha|} K_1(|\alpha| t'_A) \sum_{\epsilon\in\mathcal{O}_{\mathbb{K}}^*} \psi\left(\frac{\epsilon\alpha z_A}{\sqrt{D}}\right). \tag{3.17}$$

The problem now is that the hyperbolic Bessel function $K_1(x)$ behaves like $-\frac{1}{x}$ in the neighborhood of $x = 0$. Indeed ([Arf85, 11.117]),

$$K_n(x) = \frac{\pi}{2} i^{n+1} H_n^{(1)}(ix),$$

where H_n is the Hankel function. Thus $K_1(x) = -\frac{\pi}{2} H_1^{(1)}(ix)$ and the Laurent series expansion of $H_1^{(1)}$ around $x = 0$ starts as ([Arf85, 11.89])

$$H_1^{(1)}(ix) = -i\frac{(1-1)!}{\pi}\left(\frac{2}{x}\right)^1 + \ldots$$

Hence $K_1(x) = -\frac{\pi}{2}\left[-\frac{i}{\pi}\left(\frac{2}{ix}\right)^1 + \ldots\right] = \frac{1}{x} + \ldots$ as claimed. Thus we must stay far away from $t_A = 0$. In particular, we may not take τ and $\gamma\tau$ to be affine cusps, we must take them in $\mathcal{H}_3$. Moreover, we will only compute an approximation to $I_{\mathbf{F}}(A)$ using the truncated Fourier-Bessel equation (3.15) for $\mathbf{F}$.

$$I_{\mathbf{F}}(A) \approx \frac{t'_A}{\omega} \sum_{\substack{(\alpha)\neq(0)\\ \mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\alpha)\leq M}} K_1(|\alpha| t'_A) \sum_{\epsilon\in\mathcal{O}_{\mathbb{K}}^*} \psi\left(\frac{\epsilon\alpha z_A}{\sqrt{D}}\right) \qquad (t_A > 0) \tag{3.18}$$

We see that the size of M is crucial to get a good approximation. But a huge M requires lots of computation time, both when computing the Fourier coefficients themselves, and also when computing the sum in equation (3.18). *PARI* also requires a good approximation to the values of K_1. Thus in order to keep the computation time as small as possible, it is important to have high values of t_1 and t_2. This gives the fastest possible convergence of the series (3.17) and an easier time for *PARI* to compute values of K_1.

We show how to choose γ and τ making t_1 and t_2 as big as possible. Recall we are using ν as a generator for the level $\mathcal{N}$. With

$$\tau = (z_1, t_1), \qquad \gamma\tau = (z_2, t_2) \quad \text{and} \quad \gamma = \begin{pmatrix} a & b \\ c\nu & d \end{pmatrix} \in \Gamma_0(\mathcal{N}),$$

we compute that

$$t_2 = \frac{t_1}{|c\nu z + d|^2 + |c\nu|^2 t_1^2}.$$

Choosing a big t_1 gives a small t_2 and vice-versa. Approximations of $I_{\mathbf{F}}(\tau)$ and $I_{\mathbf{F}}(\gamma\tau)$ will be computed with the same M, thus the quality of the approximation of $\{\gamma\}$ depends on the smallest of t_1 and t_2. The best we can do is arrange so that $t_1 = t_2$. This leads to

$$t_1^2 = \frac{1 - |c\nu z + d|^2}{|c\nu|^2},$$

which is maximal when $c\nu z + d = 0$, in which case $t_1 = t_2 = 1/|c\nu|$. We must thus search for a $\gamma = \left(\begin{smallmatrix} a & b \\ c\nu & d \end{smallmatrix}\right)$ satisfying $b = \gamma a$ with the norm of c as small as possible, and then use τ and $\gamma\tau$ given by $(z_1, t_1) = (-\frac{d}{c\nu}, \frac{1}{|c\nu|})$, and $(z_2, t_2) = (\frac{a}{c\nu}, \frac{1}{|c\nu|})$. The search for γ and the computation of $\{\gamma\}$ are implemented in the routines *Find Gamma* and *Closed Modular Symbols* found in the appendix.

Even though a and b might be equivalent cusps modulo $\Gamma_0(\mathcal{N})$, it is not automatic that an element $\gamma \in \mathrm{SL}_2(\mathcal{O}_{\mathbb{K}})$ satisfying $b = \gamma a$ will lie in $\Gamma_0(\mathcal{N})$. Consider the stabilizer of $j\infty$,

$$S_\infty = \left\{ \begin{pmatrix} 1 & \kappa \\ 0 & 1 \end{pmatrix} \;\middle|\; \kappa \in \mathcal{O}_{\mathbb{K}} \right\}.$$

We do have that $S_\infty \subset \Gamma_0(\mathcal{N})$. However, stabilizers of other cusps α are given by $S_\alpha = \gamma_\alpha S_\infty \gamma_\alpha^{-1}$ where $\gamma_\alpha \in \mathrm{SL}_2(\mathcal{O}_{\mathbb{K}})$ satisfies $\gamma_\alpha j\infty = \alpha$. The existence of such a γ_α follows from the fact that we only use fields $\mathbb{K}$ that are principal ideal domains. However, not all floor cusps are equivalent to $j\infty$ modulo $\Gamma_0(\mathcal{N})$, so we may not have that $\gamma_\alpha \in \Gamma_0(\mathcal{N})$. Given that $\Gamma_0(\mathcal{N})$ is *not* a normal subgroup of $\mathrm{SL}_2(\mathcal{O}_{\mathbb{K}})$, $S_\alpha \not\subseteq \Gamma_0(\mathcal{N})$ in general. For example, $a = 0$ is definitively equivalent to $b = 0$ modulo $\Gamma_0(\mathcal{N})$, but $STS^{-1} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \notin \Gamma_o(\mathcal{N})$ stabilizes 0.

The procedure to find $\gamma \in \Gamma_0(\mathcal{N})$ is the following. We first find γ_a and γ_b in $\mathrm{SL}_2(\mathcal{O}_{\mathbb{K}})$ sending $j\infty$ to a and b respectively. Writing $a = \frac{p_1}{q_1}$ and $b = \frac{p_2}{q_2}$ in lowest terms, γ is easily found by completing the matrices $\left(\begin{smallmatrix} p_1 & * \\ q_1 & * \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} p_2 & * \\ q_2 & * \end{smallmatrix}\right)$ as elements of $\mathrm{SL}_2(\mathcal{O}_{\mathbb{K}})$ using the Euclidean algorithm. See section 3.5.3 for some explanations pertaining to the use of this algorithm. For any $\gamma_\infty \in S_\infty$, we have that $\gamma = \gamma_b \gamma_\infty \gamma_a^{-1} \in \mathrm{SL}_2(\mathcal{O}_{\mathbb{K}})$ sends a to b, and any $\gamma \in \mathrm{SL}_2(\mathcal{O}_{\mathbb{K}})$ sending a to b is of this form. We may thus loop on elements $\kappa \in \mathcal{O}_{\mathbb{K}}$ by increasing norm until $\gamma_\infty = \left(\begin{smallmatrix} 1 & \kappa \\ 0 & 1 \end{smallmatrix}\right) \in S_\infty$ is such that the corresponding $\gamma = \gamma_b \gamma_\infty \gamma_1^{-1}$ is in $\Gamma_0(\mathcal{N})$.

The theory predicts that $[\gamma] = \{\gamma\}/\Omega(\mathbf{F}) \in \mathbb{Z}$. Thus we know that we chose M big enough for accurate computations when the floating point calculation of $[\gamma]$ that is performed is indeed very close to an integer. Close attention was thus given to the number of zeroes after the decimal point appearing in the calculations. It is very clear here that the size of the conductor of the curve used will greatly influence the convergence of the computations. A theta element requires the computation of many (non-integral) modular symbols, and it will be seen in section 3.5.5 that each of these, in turn, use Hecke operators to close their paths and thus demand the calculation of many closed modular symbols. We were typically using M in the tens of thousands, and the calculation of one $I_{\mathbf{F}}$ then requires many minutes. It has thus been found necessary to store some calculations on disk.

It is not necessary to store all the computed $\{\gamma\}$ separately. The computation of $\{\gamma\}$ requires two computations of $I_{\mathbf{F}}$, and these depend only on some combinations of elements of $\gamma = \left(\begin{smallmatrix} a & b \\ c\nu & d \end{smallmatrix}\right)$. For example, $I_{\mathbf{F}}(\tau)$ depends only on $Arg1 = -\frac{d}{c\nu}$ and $Arg2 = \frac{1}{|c\nu|}$. Moreover, the computation of $I_{\mathbf{F}}$ is unchanged if we multiply $Arg1$ by a unit of $\mathcal{O}_{\mathbb{K}}$ as is easily seen from equation (3.14). We thus stored computations of $I_{\mathbf{F}}$, and these could be retrieved whenever we have the same $Arg1$ modulo units and the same $Arg2$.

This storage certainly saves time by avoiding multiple computations of the same $I_{\mathbf{F}}$, but it also has another advantage. The computation of theta elements requires many closed modular symbols. Some of them happen to require little values of M to get reasonable precision. Say M in the range 5000-10000 could lead to 4-5 digits of precision. But other integral modular symbols might require M over 100000 to get only 1 or 2 digits of precision. The storage permitted us to spend significant time with large M on the highly demanding calculations without a waste of time computing easier symbols with a uselessly big M.

