

The Birch and Swinnerton-Dyer conjecture for the Mazur-Kitagawa p -adic L -function in the presence of an exceptional zero

Gabriel Gauthier-Shalom

Master of Science

Department of Mathematics and Statistics

McGill University

Montreal, Quebec

2010-02-15

A thesis submitted to McGill University in partial fulfilment of the requirements of
the degree of Master of Science.

© Gabriel Gauthier-Shalom 2010

ACKNOWLEDGEMENTS

I would like to thank my supervisor Henri Darmon for his infinite patience and for his endlessly enthusiastic guidance. I would also like to thank Felicia Magpantay for her moral support and technical help. I would lastly like to thank NSERC for funding my graduate studies.

ABSTRACT

Starting with the work of Mazur, Tate and Teitelbaum [17], various p -adic analogues of the Birch and Swinnerton-Dyer conjecture have been formulated. The case of an elliptic curve with split multiplicative reduction at the prime p is of special interest. In this so called “exceptional zero” case, the order of vanishing of the Mazur-Swinnerton-Dyer p -adic L -function at the central point seems to be one higher than it is in the classical case. Greenberg and Stevens [10] proved results about this conjecture, using properties of the two variable Mazur-Kitagawa p -adic L -function $L_p(E, k, s)$, which was defined in [14]. Their proof relies on the fact that the Mazur-Kitagawa p -adic L -function $L_p(E, k, s)$ vanishes along the central critical line $s = \frac{k}{2}$, and the fact that the restriction to $k = 2$ is equal to the Mazur-Swinnerton-Dyer p -adic L -function attached to E . In the case where $L_p(E, k, \frac{k}{2})$ is not identically zero, a formula of Bertolini and Darmon [3] gives a formula for its second derivative at $k = 2$. Their formula is also valid for twists $L_p(E, \chi, k, \frac{k}{2})$ of the L -function by quadratic characters χ , and their method of proof relies essentially on the fact that χ is quadratic. This thesis looks into possible generalizations of the result of Bertolini and Darmon in the case of twists by Dirichlet characters of higher order.

ABRÉGÉ

Depuis les travaux de Mazur, Tate et Teitelbaum [17], diverses conjectures ont été proposées qui sont analogues à celle de Birch et Swinnerton-Dyer, dans le cas p -adique. Cette thèse traite principalement le cas d'une courbe elliptique à réduction multiplicative déployée en p ; ce cas est dit "exceptionnel". Dans ce cas, la multiplicité de zéro de la fonction L de Mazur et Swinnerton-Dyer au point central semble être une de plus que ce qui est prédit dans le cas classique. Greenberg et Stevens [10] ont prouvé des résultats concernant cette conjecture en utilisant la fonction L de Mazur et Kitagawa, qui est une fonction $L_p(E, k, s)$ de deux variables. Leur preuve se base sur le fait que la fonction L de Mazur et Kitagawa s'annule sur la ligne centrale critique $s = \frac{k}{2}$ et qu'elle est égal à la fonction L de Mazur et Swinnerton-Dyer quand $k = 2$. Quand $L_p(E, k, \frac{k}{2})$ ne s'annule pas, Bertolini et Darmon [3] ont trouvé une formule pour la dérivée seconde de $L_p(E, k, \frac{k}{2})$ en $k = 2$. Leur formule tient encore quand on tord par un caractère quadratique. Cette thèse considère des généralisations conjecturales des travaux de Bertolini et Darmon lorsque le caractère est d'ordre supérieur à deux.

TABLE OF CONTENTS

	ACKNOWLEDGEMENTS	ii
	ABSTRACT	iii
	ABRÉGÉ	iv
1	Introduction	1
	1.1 Notation and conventions	5
2	Modular forms	6
	2.1 Definition	6
	2.2 Geometric interpretation	9
	2.2.1 Fundamental domains	11
	2.3 Congruence subgroups	12
	2.4 The Hecke operators	13
	2.5 Homology	15
	2.5.1 Sign decomposition	20
	2.6 Hecke module structure	20
	2.6.1 Atkin-Lehner theory	22
	2.6.2 The w_Q operator	24
	2.7 Calculating spaces of cusp forms	25
	2.8 Ordinary submodule	25
3	L -functions and modular symbols	32
	3.1 Modular symbols	32
	3.1.1 Modular symbols attached to a cusp form	33
	3.1.2 Action of the Hecke operators	36
	3.1.3 Sign decomposition	37
	3.2 Explicit description	38
	3.3 The L -function attached to a cusp form	39
	3.3.1 Twists	41

3.4	The functional equation	43
4	Elliptic Curves	46
4.1	Definition	46
4.2	Group Structure	47
4.3	Reduction modulo primes	48
4.4	The L -function attached to an elliptic curve	50
4.5	The Modularity Theorem	51
4.6	The Birch and Swinnerton-Dyer Conjecture	52
4.7	The Twisted Birch and Swinnerton-Dyer Conjecture	54
5	The p -adic L -function	58
5.1	p -adic distributions	58
5.2	p -adic integrals	62
5.3	The p -adic L -function	64
5.4	The p -adic L -series	65
5.5	Interpolation properties	67
5.6	Functional equation	68
5.7	The p -adic Birch and Swinnerton-Dyer conjectures	69
5.8	Computational aspects	70
	5.8.1 Calculating with overconvergent modular forms	71
	5.8.2 Solving the Manin relations	73
5.9	Computing the p -adic L -function	75
6	The Mazur-Kitagawa p -adic L -function	77
6.1	Iwasawa algebras	78
6.2	Hida family	82
6.3	Measure-valued modular symbols	84
	6.3.1 Specialization maps	85
6.4	Defining properties	87
	6.4.1 Ordinary part	88
	6.4.2 The symbol μ_*	90
6.5	The Mazur-Kitagawa p -adic L -function	91
6.6	The exceptional zero conjecture	92
6.7	The Birch and Swinnerton-Dyer conjecture in two variables	93
6.8	Continuing work	95

References 96

CHAPTER 1

Introduction

The problem of finding rational solutions to polynomial equations has been a focus of mathematics since ancient times. Many advances have been made, but some of the most important questions remain unanswered. One important advance was made by Hilbert and Hurwitz, who provided a general method of to find all rational solutions to a quadratic equation in two variables (the genus 0 case). The problem of finding rational points on curves of genus greater than 0 has proven to be much more difficult. An important breakthrough was Faltings' proof of Mordell's conjecture, which states that a curve of genus greater than one has only finitely many rational points. Faltings' result is unfortunately ineffective, so many questions still remain.

In contrast to Faltings' theorem, curves of genus exactly 1 often contain infinitely many rational points. Yet again there is no known method for determining whether a genus 1 curve contains rational points. Much work has gone into classifying the set of rational points on genus 1 curves that do contain rational points; a genus 1 curve with a fixed choice of a rational point is called an elliptic curve. An essential tool in the study of an elliptic curve E is the fact that there exists a composition law on the set $E(\mathbb{Q})$ of rational points on E , which gives $E(\mathbb{Q})$ a group structure. A well known theorem of Mordell ensures that the group $E(\mathbb{Q})$ is finitely generated, though the set $E(\mathbb{Q})$ itself is often infinite (as mentioned earlier). One of the most interesting problems is that of finding the rank of $E(\mathbb{Q})$, which is the \mathbb{Z} -rank of

$E(\mathbb{Q})$ modulo torsion. The problem of computing the rank of $E(\mathbb{Q})$ would become a simple computational problem if the Birch and Swinnerton-Dyer conjecture were to be proven.

The Birch and Swinnerton-Dyer conjecture proposes that arithmetical information about the rational points $E(\mathbb{Q})$ of an elliptic curve E can be related to the combined properties of E when reduced modulo each prime. The Hasse-Weil L -function $L(E, s)$ is the analytic object which encodes the combined information about E modulo each prime. The function $L(E, s)$ turns out to be a holomorphic function on the whole complex plane, a fact which was established by the proof of the modularity theorem; see §4.5 for an explanation. The Hasse-Weil L -function satisfies a functional equation relating the values at s and $2 - s$. Of interest is the Taylor expansion of $L(E, s)$ around the *central point* $s = 1$ of the symmetry of the L -function. The Birch and Swinnerton-Dyer conjecture states that the order of vanishing of the Taylor expansion of $L(E, s)$ around $s = 1$ is equal to the rank of $E(\mathbb{Q})$. Further, generalized versions of the Birch and Swinnerton-Dyer conjecture suggest that more information about E can be gleaned from the leading coefficient of the Taylor expansion. Specifically, it seems that the leading coefficient of the expansion of $L(E, s)$ around $s = 1$ is a product of various constants which encode arithmetical information about E . More details on the Birch and Swinnerton-Dyer conjecture can be found in Wiles's millennium problem description [26].

A new direction of research arose with the introduction by Mazur and Swinnerton-Dyer [16] of a p -adic analogue $L_p(E, s)$ of the Hasse-Weil L -function. The *Mazur-Swinnerton-Dyer p -adic L -function* $L_p(E, s)$ attached to an elliptic curve E is a

p -adic analytic function which interpolates the so called “special values” of the Hasse-Weil L -function. These “special values” are the values of twists of the Hasse-Weil L -function at the central point 1. The development of the theory of p -adic L -functions led Mazur, Tate and Teitelbaum [17] to formulate a p -adic analogue to the Birch and Swinnerton-Dyer conjecture. The statement of the p -adic Birch and Swinnerton-Dyer conjecture is largely similar to the classical case, with one important modification. When E does not have split multiplicative reduction at the prime p , the statement is analogous; the order of vanishing of the p -adic L -function at the central point is conjectured to match the rank of $E(\mathbb{Q})$. There is also a formula conjecturally relating arithmetic information about E to the “leading coefficient” of the p -adic L -function.

In the remaining case, where E has split multiplicative reduction at p , the statement of the p -adic Birch and Swinnerton-Dyer conjecture is slightly more complicated. This complication is related to properties of the p -adic multiplier, which is the factor that allows the special values of the classical L -function to be p -adically interpolated. The p -adic multiplier vanishes exactly in the case of split multiplicative reduction. The order of vanishing of the p -adic L -function then appears to be thrown off, and is conjecturally one higher than the rank of $E(\mathbb{Q})$. There is also an additional factor that appears in the conjectural formula for the leading coefficient of the p -adic L -series; this factor is referred to as the p -adic \mathcal{L} -invariant for E and is denoted $\mathcal{L}_p(E)$.

The authors of [17] empirically conjectured a formula which, in the rank 0 case, expresses $\mathcal{L}_p(E)$ in terms of quantities arising from p -adic analytic properties of E . Greenberg and Stevens [10] proved this “exceptional zero conjecture”. An essential

ingredient in their proof was a two-variable p -adic L -function $L_p(E, k, s)$ called the *Mazur-Kitagawa p -adic L -function*. For a fixed integer value $k \geq 2$, the function $L_p(E, k, s)$ is a constant multiple of the one-variable Mazur-Swinnerton-Dyer p -adic L -function of a modular form f_k . The modular form f_2 is in fact the weight 2 newform attached to E via the modularity theorem, and the one-variable p -adic L -function can be recovered from $L_p(E, k, s)$ by fixing $k = 2$. Furthermore, the form f_k is part of the *Hida family* arising from f_2 . The Hida family is a collection of modular forms of varying p -adic weight whose coefficients vary continuously with the weight.

The Mazur-Kitagawa p -adic L -function $L_p(E, k, s)$ has a functional equation relating its value at (k, s) to that at $(k, k - s)$. Thus it is of interest to look at the values of the Mazur-Kitagawa p -adic L -function along the critical line $s = \frac{k}{2}$. Bertolini and Darmon [3] proved the following theorem:

Theorem 1.1. *Suppose that E has at least two primes of semistable reduction. Then there is a global point $P \in E(\mathbb{Q}) \otimes \mathbb{Q}$ and a scalar $\ell \in \mathbb{Q}^\times$ such that*

$$\frac{d^2}{dk^2} L_p(k, k/2)_{k=2} = \ell \cdot \log_E(P)^2$$

and the point P is of infinite order iff $L'(E, 1) \neq 0$.

Here \log_E is the formal group logarithm defined on E , and $L(E, s)$ is the Hasse-Weil L -function attached to E . In fact, the authors of [3] prove a more general statement involving quadratic twists of the Mazur-Kitagawa p -adic L -function as well. The purpose of this thesis is to look into possible generalizations of the results of Bertolini and Darmon to characters of higher order.

1.1 Notation and conventions

The operation given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

is called *adjugation* and will be denoted $A \mapsto \tilde{A}$; it is an anti-involution on $M_{2 \times 2}(R)$ for any ring R (i.e. $\tilde{A}\tilde{B} = \tilde{\tilde{B}\tilde{A}}$) and preserves the determinant. Note that this conveniently preserves integrality, and coincides with inversion on $\mathrm{SL}_2(\mathbb{Z})$. Note also that $\tilde{A} = \det(A)A^{-1}$. This is a useful operation for turning left actions into right ones (or vice versa).

The completion of the algebraic closure of \mathbb{Q}_p will be denoted \mathbb{C}_p . The algebraic numbers $\bar{\mathbb{Q}}$ will be viewed as being contained in \mathbb{C}_p , via a fixed choice of embedding.

CHAPTER 2

Modular forms

Modular forms are functions on the upper half-plane that satisfy many symmetries. They arise naturally in connection to problems related to quadratic forms, and many other areas of mathematics. For example, the theory of modular forms provides an easy proof to Lagrange’s four square theorem. This example and many others are contained in the paper “Elliptic Modular Forms and Their Applications” by Don Zagier [28]. The usefulness of modular forms derives in large part from the finite dimensionality of spaces of modular forms for finite index subgroups of $SL_2(\mathbb{Z})$.

Modular forms are also very useful because of a connection to elliptic curves. In fact, the coefficients of the L -function attached to a rational elliptic curve always arise from the coefficients of a modular form. This was conjectured by Shimura and Taniyama in the 1950s and proven in the early 2000s. The proof of this so called “modularity theorem” is one of the most important number theoretic results in the past century; see §4.5 for a description.

2.1 Definition

Let $\mathcal{H} = \{z \in \mathbb{C} \mid \Re(z) > 0\}$ denote the upper half-plane. The group

$$\mathrm{GL}_2(\mathbb{Q}) = \left\{ \left[\begin{array}{cc} a & b \\ c & d \end{array} \right] \mid a, b, c, d \in \mathbb{Q}, ad - bc \neq 0 \right\}$$

acts on \mathcal{H} via

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} z = \frac{az + b}{cz + d}. \quad (2.1)$$

A straightforward calculation gives the formula

$$\mathfrak{S} \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} z \right) = \frac{\mathfrak{S}(z)}{|cz + d|^2},$$

which ensures that the action does indeed preserve the sign of the imaginary part (and so is a well-defined action on \mathcal{H}). Equation (2.1) is used to define a right action of $\mathrm{GL}_2(\mathbb{Q})$ on the set of functions from \mathcal{H} to \mathbb{C} ; for an integer k , the *weight k action* of $\mathrm{GL}_2(\mathbb{Q})$ is defined, for

$$f : \mathcal{H} \rightarrow \mathbb{C} \quad \text{and} \quad \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Q})$$

by

$$(f|_k \gamma)(z) = (\det \gamma)^{k-1} j(\gamma, z)^{-k} f(\gamma z),$$

with $j(\gamma, z) := cz + d$. Note that the scalar matrix λI acts as multiplication by λ^{k-2} .