3.5.5 Computing Theta Elements

We choose a conductor $\mathcal{M}$ for the ray class field $\mathbb{T}$, denote a generator by $m \in \mathcal{O}_{\mathbb{K}}$, and compute the Galois group $G = \mathrm{Gal}(\mathbb{T}/\mathbb{K}) = (\mathcal{O}_{\mathbb{K}}/\mathcal{M})^*/\mathcal{O}_{\mathbb{K}}^*$. This is done in the routine *Galois Group* in which we use the function “idealstar” of *PARI* to get the structure of $(\mathcal{O}_{\mathbb{K}}/\mathcal{M})^*$. It returns a decomposition of $(\mathcal{O}_{\mathbb{K}}/\mathcal{M})^*$ into cyclic components and gives generators for these latter. We quotient the units ourselves (if necessary) to get G. Say G has k cyclic components of order $n_1, n_2, \ldots, n_k$ with generators $\sigma_1, \sigma_2, \ldots, \sigma_k$. Then all elements σ of the group G are easily computed by taking all multiples modulo $\mathcal{M}$ of the form $\sigma_1^{e_1}\sigma_2^{e_2}\ldots\sigma_k^{e_k}$, with $e_i = 1, \ldots, n_i$. Let $a_\sigma \in \mathcal{O}_{\mathbb{K}}$ be a lift of $\sigma + \mathcal{M} \in G$. The goal is to compute the modular symbols appearing in

$$\theta_{\mathcal{M}} = \sum_{\sigma \in G} \left[\frac{a_\sigma}{m}\right] \sigma.$$

Let $\gamma = \left(\begin{smallmatrix} a & b \\ c\nu & d \end{smallmatrix}\right) \in \Gamma_0(\mathcal{N})$. Then $\gamma(j\infty) = \frac{a}{c\nu}$. We obtain that a modular symbol $[\alpha] = \left[\frac{a}{m}\right] = \left\{\frac{a}{m}\right\}/\Omega(\mathbf{F})$ is integral if and only if $\frac{a}{m}$ in lowest terms is such that m is a multiple of ν in $\mathcal{O}_{\mathbb{K}}$, that is, if and only if $\mathcal{M}$ is a multiple of $\mathcal{N}$. Hence in general, the modular symbols $\left[\frac{a}{m}\right]$ we have to compute are not integral. They are nevertheless rational, according to theorem 3.3. Following the proof of that theorem, we may compute non-integral modular symbols the following way.

We first find a Hecke operator T_π with π of smallest possible norm satisfying claim

3.4. This is done in the routine *Hecke Operator.* Then according to equation (3.11),

$$\{\alpha\} = \frac{1}{c_\pi - 1 - \mathrm{N}(\pi)} \left(\{\pi\alpha, \alpha\} + \sum_{\gamma \bmod \pi} \{\frac{\alpha+\gamma}{\pi}, \alpha\} \right) \tag{3.19}$$

where all modular symbols appearing on the right are integral, and can thus be computed as described in the preceding section. In the above calculation, we round off each time a closed modular symbol is computed and keep track of the rounding errors. The accuracy of the computation of a modular symbol, as reported in section 3.6, is the minimum of the accuracies obtained in each of the $\mathrm{N}(\pi) + 1$ calculations of closed modular symbols required in equation (3.19).

It is very clear here that it is of the utmost importance to keep $\mathrm{N}(\pi)$ as small as possible, for it directly affects the number of integral modular symbols to be computed to get a unique modular symbol for $\theta_{\mathcal{M}}$. It was therefore very important to have an efficient proof of theorem 3.3, which was definitively not supplied by Kurčanov.

We have not found it necessary to implement the use of continued fractions to compute non-integral modular symbols. One of the important reasons is that some of the most interesting calculations we will describe in section 3.6 are done with curves that are not defined over Euclidean fields. Also, the M-symbols $(c : d)$ required in such a procedure are in one-to-one correspondence with $\mathbb{P}^1(\mathcal{O}_{\mathbb{K}}/\mathcal{N}\mathcal{O}_{\mathbb{K}})$. We figured out that the rather high levels for the curves we are using would require too many M-symbols to be calculated, each of these requiring to close the path.

3.5.6 Derivatives of Theta Elements

The role of the order of vanishing of L-functions at 1 in the Birch and Swinnerton-Dyer conjecture is replaced, in Mazur-Tate conjectures, by a belonging of theta elements to powers of augmentation ideals. Thus given some $\theta \in Z[G]$ and the augmentation ideal I, we say that θ **vanishes to order** (at least) r if $\theta \in I^r$.

We need a way to check, for given r, whether θ is in I^r or not. To this end, we may use the following results.

Theorem 3.13 Suppose $Z = \mathbb{Z}$, and $G = \langle\sigma\rangle$ is a cyclic group of prime order l. Assume also that $\theta \in I$. Then for $r \geq 2$, we have:

$$\theta \in I^r \quad \text{iff} \quad \mathrm{ord}_l \left(\prod_{\chi \in \hat{G}}{}' \chi(\theta) \right) \geq r.$$

The prime on the product means that it is taken over all characters of the dual group $\hat{G}$ of G *except* the trivial character $\chi = \mathbf{1}$.

Proof. [Gro88, p.187] ■

This result is elegant and quite easy to implement. Indeed, $\chi(\sigma)$ is a primitive l^{th} root of unity ζ, and the above product is just the absolute norm $\mathrm{N}(\chi(\theta)) = \mathrm{N}_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\chi(\theta))$ of $\chi(\theta)$ in $\mathbb{Q}(\zeta)$ for any non-trivial χ. Moreover, we get better than just a test at a given r. The valuation at l of the integer $\mathrm{N}(\chi(\theta))$ actually gives precisely the maximal value of r for which $\theta \in I^r$. This turns out to be quite handy. On the other hand, the restrictions on Z and G are quite severe. The requirement that $Z = \mathbb{Z}$ cannot be lifted easily, so we will keep it. The structure of augmentation ideals and their powers in group rings $Z[G]$ is only well understood for fields Z [Qui68]. The case $Z = \mathbb{Z}$ is not totally developed and little is known for arbitrary Z. As was done by Tan [Tan95] and was advertised in section 3.4, we will often check stronger Mazur-Tate conjectures using a modified θ. The least common multiple of the denominators appearing in $\theta \in Z[G]$ is used to multiply θ throughout and get a new $\theta \in \mathbb{Z}[G]$. But we definitively need more freedom on the structure of G. An interesting result in this direction is the following.

Theorem 3.14 Suppose $G \cong H \times K$, where K and H are two finite abelian groups of coprime exponents. Let I_G, I_H and I_K denote the augmentation ideals of $Z[G]$, $Z[H]$ and $Z[K]$ respectively. Then for any integer $r \geq 1$,

$$I_G^r / I_G^{r+1} \cong I_H^r / I_H^{r+1} \times I_K^r / I_K^{r+1}.$$

Proof. This isomorphism is induced by the natural projection of G on the components of its direct product decomposition. The details appear in [Pas78, p.249]. ■

This isomorphism does not work for $r = 0$. $I_G^0/I_G^1 = Z[G]/I_G \cong Z$ and similarly for H and K, and certainly $Z \ncong Z \times Z$. This is far from a major problem though, since it is easy to check if $\theta \in Z[G]$ or if its projections $\theta^H \in Z[H]$ and $\theta^K \in Z[K]$ are in the first power of the augmentation ideal or not. In case θ and its projections are in the augmentation ideals, then we may use theorem 3.14 recursively. In the situation where $\theta \in I^r$, then

$$\begin{aligned} \theta \in I_G^{r+1} &\iff \theta \text{ projects to 0 in } I_G^r/I_G^{r+1}, && (3.20)\\ &\iff \theta^H \text{ and } \theta^K \text{ project to 0 in } I_H^r/I_H^{r+1} \text{ and } I_K^r/I_K^{r+1}, && (3.21)\\ &\iff \theta^H \in I_H^{r+1} \text{ and } \theta^K \in I_K^{r+1}. && (3.22)\end{aligned}$$

On the other hand the coprimality of the exponents of H and K enters the proof in an essential way.

The preceding two results thus allow us to work with any finite abelian group G of squarefree order. It suffices to decompose G into cyclic components according to the fundamental structure theorem for finite abelian groups.

If G is a finite abelian group generated by $\langle \sigma_1, \sigma_2, \ldots, \sigma_g \rangle$, not necessarily of squarefree order, we have that the augmentation ideal $I \subseteq Z[G]$ is generated the following way as an ideal of $Z[G]$ (c.f. [Pas79, p.3]):

$$I = \langle \sigma_1 - 1, \sigma_2 - 1, \ldots, \sigma_g - 1 \rangle. \qquad (3.23)$$

In particular, if $G = \langle \sigma \rangle$ is cyclic, then I^k is the ideal of $Z[G]$ generated by $(\sigma - 1)^k$. We will use this to describe another approach that can be used when G, again, is cyclic of squarefree order. This is similar to the approach used by Henri Darmon in his thesis [Dar91] or in the article [Dar92].