The *modular group* is

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}.$$

This group is generated by the matrices

$$S = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad \text{and} \quad T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

The *height* of a subgroup Γ of the modular group $\mathrm{SL}_2(\mathbb{Z})$ is the minimal $h > 0$ such that the $T^h \in \Gamma$, or infinity if Γ contains no power of T . For the rest of this chapter, $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ will denote a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$. This implies that $A\Gamma A^{-1}$ is of finite height for all $A \in \mathrm{SL}_2(\mathbb{Z})$.

A meromorphic function f on \mathcal{H} satisfying $f|_k\gamma = f$ for all $\gamma \in \Gamma$ is called *weakly modular of weight k* with respect to Γ . Note then that for $A \in \mathrm{SL}_2(\mathbb{Z})$, the function $f|_kA$ is weakly modular with respect to $A^{-1}\Gamma A$ by a simple calculation. A weakly modular function f for Γ on the upper half-plane satisfies $f|_kT^h = f$ where h is the height of Γ . Thus $f(z+h) = f(z)$, so, assuming f is holomorphic on $\{z \mid \Im(z) > c\}$ for some $c > 0$, we have that f has a Fourier expansion on that set:

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n$$

with $q := e^{2\pi iz/h}$. The notation $a_n(f)$ will be used to denote the coefficient of q^n in the Fourier expansion of such an f . The function f is said to be *meromorphic at ∞* if there is some $m \in \mathbb{Z}$ such that $a_n(f) = 0$ for all $n < m$. It is said to be *holomorphic at ∞* if $a_n(f) = 0$ for all $n < 0$. It is said to *vanish at ∞* if, in addition to being holomorphic, $a_0(f) = 0$.

A meromorphic function $f : \mathcal{H} \rightarrow \mathbb{C}$ is called an *automorphic form* of weight k with respect to a subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ if

- $f|_k\gamma = f \quad \forall \gamma \in \Gamma$,
- $f|_kA$ is meromorphic at ∞ for all $A \in \mathrm{SL}_2(\mathbb{Z})$.

An automorphic form f is called a *modular form* of weight k with respect to Γ if it satisfies the following additional property:

- $f|_k A$ is holomorphic at ∞ for all $A \in \mathrm{SL}_2(\mathbb{Z})$.

Finally, a modular form f is called a *cuspidal form* if it satisfies the following additional property:

- $f|_k A$ vanishes at ∞ for all $A \in \mathrm{SL}_2(\mathbb{Z})$.

The space of automorphic forms of weight k for Γ will be denoted $\mathcal{A}_k(\Gamma)$; the corresponding spaces of modular and cusp forms will be respectively denoted $\mathcal{M}_k(\Gamma)$ and $\mathcal{S}_k(\Gamma)$. Note the inclusions $\mathcal{A}_k(\Gamma) \supset \mathcal{M}_k(\Gamma) \supset \mathcal{S}_k(\Gamma)$. A cusp form f is called *normalized* if $a_1(f) = 1$. When working with forms of a fixed weight k , the weight k action of $\mathrm{GL}_2(\mathbb{Q})$ will sometimes be denoted without the subscript (i.e. the notation $f|\gamma$ will denote $f|_k \gamma$ when the weight is understood.)

2.2 Geometric interpretation

Automorphic forms can be interpreted geometrically. To do so, we must introduce two varieties attached to a modular subgroup. The first is the *open modular curve attached to Γ* , denoted $Y(\Gamma)$. The set of complex points $Y(\Gamma)(\mathbb{C})$ of $Y(\Gamma)$ is simply \mathcal{H} modulo the action of Γ . A complex differentiable structure is defined on $Y(\Gamma)(\mathbb{C})$; details of this can be found, for example, in §2 of Diamond and Shurman's book [7].

To describe the next variety, we need to introduce the following topological set first:

$$\mathcal{H}^* := \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}) \subset \mathbb{P}^1(\mathbb{C})$$

The points corresponding to $\mathbb{P}^1(\mathbb{Q})$ are called *cusps*. The action of $\mathrm{SL}_2(\mathbb{Z})$ on \mathcal{H} extends to an action on \mathcal{H}^* in the obvious way. The topology of \mathcal{H} is extended to \mathcal{H}^* by defining the following local bases around the cusps:

- for the cusp ∞ : sets of the form $\{z \in \mathcal{H} \mid \Im(z) > N\} \cup \{\infty\}$.
- for a finite cusp r : the set of circles in \mathcal{H} tangent to the real line at r .

The action of a matrix in $\mathrm{SL}_2(\mathbb{Z})$ is seen to be continuous, since it takes members of this basis to other members of this basis. The *closed modular curve attached to* Γ is denoted $X(\Gamma)$; it has complex points $X(\Gamma)(\mathbb{C})$ corresponding to the quotient of \mathcal{H}^* by the action of Γ . There is an embedding $Y(\Gamma)(\mathbb{C}) \hookrightarrow X(\Gamma)(\mathbb{C})$, and the complement of the image of $Y(\Gamma)(\mathbb{C})$ is a finite set of points. These points are called the *cusps* of $X(\Gamma)$; they correspond to Γ -inequivalent cusps in $\mathbb{P}^1(\mathbb{Q}) \subseteq \mathcal{H}^*$. Details of the construction of $X(\Gamma)(\mathbb{C})$, and of the complex differentiable structure can be found again in §2 of [7].

Now note the following calculation:

$$\begin{aligned} d(Az) &= d\left(\frac{az+b}{cz+d}\right) = \frac{ad-bc}{(cz+d)^2} dz \\ &= \det(A)(cz+d)^{-2} dz = \det(A)j(A, z)^{-2} dz, \end{aligned} \tag{2.2}$$

which implies, for a form of weight $2k$ and $\gamma \in \Gamma$, that

$$\begin{aligned} f(\gamma z)d(\gamma z)^k &= j(\gamma, z)^{2k} f(z)(j(\gamma, z)^{-2} dz)^k \\ &= f(z)dz^k. \end{aligned}$$

Thus, $f(z)dz^k$ is invariant under the action of Γ , so should “descend” to a k -differential on $Y(\Gamma)$. This idea is made precise with the introduction of the space $\Omega(X(\Gamma))^{\otimes k}$ of meromorphic k -differentials on $X(\Gamma)$, whose details can be found in §3.3 of [7]. The following is theorem 3.3.1 of [7]:

Theorem 2.1. *The assignment $f \mapsto f(z)(dz)^k$ is an isomorphism between $\mathcal{A}_{2k}(\Gamma)$ and $\Omega(X(\Gamma))^{\otimes k}$ for any positive integer k .*

To be more explicit: if $f \in \mathcal{A}_{2k}(\Gamma)$ corresponds to $\omega \in \Omega(X(\Gamma))^{\otimes k}$ via this isomorphism, then the pullback to \mathcal{H} of ω is $f(z)dz^k$. Theorem 2.1 tells us that we can think of weight k automorphic forms for Γ as meromorphic k -differentials on $X(\Gamma)$. The subspaces of $\Omega(X(\Gamma))^{\otimes k}$ corresponding to the subspaces $\mathcal{M}_k(\Gamma)$ and $\mathcal{S}_k(\Gamma)$ of $\mathcal{A}_k(\Gamma)$ can be described explicitly with inequalities on the order of vanishing of the differentials at certain points. See §3.5 of [7] for more details.

2.2.1 Fundamental domains

A *fundamental domain* for the action of $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$ on \mathcal{H} is a region $\mathcal{F} \subset \mathcal{H}$ with the following properties:

- $\bigcup_{\gamma \in \Gamma} \gamma\mathcal{F} = \mathcal{H}$
- $\gamma\mathrm{Int}(\mathcal{F}) \cap \mathrm{Int}(\mathcal{F}) = \emptyset \quad \forall \gamma \in \Gamma$
- \mathcal{F} is simply connected.

Here $\mathrm{Int}(\mathcal{F})$ denotes the interior of \mathcal{F} . The points of a fundamental domain for Γ are in one-to-one correspondence with the points of $Y(\Gamma)$ via the quotient map. Now define T to be the (hyperbolic) triangle passing through the cusps 0, 1 and $\rho := \frac{1+\sqrt{-3}}{2}$. Note that τ fixes ρ , and cycles 0, 1 and ∞ . Define $R := T \cup \tau T \cup \tau^2 T$ to be the triangle passing through 0, 1 and ∞ .

The region T is a fundamental domain for the group $\mathrm{PSL}_2(\mathbb{Z})$. We can always find a fundamental domain for Γ that consists of a union of translates of T by matrices in G . If Γ has no torsion, then there is always a fundamental domain consisting of translates of R . Fundamental domains are useful for explicitly describing spaces of

modular symbols, as will be explained in chapter 5, following Pollack and Stevens [19].

2.3 Congruence subgroups

Now we will introduce the congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. The most important congruence subgroups are:

$$\begin{aligned} \Gamma(N) &:= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}, \\ \Gamma_1(N) &:= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}, \\ \Gamma_0(N) &:= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod{N} \right\}. \end{aligned}$$

Note the inclusions $\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N)$. More generally, a subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Q})$ is called a *congruence* subgroup if $\exists N$ with $\Gamma(N) \subseteq \Gamma$. In this case, the smallest such N is called the *level* of Γ . Now we generalize the notion of modular form. A Dirichlet character χ of period N can be viewed as a character on $\Gamma_0(N)$ by the rule

$$\chi \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) = \chi(d)$$

A simple calculation reveals that χ is indeed multiplicative for matrices in $\Gamma_1(N)$.

Definition 2.2. A modular form f for $\Gamma_1(N)$ is called a modular form for $\Gamma_0(N)$ of weight k and character χ if it satisfies the additional property that $f|_\gamma = \chi(\gamma)f$ for all $\gamma \in \Gamma_0(N)$.

The space of all modular forms for $\Gamma_0(N)$ of weight k and character χ is denoted $\mathcal{M}_k(N, \chi)$. Note that if χ is the trivial character modulo N , then $\mathcal{M}_k(N, \chi) = \mathcal{M}_k(\Gamma_0(N))$. The space of cusp forms with character is similarly defined. We will use the notation $X_0(N) := X(\Gamma_0(N))$, $X_1(N) := X(\Gamma_1(N))$ and $X(N) := X(\Gamma(N))$.

2.4 The Hecke operators

An important tool for explicitly describing spaces of modular forms is the Hecke operator. This is an instance of a *double coset operator*, which transforms a modular form for one group into a modular form for another group. Details of the double coset operator construction can be found in §5 of [7]. This section will outline some important properties of Hecke operators. For a prime p , define the following matrices:

$$\gamma_a = \begin{bmatrix} 1 & a \\ 0 & p \end{bmatrix} \quad \text{for } a \in \mathbb{Z}, \quad \gamma_\infty = \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}.$$

The Hecke operator T_p is then defined for $f \in \mathcal{M}_k(N, \chi)$ by

$$f|T_p := \sum_{a=0}^{p-1} f|\gamma_a + \chi(p)f|\gamma_\infty$$

Note that if p divides N , then $\chi(p) = 0$. Note also that $f|\gamma_a$ only depends on a modulo p since

$$f|\gamma_a = f|T^n\gamma_a = f|\gamma_{a+np}$$

for any $n \in \mathbb{Z}$. We inductively define

$$T_{p^n} := T_p T_{p^{n-1}} - \chi(p) p^{k-1} T_{p^{n-2}} \quad \text{for } n \geq 2.$$

It is clear then that T_{p^n} can be expressed as a polynomial in T_p . For primes $p \neq q$, it can be shown by direct calculation that T_p and T_q commute (5.2.4 in [7]). These two facts combine to allow us to define T_n for any positive integer n :

$$T_n := \prod_p T_{p^{\text{ord}_p(n)}}.$$

Since these operators commute, the Hecke operators can be seen as acting on the left or on the right. Thus $f|T_n$ will sometimes be denoted $T_n f$. The following theorem gives the action of the Hecke operators on the Fourier expansion of a modular form:

Theorem 2.3. *For a modular form $f \in \mathcal{M}_k(N, \chi)$, let*

$$f(z) = \sum_{n=0}^{\infty} a_n q^n$$

be the Fourier expansion of f , where $q = e^{2\pi ni}$. For p prime, we then have

$$(f|T_p)(z) = \sum_{n=0}^{\infty} a_{pn} q^n + \chi(p) p^{k-1} \sum_{n=0}^{\infty} a_n q^{pn}.$$

In other words,

$$a_n(f|T_p) = a_{pn}(f) + \chi(p) p^{k-1} a_{n/p}$$

(where $a_{n/p}$ is understood to be zero if $p \nmid n$). Further, we have

$$a_1(f|T_n) = a_n(f)$$

for any positive integer n .

Proof. This is contained in the statements of theorems 5.2.2 and 5.3.1 in [7]. □

2.5 Homology

Homology is an important tool in the study of the action of the Hecke operators on cusp forms. The importance arises from the fact that there exists a Hecke-equivariant duality between spaces of cusp forms and homology space. The duality theorems will be presented in this section.

Suppose Γ is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Consider the curve $X(\Gamma)$ introduced in §2.2, and let C denote the set of cusps in $X(\Gamma)$. The homology group

$$H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z})$$

can be defined as the abelianization of the fundamental group of $X(\Gamma)(\mathbb{C})$, with an arbitrary basepoint (noting that this surface is connected). Let g denote the genus of the Riemann surface $X(\Gamma)(\mathbb{C})$. The homology group $H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z})$ is then simply the free abelian group on $2g$ generators. This is because the fundamental group of $X(\Gamma)(\mathbb{C})$ is generated by $2g$ loops which satisfy a single relation, and that relation is a product of commutators. We also define, for a ring R ,

$$H_1(X(\Gamma)(\mathbb{C}), R) := H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z}) \otimes R,$$

which is a free R -module on $2g$ generators.

For Γ -equivalent cusps r and s , let $\{r \rightarrow s\}$ denote the geodesic path in \mathcal{H}^* joining r to s ; here geodesicity is relative to the hyperbolic measure, which will be defined in §2.6. To be more explicit: if the cusps r and s are finite, $\{r \rightarrow s\}$ is a semicircle whose diameter has endpoints r and s , while if one of the cusps r and s is infinite, $\{r \rightarrow s\}$ is a vertical line. The notation $\{r \rightarrow s\}$ will also denote the image

in $H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z})$ of the geodesic path connecting r to s in \mathcal{H}^* , by a slight abuse of notation.