Consider the group ring $Z[G]$ with augmentation ideal I in the case where $G = \langle \sigma \rangle$ is a finite cyclic abelian group of order n. For simplicity, let us write elements of $Z[G]$ in the form $\sum_{j=0}^{n-1} a_j \sigma^j$ with no powers of σ higher than $n-1$. For $k = 0, 1, \ldots, n-1$, we define linear operators

$$\begin{array}{llll} \delta_k: & Z[G] & \to Z \\ & \sum_{j=0}^{n-1} a_j \sigma^j & \mapsto a_k. \end{array}$$

Here δ_k is similar to a Kronecker delta function: $\delta_k(\sigma^j) = 1$ if $j = k$, and 0 otherwise. Note that δ_k actually depends on a choice of generator for G. Next, we build on this to define another linear operator $D_k: Z[G] \to Z$ by

$$D_k = \sum_{j=0}^{n-1} \begin{pmatrix} j \\ k \end{pmatrix} \delta_j,$$

where it is understood that $\binom{j}{k} = 0$ whenever $k > j$. We claim that D_k acts as a k^{th}-order differentiation operator in the sense that it gives the coefficients of a "Taylor-like" expansion of $\theta \in Z[G]$ around the augmentation ideal.

Proposition 3.15 Let G and D_k be as above, and let θ be an element of $Z[G]$. Then

$$\theta = \sum_{k=0}^{n-1} (D_k\theta)(\sigma - 1)^k.$$

Proof. Let $\theta = \sum_{j=0}^{n-1} a_j \sigma^j$. Then

$$\begin{aligned} \sum_{k=0}^{n-1} (D_k\theta)(\sigma - 1)^k &= \sum_{k=0}^{n-1} \left(\sum_{i=0}^{n-1} \begin{pmatrix} i \\ k \end{pmatrix} \delta_i \right) \left(\sum_{j=0}^{n-1} a_j \sigma^j \right) (\sigma - 1)^k \\ &= \sum_{k=0}^{n-1} \left(\sum_{j=0}^{n-1} \begin{pmatrix} j \\ k \end{pmatrix} a_j \right) (\sigma - 1)^k \\ &= \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} \begin{pmatrix} j \\ k \end{pmatrix} a_j (\sigma - 1)^k \\ &= \sum_{j=0}^{n-1} a_j \sum_{k=0}^{j} \begin{pmatrix} j \\ k \end{pmatrix} (\sigma - 1)^k 1^{j-k} \\ &= \sum_{j=0}^{n-1} a_j [(\sigma - 1) + 1]^j \\ &= \theta \end{aligned}$$

■

We then have the following criterion to check if $\theta \in I^r$ for $0 \leq r \leq n$.

Proposition 3.16 Suppose $G = \langle \sigma \rangle$ is cyclic of prime order p, and let $\theta \in \mathbb{Z}[G]$. For $k = 0, \ldots, p-1$, let $A_k = D_k(\theta) \in \mathbb{Z}$. Then

$$\theta \in I \iff A_0 = 0.$$

Supposing $\theta \in I$, then for $2 \leq r \leq p$,

$$\theta \in I^r \iff A_k \equiv 0 \pmod{p} \quad \forall\, 1 \leq k < r.$$

Proof. If $\theta = \sum_{j=0}^{p-1} a_j \sigma^j$, then $A_k = \sum_{j=0}^{p-1} \left(\begin{array}{c} j \\ k \end{array} \right) a_j$.

In particular, $A_0 = \sum_{j=0} p-1 \left(\begin{array}{c} j \\ 0 \end{array} \right) a_j = \sum_{j=0}^{p-1} a_j$.

The first statement follows from the very definition of the augmentation ideal I.

Then certainly, if $D_k(\theta) = 0$ for all $k = 0, 1, \ldots, r-1$, we have that $\theta \in I^r$.

The reason for the congruences follow from the following lemma. ■

Lemma 3.17 Let G be a group of prime exponent p, and let I be the augmentation ideal of $\mathbb{Z}[G]$. Then $pI \subset I^p$.

Proof. [Pas68, p.139] ■

Using theorem 3.14 recursively as shown in equation (3.22), we extend proposition 3.16 to

Proposition 3.18 Let G be a cyclic group of squarefree order $n = p_1 p_2 \ldots p_s$ with $p_1 < p_2 < \ldots < p_s$. Suppose $\theta \in \mathbb{Z}[G]$ is in I. Then for $2 \leq r \leq p_1$,

$$\theta \in I^r \iff A_k \equiv 0 \pmod{n} \quad \forall\, 1 \leq k < r.$$

■

Remark 3.7 One could actually check that lemma 3.17 holds for more general Z. This shows why conjectures made with $Z = \mathbb{Z}$ are stronger than if Z contains inverted primes. For example, if p were invertible in Z, then $pI = I$ so that $I = I^p$. Hence $I = I^k$ for all $k \geq 1$. For us, this phenomenon is rather uninteresting. One could show that for more arbitrary G, this actually occurs whenever the exponent of G is invertible in Z. $\square$

We have actually implemented algorithms for both, theorems 3.13 and 3.16, in the routine *Differentiation*. Certainly, theorem 3.13 has the advantage of working with powers I^k with k greater than the order of the group. On the other hand, theorem 3.16 has the advantage of having an extension to groups of squarefree order (theorem 3.18). However, we always decomposed G into its p-cyclic components at the start. Hence the advantage of having both methods implemented is rather a consistency check. Whenever possible, both methods have been applied, and in each case, the results were indeed consistent.

In some cases, we really wanted to perform tests with a group G that is not of squarefree order. In such a case, we could still use a "brute force" search approach. It is highly inelegant, but it does have some advantages. It uses linear algebra, and this can be solved by numerous available packages. We used *Maple*. The method is not restricted to $Z = \mathbb{Z}$, it works with any finite cyclic G, and with some patience, it can be used for any power r of the augmentation ideal as well. With some extra work, one could also use such a method with non-cyclic G, but we did not push this. We describe the approach.

Following equation (3.23), we saw that for $G = \langle \sigma \rangle$ cyclic, I^k is the $Z[G]$-ideal generated by $(\sigma - 1)^k$. Therefore

$$\theta \in I^k \iff \exists z \in Z[G] \text{ such that } \theta = z(\sigma - 1)^k. \tag{3.24}$$

Write $\theta = \theta_0 e + \theta_1 \sigma + \theta_2 \sigma^2 + \ldots + \theta_{n-1}\sigma^{n-1}$ and $z = z_0 e + z_1 \sigma + z_2 \sigma^2 + \ldots + z_{n-1}\sigma^{n-1}$. The $\theta_0, \ldots, \theta_{n-1}$ are computed by the program. Expanding $(\sigma - 1)^k$, we may try to solve equation (3.24) for $z_0, \ldots, z_{n-1}$. This yields n *linear* equations in n unknowns. n will never be big enough to prevent us from using linear algebra to analyze this system of equations! Typically, the matrix of coefficients of the system has rank less than n, thus getting a solution for z is not a triviality. One also has to be careful at checking that the coefficients obtained for z do live in the desired Z, with no more inverted primes.

With all these results at hand, we are now ready to perform the tests.

3.6 Experimental Tests

> *Quand je lançais un calcul, il n'y avait de certitude qu'il concorderait avec les conjectures. Or à chaque fois, celles-ci furent confirmées. J'avais l'impression de faire de la magie.*

When working with elliptic curves defined over $\mathbb{Q}$, one has access to significant tables of data gathered for many curves. The "Antwerp tables" [BK75] used to form a good source of information, until John Cremona made extensive numerical computations on such elliptic curves. A recent account of these is found in the second edition of his book, [Cre97], or on his web site [Cre]. The situation is very different when it comes to working with non-rational elliptic curves. John Cremona has made lots of computations in his thesis [Cre81] to provide experimental evidence for a Shimura-Taniyama correspondence between elliptic curves defined over Euclidean quadratic imaginary fields $\mathbb{K}$ and cusp forms for $\mathrm{GL}_2(\mathbb{A}_{\mathbb{K}})$. His thesis and the subsequent article [Cre84] contain many examples of modular elliptic curves defined over $\mathbb{K}$.

However for our tests, a key information is required that is not available in the above sources. We need some knowledge of the rank of the elliptic curves with which we work. The best source of information we have then is provided in an article by Cremona and Whitley [CW94] in which they experimentally test the (complex) Birch and Swinnerton-Dyer conjecture for some elliptic curves defined over $\mathbb{K}$. The curves we are using for our experimental tests come from there; we have listed them in Table 1.

It should be noted that our *PARI* code can be used with any elliptic curve defined over a quadratic imaginary field $\mathbb{K}$ that is a principal ideal domain. One could give random coefficients defining such a curve and the program will go through. One only needs to check that the curve is non-singular (genus 1), and furnish the conductor. In the case of semistable curves, the conductor is easy to compute. Unfortunately, *PARI* does not have at the present moment Tate's algorithm [Tat75] for computing the conductor when the elliptic curve is not defined over the rationals. At worst, one could work with the discriminant instead of the conductor and still be able to retrieve good results, being careful in a few places. The important information missing would really be the rank of the curve. It might still be interesting though to perform further tests with curves of unknown rank and see what happens when using theta elements defined with the use of many primes of split multiplicative reduction. We did not pursue this avenue though. The reasons are that the use of multiple primes in the conductor of the ray class field extension tends to increase the requirements on the computing power, and usually leads to non-cyclic Galois groups.