Lemma 2.4. *Every element h in $H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z})$ is of the form $\{r \rightarrow s\}$ for some cusps r and s .*

Proof. Given an element h of $H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z})$, take an arbitrary lift of h to a homotopy class of loops $[\ell]$ in the fundamental group of $X(\Gamma)(\mathbb{C})$. Choose a loop ℓ representing $[\ell]$ such that the basepoint of ℓ is a cusp $c \in X(\Gamma)(\mathbb{C})$, then lift ℓ to a path p in \mathcal{H}^* , via the quotient map. The endpoints $r, s \in \mathcal{H}^*$ of p both map to $c \in X(\Gamma)(\mathbb{C})$ in the quotient, so r and s are Γ -equivalent cusps in \mathcal{H}^* . The path p is homotopic to the geodesic path between its endpoints, since \mathcal{H} is simply connected; thus h is the image of $\{r \rightarrow s\}$. \square

The representation of homology elements as images of geodesic paths in \mathcal{H}^* leads to a natural pairing

$$\langle \cdot, \cdot \rangle : \mathcal{S}_2(\Gamma) \times H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z}) \rightarrow \mathbb{C}$$

given by integration:

$$\langle f, \{r \rightarrow s\} \rangle := 2\pi i \int_r^s f(z) dz.$$

The details about this, including a proof of well-definedness, can be found in chapter 2 of John Cremona's book [5] (the convergence of the integral is also proven in §3.1 of this thesis). The integration pairing can be linearly extended to real homology:

$$\langle \cdot, \cdot \rangle : \mathcal{S}_2(\Gamma) \times H_1(X(\Gamma)(\mathbb{C}), \mathbb{R}) \rightarrow \mathbb{C}$$

Theorem 2.5. *The integration pairing $\mathcal{S}_2(\Gamma) \times H_1(X(\Gamma)(\mathbb{C}), \mathbb{R}) \rightarrow \mathbb{C}$ is an exact pairing of \mathbb{R} -vector spaces; that is, the kernel on the left is zero, as is the kernel on the right.*

Proof. The proof is explained in chapter 2 of Cremona's book [5]. □

Theorem 2.5 gives a rich structure on the real homology; in particular, the real homology

$$H_1(X(\Gamma)(\mathbb{C}), \mathbb{R})$$

inherits a \mathbb{C} -structure from the space $\mathcal{S}_2(\Gamma)$. This complex structure allows us to reinterpret the duality in theorem 2.5 as an exact duality of \mathbb{C} -vector spaces. It also follows that for arbitrary points r and s in \mathcal{H}^* , the \mathbb{C} -linear map

$$\mathcal{S}_2(\Gamma) \rightarrow \mathbb{C}, \quad f \mapsto 2\pi i \int_r^s f(z) dz$$

corresponds to a unique element of $H_1(X(\Gamma)(\mathbb{C}), \mathbb{R})$ via the duality. Let $\{r \rightarrow s\}$ denote this element of the real homology. An important result is the following:

Theorem 2.6 (Manin-Drinfeld). *For arbitrary cusps r and s , the inclusion $\{r \rightarrow s\} \in H_1(X(\Gamma)(\mathbb{C}), \mathbb{Q})$ holds; that is, there exists an integer n and an element $h \in H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z})$ such that $n\{r \rightarrow s\}$ and h correspond to the same element of the dual of $\mathcal{S}_2(\Gamma)$ via the integration pairing.*

Now we will restrict our attention to $\Gamma = \Gamma_0(N)$. The duality result above (theorem 2.5) allows us to define a Hecke operator on the homology, by defining $T_p h$ to be the element of $H_1(X(\Gamma)(\mathbb{C}), \mathbb{R})$ satisfying

$$\langle f, T_p h \rangle = \langle T_p f, h \rangle$$

for all $f \in \mathcal{S}_2(\Gamma)$. We can be more explicit about this. First consider the action of $\mathrm{GL}_2(\mathbb{Q})$ on homology, which is inherited (via duality) from the action of $\mathrm{GL}_2(\mathbb{Q})$ on $\mathcal{S}_2(\Gamma)$. This action is characterized by

$$\langle f|A, h \rangle = 2\pi i \int_h (f|A)(z) dz = 2\pi i \int_{Ah} f(z) dz = \langle f, Ah \rangle.$$

It is now simple to see that the action of a matrix A on a symbol is given by

$$A\{r \rightarrow s\} = \{Ar \rightarrow As\}. \quad (2.3)$$

So, by linear extension, equation (2.3) explicitly gives the action of $\mathrm{GL}_2(\mathbb{Q})$ on homology. Thus, the action of a Hecke operator is given by

$$T_p h := \sum_{a \bmod p} \gamma_a h + \chi(p) \gamma_\infty h,$$

with γ_* as in §2.4, and where χ is the trivial character modulo N . The Manin-Drinfeld theorem then assures us that the Hecke operators preserve the rational homology, since all the matrices in the definition of the Hecke operators are rational. In fact, the Hecke operators also preserve integral homology:

Lemma 2.7. *The Hecke operator $T_p : H_1(X(\Gamma)(\mathbb{C}), \mathbb{R}) \rightarrow H_1(X(\Gamma)(\mathbb{C}), \mathbb{R})$ preserves integrality. That is, $T_p(H_1(X(\Gamma), \mathbb{Z})) \subseteq H_1(X(\Gamma), \mathbb{Z})$.*

Proof. Any element of $H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z})$ can be represented as $\{\infty \rightarrow \alpha\}$ for some cusp $\alpha \in \mathcal{H}^*$, by lemma 2.4. The cusp α is $\Gamma_0(N)$ -equivalent to ∞ ; note that this property is equivalent to being of the form $\frac{a}{cN}$ for some integers a and c , with $\mathrm{gcd}(a, cN) = 1$. A simple calculation then shows that each γ_* preserves the property of being $\Gamma_0(N)$ -equivalent to ∞ . Note that this is false for γ_∞ if $p \mid N$, but then $\chi(p) = 0$, so γ_∞

need not be considered. Furthermore, γ_* preserves ∞ . Thus $T_p\{\infty \rightarrow \alpha\}$ is a sum of elements of $H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z})$, so is in that space. \square

The following theorem is essential, and is a consequence of lemma 2.7 when $k = 2$:

Theorem 2.8. *For any newform $f \in \mathcal{S}_k(\Gamma_0(N))$, the coefficients of f are algebraic integers which generate a finite extension K_f of \mathbb{Q} .*

Proof. This is theorem 6.5.1 of [7], and the general proof is found there. The proof for general k is analogous to the case $k = 2$, which will now be explained. First we check that the Hecke operators generate a \mathbb{Z} -subalgebra $\mathbb{T}_{\mathbb{Z}}$ of $\text{End}_{\mathbb{C}}(\mathcal{S}_2(\Gamma_0(N)))$ that is finitely generated and free as a \mathbb{Z} -module. To do so, we take advantage of theorems 2.5 and 2.7 to view elements of $\mathbb{T}_{\mathbb{Z}}$ as endomorphisms of the finite free \mathbb{Z} -module $H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z})$. Thus $\mathbb{T}_{\mathbb{Z}}$ lies in the finite free \mathbb{Z} -module $\text{End}_{\mathbb{Z}}(H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z}))$, so is itself finite and free.

The newform f then gives rise to an algebra homomorphism $\eta : \mathbb{T}_{\mathbb{Z}} \rightarrow \mathbb{C}$, defined by

$$T_n \mapsto a_n(f).$$

It follows that the \mathbb{Z} -subalgebra of \mathbb{C} generated by the coefficients of f , which is simply $\eta(\mathbb{T}_{\mathbb{Z}})$, is finitely generated as a \mathbb{Z} -module; thus all the coefficients of f are algebraic integers, and they generate a finite extension of \mathbb{Q} . \square

2.5.1 Sign decomposition

The duality in theorem 2.5 can be refined somewhat if we decompose the spaces occurring there into real and imaginary parts first. Define

$$c := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

The matrix c acts on \mathcal{H}^* via $z \mapsto -\bar{z}$. This gives an action of c on $\mathcal{S}_2(\Gamma_0(N))$, given by $f^*(z) = \overline{f(z^*)}$. The eigenspaces for $+1$ and -1 are then respectively denoted $\mathcal{S}_2(\Gamma_0(N))_{\mathbb{R}}$ and $i\mathcal{S}_2(\Gamma_0(N))_{\mathbb{R}}$; implied in this notation is that $\mathcal{S}_2(\Gamma_0(N))_{\mathbb{R}}$ is the subspace of cusp forms with real Fourier coefficients, and $i\mathcal{S}_2(\Gamma_0(N))_{\mathbb{R}}$ is that with purely imaginary coefficients. Take $H_1^{\pm}(X(\Gamma_0(N))(\mathbb{C}), \mathbb{R})$ to be the ± 1 -eigenspace for the action of c in homology; here c acts on homology via symbols, as described earlier. Then the refined duality is given by:

Theorem 2.9. *The integration pairing $\mathcal{S}_2(\Gamma_0(N))_{\mathbb{R}} \times H_1^+(X(\Gamma_0(N))(\mathbb{C}), \mathbb{R}) \rightarrow \mathbb{R}$ is an exact pairing of \mathbb{R} -vector spaces.*

The proof of this and further details can be found in §2.1.3 of [5]. It is simple to see that c commutes with any T_p , so the Hecke operators respect the sign decomposition.

2.6 Hecke module structure

The purpose of this section is to give an explicit description of $\mathcal{S}_2(\Gamma_0(N))$, and of the action of the Hecke operators on that space. There are two tools essential to describing $\mathcal{S}_2(\Gamma_0(N))$: the first is the duality of $\mathcal{S}_2(\Gamma_0(N))$ and $H_1(X(\Gamma_0(N))(\mathbb{C}), \mathbb{R})$,

which was described in the previous section. The second is the Petersson scalar product, which will now be defined.

Let \mathcal{F} denote a fundamental domain for $\Gamma_0(N)$. Let

$$d\mu(x + yi) = \frac{dx dy}{y^2}$$

be the hyperbolic measure on \mathcal{H} . Define

$$V_{\Gamma_0(N)} = \int_{\mathcal{F}} d\mu(z).$$

The Petersson scalar product is defined by

$$\langle f, g \rangle := \frac{1}{V_{\Gamma_0(N)}} \int_{\mathcal{F}} f(z) \overline{g(z)} \Im(z)^k d\mu(z)$$

for $f, g \in \mathcal{S}_k(\Gamma_0(N))$. A simple calculation shows that the integrand is invariant under the action of $\Gamma_0(N)$, which implies the well-definedness of the Petersson scalar product. See §5.4 of [7] for details. We have the following important property (theorem 5.5.3 of [7]):

Theorem 2.10. *The Hecke operators T_n with n prime to N are self-adjoint with respect to the Petersson scalar product. That is,*

$$\langle f, T_n g \rangle = \langle T_n f, g \rangle$$

for all $f, g \in \mathcal{S}_k(\Gamma_0(N))$, whenever n is prime to N .

Theorem 2.10 allows us to use results from linear algebra to describe a basis for $\mathcal{S}_k(\Gamma_0(N))$ with nice properties (theorem 5.5.4 of [7]):

Theorem 2.11. *The vector space $\mathcal{S}_k(\Gamma_0(N))$ has an orthogonal basis of simultaneous eigenvectors for all of the Hecke operators T_n with n prime to N .*

The ideal situation would be for the Hecke operators to cut out one-dimensional eigenspaces. Unfortunately, this is not the case, but Atkin-Lehner theory allows us to say more.

2.6.1 Atkin-Lehner theory

This section follows the work in the paper [2] of Atkin and Lehner. Atkin-Lehner theory gives us constructions for changing the level of a cusp form. These constructions allow us to decompose $\mathcal{S}_k(\Gamma_0(N))$ into Hecke-stable subspaces. The decomposition aids greatly in the study of the Hecke module structure on $\mathcal{S}_k(\Gamma_0(N))$.

Lemma 2.12. *Suppose $Md \mid N$ for positive integers M and d . Let*

$$\delta_d := \begin{bmatrix} d & 0 \\ 0 & 1 \end{bmatrix}.$$

Then for $g(z) \in \mathcal{S}_k(\Gamma_0(M))$, we get $g|\delta_d \in \mathcal{S}_k(\Gamma_0(N))$.

Proof. By direct calculation, for any

$$\begin{bmatrix} a & b \\ Nc & e \end{bmatrix} \in \Gamma_0(N),$$

we calculate

$$\delta_d \begin{bmatrix} a & b \\ Nc & e \end{bmatrix} \delta_d^{-1} = \begin{bmatrix} a & db \\ Nc/d & e \end{bmatrix} = \begin{bmatrix} a & db \\ Mc & e \end{bmatrix} \in \Gamma_0(M).$$

So if we let $f := g|\delta_d$ and take $\gamma \in \Gamma_0(N)$, we get

$$f|\gamma = g|\delta_d\gamma = g|\delta_d\gamma\delta_d^{-1}|\delta_d = g|\delta_d = f,$$

since $\delta_d\gamma\delta_d^{-1} \in \Gamma_0(M)$ by the above calculation. So f is a modular form with respect to $\Gamma_0(N)$. \square

Define $\mathcal{S}_k(\Gamma_0(N))^{\text{old}}$ to be the subspace of $\mathcal{S}_k(\Gamma_0(N))$ spanned by $f|\delta_d$ for all choices of M and d with $Md | N$, and all choices of cusp forms f of level $M < N$. Take $\mathcal{S}_k(\Gamma_0(N))^{\text{new}}$ to be the orthogonal complement of $\mathcal{S}_k(\Gamma_0(N))^{\text{old}}$ with respect to the Petersson scalar product. We then have

$$\mathcal{S}_k(\Gamma_0(N)) = \mathcal{S}_k(\Gamma_0(N))^{\text{new}} \oplus \mathcal{S}_k(\Gamma_0(N))^{\text{old}}.$$

Furthermore, theorem 5.6.2 in [7] tells us that the Hecke operators preserve the spaces $\mathcal{S}_k(\Gamma_0(N))^{\text{new}}$ and $\mathcal{S}_k(\Gamma_0(N))^{\text{old}}$. We can now make theorem 2.11 more specific:

Theorem 2.13. *The space $\mathcal{S}_k(\Gamma_0(N))^{\text{new}}$ has an orthogonal basis of normalized cusp forms that are eigenvectors for all of the T_n .*

A member of this basis is called a *newform*. More generally, a cusp form f that is an eigenvector for T_n for all positive integers n is called an *eigenform*. An important consequence of theorem 2.3 is that for a normalized eigenform f , the eigenvalue for T_n is a_n , since $a_1(T_n f) = a_n(f)$ and $a_1(f) = 1$. Thus a normalized eigenform is completely determined by its eigenvalues for the Hecke operators. So theorem 2.13 implies that the Hecke operators decompose $\mathcal{S}_k(\Gamma_0(N))^{\text{new}}$ into one dimensional eigenspaces.

Theorem 2.13 can also be used to give an explicit description of a basis for $\mathcal{S}_k(\Gamma_0(N))$ (theorem 5.8.3 of [7]):

Theorem 2.14. *The set*

$$\{f(dz) : f \text{ is a newform in } \mathcal{S}_k(\Gamma_0(M))^{\text{new}}, Md \mid N\}$$

is a basis for $\mathcal{S}_k(\Gamma_0(N))$.

2.6.2 The w_Q operator

Suppose $N = Q \cdot M$, with $(Q, M) = 1$. Then for any choice of integers x, y, z, t satisfying $Qxt - Myz = 1$, define

$$W_Q := \begin{bmatrix} Qx & y \\ Nz & Qt \end{bmatrix},$$

and then define the operator w_Q by

$$w_Q(f) := Q^{1-\frac{k}{2}} f|W_Q$$

for $f \in \mathcal{S}_k(\Gamma_0(N))$. The operator w_Q has the following properties, all of which are proved in [2]:

- $w_Q(f) \in \mathcal{S}_k(\Gamma_0(N))$ for all $f \in \mathcal{S}_k(\Gamma_0(N))$.
- The operator w_Q does not depend on the choice of $x, y, z, t \in \mathbb{Z}$.
- For any $f \in \mathcal{S}_k(\Gamma_0(N))$, $w_Q^2(f) = f$.
- For any n with $(n, N) = 1$, w_Q and T_n commute on $\mathcal{S}_k(\Gamma_0(N))$.
- For any newform $f \in \mathcal{S}_k(\Gamma_0(N))^{\text{new}}$, we have $w_Q(f) = \pm f$.

These operators will be useful when studying L -functions in §3.3.

2.7 Calculating spaces of cusp forms

The discussion in §2.6 outlines an interesting idea, which is the basis for many algorithms used to calculate spaces of cusp forms. The idea is to go through the discussion in reverse order. That is, we start by computing $H_1(X(\Gamma_0(N))(\mathbb{C}), \mathbb{Q})$, which can be accomplished with simple algebra (as outlined in the proof of theorem 2.1.4 of [5]). The Hecke action is then computed on the rational homology, and is linearly extended to $H_1(X(\Gamma_0(N))(\mathbb{C}), \mathbb{R})$. Now we can simply *define* $\mathcal{S}_2(\Gamma_0(N))$ to be the module $\text{Hom}_{\mathbb{R}}(H_1(X(\Gamma_0(N))(\mathbb{C}), \mathbb{R}), \mathbb{C})$, which inherits the Hecke-action from homology. (Note that it is nicer if we split into real and imaginary spaces first; that is, $\mathcal{S}_2(\Gamma_0(N))_{\mathbb{R}}$ is the \mathbb{R} -dual of $H_1^+(X(\Gamma_0(N)), \mathbb{R})$, and $\mathcal{S}_2(\Gamma_0(N)) = \mathcal{S}_2(\Gamma_0(N))_{\mathbb{R}} \oplus i\mathcal{S}_2(\Gamma_0(N))_{\mathbb{R}}$.) This gives an effective algorithm for computing the Hecke-module of cusp forms.

To give a more explicit description, we must calculate the q -expansions of our cusp forms. To do so, we use Atkin-Lehner theory to cut out the subspace $\mathcal{S}_2(\Gamma_0(N))^{\text{new}}$ of $\mathcal{S}_2(\Gamma_0(N))$. Then the Hecke operators decompose $\mathcal{S}_2(\Gamma_0(N))^{\text{new}}$ into 1-dimensional eigenspaces. For each eigenspace, the q -expansion of the corresponding newform is then obtained by packaging the Hecke-eigenvalues into a formal q -expansion.

2.8 Ordinary submodule

Let p denote a fixed prime greater than 3. This section will define the p -ordinary submodule of the space $\mathcal{S}_k(\Gamma_0(N))$. Regardless of level, we take

$$U_p := \sum_{a=0}^{p-1} \gamma_a$$

with the matrices γ_* defined as in section 2.4:

$$\gamma_a = \begin{bmatrix} 1 & a \\ 0 & p \end{bmatrix} \quad \text{for } a \in \mathbb{Z}, \quad \gamma_\infty = \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix},$$

and

$$\delta_d := \begin{bmatrix} d & 0 \\ 0 & 1 \end{bmatrix}.$$

Here we are considering U_p as an operator on $\mathcal{S}_k(\Gamma_0(N))$ with varying level N . Note that the Hecke operator on $\mathcal{S}_k(\Gamma_0(N))$ corresponding to the prime p is $U_p + \chi_N(p)\delta_p$, where χ_N is the trivial Dirichlet character modulo N .

For the next definition, we will need the following lemma:

Lemma 2.15. *Suppose $a \in \overline{\mathbb{Q}}$ is an algebraic integer. Recall that we have fixed an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$. In \mathbb{C}_p ,*

$$\lim_{n \rightarrow \infty} a^{n!} = \begin{cases} 1 & \text{if } a \text{ is a unit} \\ 0 & \text{if } a \text{ is a non-unit.} \end{cases}$$

Proof. If a is not a unit, then it has positive (additive) p -adic valuation; thus the limit of $a^{n!}$ is clearly 0. So suppose a is a unit contained in the ring of integers \mathcal{O} of a finite extension K of \mathbb{Q}_p . Take a prime ideal $\mathfrak{p} \subseteq \mathcal{O}$ above $p\mathbb{Z}_p$. Now a is a unit, so by basic number theory,

$$a^{|\mathcal{O}/\mathfrak{p}^k|-1} \equiv 1 \pmod{\mathfrak{p}^k}.$$

For n large enough, $|\mathcal{O}/\mathfrak{p}^k| - 1$ divides $n!$, so the desired result follows by taking the limit $n \rightarrow \infty$. □

Hida's projector to the ordinary part is defined as

$$e_{\text{ord}} = \lim_{n \rightarrow \infty} U_p^{n!}.$$

An eigenform for $\Gamma_0(N)$ is called *ordinary at p* if its U_p -eigenvalue is a p -adic unit. Lemma 2.15 tells us that an eigenform f is fixed by e_{ord} exactly if it is ordinary, and otherwise e_{ord} maps f to 0. The *ordinary submodule* of $\mathcal{S}_k(\Gamma_0(N))$ is

$$\mathcal{S}_k^{\text{ord}}(\Gamma_0(N)) := e_{\text{ord}}\mathcal{S}_k(\Gamma_0(N)).$$

To describe the ordinary submodule (and to prove well-definedness), we will consider the action of the operator e_{ord} on a basis for $\mathcal{S}_k(\Gamma_0(N))$. The following lemma is needed:

Lemma 2.16. *If $p \nmid d$, then the operators δ_d and U_p commute on $\mathcal{S}(\Gamma_0(N))$ for any positive integer N . Also, $\delta_p U_p$ acts as p^{k-1} on $\mathcal{S}(\Gamma_0(N))$.*

Proof. A simple calculation shows that

$$\delta_d U_p = \delta_d \left(\sum_{a=0}^{p-1} \gamma_a \right) = \left(\sum_{a=0}^{p-1} \gamma_{da} \right) \delta_d = U_p \delta_d$$

since the action of γ_a only depends on a modulo p (as mentioned in section 2.4), and d is prime to p . Also, recalling that scalar matrices act via the $(k-2)$ power map, we get:

$$\delta_p U_p = \delta_p \left(\sum_{a=0}^{p-1} \gamma_a \right) = \sum_{a=0}^{p-1} \begin{bmatrix} p & pa \\ 0 & p \end{bmatrix} = p^{k-2} \sum_{a=0}^{p-1} \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix},$$

which acts as p^{k-1} . □

Note that lemma 2.16 implies that e_{ord} commutes with δ_d if $p \nmid d$. Theorem 2.14 gives the following basis for $\mathcal{S}_k(\Gamma_0(N))$:

$$\{f|\delta_d : f \text{ is a newform in } \mathcal{S}_k(\Gamma_0(N'))^{\text{new}}, dN' \mid N\}.$$

The following lemma gives the action of e_{ord} on members of this basis:

Lemma 2.17. *Suppose d and N' are positive integers such that $dN' \mid N$, and suppose f is a newform of level N' . If $a_p(f)$ is not a p -adic unit, then*

$$e_{\text{ord}}(f|\delta_d) = 0.$$

If $a_p(f)$ is a p -adic unit, let α, β be the roots of Frobenius of f ; that is, the roots of $x^2 - a_p(f)x + \chi_{N'}(p)p^{k-1}$. Assume the roots are ordered so that α is a unit and β is a non-unit. Then

$$e_{\text{ord}}(f|\delta_d) = \frac{\alpha}{\alpha - \beta}(f|\delta_d - \beta p^{1-k} f|\delta_{pd})$$

if $(p, d) = 1$, and

$$e_{\text{ord}}(f|\delta_d) = \frac{p^{k-1}}{\alpha - \beta}(f|\delta_{d/p} - \beta p^{1-k} f|\delta_d)$$

if $p \mid d$.

Proof. Note that $\delta_a \delta_b = \delta_{ab}$, so δ_a and δ_b always commute. Note also that δ_d commutes with e_{ord} when $(p, d) = 1$, since δ_d commutes with U_p . Thus we can assume without loss of generality that $d = 1$ or p . We have, since f is a newform at level N' , that

$$f|(U_p + \chi_{N'}(p)\delta_p) = a_p f,$$

so

$$f|U_p = a_p f - \chi_{N'}(p)f|\delta_p.$$

Lemma 2.16 implies that

$$(f|\delta_p)|U_p = p^{k-1}f,$$

so

$$\begin{bmatrix} f & f|\delta_p \end{bmatrix} | U_p = \begin{bmatrix} f & f|\delta_p \end{bmatrix} \begin{bmatrix} a_p & p^{k-1} \\ -\chi_{N'}(p) & 0 \end{bmatrix}.$$

Let A denote the 2×2 matrix on the right. If a_p is a non-unit, then a simple calculation shows that all entries of A^2 have positive (additive) valuation; it follows then that

$$\begin{bmatrix} f & f|\delta_p \end{bmatrix} | U_p^{n!} = \begin{bmatrix} f & f|\delta_p \end{bmatrix} A^{n!}$$

tends to 0 as $n \rightarrow \infty$. Now suppose that a_p is a unit, noting that this excludes the case $\alpha = \beta$ (since $\alpha\beta = \chi_{N'}(p)p^{k-1}$ is a non-unit). By diagonalizing A , we get

$$p^{k-1}(\alpha - \beta)f = \alpha(p^{k-1}f - \beta f|\delta_p) - \beta(p^{k-1}f - \alpha f|\delta_p), \quad (2.4)$$

with

$$f_\alpha := p^{k-1}f - \beta f|\delta_p \quad \text{and} \quad f_\beta := p^{k-1}f - \alpha f|\delta_p$$

being eigenvectors of U_p with respective eigenvalues α and β . Lemma 2.15 implies that $e_{\text{ord}}(f_\alpha) = f_\alpha$ and $e_{\text{ord}}(f_\beta) = 0$. So by applying Hida's projector to equation (2.4), we get

$$e_{\text{ord}}(f) = \frac{\alpha}{p^{k-1}(\alpha - \beta)}(p^{k-1}f - \beta f|\delta_p) = \frac{\alpha}{\alpha - \beta}(f - \beta p^{1-k}f|\delta_p).$$

Similarly,

$$(\alpha - \beta)f|\delta_p = (p^{k-1}f - \beta f|\delta_p) - (p^{k-1}f - \alpha f|\delta_p),$$

so

$$e_{\text{ord}}(f|\delta_p) = \frac{p^{k-1}}{(\alpha - \beta)}(f - \beta p^{1-k}f|\delta_p).$$

□

Definition 2.18. *Suppose $f \in \mathcal{S}_k(\Gamma_0(N))$ is a p -ordinary cusp form which is an eigenvector for T_p , and let β denote its non-unit root of Frobenius at p . The p -stabilized cusp form g corresponding to f is the cusp form*

$$g := f - \beta p^{1-k}f|\delta_p,$$

which satisfies

$$g(z) = f(z) - \beta f(pz).$$

Note that the if p divides N , then $\beta = 0$, so f is already p -stabilized. Otherwise, $g \in \mathcal{S}_k(\Gamma_0(Np))$.

Corollary 2.19. *The space $\mathcal{S}_k^{\text{ord}}(\Gamma_0(N))$ has basis*

$$B = \{f(dz) - \beta f(pdz) : f \text{ is a } p\text{-ordinary newform in } \mathcal{S}_k(\Gamma_0(N'))^{\text{new}}, \\ (p, d) = 1, dN' \mid N\},$$

where β denotes the non-unit root of Frobenius of f at p .

Proof. Lemma 2.17 implies that B spans the ordinary subspace, since every basis element for $\mathcal{S}_k(\Gamma_0(N))$ (from theorem 2.14) maps to a multiple of an element of B

under e_{ord} . Linear independence follows from the linear independence of the basis in theorem 2.14. \square

CHAPTER 3
***L*-functions and modular symbols**

The L -function of a cusp form f is an analytic function which encodes the Fourier coefficients of f . Values of the L -function can be expressed in terms of modular symbols. Modular symbols encode line integrals along geodesic paths in the upper half plane. These symbols greatly aid the computation of the values of L -functions since the calculation of modular symbols can be reduced to linear algebra. Modular symbols are also indispensable when defining p -adic L -functions.

3.1 Modular symbols

Define

$$\Delta_0 = \text{Div}^0(\mathbb{P}^1(\mathbb{Q})) := \left\{ \sum_{r \in S \subset \mathbb{P}^1(\mathbb{Q})} a_r \cdot [r] \mid a_r \in \mathbb{Z}, S \text{ finite}, \sum_{r \in S} a_r = 0 \right\}$$

to be the group of degree 0 divisors. Also, let $\Delta_0(R) := \Delta_0 \otimes R$. For an abelian group A , we define the space of A valued symbols

$$\text{Symb}(A) := \{\phi : \Delta_0 \rightarrow A\}$$

to be the abelian group of homomorphisms from Δ_0 to A . Now suppose Γ is a subgroup of $\text{SL}_2(\mathbb{Z})$ or $\text{PSL}_2(\mathbb{Z})$. The group Γ then acts on Δ_0 (on the left) by linear fractional transformations, as defined in chapter 2. If A is a right Γ -module, we

define a right action of Γ on $\text{Symb}(A)$ by the rule:

$$(\phi|\gamma)(D) = \phi(\gamma D)|\gamma.$$

Then we define

$$\text{Symb}_\Gamma(A) := \{\phi \in \text{Symb}(A) \text{ such that } \phi(\gamma D) = \phi(D)|\gamma^{-1} \quad \forall \gamma \in \Gamma\}$$

to be the Γ invariant subspace of $\text{Symb}(A)$. For a modular symbol ϕ and $r, s \in \mathbb{P}^1(\mathbb{Q})$, we will use the notation

$$\phi\{r \rightarrow s\}$$

to denote the value of ϕ at the divisor $[s] - [r]$.

3.1.1 Modular symbols attached to a cusp form

Define $\mathfrak{P}_k(K)$ to be the set of homogeneous polynomials in two variables of degree $k - 2$, with coefficients in the field K . Let $V_k(K)$ denote the K -linear dual of $\mathfrak{P}_k(K)$. There is a natural right action of $GL_2(K)$ on $\mathfrak{P}_k(K)$ given by

$$(P|A)(x, y) := P(ax + by, cx + dy) \quad \text{for } A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

(Note that scalar matrices act via the $k - 2$ power map.) This action gives rise to a right action of $GL_2(K)$ on $V_k(K)$ given by $(v|A)(P) = v(P|\tilde{A})$ for $v \in V_k(K)$ (recall that $\tilde{A} = \det(A)A^{-1}$). To a cusp form $f \in \mathcal{S}_k(\Gamma_0(N))$, we attach the $V_k(\mathbb{C})$ -valued symbol I_f defined by

$$I_f\{r \rightarrow s\}(P) := 2\pi i \int_r^s f(z)P(z, 1)dz.$$

The path of integration is the geodesic path connecting the cusp r to s , with the hyperbolic metric (as described in section 2.6). A note should be made about convergence:

Lemma 3.1. *For a cusp form $f \in \mathcal{S}_k(\Gamma_0(N))$, the integral*

$$\int_r^s f(z)g(z)dz$$

converges absolutely for any polynomial g .

Proof. Pick an arbitrary point $\alpha \in \mathcal{H}$ along $\{r \rightarrow s\}$. The group $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on the cusps, so there is a matrix A such that $A\infty = s$. By a change of variables $z \mapsto Az$ and by equation (2.2),

$$\begin{aligned} \int_\alpha^s f(z)g(z)dz &= \int_{A^{-1}\alpha}^\infty f(Az)g(Az)d(Az) \\ &= \int_{A^{-1}\alpha}^\infty (f|A)(z)j(A, z)^{k-2}g(Az)dz. \end{aligned} \quad (3.1)$$

Note that the path of integration is a vertical line for the last integral. The form f is cuspidal, so by definition, $(f|A)(z)$ has a Fourier expansion with which contains only positive powers of $q = e^{2\pi iz}$. Thus as $\Im(z) \rightarrow \infty$, the absolute value of $(f|A)(z)$ tends to 0 exponentially. Also, $j(A, z)^{k-2}g(Az)$ has subexponential growth, so the integral on the right of equation (3.1) converges absolutely. Similarly, the integral from r to α converges absolutely, so the integral from r to s converges. \square

The modular symbol I_f has two important properties:

- $I_f \in \mathrm{Symb}_{\Gamma_0(N)}(V_k(\mathbb{C}))$ (i.e. it is invariant under the action of $\Gamma_0(N)$.)
- I_f is \mathbb{C} -linear in f .