3.6.1 Introduction to the Tables

We present the curves with which we work in Table 1. In there, we give the field of definition $\mathbb{K}$ of the elliptic curve E, which is defined by providing the coefficients of an equation in Weierstraß form:

$$E_{/\mathbb{K}}: \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We use w to denote an abstract root of the characteristic polynomial of $\mathbb{K}/\mathbb{Q}$ in here, but x is used in the *PARI* code provided in the appendix. $\mathcal{N}_E$ is the conductor of E that we give with its factorization into prime ideals of $\mathcal{O}_{\mathbb{K}}$. Isogenous curves are given numbers with the same integral part. These curves are associated to the same rational plusform, but some other data associated to them differ. For example, the degree of the isogenies correspond to the ratio between the periods $\Omega(E)$ given in Table 2. We have adjusted these discrepancies in the calculations, so any curve in the isogeny class gives the same results.

In Table 2, we give properties of the curves that are relevant for the computations. We exhibit the complex period of the elliptic curve $\Omega(E)$, the order of the torsion group $|T|$, the multiplicity of the local fibers $c_{\mathcal{P}}$ for the primes of bad reduction, the order of the Tate-Shafarevich group $|Ш|$ and the known rank of the curve. Do not confuse $c_{\mathcal{P}}$ with the Fourier-Bessel coefficients $c(\mathcal{P})$. We also enunciate primes $\mathcal{L}$ of split multiplicative reduction for E with their norms.

For a prime of multiplicative reduction $\mathcal{P}$, we check whether the reduction is split or not simply by looking at the corresponding trace of Frobenius. The value of $c(\mathcal{P})$ is computed by the program directly by counting points on the reduced curve modulo $\mathcal{P}$. The reduction at $\mathcal{P}$ is split if $a_{\mathcal{P}} = 1$, otherwise $a_{\mathcal{P}} = -1$ and the reduction is non split. The value of $|Ш|$ given is the value that would be required for it to satisfy the Birch and Swinnerton-Dyer conjecture. The conjectural value given is always a square, in agreement with Cassels' result (theorem 2.1). Cremona and Whitley can calculate this value in the cases where the elliptic curve has rank 0. We thus give the value of $|Ш|$ only in these cases. The blanks in the table correspond to non available data. Finally, by *known* rank r, we mean that r independent $\mathbb{K}$-rational points have been found on the curve. The true rank might possibly be higher, although this is not expected for any of the curves presented here. Note that the number of independent points found agrees with the sign of a functional equation discussed in [CW94]. Thus the claimed rank r, if underestimated, would conjecturally differ from the true rank by an even number, which makes it even more improbable. There is one exception to this. Curve 10 has rank exactly equal to 2. This curve is defined over $\mathbb{Q}(\sqrt{-19})$ but descends to $\mathbb{Q}$. 2-descents have been performed to compute the rank of the curve over $\mathbb{Q}$ and that of its (-19)-twist, which are both 1. It is also worth pointing out that the calculations of theta elements and their order of vanishing that we are about to present will end up supporting the values listed for the ranks.

In the following table, we list the defining elements of the calculations we have performed using our program. We number these calculations for easy reference. We thus mention the curve used, the layer $\mathcal{M}$ for the theta element to be computed together with its norm, the number s of primes of split multiplicative reduction for E dividing $\mathcal{M}$ and the structure of the Galois group $G = G_{\mathcal{M}}$. Since it is difficult to work with group rings $Z[G]$ when G is not cyclic, we have only reported those cases for which G is indeed cyclic. The group is then determined by its order and a generator σ. It is important to fix a generator in order to know how the theta elements will be reported in Table 4. For all curves except 3, 8 and isogeny class 4, $\mathcal{M} = \mathcal{N}_E$ leads to non-cyclic Galois groups. This unfortunately prevents the use of both primes of split multiplicative reduction together for curves 9 and the isogeny class 5.

In Table 4, we report the theta elements computed by our program. If $\theta = \sum_{i=0}^{|G|-1} a_i\sigma^i$, then we write θ as $[a_0, a_1, a_2, \ldots, a_{|G|-1}]$, starting with the coefficient a_0 of the identity element $e \in G$. The same convention applies to the projection of θ to its p-cyclic components $\tilde{\theta}$.

We first give θ as it is originally calculated, possibly with denominators. We give the number of digits of precision to which each modular symbol appearing in θ has been calculated. The modular symbols appearing in θ in general require many computations of integral modular symbols. The accuracy reported here corresponds to the minimum number of zeroes appearing after the decimal in the calculation of these integral modular symbols. When an accuracy of "∞" significant digits is reported, it means that the value reported for the modular symbol, always zero in that case, is forced to be zero from the theory. This happens when the modular symbol given is of the form $\{\alpha, \beta\}$ with the two cusps α and β being translations of one another by an element of $\mathcal{O}_{\mathbb{K}}$. Finally, in order to perform the vanishing tests, we need to kill the denominators in θ. So we actually report the consequent projections of θ into its p-cyclic components without denominators.

Table 5, the crowning of the thesis, presents the order of vanishing of the theta elements computed, and clearly indicates the maximal power of the augmentation ideal to which θ belongs. We recall the known rank r of the curve and the number s of primes of split multiplicative reduction used. We write $\tilde{\theta}$ to represent a projected p-cyclic component of θ. For each p-cyclic component of prime order, we give the derivatives $[A_0, A_1, A_2, \ldots]$ pertaining to proposition 3.16, and when $A_0 = 0$, we compute the norm $\mathrm{N}(\chi(\tilde{\theta}))$ appearing in theorem 3.13. Note that whenever both the derivatives and the norm are computed, they always give the same order of vanishing for $\tilde{\theta}$. According to theorem 3.14, the order of vanishing of θ itself is then the minimum of those of its components.

3.6.2 Tables of Calculations

Table 1: Curve Definitions

Curve	$\mathbb{K}$	$E:\ a_1,\ a_2,\ a_3,\ a_4,\ a_6$	$\mathcal{N}_E$	$\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\mathcal{N}_E)$
1.1	$\mathbb{Q}(\sqrt{-2})$	$0,\ w-1,\ 1,\ 1-w,\ w$	$(13+8w)=(1-w)^3(3+w)$	$297=3^3\times 11$
1.2	$\mathbb{Q}(\sqrt{-2})$	$0,\ w-1,\ 1,\ 11-11w,\ 3w-27$	$(13+8w)=(1-w)^3(3+w)$	$297=3^3\times 11$
1.3	$\mathbb{Q}(\sqrt{-2})$	$0,\ w-1,\ 1,\ 39w-9,\ -39w-210$	$(13+8w)=(1-w)^3(3+w)$	$297=3^3\times 11$
2	$\mathbb{Q}(\sqrt{-2})$	$0,\ 1-w,\ 1,\ 2-2w,\ 1$	$(13+8w)=(1-w)^3(3+w)$	$297=3^3\times 11$
3	$\mathbb{Q}(\sqrt{-1})$	$0,\ 1-w,\ w,\ -w,\ 0$	$(13+8w)=(13+8w)$	$233=233$
4.1	$\mathbb{Q}(\sqrt{-19})$	$w,\ 1-w,\ 1,\ -1,\ 0$	$(2w)=(2)(w)$	$20=4\times 5$
4.2	$\mathbb{Q}(\sqrt{-19})$	$w,\ 1-w,\ 1,\ 9-5w,\ -24-2w$	$(2w)=(2)(w)$	$20=4\times 5$
4.3	$\mathbb{Q}(\sqrt{-19})$	$w,\ 1-w,\ 1,\ -31-15w,\ -60-54w$	$(2w)=(2)(w)$	$20=4\times 5$
5.1	$\mathbb{Q}(\sqrt{-3})$	$0,\ -w,\ 1,\ w-1,\ 0$	$(19)=(3+2w)(2+3w)$	$361=19\times 19$
5.2	$\mathbb{Q}(\sqrt{-3})$	$0,\ -w,\ 1,\ 9-9w,\ -15$	$(19)=(3+2w)(2+3w)$	$361=19\times 19$
5.3	$\mathbb{Q}(\sqrt{-3})$	$0,\ -w,\ 1,\ 769-769w,\ -8470$	$(19)=(3+2w)(2+3w)$	$361=19\times 19$
5.4	$\mathbb{Q}(\sqrt{-3})$	$0,\ -w,\ 1,\ -31-99w,\ 74-498w$	$(19)=(3+2w)(2+3w)$	$361=19\times 19$
5.5	$\mathbb{Q}(\sqrt{-3})$	$0,\ -w,\ 1,\ 99+31w,\ 498w-424$	$(19)=(3+2w)(2+3w)$	$361=19\times 19$
6.1	$\mathbb{Q}(\sqrt{-1})$	$0,\ 1,\ 0,\ 1,\ 0$	$(6+6w)=(1+w)^3(3)$	$72=2^3\times 9$
6.2	$\mathbb{Q}(\sqrt{-1})$	$1+w,\ -w,\ 1+w,\ 1-w,\ -w$	$(6+6w)=(1+w)^3(3)$	$72=2^3\times 9$
6.3	$\mathbb{Q}(\sqrt{-1})$	$1+w,\ -w,\ 1+w,\ 6-w,\ 4w$	$(6+6w)=(1+w)^3(3)$	$72=2^3\times 9$
6.4	$\mathbb{Q}(\sqrt{-1})$	$1+w,\ -w,\ 1+w,\ 16-w,\ -28w$	$(6+6w)=(1+w)^3(3)$	$72=2^3\times 9$
6.5	$\mathbb{Q}(\sqrt{-1})$	$1+w,\ -w,\ 1+w,\ -4-w,\ 22w$	$(6+6w)=(1+w)^3(3)$	$72=2^3\times 9$
6.6	$\mathbb{Q}(\sqrt{-1})$	$1+w,\ -w,\ 1+w,\ 96-w,\ 346w$	$(6+6w)=(1+w)^3(3)$	$72=2^3\times 9$
7.1	$\mathbb{Q}(\sqrt{-19})$	$0,\ 1,\ 1,\ 20,\ -32$	$(3-6w)=(3)(2w-1)$	$171=9\times 19$
7.2	$\mathbb{Q}(\sqrt{-19})$	$0,\ 1,\ 1,\ -4390,\ -113432$	$(3-6w)=(3)(2w-1)$	$171=9\times 19$
8	$\mathbb{Q}(\sqrt{-43})$	$0,\ -w,\ 1+w,\ -2,\ 1-w$	$(13+w)=(13+w)$	$193=193$
9	$\mathbb{Q}(\sqrt{-67})$	$w,\ 1+w,\ w,\ -1-3w,\ 16-5w$	$(3w)=(3)(w)$	$153=9\times 17$
10	$\mathbb{Q}(\sqrt{-19})$	$0,\ -1,\ 1,\ -2,\ 2$	$(3-6w)=(3)(2w-1)$	$171=9\times 19$