The first of these follows from the corollary to the following lemma, and the second is clear from the definition.

Lemma 3.2. *for $A \in GL_2^+(\mathbb{R})$ (i.e. a 2×2 real matrix with positive determinant), we have*

$$I_{f|A}\{r \rightarrow s\}(P|A) := \det(A)^{k-2} I_f\{Ar \rightarrow As\}(P)$$

Corollary 3.3.

$$I_f|A = I_{f|A}$$

Corollary 3.4. *I_f is invariant under $\Gamma_0(N)$.*

Proof. By a simple calculation (done in section 2.2),

$$d(Az) = d\left(\frac{az+b}{cz+d}\right) = \det(A)(cz+d)^{-2}dz \quad (3.2)$$

so

$$\begin{aligned} & (f|A)(z)(P|A)(z, 1)dz \\ &= \det(A)^{k-1}(cz+d)^{-k}f(Az)P(az+b, cz+d)dz \\ &= \det(A)^{k-1}(cz+d)^{-k}f(Az)(cz+d)^{k-2}P\left(\frac{az+b}{cz+d}, 1\right)dz \\ &= \det(A)^{k-2}f(Az)P(Az, 1)\det(A)(cz+d)^{-2}dz \\ &= \det(A)^{k-2}f(Az)P(Az, 1)d(Az), \end{aligned}$$

and hence

$$\begin{aligned}
I_{f|A}\{r \rightarrow s\}(P|A) &= 2\pi i \int_r^s (f|A)(z)(P|A)(z, 1) dz \\
&= 2\pi i \det(A)^{k-2} \int_r^s f(Az)P(Az, 1) d(Az) \\
&= 2\pi i \det(A)^{k-2} \int_{Ar}^{As} f(z)P(z, 1) dz \\
&= \det(A)^{k-2} I_f\{Ar \rightarrow As\}(P).
\end{aligned}$$

The corollary then follows easily:

$$\begin{aligned}
(I_{f|A}\{r \rightarrow s\})(P) &= ((I_f\{Ar \rightarrow As\})|A)(P) \\
&= I_f\{Ar \rightarrow As\}(P|\tilde{A}) \\
&= \det(A)^{2-k} I_{f|A}\{r \rightarrow s\}(P|\tilde{A}A) \\
&= \det(A)^{2-k} \det(A)^{k-2} I_{f|A}\{r \rightarrow s\}(P) \\
&= I_{f|A}\{r \rightarrow s\}(P),
\end{aligned}$$

noting that

$$\tilde{A}A = \begin{bmatrix} \det A & 0 \\ 0 & \det A \end{bmatrix}.$$

□

3.1.2 Action of the Hecke operators

Recall the following notation from section 2.4: for a prime p , we take

$$\gamma_a = \begin{bmatrix} 1 & a \\ 0 & p \end{bmatrix} \quad \text{for } 0 \leq a \leq p-1, \quad \gamma_\infty = \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}.$$

We define the Hecke operators on modular symbols as follows for a right $\Gamma_0(N)$ -module A (with χ being the trivial character modulo N):

$$I|T_p := I \left| \left(\sum_{a \bmod p} \gamma_a + \chi(p)\gamma_\infty \right) \right. \quad (3.3)$$

for $I \in \text{Symb}_{\Gamma_0(N)}(A)$, so that corollary 3.3 implies that

$$I_f|T_p = I_f|_{T_p}.$$

3.1.3 Sign decomposition

The section is analogous to §2.5.1. The matrix

$$c := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

normalizes $\Gamma_0(N)$, by a simple calculation. The matrix c thus induces an involution on $\text{Symb}_{\Gamma_0(N)}(V_k(\mathbb{C}))$, sending I to $I|c$; note then that for all $\gamma \in \Gamma_0(N)$

$$I|c\gamma = I|(c\gamma c^{-1})c = I|c,$$

so $I|c$ is $\Gamma_0(N)$ -invariant. We can decompose I_f into the sum of its eigencomponents:

$$I_f = I_f^+ + I_f^-, \text{ where } I_f^+ = \frac{I_f + I_f|c}{2}, \quad I_f^- = \frac{I_f - I_f|c}{2}.$$

Suppose the coefficients of the q -expansion of f generate the number field K_f (recalling theorem 2.8), with ring of integers \mathcal{O}_f . A theorem of Hatada (theorem 3 of [12]) implies the following:

Theorem 3.5. *There exist periods Ω^+ and Ω^- such that the symbols defined by*

$$\phi_f^\pm := (\Omega^\pm)^{-1} I_f^\pm$$

take values in $V_k(\mathcal{O}_f)$.

Theorem 3.5 will be essential when trying to interpolate modular symbols p -adically. The symbol ϕ_f^\pm will be referred to as the *normalized modular symbol* attached to f of sign ± 1 .

3.2 Explicit description

This section will explain a result of Manin which gives an explicit description of a modular symbol space. To do so for a subgroup $\Gamma \subseteq G := \mathrm{PSL}_2(\mathbb{Z})$, we need a description of Δ_0 as a Γ -module. There is a map from G to Δ_0 defined by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} a \\ c \end{bmatrix} - \begin{bmatrix} b \\ d \end{bmatrix}.$$

We extend this linearly to a map

$$d : \mathbb{Z}[G] \rightarrow \Delta_0.$$

A result of Manin, found in §2.2 of [19], states the following:

Theorem 3.6. *The map d defined above is surjective. The kernel is*

$$I = \mathbb{Z}[G](1 + \tau + \tau^2) + \mathbb{Z}[G](1 + \sigma)$$

where

$$\tau = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

which are 3 and 2-torsion elements respectively.

Theorem 3.6 gives rise to a complete (though complicated) description of the Γ -module Δ_0 , since $\mathbb{Z}[G]$ is a free $\mathbb{Z}[\Gamma]$ -module; if $G = \bigsqcup_{i=1}^r \Gamma g_i$, then

$$\mathbb{Z}[G] = \bigoplus_{i=1}^r \mathbb{Z}[\Gamma]g_i.$$

To describe Δ_0 as a Γ -module, we translate the relations from theorem 3.6 into relations among the g_i . For example,

$$g_i(1 + \sigma) = g_i + \gamma_{ij}g_j$$

where g_j is the right coset representative for $g_i\sigma$ for each i . There are similar relations for τ . In principle, this could be sufficient to describe any Γ -homomorphism from Δ_0 , but to do so, we would have to simultaneously solve many equations in the target space. So realistically, we need a more explicit description to continue. The approach of Pollack and Stevens [19] will be outlined in section 5.8.

3.3 The L -function attached to a cusp form

Suppose $f \in \mathcal{S}_k(\Gamma_0(N))$ has q -expansion

$$f(z) = \sum_{n \geq 1} a_n q^n, \quad q = e^{2\pi iz}.$$

The L -series attached to f is defined by

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

for s such that $\Re(s) > \frac{k}{2} + 1$.

Lemma 3.7. *The L-series attached to f has the following integral representation:*

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

for s with $\Re(s) > \frac{k}{2} + 1$. Furthermore, the L-series extends to a holomorphic function on the whole complex plane, called the L-function attached to f .

Proof. This is found in §5.10 of [7]; an outline will be presented here. The integral representation is verified by expanding f into its q -expansion, then integrating term by term. The argument in the proof of lemma 3.1 can be applied here to show that the integral above is in fact absolutely convergent for any value of $s \in \mathbb{C}$. Also, $\Gamma(s)^{-1}$ is well known to be an entire function, so $L(f, s)$ extends to an entire function. \square

Corollary 3.8. *For integer values of j in the range $1 \leq j \leq k - 1$,*

$$L(f, j) = \frac{(-2\pi i)^{j-1}}{(j-1)!} I_f\{\infty \rightarrow 0\}(x^{j-1}y^{k-j-1}).$$

Proof. Using lemma 3.7:

$$\begin{aligned} I_f\{0 \rightarrow \infty\}(x^{j-1}y^{k-j-1}) &= 2\pi i \int_0^\infty f(z)z^{j-1} dz \\ &= 2\pi i \int_0^\infty f(it)(it)^{j-1} d(it) \\ &= 2\pi i^{j+1} \int_0^\infty f(it)t^j \frac{dt}{t} \\ &= -\frac{(j-1)!}{(-2\pi i)^{j-1}} L(f, j). \end{aligned}$$

\square

The values of $L(f, j)$ for j in the range $1 \leq j \leq k - 1$ are called the *critical values* of $L(f, s)$. Corollary 3.8 expresses these critical values in terms of the modular symbol attached to f . In fact, a similar result also holds if we twist f by a Dirichlet character.

3.3.1 Twists

For a modular form f , the twist of f by a Dirichlet character χ is defined to be

$$f_\chi(z) := \sum_{n=0}^{\infty} \chi(n) a_n q^n$$

The function f_χ can be expressed in terms of the original function f as follows. For simplicity, we assume χ is a primitive character of conductor m . Define the usual Gauss sums as

$$\tau(n, \chi) = \sum_{a \bmod m} \chi(a) e^{2\pi i n a / m}, \quad \tau(n) = \tau(1, \chi)$$

The following calculation will allow us to give a different representation of f_χ :

Lemma 3.9. $\tau(n, \chi) = \bar{\chi}(n) \cdot \tau(\chi)$ for n prime to m .

Proof.

$$\begin{aligned} \tau(n, \chi) &= \sum_{a \bmod m} \chi(a) e^{2\pi i n a / m} \\ &= \bar{\chi}(n) \sum_{a \bmod m} \chi(na) e^{2\pi i n a / m} \\ &= \bar{\chi}(n) \sum_{a \bmod m} \chi(a) e^{2\pi i a / m} = \bar{\chi}(n) \cdot \tau(\chi) \end{aligned}$$

where the last line follows since $(m, n) = 1$, so $n \mapsto an$ is a bijection modulo m . \square

Lemma 3.9 can then be used to obtain the aforementioned representation of f_χ :

Lemma 3.10 (Birch's Lemma). *Suppose f is a modular form in $\Gamma_0(N)$, and χ is a primitive character of conductor m . Then*

$$f_{\bar{\chi}} = \frac{1}{\tau(\chi)} \sum_{a \bmod m} \chi(a) f \left| \begin{bmatrix} 1 & a/m \\ 0 & 1 \end{bmatrix} \right.$$

Proof. By lemma 3.9,

$$\begin{aligned} f_{\bar{\chi}}(z) &= \sum_n \bar{\chi}(n) a_n e^{2\pi i n z} = \sum_n \frac{\tau(n, \chi)}{\tau(\chi)} a_n e^{2\pi i n z} \\ &= \frac{1}{\tau(\chi)} \sum_n \sum_{a \bmod m} \chi(a) e^{2\pi i n a / m} a_n e^{2\pi i n z} \\ &= \frac{1}{\tau(\chi)} \sum_{a \bmod m} \chi(a) \sum_n a_n e^{2\pi i n (z + a/m)} \\ &= \frac{1}{\tau(\chi)} \sum_{a \bmod m} \chi(a) f \left(z + \frac{a}{m} \right) \end{aligned}$$

□

Now consider a primitive character χ modulo m . Birch's lemma (lemma 3.10) gives the twisting rule, where

$$\delta_a = \begin{bmatrix} 1 & a/m \\ 0 & 1 \end{bmatrix}$$

is the matrix in that lemma:

$$\begin{aligned} I_{f_{\bar{\chi}}} \{r \rightarrow s\} (P) &= \frac{1}{\tau(\chi)} \sum_{a \bmod m} \chi(a) I_{f|\delta_a} \{r \rightarrow s\} (P) \\ &= \frac{1}{\tau(\chi)} \sum_{a \bmod m} \chi(a) I_f \{\delta_a r \rightarrow \delta_a s\} (P|\delta_{-a}), \end{aligned}$$

where we use lemma 3.2 for the last step, and note that $\tilde{\delta}_a = \delta_{-a}$. Now corollary 3.8 tells us that for $1 \leq j \leq k - 1$:

$$\begin{aligned} L(f_{\bar{\chi}}, j) &= \frac{(-2\pi i)^{j-1}}{(j-1)!} I_{f_{\bar{\chi}}} \{ \infty \rightarrow 0 \} (x^{j-1} y^{k-j-1}) \\ &= \frac{(-2\pi i)^{j-1}}{(j-1)! \tau(\chi)} \sum_{a \bmod m} \chi(a) I_f \left\{ \infty \rightarrow \frac{a}{m} \right\} \left(\left(x - \frac{a}{m} y \right)^{j-1} y^{k-j-1} \right). \end{aligned}$$

Thus all the special values of all twists of the L -function of f can be expressed in terms of the values of the modular symbol I_f .

3.4 The functional equation

The L -function attached to a newform satisfies a certain functional equation. Among other uses, this functional equation allows us to study the order of vanishing of the L -function at the central critical point. To state the functional equation, it is convenient to first multiply the L -function by some additional factors:

Definition 3.11. *For a cusp form $f \in \mathcal{S}_k(\Gamma_0(N))$, we set*

$$\Lambda(f, s) := N^{\frac{s}{2}} \int_0^\infty f(it) t^s \frac{dt}{t} = N^{\frac{s}{2}} (2\pi)^{-s} \Gamma(s) L(f, s),$$

recalling lemma 3.7.

Now recall the w_Q operator from section 2.6.2. Recall also the fact that any newform of level N is an eigenvector for the w_N operator.

Theorem 3.12. *For $f \in \mathcal{S}_k(\Gamma_0(N))$, the following relation holds:*

$$\Lambda(w_N(f), s) = i^{-k} \Lambda(f, k - s).$$

Corollary 3.13. *Suppose $f \in \mathcal{S}_k(\Gamma_0(N))$ is an eigenvector for the w_N operator, with eigenvalue $c = \pm 1$, then*

$$\Lambda(f, s) = ci^{-k}\Lambda(f, k - s).$$

The parity of the order of vanishing n of $\Lambda(f, s)$ at $s = \frac{k}{2}$ is determined by

$$c = (-1)^{n - \frac{k}{2}}.$$

Proof. By definition,

$$w_N(f)(z) = N^{1 - \frac{k}{2}} \left(f \left| \left[\begin{array}{cc} 0 & -1 \\ N & 0 \end{array} \right] \right. \right) (z) = N^{-\frac{k}{2}} z^{-k} f \left(\frac{-1}{Nz} \right),$$

so

$$\begin{aligned} \Lambda(w_N(f), s) &= N^{\frac{s}{2}} \int_0^\infty (w_N f)(it) t^s \frac{dt}{t} \\ &= N^{\frac{s}{2} - \frac{k}{2}} i^{-k} \int_0^\infty f \left(\frac{-1}{Nit} \right) t^{s-k} \frac{dt}{t} \end{aligned}$$

which, by the change of variable $u = \frac{1}{Nt}$, gives

$$\begin{aligned} \Lambda(w_N(f), s) &= N^{\frac{k-s}{2}} i^{-k} \int_0^\infty f(iu) u^{k-s} \frac{du}{u} \\ &= i^{-k} \Lambda(f, k - s). \end{aligned}$$

The corollary follows from considering the Taylor expansion of $\Lambda(f, s)$ around $s = \frac{k}{2}$.

If the order of vanishing of $\Lambda(f, s)$ is n at $s = \frac{k}{2}$, then the functional equation tells

us, by taking n th coefficients on each side, that

$$c = i^{-k}(-1)^n = (-1)^{n-\frac{k}{2}}.$$

□

In fact, there is also a functional equation for twists of L -functions attached to cusp forms. The proof is largely similar, although the details of the calculation are more involved, so will be omitted.

Theorem 3.14. *Suppose $f \in \mathcal{S}_k(\Gamma_0(N))$ is a w_N -eigenvector with eigenvalue c , and ψ is a primitive Dirichlet character of conductor m which is relatively prime to N . The following relation holds:*

$$\tau(\psi)^{-1} \Lambda(f_\psi, s) = c N^{\frac{k}{2}-s} \psi(-N) \tau(\overline{\psi})^{-1} \Lambda(f_{\overline{\psi}}, k-s),$$

where $\tau(\psi)$ denotes the Gauss sum associated to ψ .

Note that for a quadratic Dirichlet character ψ , we have $\overline{\psi} = \psi$, so we can again use the functional equation to determine the order of vanishing of the L -function at the central critical point.

CHAPTER 4 Elliptic Curves

One of the central interests in number theory is the solution of polynomial equations over \mathbb{Q} . Unfortunately, this problem becomes difficult very quickly as the degrees of the polynomials increase. For quadratic equations, the solution is made easier by the fact that the Hasse principle holds:

Definition 4.1. *A class of algebraic varieties defined over a number field K is said to satisfy the Hasse principle if, for each variety V in the class,*

$$V(K) \neq \emptyset \iff V(K_\nu) \neq \emptyset \quad \forall \nu,$$

where ν varies over all the places of K , and K_ν is the localization at ν . Thus a quadratic polynomial has a solution over \mathbb{Q} if and only if it does modulo all prime powers and in the real numbers. The Hasse principle fails for equations of degree greater than 2, which makes the problem of finding solutions much harder. The case of degree 3 equations reduces to the problem of finding points on elliptic curves. This chapter gives an overview of some properties of elliptic curves that will be used, following Silverman's book [21].

4.1 Definition

Definition 4.2. *An elliptic curve over a field K is a pair (E, O) , with E a smooth projective curve of genus 1 over K , and $O \in E(K)$.*

Generally an elliptic curve (E, O) will be denoted simply E , with O being understood from the context. Every elliptic curve can be written in Weierstrass form: E is the set of (projective) solutions to the equation:

$$y^2 + a_1yx + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{4.1}$$

for some constants a_1, a_2, a_3, a_4 and a_6 in K , with the distinguished point O being the point at infinity. It is useful to more generally consider curves defined by equations of the form (4.1) that give rise to possibly singular (i.e. non-smooth) curves. There are several important quantities related to the curve E : the discriminant Δ of the curve E is a quantity which vanishes iff E is singular; another quantity, denoted c_4 , is important when $\Delta = 0$ (that is, when E is singular). The quantities Δ and c_4 are both defined as polynomials in the coefficients a_i , with integer coefficients. The formulae defining Δ and c_4 can be found in [21], §III.

Note that E is singular iff there is a point on E for which the Jacobian matrix related to the Weierstrass equation has less than full rank. When E is singular, it is simple to check that there is exactly one singularity. There are two possible behaviors for an elliptic curve at a singularity; either there are two tangent directions, or there is only one. A singularity is called a *node* in the case of two tangent directions, which occurs if $c_4 \neq 0$, and is called a *cusp* when there is only one tangent direction, which occurs if $c_4 = 0$.

4.2 Group Structure

Now we consider the set $E(K)$ of points on E defined over K . Given points $P, Q \in E(K)$, we define $P \star Q$ to be the third point of intersection with E of the

line passing through P and Q . An elementary computation shows that $P \star Q$ also lies on $E(K)$. Then we define addition on the curve by $P + Q = O \star (P \star Q)$. This composition law can be proven to be commutative and associative, with O as the identity element. The set $E(K)$ thus has an abelian group structure, and much work has gone into describing its properties.

A crucial result is the Mordell theorem, which can be found in Chapter VIII of [21]: for a number field K , the Mordell theorem tells us that the group $E(K)$ is finitely generated. Thus the structure theorem for abelian groups tells us that

$$E(K) \cong \prod_{i=1}^k \frac{\mathbb{Z}}{n_i \mathbb{Z}} \times \mathbb{Z}^r \quad (4.2)$$

for some positive integers n_1, \dots, n_k and r . The integer r is called the *rank* of $E(K)$. So Mordell's theorem tells us that the rank of $E(K)$ is finite for any number field K . Unfortunately, the proof of Mordell's theorem is not effective, so the problem of finding an algorithm to compute the group structure of $E(K)$ is still open.

4.3 Reduction modulo primes

Fix a prime p . Suppose E is an elliptic curve defined over \mathbb{Q} by an equation of the form 4.1 with integer coordinates. Take \tilde{E} to be the curve over \mathbb{F}_p defined by the modulo p reduction of the Weierstrass equation of E .

The quantities $\tilde{\Delta}, \tilde{c}_4$ corresponding to \tilde{E} can then be seen to be the reduction modulo p of the quantities Δ, c_4 related to E , since Δ and c_4 are integer polynomials in the coefficients of the Weierstrass equation of E . We say E has

- good (or stable) reduction modulo p if $\tilde{\Delta} \neq 0$, i.e. $p \nmid \Delta$

- bad reduction of multiplicative type (or is semi-stable) if $\tilde{\Delta} = 0$, and the singularity is a node (i.e. $\tilde{c}_4 \neq 0$)
- bad reduction of additive type (or is unstable) if $\tilde{\Delta} = 0$, and the singularity is a cusp (i.e. $\tilde{c}_4 = 0$)

Further, if E has multiplicative reduction, we say that the reduction is *split* if the tangent slopes at the singularity lie in \mathbb{F}_p , and that the reduction is *non-split* otherwise. The determinant Δ encapsulates information about the reduction of E modulo all of the primes. That said, Δ does not distinguish between different types of bad reduction; the *conductor* is a quantity similar to Δ which encodes extra information about the reduction of E . The conductor of E is defined as

$$n_E := \prod_{p \text{ prime}} p^{f_E(p)}$$

where, for $p > 3$, the exponent $f_E(p)$ is 0 if E has good reduction modulo p , is 1 for multiplicative reduction, and is 2 for additive reduction. For $p = 2$ or $p = 3$, the formula is slightly more complicated; see [20] §IV.10 for more information about the conductor. The conductor has the same prime divisors as the discriminant, though the powers appearing in the conductor are always small.

Given a point $P = [X, Y, Z] \in \mathbb{P}^2(\mathbb{Q})$, we can always rescale the coordinates so that they are relatively prime integers; the resulting coordinates will be called *reduced coordinates* for P . Suppose P is a projective point on E with reduced coordinates $[X, Y, Z]$. The reduction of P modulo the prime p gives a point \tilde{P} in $\mathbb{P}^2(\mathbb{F}_p)$, since not all coordinates of P are 0 modulo p (lest the coordinates share a common factor). The point \tilde{P} can easily be seen to lie on \tilde{E} . So we get a map $E \rightarrow \tilde{E}$; thus we can

extract information about E over \mathbb{Q} by analyzing the curve \tilde{E} defined over the finite field \mathbb{F}_p , since any rational point on E is a lift of a point in \tilde{E} .

4.4 The L -function attached to an elliptic curve

Recall that in the case of a quadratic equation, the problem of determining whether a rational solution exists is made easier by the validity of Hasse's principle; that is, the fact that the equation need only be solved modulo prime powers and in \mathbb{R} . If a solution is found, it is then easy to find all the others, by projecting onto a line. Unfortunately, Hasse's local-global property fails to hold in the cases of degree higher than 2. In the case of an elliptic curve E , the Birch and Swinnerton-Dyer conjectures suggest that global information can be gleaned from the combined local information, despite the failure of Hasse's principle. There is strong numerical evidence in support of the Birch and Swinnerton-Dyer conjectures.

To study the local properties of a rational elliptic curve E , the following functions are defined: the local zeta function of a rational elliptic curve E at a prime p of good reduction is

$$Z_p(E, z) = \exp \left(\sum_{n=1}^{\infty} \frac{\#E(\mathbb{F}_{p^n})}{n} z^n \right).$$

The local zeta function can be shown to be a rational function. More specifically, in §C.16 of [21], the following is shown:

$$Z_p(E, z) = \frac{L_p(z)}{(1-z)(1-pz)}$$

with $L_p(z) = 1 - a_p z + pz^2$. The a_p in this equation is equal to $p + 1 - \#E(\mathbb{F}_p)$. In the case of bad reduction, we define $L_p(z) = 1 - a_p z$, with a_p being 0 in the

case of additive reduction, 1 for split multiplicative reduction and -1 for non-split multiplicative reduction.

The zeta functions encode all the information about E modulo prime powers. We combine this local information into the following object, called the Hasse-Weil L -function attached to the elliptic curve E :

$$L(E, s) := \prod_p L_p(p^{-s})^{-1} = \prod_{p \nmid \Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1} \cdot \prod_{p \mid \Delta} L_p(p^{-s})^{-1}.$$

A theorem of Hasse ensures that $|a_p| \leq 2\sqrt{p}$, which implies that this function converges for $\Re(k) > \frac{3}{2}$. The product defining $L(E, s)$ can be expanded into an L -series:

$$L(E, s) := \sum_{n \geq 1} a_n n^{-s},$$

which will converge on the same half-plane. The modularity theorem, which is described in §4.5, implies that $L(E, s)$ extends to be holomorphic on the whole complex plane.

In the case of an elliptic curve E defined over a number field K , the L -function $L(E/K, s)$ can be defined similarly. See §II.10 of [20] for details of the construction of $L(E/K, s)$.

4.5 The Modularity Theorem

Starting with a rational modular form f for $\Gamma_0(N)$, a construction of Eichler and Shimura associates to f a rational elliptic curve E of conductor N . The elliptic curve E has the property that its L -function is equal to that of f . The Eichler-Shimura construction and the aforementioned results are explained in §XI of [15] (see theorem

11.74). A natural question follows; do all elliptic curves arise from the Eichler-Shimura construction? Shimura and Taniyama conjectured the affirmative answer to this question for all rational elliptic curves. The Shimura-Taniyama conjecture was proven in 2001 by the work of Breuil, Conrad, Diamond and Taylor [4], and will be referred to as the *modularity theorem* for the rest of this thesis. The proof of the modularity theorem was a continuation of a breakthrough of Wiles [27] and of Taylor and Wiles [23], who proved the Shimura-Taniyama conjecture for a large class of elliptic curves. The modularity theorem has far-reaching consequences, one of which is a proof of Fermat's Last Theorem, a problem which had stood unproved for over 300 years. A concise but comprehensive summary of the Shimura-Taniyama conjecture and its proof can be found in [6].

The modularity theorem is very useful for working with elliptic curves, and in particular L -functions of elliptic curves, since modular forms are often easier to work with directly. For example, the L -series of a cusp form can easily be shown to extend to a holomorphic function on the entire complex plane, whereas that of an elliptic curve is much more difficult to extend. In particular, the modularity theorem allows us to extend the L -function of an elliptic curve to $s = 1$, so that the statement of the Birch and Swinnerton-Dyer conjecture makes sense. The modularity theorem is also useful when defining p -adic L -functions, again because modular forms are easier to work with directly.

4.6 The Birch and Swinnerton-Dyer Conjecture

The Birch and Swinnerton-Dyer conjecture states that at $s = 1$, the Hasse-Weil L -function $L(E, s)$ attached to a rational elliptic curve E has order of vanishing equal

to the rank of E . Thus the BSD conjecture relates the global arithmetic properties of the elliptic curve E to the analytic properties of the L -function $L(E, s)$, which encodes the local information about E . In fact, the Birch and Swinnerton-Dyer conjecture has been generalized to say that even more information can be extracted from the L -function. Specifically, a conjectural formula for the leading coefficient of the Taylor series of $L(E, s)$ around $s = 1$ is given, which expresses the coefficient as a product of terms related to the arithmetic properties of E . The following version of the Birch and Swinnerton-Dyer conjecture and a concise outline of the conjecture can be found in Wiles's article [26].

Conjecture 4.3 (The Birch and Swinnerton-Dyer Conjecture). *The L -function $L(E, s)$ of an elliptic curve E has a Taylor expansion at $s = 1$ satisfying:*

$$L(E, s) = c \cdot (s - 1)^r + \text{higher order terms}$$

and further,

$$c = \frac{\Omega_E \cdot \prod c_p \cdot |\text{III}(E/\mathbb{Q})| \cdot \text{Reg}(E/\mathbb{Q})}{|E(\mathbb{Q})_{\text{torsion}}|^2}$$

All of the quantities appearing in this factorization are defined in terms of the arithmetic properties of E . One of the most important partial results to date is the following theorem of Kolyvagin, building on the work of Gross, Zagier and others (which is discussed in [26]):

Theorem 4.4 (Kolyvagin's Theorem). *If $L(E, s)$ vanishes to exact order 0 or 1 at $s = 1$, then the Birch and Swinnerton-Dyer conjecture holds, i.e. the rank of E is equal to the order of vanishing of $L(E, s)$ at $s = 1$.*

As for numerical evidence, Cremona (for example) has done computations for large classes of rational elliptic curves, and the results have always been consistent with the Birch and Swinnerton-Dyer conjecture. See [5] for more information on Cremona’s work. Note that the modularity theorem is a big advancement in regards to the Birch and Swinnerton-Dyer conjecture; it guarantees that the L -function of a rational elliptic curve E is entire, so in particular, $L(E, s)$ is analytic around $s = 1$. The modularity theorem is also a big advancement since, prior to the proof, many theorems (including Kolyvagin’s theorem) were only known to hold for modular elliptic curves.

4.7 The Twisted Birch and Swinnerton-Dyer Conjecture

Take E to be an elliptic curve defined over \mathbb{Q} , and suppose K/\mathbb{Q} is a finite abelian extension of \mathbb{Q} with galois group G . It is possible to decompose the vector space $E(K) \otimes \overline{\mathbb{Q}}$ into a direct sum, based on the action of G . It is also possible to decompose the L -function $L(E/K, s)$ into a product of “twisted” L -functions. These decompositions can be matched up to provide a refinement of the Birch and Swinnerton-Dyer conjecture. Kisilevsky and Fearnley [8, 9] and others have worked on precise formulations of these refined conjectures, and have compiled numerical evidence in their support. This section summarizes the work in [8], which provides motivation for formulating new analogues of the Birch and Swinnerton-Dyer conjectures, as will be done in §6.7.

The group G acts on $E(K)$ by the following formula on Weierstrass coordinates:

$$P^\sigma := (x^\sigma, y^\sigma) \text{ for } P = (x, y) \in E(K).$$

Note that we assumed that E was defined over \mathbb{Q} , so that P^σ can easily be seen to lie again on $E(K)$ by applying σ to the Weierstrass equation. This action gives rise to an action of G on $E(K) \otimes \overline{\mathbb{Q}}$. Note that the Mordell theorem, in the form of equation (4.2), implies that $E(K) \otimes \overline{\mathbb{Q}}$ is free over $\overline{\mathbb{Q}}$ of dimension r equal to the rank of $E(K)$ (since the integers n_i appearing in equation (4.2) are invertible). Define \hat{G} to be the group of characters χ of G ; that is, homomorphisms $\chi : G \rightarrow \overline{\mathbb{Q}}^\times$.

Definition 4.5. For a character $\chi \in \hat{G}$, the χ -part of E is

$$(E(K) \otimes \overline{\mathbb{Q}})^\chi := \{P \in E(K) \otimes \overline{\mathbb{Q}} \text{ such that } P^\sigma = \chi(\sigma)P \ \forall \sigma \in G\}.$$

The χ -rank of $E(K)$ is the $\overline{\mathbb{Q}}$ -dimension of $(E(K) \otimes \overline{\mathbb{Q}})^\chi$, and is denoted $r_\chi(E(K))$.