Table 2: Curve Properties

Curve	$\Omega(E)$	$\lvert T\rvert$	$c_{\mathcal{P}}$	$\lvert Ш\rvert$	rank	$\mathcal{L}$; $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\mathcal{L})$
1.1	7.48086553	3	1,1	1	0	—
1.2	2.49362184	3	3,1	1	0	—
1.3	0.831207281	1	1,1	1	0	—
2	3.99896686	1	1,1	1	0	—
3	8.80694160	1	1		1	—
4.1	9.37616501	3	1,2	1	0	$(2);\ 4$
4.2	3.12538833	3	3,2	1	0	$(2);\ 4$
4.3	1.04179611	1	1,2	1	0	$(2);\ 4$
5.1	8.41778107	3	1,1		1	$(3+2w),(2+3w);\ 19,19$
5.2	2.80592702	9	3,3		1	$(3+2w),(2+3w);\ 19,19$
5.3	0.935309008	3	1,1		1	$(3+2w),(2+3w);\ 19,19$
5.4	0.935309008	3	1,9		1	$(3+2w),(2+3w);\ 19,19$
5.5	0.935309008	3	9,1		1	$(3+2w),(2+3w);\ 19,19$
6.1	7.27069403	8	4,1	1	0	$(3);\ 9$
6.2	7.27069403	8	2,2	1	0	$(3);\ 9$
6.3	3.63534701	8	2,4	1	0	$(3);\ 9$
6.4	3.63534701	4	2,1	1	0	$(3);\ 9$
6.5	1.81767350	8	2,8	1	0	$(3);\ 9$
6.6	1.81767350	4	2,2	1	0	$(3);\ 9$
7.1	1.35882915	5	10,2	4	0	$(3);\ 9$
7.2	0.271765830	1	2,2	4	0	$(3);\ 9$
8	7.21827612	1	1		1	—
9	2.17153248	1	5,4		1	$(3),(w);\ 9,17$
10	5.32864411				2	$(3);\ 9$

Table 3: Computations Performed

Trial	E	$\mathcal{M}$	$\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\mathcal{M})$	$\|G\|, \langle\sigma\rangle$	s
11	1.3	$(w) = (w)$	2=2	$1, \langle 1\rangle$	0
12	1.1	$(2) = (w)^2$	$4 = 2^2$	$2, \langle 1+w\rangle$	0
13	1.1	$(1-w) = (1-w)$	3=3	$1, \langle 1\rangle$	0
14	1.1	$(-1-2w) = (1-w)^2$	$9 = 3^2$	$3, \langle 2\rangle$	0
15	1.2	$(3+w) = (3+w)$	11=11	$5, \langle 2\rangle$	0
16	1.3	$(2-2w) = (w)^2(1-w)$	$12 = 2^2 \times 3$	$2, \langle 1+w\rangle$	0
21	2	$(3-w) = (3-w)$	$11 = 11$	$5, \langle 2\rangle$	0
31	3	$(2+3w) = (2+3w)$	13=13	$3, \langle 2\rangle$	0
32	3	$\mathcal{N}_E = (13+8w)$	233=233	$58, \langle 3\rangle$	0
41	4.1	$(1-w) = (1-w)$	5=5	$2, \langle 2\rangle$	0
42	4.2	$(2) = (2)$	4=4	$3, \langle w\rangle$	1
43	4.3	$(w) = (w)$	5=5	$2, \langle 2\rangle$	0
44	4.1	$\mathcal{N}_E = (2)(w)$	$20 = 4 \times 5$	$6, \langle w+3\rangle$	1
51	5.1	$(3+2w) = (3+2w)$	19=19	$3, \langle 2\rangle$	1
52	5.2	$(2+3w) = (2+3w)$	19=19	$3, \langle 2\rangle$	1
53	5.3	$(1+5w) = (1+5w)$	31=31	$5, \langle 3\rangle$	0
54	5.1	$(7-4w) = (7-4w)$	37=37	$6, \langle 2\rangle$	0
61	6.5	$(2+w) = (2+w)$	5=5	$1, \langle 1\rangle$	0
62	6.5	$(1+w) = (1+w)$	2=2	$1, \langle 1\rangle$	0
63	6.4	$(3) = (3)$	9=9	$2, \langle w+1\rangle$	1
64	6.6	$(2) = (1+w)^2$	$4 = 2^2$	$1, \langle 1\rangle$	0
71	7.1	$(2) = (2)$	4=4	$3, \langle w\rangle$	0
72	7.2	$(3) = (3)$	9=9	$4, \langle w\rangle$	1
81	8	$\mathcal{N}_E = (13+w)$	193=193	$96, \langle 5\rangle$	0
91	9	$(3) = (3)$	9=9	$4, \langle w\rangle$	1
92	9	$(w) = (w)$	17=17	$8, \langle 3\rangle$	1
101	10	$(3-w) = (3-w)$	11=11	$5, \langle 2\rangle$	0
102	10	$(3) = (3)$	9=9	$4, \langle w\rangle$	1

Table 4: Theta Elements

Trial	θ	Digits	Projections
11	$[-\frac{4}{3}]$	$[5]$	$[-4]$
12	$[\frac{8}{3}, -\frac{10}{3}]$	$[3, 5]$	$[8, -10]$
13	$[-\frac{1}{3}]$	$[9]$	$[-1]$
14	$[0, -2, 2]$	$[4, 4, 3]$	$[0, -2, 2]$
15	$[-\frac{4}{3}, \frac{5}{3}, -\frac{4}{3}, \frac{5}{3}, -\frac{4}{3}]$	$[3, 3, 3, 3, 3]$	$[-4, 5, -4, 5, -4]$
16	$[\frac{5}{3}, -\frac{4}{3}]$	$[3, 3]$	$[5, -4]$
21	$[0, -2, -2, 0, -3]$	$[3, 3, 3, 3, 3]$	$[0, -2, -2, 0, -3]$
31	$[0, -1, 1]$	$[4, 4, 4]$	$[0, -1, 1]$
32	T^*	S^*	$[0, 0]$, P^*
41	$[-\frac{2}{3}, -\frac{2}{3}]$	$[4, 5]$	$[-2, -2]$
42	$[2, 0, -2]$	$[7, 9, 7]$	$[2, 0, -2]$
43	$[-\frac{2}{3}, -\frac{2}{3}]$	$[3, 3]$	$[-2, -2]$
44	$[0, -1, -2, 0, 2, 1]$	$[8, 9, 9, \infty, 9, 9]$	$[0, 0]$, $[0, 1, -1]$
51	$[\frac{2}{3}, -\frac{1}{3}, -\frac{1}{3}]$	$[4, 4, 4]$	$[2, -1, -1]$
52	$[\frac{2}{3}, -\frac{1}{3}, -\frac{1}{3}]$	$[5, 4, 4]$	$[2, -1, -1]$
53	$[1, -1, 0, 0, 0]$	$[2, 2, 3, 2, 3]$	$[1, -1, 0, 0, 0]$
54	$[0, 0, 0, -1, 1, 0]$	$[2, 2, 2, 2, 3, 3]$	$[1, -1]$, $[-1, 1, 0]$
61	$[-\frac{1}{2}]$	$[4]$	$[-1]$
62	$[-\frac{1}{2}]$	$[9]$	$[-1]$
63	$[\frac{1}{2}, -\frac{1}{2}]$	$[5, 5]$	$[1, -1]$
64	$[0]$	$[9]$	$[0]$
71	$[\frac{12}{5}, -\frac{38}{5}, -\frac{38}{5}]$	$[4, 6, 3]$	$[12, -38, -38]$
72	$[2, 0, -2, 0]$	$[4, 4, 3, 4]$	$[2, 0, -2, 0]$
81	T_2^*	S_2^*	$[0, 4, -4]$, P_2^*
91	$[2, -2, -2, 2]$	$[2, 2, 2, 1]$	$[2, -2, -2, 2]$
92	$[2, 9, -8, -3, -3, -8, 9, 2]$	$[1, 1, 1, 1, 2, 2, 1, 1]$	$[2, 9, -8, -3, -3, -8, 9, 2]$
101	$[0, 1, 1, 0, -2]$	$[2, 1, 1, 1, 2]$	$[0, 1, 1, 0, -2]$
102	$[2, 0, -2, 0]$	$[4, 4, 4, 4]$	$[2, 0, -2, 0]$

* Given after Table 5.

Table 5: Vanishing

Trial	r, s	$\mathrm{N}(\chi(\tilde{\theta}))$	Derivatives	$\mathrm{ord}(\tilde{\theta})$	$\theta \in I^{r+s}$?	$\theta \in I^{r+s+1}$?
11	$0,0$	—	$[-4]$	0	Yes	No
12	$0,0$	—	$[-2,-10]$	0	Yes	No
13	$0,0$	—	$[-1]$	0	Yes	No
14	$0,0$	12	$[0,2,2]$	1	Yes	Yes
15	$0,0$	—	$[-2,-4,-13,-11,-4]$	0	Yes	No
16	$0,0$	—	$[1,-4]$	0	Yes	No
21	$0,0$	—	$[-7,-18,-20,-12,-3]$	0	Yes	No
31	$1,0$	3	$[0,1,1]$	1	Yes	No
32	$1,0$	0, 351403469	$[0,0]$, D^*	$\infty, 1$	Yes	No
41	$0,0$	—	$[-4,-2]$	0	Yes	No
42	$0,1$	12	$[0,-4,-2]$	1	Yes	No
43	$0,0$	—	$[-4,-2]$	0	Yes	No
44	$0,1$	0, 3	$[0,0]$, $[0,-1,-1]$	$\infty, 1$	Yes	No
51	$1,1$	9	$[0,-3,-1]$	2	Yes	No
52	$1,1$	9	$[0,-3,-1]$	2	Yes	No
53	$1,0$	5	$[0,-1,0,0,0]$	1	Yes	No
54	$1,0$	2,3	$[0,-1]$, $[0,1,0]$	1, 1	Yes	No
61	$0,0$	—	$[-1]$	0	Yes	No
62	$0,0$	—	$[-1]$	0	Yes	No
63	$0,1$	2	$[0,-1]$	1	Yes	No
64	$0,0$	—	$[0]$	∞	Yes	Yes
71	$0,0$	—	$[-64,-114,-38]$	0	Yes	No
72	$0,1$	—	—	3	Yes	Yes
81	$1,0$	48, —	$[0,-4,-4]$, —	$1, \geq 1$	Yes	No
91	$1,1$	—	—	2	Yes	No
92	$1,1$	—	—	2	Yes	No
101	$2,0$	25	$[0,-5,-11,-8,-2]$	2	Yes	No
102	$2,1$	—	—	3	Yes	No

* Given next page.

Tables 4 and 5 include the following data:

T = [0, 1, -1, 0, 0, -1, 1, 0, 0, 0, 0, 0, 0, -1, 0, 0, 1, 0, 0, 0, 1, 0, 0, -1, 0, 0, 0, -1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, -1, 0, 0, 0, -1, 0, 0, 1, 0, 0, 0, 0, 0, 0, -1, 1, 0, 0, 1, -1],

S = [20, 8, 9, 10, 11, 8, 9, 6, 11, 10, 10, 10, 10, 8, 10, 11, 8, 9, 10, 10, 8, 11, 10, 8, 10, 10, 10, 8, 11, 19, 11, 8, 10, 10, 10, 8, 10, 11, 8, 10, 10, 9, 8, 11, 10, 8, 10, 10, 10, 10, 11, 6, 9, 8, 11, 10, 9, 8],

P = [0, 1, 0, 0, 0, -1, 2, 0, 0, -1, 0, 0, 0, -2, 0, 0, 2, 0, 0, 0, 1, 0, 0, -2, 1, 0, 0, 0, -1],

T_2 = [0, 1, 0, 0, -4, 1, 2, 2, 2, -2, 2, -1, -1, -1, -1, 0, -1, 0, 0, 0, 1, 0, 1, 1, -3, 3, 0, -3, -2, -1, -1, 2, 0, 2, 2, 3, 0, 0, 0, 0, 0, -2, 1, 0, 1, 1, 1, -2, 0, 2, -1, -1, -1, 0, -1, 2, 0, 0, 0, 0, 0, -3, -2, -2, 0, -2, 1, 1, 2, 3, 0, -3, 3, -1, -1, 0, -1, 0, 0, 0, 1, 0, 1, 1, 1, 1, -2, 2, -2, -2, -2, -1, 4, 0, 0, -1],

S_2 = [∞, 8, 10, 4, 8, 8, 8, 7, 9, 4, 7, 9, 8, 4, 8, 8, 4, 10, 8, 10, 7, 10, 8, 8, 8, 8, 9, 8, 8, 9, 8, 8, 10, 7, 8, 7, 4, 8, 10, 11, 8, 5, 8, 11, 9, 8, 9, 8, ∞, 8, 9, 8, 9, 11, 8, 5, 8, 11, 10, 8, 4, 7, 8, 7, 10, 8, 8, 9, 8, 8, 9, 8, 8, 8, 8, 10, 7, 10, 8, 10, 4, 8, 8, 4, 8, 9, 7, 4, 9, 7, 8, 8, 8, 4, 10, 8],

P_2 = [0, 1, 3, 4, -2, 4, 2, -1, 5, -5, 2, -1, -1, 0, 0, -2, 0, 2, 0, 0, 1, 1, -2, 5, -5, 1, -2, -4, 2, -4, -3, -1] and

D = [0, -25, -350, -3160, -20605, -101523, -392776, -1231318, -3204135, -7044367, -13249786, -21505652, -30292171, -37155510, -39750724, -37099748, -30171751, -21328830, -13055622, -6882086, -3101020, -1182522, -376510, -98258, -20474, -3276, -378, -28, -1].

3.6.3 Discussion of the Results

We note from Table 4 that in some cases, the number of digits of precision reached is rather low. We have been limited by CPU time requirements. We nevertheless have reasons to believe that the calculated theta elements are good. The theta elements have been calculated gradually with higher and higher precision by increasing the maximal norm M. Had we not converged on the right integer, we would have seen the integral modular symbols jumping integer values as M increased. This was not happening, the integer values were seen stable. Moreover, in many cases, the fact that the calculated θ is in the augmentation ideal is already a check on the calculation, and in all cases, it so happened that θ was miraculously verifying the conjectures !

We have made calculations of different kinds. We have the least interesting cases where $r = s = 0$, and in most cases, we got $\theta \notin I$. In two cases, trials 14 and 64, we nevertheless got $\theta \in I$. This does not contradict our conjectures; we will discuss these cases below. We have a few cases with $r = 1, s = 0$. In each case we got $\theta \in I \setminus I^2$. Positive results had to be expected here if we trust the Birch and Swinnerton-Dyer conjecture. As explained in section 3.4, the Mazur-Tate conjectures in such a case follow from the Birch and Swinnerton-Dyer conjecture and modularity. Also the case $r = 0, s = 1$ has been tested and we always obtained that θ is in I. But again this is not a conjecture, apart from the modularity assumption which is the only thing that has indirectly been tested here. In one of these cases, trial 72, we actually obtained that θ belongs to I^3. We will also come back to this case below.

Cases with $r + s \geq 2$ are more interesting, for these are genuine Mazur-Tate conjectures. We have a number of these cases, namely trials 51, 52, 91, 92, 101 and 102. Trials 51, 52, 91 and 92 are all of the form $r = s = 1$, and they all give that $\theta \in I^2 \setminus I^3$ as desired. Also, trial 101 has $r = 2, s = 0$ and we also get in this case that θ belongs exactly to I^2. The culminating case is trial 102 with the same curve, hence $r = 2$, and with 1 prime of split multiplicative reduction in the layer of θ, so that $r + s = 3$. A calculation using linear algebra described below satisfactorily yields that $\theta \in I^3 \setminus I^4$!