It follows from the theory of representations of finite groups that we have a decomposition

$$E(K) \otimes \overline{\mathbb{Q}} = \bigoplus_{\chi \in \hat{G}} (E(K) \otimes \overline{\mathbb{Q}})^\chi.$$

From this it follows that

$$\sum_{\chi \in \hat{G}} r_\chi(E(K)) = r(E(K)).$$

The next step is to decompose the L -function $L(E/K, s)$ into a product, with each factor corresponding to an element of \hat{G} . Using class field theory, we can associate to any $\chi \in \hat{G}$ a Dirichlet character, also denoted χ by abuse of notation. The Dirichlet character χ has period D equal to the discriminant of K/\mathbb{Q} . The primitive Dirichlet character associated to χ will be denoted χ^* . Now we define twists of L -functions by Dirichlet characters:

Definition 4.6. *The L-series of E/\mathbb{Q} twisted by a Dirichlet character ψ is the function*

$$L(E, \psi, s) := \sum_{n \geq 1} \psi(n) a_n n^{-s},$$

where

$$L(E, s) := \sum_{n \geq 1} a_n n^{-s}$$

is the L-series of E/\mathbb{Q} . The holomorphic extension of $L(E, \psi, s)$ to the whole complex plane is called the L-function of E twisted by ψ .

This allows us to define twists by characters $\chi \in \hat{G}$:

Definition 4.7. *The L-function of E/\mathbb{Q} twisted by a character $\chi \in \hat{G}$ is*

$$L(E, \chi, s) := L(E, \chi^*, s)$$

where χ^* is the primitive Dirichlet character associated to χ .

This definition allows us to decompose the function $L(E/K, s)$ into a product:

Theorem 4.8.

$$L(E/K, s) = \prod_{\chi \in \hat{G}} L(E, \chi, s).$$

The decompositions of $L(E/K, s)$ and $E(K) \otimes \overline{\mathbb{Q}}$ lead to a natural generalization of the Birch and Swinnerton-Dyer conjecture to the case of twisted L-functions:

Conjecture 4.9 (The Twisted Birch and Swinnerton-Dyer Conjecture). *For an abelian extension K/\mathbb{Q} and a character $\chi : \text{Gal}(K/\mathbb{Q}) \rightarrow \mathbb{C}^\times$, the order of vanishing of $L(E, \chi, s)$ at $s = 1$ is equal to the rank r_χ of $(E(K) \otimes \overline{\mathbb{Q}})^\chi$.*

In fact, Fearnley and Kisilevsky [8, 9] further provide a (conjectural) formula for the leading coefficient of $L(E, \chi, s)$, which decomposes the formula found in conjecture 4.3. The authors also provide numerical data in support of their conjecture.

CHAPTER 5

The p -adic L -function

The special values of L -functions twisted by characters can be interpolated p -adically in different ways to give p -adic analogues of L -functions. This section will outline the construction and computation of the Mazur-Swinnerton-Dyer p -adic L -function, following the paper "On p -adic analogues of the conjectures of Birch and Swinnerton-Dyer" by Mazur, Tate and Teitelbaum [17].

Throughout, $\mathcal{M}_k(N, \chi)$ denotes the space of modular forms of weight k , level $\Gamma_0(N)$ and character χ , and $\mathcal{S}_k(N, \chi)$ is the corresponding space of cusp forms. We fix a "sign at infinity" $w_\infty = \pm 1$, and take ϕ_f to be the normalized modular symbol attached to a cusp form f of sign w_∞ , which was introduced in §3.1.3. Finally, p will denote a fixed prime greater than 3.

5.1 p -adic distributions

Let X be a compact open subset of \mathbb{Q}_p^n for some n . A p -adic distribution on X is a finitely additive function from the set of compact open subsets of X to a vector space over \mathbb{C}_p with an additive valuation ν . If a distribution μ is uniformly bounded (i.e. $\exists K \in \mathbb{R}$ with $\nu(\mu(U)) \geq K$ for all compact open subsets U of X), then μ is called a *measure*. There is an important difference between the concept of distribution and measure; a priori, the notion of integrating a continuous function against a distribution is not well defined unless the distribution is in fact a measure. Nonetheless, as is explained in this chapter, a useful notion of integration can be

defined from some distributions. More information about distributions and measures can be found in Washington's book [25].

Fix a prime p and an eigenform $f \in \mathcal{S}_k(N, \chi)$ of T_p with eigenvalue a_p . The purpose of this section is to use the modular symbol I_f attached to a cusp form f to define a p -adic distribution with values in $V_k(\mathbb{C}_p)$. This distribution will be defined on the space

$$\mathbb{Z}_{p,M}^\times := \varprojlim \left(\frac{\mathbb{Z}}{p^j M \mathbb{Z}} \right)^\times \subseteq \mathbb{Z}_{p,M} := \varprojlim \frac{\mathbb{Z}}{p^j M \mathbb{Z}}$$

where M is an integer prime to p . Recall from lemma 2.17 that a root of $x^2 - a_p x + \chi(p)p^{k-1}$ is called a root of Frobenius. Now fix a non-zero root of Frobenius α , if one exists. Let ν be the normalized p -adic (additive) valuation. Now we define, for $f \in \mathcal{S}_k(N, \chi)$:

$$\begin{aligned} S_{f,\alpha}(a, m) &:= \alpha^{-\nu(m)-1} \phi_f \left| \left(\alpha \begin{bmatrix} 1 & a \\ 0 & m \end{bmatrix} - \chi(p) \begin{bmatrix} p & pa \\ 0 & m \end{bmatrix} \right) \right. \\ &= \alpha^{-\nu(m)-1} \phi_f \left| \left(\alpha \begin{bmatrix} 1 & a \\ 0 & m \end{bmatrix} - \chi(p)p^{k-2} \begin{bmatrix} 1 & a \\ 0 & \frac{m}{p} \end{bmatrix} \right) \right. \end{aligned}$$

The symbol $S_{f,\alpha}(a, m)$ is an element of $\text{Symb}(V_k(\mathbb{Q}(\alpha)))$, recalling that we have fixed an embedding of the algebraic numbers into \mathbb{C}_p . The modular symbol $S_{f,\alpha}$ is defined to “massage” ϕ_f so that it has nice p -adic interpolation properties:

Proposition 5.1 (Distribution property).

$$\sum_{u \bmod p} S_{f,\alpha}(a + um, pm) = S_{f,\alpha}(a, m)$$

Proof.

$$\begin{aligned}
& \sum_{u \bmod p} S_{f,\alpha}(a + um, pm) \\
&= \alpha^{-\nu(m)-2} \phi_f \left| \sum \left(\alpha \begin{bmatrix} 1 & a + um \\ 0 & pm \end{bmatrix} - \chi(p)p^{k-2} \begin{bmatrix} 1 & a + um \\ 0 & m \end{bmatrix} \right) \right. \\
&= \alpha^{-\nu(m)-2} \phi_f \left| \sum \left(\alpha \begin{bmatrix} 1 & a + um \\ 0 & pm \end{bmatrix} - \chi(p)p^{k-2} \begin{bmatrix} 1 & a \\ 0 & m \end{bmatrix} \right) \right. \\
&= \alpha^{-\nu(m)-2} \phi_f \left(\alpha \sum_{u \bmod m} \begin{bmatrix} 1 & u \\ 0 & p \end{bmatrix} - \chi(p)p^{k-1} \right) \begin{bmatrix} 1 & a \\ 0 & m \end{bmatrix} \\
&= \alpha^{-\nu(m)-2} \phi_f \left(\alpha \left(T_p - \chi(p) \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} \right) - \chi(p)p^{k-1} \right) \begin{bmatrix} 1 & a \\ 0 & m \end{bmatrix} \\
&= \alpha^{-\nu(m)-2} \phi_f \left((\alpha a_p - \chi(p)p^{k-1}) - \alpha \chi(p) \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix} \right) \begin{bmatrix} 1 & a \\ 0 & m \end{bmatrix} \\
&= \alpha^{-\nu(m)-2} \phi_f \left(\alpha^2 - \alpha \chi(p) \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix} \right) \begin{bmatrix} 1 & a \\ 0 & m \end{bmatrix} \\
&= \alpha^{-\nu(m)-1} \phi_f \left(\alpha \begin{bmatrix} 1 & a \\ 0 & m \end{bmatrix} - \chi(p) \begin{bmatrix} p & ap \\ 0 & m \end{bmatrix} \right)
\end{aligned}$$

using equation (3.3), and the fact that T_p acts as a_p on f . We also use the equation $\alpha^2 - a_p \alpha + \chi(p)p^{k-1} = 0$. □

Now if $(M, p) = 1$ and $j \geq 1$, define

$$\mu_{f,\alpha}(a + p^j M \mathbb{Z}_{p,M}; P) := S_{f,\alpha}(-a, p^j M) \{\infty \rightarrow 0\}(P).$$

For any fixed polynomial P , $\mu_{f,\alpha}$ is a well defined distribution on $\mathbb{Z}_{p,M}^\times$ because of proposition 5.1. When P is omitted, it is taken to be 1 by default. We will be interested in integrating p -adic functions against the distribution $\mu_{f,\alpha}$.

There is another way of interpreting the construction of $\mu_{f,\alpha}$ in the case where α is a unit. Suppose p does not divide the level N of the ordinary newform $f \in \mathcal{S}_k(\Gamma_0(N))$. Let α and β respectively denote the unit and non-unit root of Frobenius for f . Let g denote the p -stabilized eigenform corresponding to f , recalling the notation from §2.8; so $g(z) = f(z) - \beta f(pz)$, which is a cusp form of level Np . Note that

$$a_p(g) = a_p(f) - \beta a_1(f) = \alpha$$

(since $\alpha + \beta = a_p(f)$, and $a_1(f) = 1$), so the characteristic polynomial of Frobenius for g is $x^2 - \alpha x$. Thus α is the non-unit root of Frobenius for g . We have

$$g = f \left| \left(1 - \beta p^{1-k} \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} \right) \right. = f \left| \left(1 - \frac{\chi(p)}{\alpha} \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} \right) \right.,$$

so

$$\begin{aligned} S_{f,\alpha}(a, m) &= \alpha^{-\nu(m)} \phi_f \left| \left(1 - \frac{\chi(p)}{\alpha} \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} \right) \right. \left[\begin{array}{c} 1 & a \\ 0 & m \end{array} \right] \\ &= \alpha^{-\nu(m)} \phi_g \left[\begin{array}{c} 1 & a \\ 0 & m \end{array} \right] = S_{g,\alpha}(a, m). \end{aligned}$$

So when α is a unit, $\mu_{f,\alpha}$ could be defined as the measure associated to the p -stabilized cusp form g corresponding to f . This is helpful because the formula for $\mu_{g,\alpha}$ is simple since g 's level is divisible by p . Explicitly, $\mu_{g,\alpha}$ is given by:

$$\begin{aligned}\mu_{g,\alpha}(a + p^j M \mathbb{Z}_{p,M}; P) &= S_{g,\alpha}(-a, p^j M) \{\infty \rightarrow 0\}(P(z)) \\ &= \alpha^{-j} \varphi_g \left\{ \infty \rightarrow -\frac{a}{p^j M} \right\} (P(p^j M z + a))\end{aligned}$$

where $\alpha = a_p(g)$.

5.2 p -adic integrals

If α is a unit, then the $\mu_{f,\alpha}$ is a measure, so we can integrate continuous functions against it using Riemann sums. On the other hand, $\mu_{f,\alpha}$ is generally not a measure if α is not a unit, so the error in estimating an integral by a Riemann sum cannot easily be bounded. Nonetheless, under the assumption that the additive valuation α is less than $k + 1$ (that is, $\nu(\alpha) < k - 1$), we can define an integral on the space of locally analytic functions. Let x_p denote the image in \mathbb{Z}_p of $x \in \mathbb{Z}_{p,M}$ via the canonical projection.

Definition 5.2. *A function F on $U \subseteq \mathbb{Z}_{p,M}$ is called locally analytic if U has a covering by subsets of the form $D(a, j) := a + p^j M \mathbb{Z}_{p,M}$ on which F has a convergent power series expansion*

$$F(x) = \sum_{n \geq 0} c_n (x - a)_p^n.$$

Assume that $\nu(\alpha) < k - 1$. In §11 of [17] (which follows Vishik [24] and Amice-Vélu [1]) the authors define an integration map, denoted

$$(U, F) \mapsto \int_U F \mu_{f,\alpha} \in \mathbb{C}_p,$$

for a compact open subset U of $\mathbb{Z}_{p,M}^\times$ and a locally analytic function F on U . Let \mathcal{O}_p denote the ring of integers of \mathbb{C}_p . The integral map is characterized by the following properties, assuming $(a, pM) = 1$ and $j \geq 1$:

- I. $\int_U F \mu_{f,\alpha}$ is linear in F and finitely additive in U .
- II. $\int_{D(a,j)} P(x_p) = \mu_{f,\alpha}(D(a,j); P)$ for P of degree $\leq k-2$
- III. $\int_{D(a,j)} (x-a)_p^n \in \left(\frac{p^n}{\alpha}\right)^j \alpha^{-1} \mathcal{O}_p$.
- IV. $\int_{D(a,j)} \sum_{n \geq 0} c_n (x-a)_p^n = \sum_{n \geq 0} \int_{D(a,j)} c_n (x-a)_p^n$ when the series converges.

The properties above can be used to estimate the value of an integral, by partitioning the region of integration into disks of small radius. This process involves the evaluation of an exponential number of terms, so is quite unwieldy for explicit calculations. Note that in the case where α is a p -adic unit, μ is a measure, so the two following conditions characterize the integral by the usual Riemann sum construction:

- I. $\int_U F \mu_{f,\alpha}$ is linear in F and finitely additive in U .
- II'. $\int_{D(a,j)} 1 = \mu_{f,\alpha}(D(a,j))$.

5.3 The p -adic L -function

A continuous group homomorphism

$$\chi : \mathbb{Z}_{p,M}^\times \rightarrow \mathbb{C}_p^\times$$

is called a p -adic character. The p -adic character χ is *primitive* if χ does not factor through $\mathbb{Z}_{p,M'}^*$ for any $M'|M$ (via the canonical surjection). For a primitive p -adic character χ , the p -adic L -function attached to f is defined as:

$$L_p(f, \alpha, \chi) := \int_{\mathbb{Z}_{p,M}^\times} \chi(x) d\mu_{f,\alpha}(x).$$

This integral is well-defined since a p -adic character is always locally analytic (as mentioned in §13 of [17]; analyticity will be proven in all cases where it is not obvious).

For $s \in \mathbb{Z}_p$, we also define

$$L_p(f, \alpha, \chi, s) := \int_{\mathbb{Z}_{p,M}^\times} \chi(x) \langle x_p \rangle^{s-1} d\mu_{f,\alpha}(x). \quad (5.1)$$

Here $\langle \cdot \rangle$ is the map from \mathbb{Z}_p to $1 + p\mathbb{Z}_p$ characterized by the equation

$$z = \omega(z) \langle z \rangle$$

with $\omega(z)$ being a $(p-1)^{\text{st}}$ root of unity. Note that ω is the usual Teichmüller character, which can be defined by $\omega(z) = \lim_{n \rightarrow \infty} z^{p^n}$. The Teichmüller character has period p . Now we must show that the integrand in equation (5.1) is locally analytic.