In trials 72, 91, 92 and 102, the calculation of the order of vanishing of θ was different from the other trials since G could not be decomposed into factors of prime order. We had to rely on linear algebra as described at the end of section 3.5.6. For the most interesting of these cases, trial 102, we need to find $z = z_0\sigma^0 + z_1\sigma^1 + z_2\sigma^2 + z_3\sigma^3$ such that $\theta = 2\sigma^0 - 2\sigma^2 = z(\sigma - 1)^3$. A straight forward calculation assisted by the linear algebra package of *Maple* gave that this system is indeed solvable, and $z = -\sigma - \sigma^2 \in \mathbb{Z}[G]$, so that $\theta \in I^3$, and $z \notin I$ implies $\theta \notin I^4$. Similarly, for trial 91, we have $\theta = z(\sigma - 1)^2$ with $z = 2\sigma^0 + 2\sigma^1 \in \mathbb{Z}[G] \setminus I$, so that $\theta \in I^2 \setminus I^3$, and in trial 92, $\theta = z(\sigma - 1)^2$ with $z = 2e + 13\sigma + 16\sigma^2 + 16\sigma^3 + 13\sigma^4 + 2\sigma^5$ and we conclude that $\theta \in I^2 \setminus I^3$ as well. Trial 72 is identical to trial 102.

We have 3 examples where the theta element belongs to a power of the augmentation ideal higher than just the required $r + s$. These are trials 14, 64 and 72. Trial 64 is somewhat uninteresting, since G is trivial, and θ has only one component. If $\theta \neq [0]$ then $\theta \notin I$, or else $\theta = [0]$ and it automatically vanishes to infinite order, for a trivial θ necessarily belongs to any power of the augmentation ideal of any group ring. Another point of view is just that when G is trivial, then all non-zero powers of the augmentation ideal are the same, namely zero:

$$Z \cong Z[G] = I^0 \neq (0) = I = I^2 = I^3 = I^4 = \dots$$

Trial 14 is not as trivial and is thus more interesting. It is not our goal in this thesis in general to predict values for elements θ projected to I^k/I^{k+1} when $\theta \in I^k$. However any attempt to do this should take into consideration the quantities involved in the Birch and Swinnerton-Dyer conjecture when stating the value of the first non-zero Taylor coefficient. In particular the order of the torsion group T appears in the denominator. This means that an attempt to give a value for θ in I^k/I^{k+1} must be stated in a context where $|T|$ is invertible in $Z \neq \mathbb{Z}$. The extra vanishing of θ must be coming from the fact that in trial 14, $|G| = |T| = 3$. Note that in trials 11, 12, 13, 15, 16, all made with the same isogeny class of curve as trial 14, this "superfluous vanishing" does not occur, and the order of G is always coprime to 3 in these cases.

It is also worth pointing out that the extra vanishing of trials 14 and 64 is consistent with the compatibility relations between layers given in lemma 3.8. Indeed, the layer of these trials contains a prime $\mathcal{P}$ of additive reduction appearing with multiplicity 2. Lemma 3.8 part 1 applied with $\mathcal{L} = \mathcal{P}$ has $c(\mathcal{L}) = 0$, so that the theta element must necessarily be at least in I^1.

Regarding trial 72, the belonging of θ to a higher power of the augmentation ideal is due to the torsion nature of I^k/I^{k+1}. Indeed, when G is cyclic, we have that I^k/I^{k+1} is isomorphic to G itself for all $k \geq 1$ ([Pas68, p.127]). In our case, G is cyclic of order 4. Again, if we were to predict a value for the projection of θ in I^k/I^{k+1}, as in strong forms of the Birch and Swinnerton-Dyer conjectures, this value would have to involve data like the order of the Tate-Shafarevich group and the local reduction factors. As we can see from Table 2, the values of $|\text{Ш}|$ and $c_{\mathcal{P}}$ for curves 7.1 and 7.2 involve numerous powers of 2.

Conclusion

In the last few decades, elliptic curves over $\mathbb{Q}$ have been investigated in great depth. Although there do remain many interesting open questions there, many of them are quite hard, and researchers are more and more turning to the study of elliptic curves defined over more general number fields $\mathbb{F}$. As we have seen, there is still enormous research to be done around these latter, their properties being much less understood. This is evident when we realize that an important piece of work leading to the proof of Fermat's last theorem, the modularity of elliptic curves over $\mathbb{Q}$, is completely settled by now, whereas not much is known about the modularity of arbitrary elliptic curves defined over non-trivial extensions of the rationals, particularly over fields which are not totally real.

In this thesis, we have been studying another very important aspect of elliptic curves defined over some extensions of $\mathbb{Q}$. We have investigated the spirit of the beautiful Birch and Swinnerton-Dyer conjecture, in the case where the elliptic curves are defined over quadratic imaginary fields $\mathbb{K}$ of class number 1. Results for the Birch and Swinnerton-Dyer conjecture in general have so far been very hard to obtain, even for elliptic curves defined over $\mathbb{Q}$. So we actually turned our attention to analogous conjectures, namely conjectures like those formulated by Mazur and Tate in [MT87] for elliptic curves over $\mathbb{Q}$.

Our research generalizes the conjectures of Mazur and Tate to elliptic curves defined over $\mathbb{K}$, and we have experimentally constructed theta elements $\theta_{\mathcal{M}}$ for a number of curves and tested with success the belonging of these to the relevant powers of the augmentation ideal I. This required a careful understanding of the meaning of modularity for elliptic curves defined over $\mathbb{K}$, and the mastery of the properties of modular symbols associated to these curves, in particular, their integrality properties. Interestingly, the power of I to which the theta element belongs is not only given by the rank of the curve. It is augmented by the number of primes of split multiplicative reduction for the curve that divide the "layer" $\mathcal{M}$ used for the construction of $\theta_{\mathcal{M}}$. This is very similar to the (conjectural) behavior of p-adic L-functions, as described in [MTT86].

We have tested the conjectures in a few cases, including a culminating case in which the curve has rank 2 and 1 prime of split multiplicative reduction is involved. We did get that θ is exactly in the third power of the augmentation ideal. Unfortunately, trying to use 2 primes of split multiplicative reduction in the layer $\mathcal{M}$ of $\theta_{\mathcal{M}}$ typically leads to a Galois group that is not cyclic. This makes it harder to figure out the power of the augmentation ideal to which $\theta_{\mathcal{M}}$ belongs. We have not performed such tests, but it would be interesting to do so in the future.

Finally, let us mention that this work could also be extended in a number of other ways. For an elliptic curve $E_{/\mathbb{K}}$, we have conjectured that $\theta_{\mathcal{M}}$ belongs to I^{r+s}, where r is the rank of $E_{/\mathbb{K}}$ and s is the number of primes of split multiplicative reduction for $E_{/\mathbb{K}}$ dividing the layer $\mathcal{M}$. A first avenue would be to make up stronger conjectures by predicting a value for the projection of $\theta_{\mathcal{M}}$ in the quotient I^{r+s}/I^{r+s+1}. This is analogous to giving the value of the first non-zero Taylor coefficient in the strong form of the Birch and Swinnerton-Dyer conjectures. A second avenue would be to look at how Elise Whitley dealt with the non-Euclidean quadratic imaginary fields of class number 1 in her thesis [Whi90], or how Jeremy Bygott recently managed to do modular symbols calculations with quadratic imaginary fields of class number 2 [Byg98]. It might be that Mazur-Tate type conjectures could be amenable to computational testing in these cases as well. One could also wonder how to generalize this all to arbitrary number fields...

Bibliography

[Arf85] G. Arfken, *Mathematical Methods for Physicists*, Academic Press, Inc., San Diego, 1985.

[BG72] F. Bachmann and L. Grünenfelder, *Über Lie Ringe von Gruppen und ihre Universellen Enveloppen*, Comment. Math. Helv. **47** (1972), 332–340.

[Bir71] B. J. Birch, *Elliptic Curves over $\mathbb{Q}$: A Progress Report*, Proceedings of the 1969 Summer Institute on Number Theory (Stony Brook, New York), AMS, 1971, pp. 396–400.

[BK75] B. J. Birch and W. Kuyk, *Modular Functions of One Variable IV*, Lecture Notes in Math., no. 476, Springer-Verlag, 1975.

[BSD65] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on Elliptic Curves (II)*, J. reine u. ungewandte Math. **218** (1965), 79–108.

[Byg98] J. S. Bygott, *Modular Forms and Modular Symbols over Imaginary Quadratic Fields of Class Number 2*, Ph.D. thesis, Exeter University, 1998.

[Cas62] J. W. S. Cassels, *Arithmetic on Curves of Genus 1, (IV). Proof of the Hauptvermutung.*, J. reine u. ungewandte Math. **211** (1962), 95–112.

[Cas65] J. W. S. Cassels, *Arithmetic on Curves of Genus 1, (VIII). On the Conjectures of Birch and Swinnerton-Dyer* , J. reine u. ungewandte Math. **217** (1965), 180–189.

[Cas91] J. W. S. Cassels, *Lectures on Elliptic Curves*, London Mathematical Society Student Texts, no. 24, Cambridge University Press, Cambridge, 1991, 1995 reprint.

[Cox84] D. A. Cox, *The Arithmetic-Geometric Mean of Gauss*, Enseignement Math. **30** (1984), 275–330.

[Cre] J. E. Cremona, *Website homepage*, www.maths.nott.ac.uk/personal/jec.

[Cre81] J.E. Cremona, *Modular Symbols*, Ph.D. thesis, Worchester College, Oxford University, Oxford, 1981.

[Cre84] J. E. Cremona, *Hyperbolic Tesselations, Modular Symbols, and Elliptic Curves over Complex Quadratic Fields*, Compositio Math. **51** (1984), 275–323.

[Cre97] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, 2nd ed., Cambridge University Press, Cambridge, 1997.

[CW77] J. Coates and A. Wiles, *On the Conjecture of Birch and Swinnerton-Dyer* , Invent. Math. **39** (1977), 223–251.

[CW94] J. E. Cremona and E. Whitley, *Periods of Cusp Forms and Elliptic Curves over Imaginary Quadratic Fields*, Math. Comp. **62** (1994), no. 205, 407–429.

[Dar] H. R. Darmon, *Integration on $\mathcal{H}_p \times \mathcal{H}$ and Arithmetic Applications*, Annals of Mathematics, to appear.

[Dar91] H. R. Darmon, *Refined Class Number Formulas for Derivatives of L-Series*, Ph.D. thesis, Harvard University, 1991.

[Dar92] H. R. Darmon, *A Refined Conjecture of Mazur-Tate Type for Heegner Points*, Invent. Math. **110** (1992), no. 1, 123–146.

[Dar94] H. R. Darmon, *Euler Systems and Refined Conjectures of Birch Swinnerton-Dyer Type*, p-Adic Monodromy and the Birch and Swinnerton-Dyer Conjecture, Contemporary Mathematics, vol. 165, American Mathematical Society, 1994, pp. 265–276.

[Dar99] H. R. Darmon, *A Proof of the Full Shimura-Taniyama-Weil Conjecture is Announced*, Notices Amer. Math. Soc. **46** (1999), no. 11, 1397–1401.

[EGM98] J. Elstrodt, F. Grunewald, and J. Mennicke, *Groups Acting on Hyperbolic Space, Harmonic Analysis and Number Theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin Heidelberg, 1998.

[Gel76] S. Gelbart, *Elliptic Curves and Automorphic Representations*, Advances in Math. **21** (1976), 235–292.

[Gro88] B. H. Gross, *On the Values of Abelian L-Functions at $s = 0$*, J. Fac. Sci. Univ. Tokyo **35** (1988), 177–197.

[GZ86] B. Gross and D. Zagier, *Heegner Points and Derivatives of L-Series*, Invent. Math. **84** (1986), 225–320.

[Har86] S. Haran, *p-Adic L-Functions for Modular Forms*, Compositio Math. **62** (1986), 31–46.

[HST93] M. Harris, D. Soudry, and R. L. Taylor, *l-adic Representations Associated to Modular Forms over Imaginary Quadratic Fields. I. Lifting to* $\mathrm{GSp}_4(\mathbb{Q})$, Invent. Math. **112** (1993), no. 2, 377–411.

[IR90] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, second ed., Graduate Texts in Mathematics, no. 84, Springer-Verlag, New York, 1990, corrected fifth printing: 1998.

[Kna92] A. W. Knapp, *Elliptic Curves*, Princeton University Press, Princeton, New Jersey, 1992.

[Kob93] Koblitz, N., *Introduction to Elliptic Curves and Modular Forms*, second ed., Graduate Texts in Mathematics, no. 97, Springer-Verlag, New York, 1993.

[Kol89] V. A. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Ш(E,\mathbb{Q})$ for a Class of Weil Curves*, Math. of the USSR Izvestiya **32** (1989), 523–542.

[Kur78] P. F. Kurčanov, *Cohomology of Discrete Groups and Dirichlet Series Connected with Jacquet-Langlands Cusp Forms*, Math. USSR Izvestija **12** (1978), no. 3, 543–555.

[Lan76] S. Lang, *Introduction to Modular Forms*, Grundlehren der mathematischen Wissenschaften, no. 222, Springer-Verlag, Berlin Heidelberg, 1976.

[Lan80] R. P. Langlands, *Base Change for GL(2)*, Annals of Mathematics Studies, no. 96, Princeton University Press, Princeton, N.J., 1980.

[Lan91] S. Lang (ed.), *Number Theory III*, Encyclopaedia of Mathematical Sciences, vol. 60, Springer-Verlag, Berlin Heidelberg, 1991.

[Man72] Ju. I. Manin, *Parabolic Points and Zeta-Functions of Modular Curves*, Math. USSR Izvestija **6** (1972), no. 1, 19–64.

[Maz72] B. Mazur, *Courbes Elliptiques et Symboles Modulaires*, Séminaire Bourbaki **24** (1972), no. 414, 277–294.

[Miy89] T. Miyake, *Modular Forms*, Springer-Verlag, Berlin Heidelberg, 1989.

[MSD74] B. Mazur and H. P. F. Swinnerton-Dyer, *Arithmetic of Weil Curves*, Invent. Math. **25** (1974), 1–61.

[MT83] B. Mazur and J. Tate, *Canonical Height Pairings via Biextensions*, Arithmetic and Geometry, vol. 1, Progress in Mathematics, no. 35, Birkhauser Boston, 1983.

[MT87] B. Mazur and J. Tate, *Refined Conjectures of the "Birch and Swinnerton-Dyer Type"*, Duke Math. J. **54** (1987), no. 2, 711–750.

[MT91] B. Mazur and J. Tate, *The p-Adic Sigma Function*, Duke Math. J. **62** (1991), no. 3, 663–688.

[MTT86] B. Mazur, J. Tate, and J. Teitelbaum, *On p-Adic Analogues of the Conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), 1–48.

[Pas68] I. B. S. Passi, *Polynomial Maps on Groups*, J. Algebra **9** (1968), 121–151.

[Pas78] I. B. S. Passi, *The Associated Graded Ring of a Group Ring*, Bull. London Math. Soc. **10** (1978), 241–255.

[Pas79] I. B. S. Passi, *Group Rings and Their Augmentation Ideals*, Lecture Notes in Math., no. 715, Springer-Verlag, Berlin Heidelberg, 1979.

[Qui68] D. Quillen, *On the Associated Graded Ring of a Group Ring*, J. Algebra **10** (1968), 411–418.

[Ram94] D. Ramakrishnan, *A Refinement of the Strong Multiplicity One Theorem for* GL(2), Invent. Math. **116** (1994), no. 1-3, 645–649, Appendix to: l-adic Representations Associated to Modular Forms over Imaginary Quadratic Fields. II. [Invent. Math. {116}(1994), no. 1-3, 619-643] by R. Taylor.

[Rub87] K. Rubin, *Tate-Shafarevich groups and L-functions of Elliptic Curves with Complex Multiplication*, Invent. Math. **89** (1987), 527–560.

[Ser68] J.-P. Serre, *Abelian l-adic Representations and Elliptic Curves*, W. A. Benjamin Inc., New York, 1968.

[Shi71] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, Princeton, New Jersey, 1971, First Princeton Paperback printing, 1994.

[Sil86] Silverman, J., *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, no. 106, Springer-Verlag, New York, 1986, corrected 3rd printing.

[Sil94] Silverman, J., *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, no. 151, Springer-Verlag, New York, 1994.

[Spi74] Spiegel, M. R., *Formules et tables de mathématiques*, Série Schaum, McGraw-Hill Inc., Paris, 1974.

[Tan95] K.-S. Tan, *Refined Theorems of the Birch and Swinnerton-Dyer Type*, Ann. Inst. Fourier (Grenoble) **45** (1995), no. 2, 317–374.

[Tat66] J. Tate, *On the Conjectures of Birch and Swinnerton-Dyer and a Geometric Analog*, Séminaire Bourbaki **18** (1966), no. 306, 1–26.

[Tat74] J. Tate, *The Arithmetic of Elliptic Curves*, Invent. Math. **23** (1974), 179–206.

[Tat75] J. Tate, *Algorithm for Determining the Type of a Singular Fiber in an Elliptic Pencil*, Modular Functions of One Variable IV, Lecture Notes in Math., vol. 476, Springer-Verlag, 1975, pp. 33–52.

[Tay94] R. L. Taylor, *l-adic Representations Associated to Modular Forms over Imaginary Quadratic Fields. II*, Invent. Math. **116** (1994), no. 1-3, 619–643.

[TW95] R. L. Taylor and A. Wiles, *Ring-Theoretic Properties of Certain Hecke Algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572.

[Was97] Washington, L. C., *Introduction to Cyclotomic Fields*, second ed., Graduate Texts in Mathematics, no. 83, Springer-Verlag, New York, 1997, corrected 3rd printing.

[Wei71] A. Weil, *Dirichlet Series and Automorphic Forms*, Lecture Notes in Math., no. 189, Springer-Verlag, Berlin Heidelberg, 1971.

[Whi90] E. Whitley, *Modular Symbols and Elliptic Curves over Imaginary Quadratic Number Fields*, Ph.D. thesis, Exeter University, 1990.

[Wil95] A. Wiles, *Modular Elliptic Curves and Fermat's Last Theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

Appendix

PARI-GP Codes