The character ω is constant on $a + p\mathbb{Z}_{p,M} = \omega(a) + p\mathbb{Z}_{p,M}$, so on this disk,

$$\begin{aligned} \log \langle x_p \rangle &= - \sum_{n=1}^{\infty} \frac{(1 - \langle x_p \rangle)^n}{n} = - \sum_{n=1}^{\infty} \frac{1}{n} \left(1 - \frac{x_p}{\omega(x_p)} \right)^n \\ &= \sum_{n=1}^{\infty} (-1)^{n-1} \frac{\omega(a)^{-n}}{n} (x_p - \omega(a))^n \end{aligned}$$

and thus $x \mapsto \log \langle x_p \rangle$ is locally analytic. It then follows, from simple approximations to the p -adic valuation of the factorial function, that the map

$$x \mapsto \langle x_p \rangle^{s-1} = \exp((s-1) \log \langle x_p \rangle) = \sum_{r=0}^{\infty} \frac{(s-1)^r}{r!} (\log \langle x_p \rangle)^r$$

is locally analytic for a fixed $s \in \mathbb{Z}_p$. It now follows from the properties described in §5.2 that for a Dirichlet character ψ of conductor $p^\nu M$:

$$L_p(f, \alpha, \psi, s) = \sum_{r=0}^{\infty} \frac{(s-1)^r}{r!} \sum_{a \bmod p^\nu M} \psi(a) \int_{D(a, \nu)} (\log_p(x_p))^r$$

and this can be calculated using those same properties. Additional details can be found in [24].

5.4 The p -adic L -series

There is an alternate representation of the Mazur-Swinnerton-Dyer p -adic L -function as a series. This representation will be used to state the p -adic analog of the Birch and Swinnerton-Dyer conjecture. Suppose ψ is a Dirichlet character of conductor $p^\nu M$, with $(p, M) = 1$. Let γ denote a topological generator for $1 + p\mathbb{Z}_p$ which is congruent to 1 modulo M . The \mathcal{L} -series is the function $\mathcal{L}(f, \alpha, \psi, T)$ satisfying

$$\mathcal{L}(f, \alpha, \psi, \gamma^{s-1} - 1) = L(f, \alpha, \psi, s).$$

So, by taking s satisfying $T := \gamma^{s-1} - 1$, we calculate that:

$$\begin{aligned} \mathcal{L}(f, \alpha, \psi, T) &:= \int_{\mathbb{Z}_{p,M}^\times} \psi(x) \langle x_p \rangle^{s-1} d\mu_{f,\alpha}(x) \\ &= \int_{\mathbb{Z}_{p,M}^\times} \psi(x) (1+T)^{\frac{\log_p \langle x_p \rangle}{\log_p(\gamma)}} d\mu_{f,\alpha}(x). \end{aligned}$$

This representation of the L -function has some advantages; for example, the following theorem simplifies the calculation of the coefficients of $\mathcal{L}(f, \alpha, \psi, T)$, in the case when α is a unit. Define ω_M to the map sending a to the element of $\mathbb{Z}_{p,M}$ congruent to the Teichmüller lift of a modulo p , and congruent to a modulo M .

Theorem 5.3. *If α is a p -adic unit, then $\mathcal{L}(f, \alpha, \psi, T)$ is equal to the limit of the sequence*

$$\sum_{a \bmod p^\nu M} \left(\psi(a) \sum_{j=0}^{p^{n-1}-1} \mu_{f,\alpha}(\omega_M(a)\gamma^j + p^n M\mathbb{Z}_{p,M}) \cdot (1+T)^j \right) \quad (5.2)$$

as $n \rightarrow \infty$, with term by term convergence.

Proof.

$$\begin{aligned} \mathcal{L}(f, \alpha, \psi, T) &= \int_{\mathbb{Z}_{p,M}^\times} \psi(x) (1+T)^{\frac{\log_p \langle x_p \rangle}{\log_p(\gamma)}} d\mu_{f,\alpha}(x) \\ &= \sum_{a \bmod p^\nu M} \psi(a) \int_{a+p^\nu M\mathbb{Z}_{p,M}} (1+T)^{\frac{\log_p \langle x_p \rangle}{\log_p(\gamma)}} d\mu_{f,\alpha}(x) \quad (5.3) \end{aligned}$$

Integrals against $\mu_{f,\alpha}$ can be estimated with Riemann sums since α is a unit. So we estimate the integral in equation (5.3) by taking sample points $\omega_M(a)\gamma^j \in \omega_M(a)\gamma^j + p^n M\mathbb{Z}_{p,M}$ for $j = 0, 1, \dots, p^{n-1} - 1$. These estimates give the polynomials in equation

(5.2), and thus the sequence converges to $\mathcal{L}(f, \alpha, \psi, T)$. The fact that there is term by term convergence follows from the calculations in §3 of [22]. \square

5.5 Interpolation properties

This section follows §14 of [17]. For a Dirichlet character ψ of conductor $m = p^\nu M$ and $1 \leq j \leq k - 1$, define:

$$e_p(\alpha, j, \psi) := \alpha^{-\nu} \left(1 - \frac{\bar{\psi}(p)\chi(p)p^{k-1-j}}{\alpha} \right) \left(1 - \frac{\psi(p)p^{j-1}}{\alpha} \right)$$

This is the *p-adic multiplier*. Note that $\chi(p)$ is 0 if $p|N$, and that $e_p = \alpha^{-\nu}$ if $\nu \geq 1$.

We then have:

Theorem 5.4. *Suppose ψ is a Dirichlet character of conductor $m=p^\nu M$. Take ψ_j to be the p-adic character defined by $\psi_j(x) = x_p^{j-1}\psi(x)$. Then for $1 \leq j \leq k - 1$, we have:*

$$L_p(f, \alpha, \psi_j) = e_p(\alpha, j, \psi) \frac{m^j}{(-2\pi i)^{j-1}} \frac{(j-1)!}{\tau(\bar{\psi})} L(f_{\bar{\psi}}, j).$$

Proof. This is proved in §14 of [17]. \square

Theorem 5.4 is consistent with the fact, mentioned in the introduction, that the *p*-adic *L*-function could be defined through interpolation of the critical values of the classical *L*-function. But to do so, the critical values need to be “smoothed” out *p*-adically first, a process which introduces the *p*-adic multiplier. This multiplier can vanish at certain points, which adds interesting new features to the formulation of the *p*-adic Birch and Swinnerton-Dyer conjecture. The general cases where it vanishes are covered in §15 of [17]. We will only be interested in the cases of significance to the Birch and Swinnerton-Dyer conjecture.

Theorem 5.5. *Assume that f is a newform attached to an elliptic curve E via the modularity theorem. Then the p -adic multiplier $e_p(\alpha, j, \psi)$ of f vanishes at $j = 1$ iff E has multiplicative reduction at p , and $\psi(p) = a_p$.*

Proof. Since f corresponds to an elliptic curve, the weight k of f must be 2 and the coefficients of f must be rational integers. Recall that the roots of Frobenius α, β associated to f satisfy $\alpha + \beta = a_p$ and $\alpha\beta = \chi(p)p^{k-1} = \chi(p)p$. It is clear then from the definition that the multiplier e_p vanishes (at $j = 1$) iff $\alpha = \psi(p)$ or $\bar{\psi}(p)\chi(p)$. Since $\alpha \neq 0$, this excludes the case $\psi(p) = 0$, so $|\psi(p)| = 1$. Also, when $\alpha = \psi(p)$ or $\bar{\psi}(p)\chi(p)$, the respective value of $\beta = \alpha^{-1} \cdot \chi(p)p$ will be $\bar{\psi}(p)\chi(p)p$ or $\psi(p)p$. Thus $a_p = \psi(p) + \bar{\psi}(p)\chi(p)p$ or $\bar{\psi}(p)\chi(p) + \psi(p)p$. If $\chi(p) \neq 0$, then $|a_p| \geq p - 1$ by the triangle inequality. But a theorem of Hasse (theorem 1.1 in [21]) tells us that $|a_p| \leq 2\sqrt{p}$, so $p - 1 \leq 2\sqrt{p}$, which contradicts the assumption that $p > 3$. Thus $\chi(p) = 0$, so $a_p = \psi(p)$ or $\psi(p)p$; Hasse's theorem excludes the latter case. Thus $a_p = \psi(p) = \pm 1$, since $\psi(p)$ must be a root of unity, and a_p is an integer. It follows from $a_p = \pm 1$ that E has multiplicative reduction modulo p . \square

5.6 Functional equation

Here we will suppose that f is a newform of (even) weight k for $\Gamma_0(N)$, with trivial character. In this case, for any $Q|N$ with $(Q, N/Q) = 1$, the newform f will be an eigenform for w_Q , and the eigenvalue will be denoted c_Q ; it must be ± 1 since w_Q is an involution (see §2.6.2). Then the Mazur-Swinnerton-Dyer p -adic L -function satisfies the following functional equation:

$$L_p(f, \alpha, \psi x_p^{\frac{k}{2}-1}, s) = \langle Q \rangle^{-s} (-1)^{\frac{k}{2}} \psi(-Q) c_Q L_p(f, \alpha, \psi x_p^{\frac{k}{2}-1}, 2-s)$$

for any quadratic character ψ . A more general form of this equation can be found in §17 of [17].

5.7 The p -adic Birch and Swinnerton-Dyer conjectures

As the paper by Mazur, Tate and Teitelbaum [17] explains, the p -adic analogue of the Birch and Swinnerton-Dyer conjecture has an added difficulty in the p -adic multiplier introduced in the previous section, which is not readily interpreted arithmetically. The p -adic multiplier can even vanish at the central point, thus requiring an important modification to the statement of the Birch and Swinnerton-Dyer conjecture. This “exceptional case” happens exactly when the curve has split multiplicative reduction at p . The statement of the p -adic Birch and Swinnerton-Dyer conjecture presented in this section is taken from [17], but in terms of the series in T introduced in section 5.4, as in [22].

Any elliptic curve E over \mathbb{C}_p with multiplicative reduction is isomorphic to a quotient of \mathbb{C}_p^\times by a discrete cyclic subgroup of infinite order. The Tate period q of E is a generator for that discrete subgroup.

Conjecture 5.6 (p -adic Birch and Swinnerton-Dyer conjecture). *If E has rank r , then the order of vanishing of $\mathcal{L}_p(E, T)$ at $T = 0$ is equal r , unless E has split multiplicative reduction, in which case the order of vanishing is $r + 1$. Furthermore, the leading term $\mathcal{L}^*(E, 0)$ of the series satisfies:*

$$\mathcal{L}^*(E, 0) = \frac{e_p(E)}{\log(\gamma)^r} \frac{\Omega_E \cdot \prod c_p \cdot |\Sha(E/\mathbb{Q})| \cdot \text{Reg}_p(E/\mathbb{Q})}{|E(\mathbb{Q})_{\text{torsion}}|^2}$$

unless the reduction is split multiplicative, in which case

$$\mathcal{L}^*(E, 0) = \frac{\mathcal{L}_p}{\log(\gamma)^{r+1}} \frac{\Omega_E \cdot \prod c_p \cdot |\text{III}(E/\mathbb{Q})| \cdot \text{Reg}_p(E/\mathbb{Q})}{|E(\mathbb{Q})_{\text{torsion}}|^2}$$

In these equations, $e_p(E) := e_p(f, 0, \psi_{\text{triv}})$ is the p -adic multiplier defined earlier.

Also, \mathcal{L}_p is the p -adic \mathcal{L} invariant of E , which is defined to be the ratio

$$\mathcal{L}_p = \frac{\log_p(q)}{\text{ord}_p(q)}$$

with q being the Tate period of E .

The quantities in the factorization are various arithmetic quantities related to the elliptic curve. The quantities $|\text{III}(E/\mathbb{Q})|$, c_p and $|E(\mathbb{Q})_{\text{torsion}}|$ appear in the classical conjecture as well.

5.8 Computational aspects

This section will outline a method for computing the p -adic L -functions. In principle, the Mazur-Swinnerton-Dyer p -adic L -function could be calculated from the definition; that is, the integral could be approximated by Riemann sums (when α is a unit). In practice, this computation is extremely slow. There is a faster method which is outlined in the paper “Overconvergent modular symbols and p -adic L -functions” ([19]) of Robert Pollack and Glenn Stevens. Their method will be summarized here. The idea of their method applies to calculating the Mazur-Kitagawa p -adic L -function as well.

Recall that

$$L_p(f, \alpha, \psi, s) := \int_{\mathbb{Z}_{p,M}^\times} \psi(x) \langle x_p \rangle^{s-1} d\mu_{f,\alpha}(x)$$

for a Dirichlet character ψ of conductor $p^j M$. If α is a unit, then we can estimate this integral with a Riemann sum, and the error is simple to bound since $\mu_{f,\alpha}$ is bounded. But to get an error term on the order of p^n , you need to take $p^n M$ sample points, and thus the calculation is very inefficient, and unsatisfying for purposes of verifying the p -adic Birch and Swinnerton-Dyer conjecture numerically.

5.8.1 Calculating with overconvergent modular forms

This section will summarize the method of Robert Pollack and Glenn Stevens in [19] for quickly computing with the p -adic L -function. Suppose $N = pM$, with $p \nmid M$. Let $\mathcal{A}(\mathbb{Z}_p)$ denote the space of locally analytic \mathbb{Q}_p -valued functions on \mathbb{Z}_p . A locally analytic distribution μ is a continuous \mathbb{Q}_p -linear functional on $\mathcal{A}(\mathbb{Z}_p)$; the value of μ at g is denoted $\int g d\mu$. The space of locally analytic distributions will be denoted $\mathcal{D}_k(\mathbb{Q}_p)$. The space $\mathcal{A}(\mathbb{Z}_p)$ is endowed with the weight k right action of $\mathrm{SL}_2(\mathbb{Z})$, defined by

$$g|_k \begin{bmatrix} a & b \\ c & d \end{bmatrix} = (cz + d)^{k-2} g \left(\frac{az + b}{cz + d} \right).$$

The distribution space $\mathcal{D}_k(\mathbb{Z}_p)$ inherits a weight k right action of $\mathrm{SL}_2(\mathbb{Z})$, defined by

$$\phi|_k \gamma(g) := \phi(g|_k \tilde{\gamma})$$

for $\phi \in \mathcal{D}_k(\mathbb{Z}_p)$ and $g \in \mathcal{A}(\mathbb{Z}_p)$. We define a specialization map to $V_k = V_k(\mathbb{Z}_p)$:

$$\rho_k : \mathcal{D}_k(\mathbb{Z}_p) \rightarrow V_k, \quad \rho_k(\mu)(P) = \int P(z, 1) d\mu.$$

This map can easily be seen to be equivariant under the action of $\mathrm{SL}_2(\mathbb{Z})$. There is an induced map on symbols:

$$\rho_{k,*} : \mathrm{Symb}_{\Gamma_0(N)}(\mathcal{D}_k(\mathbb{Z}_p)) \rightarrow \mathrm{Symb}_{\Gamma_0(N)}(V_k)$$

given by composition with ρ_k ; this map is also $\mathrm{SL}_2(\mathbb{Z})$ -equivariant. The equivariance of $\rho_{k,*}$ under $\mathrm{SL}_2(\mathbb{Z})$ implies Hecke-equivariance.

For a U_p -eigensymbol φ , the slope of U_p on φ is the p -adic valuation of the U_p -eigenvalue of φ . The essential ingredient to the method of Pollack and Stevens is the following:

Theorem 5.7. *The specialization map restricted to the subspace where U_p acts with slope strictly less than $k - 1$*

$$\mathrm{Symb}_{\Gamma_0(N)}(\mathcal{D}_k(\mathbb{Z}_p))^{(<k-1)} \longrightarrow \mathrm{Symb}_{\Gamma_0(N)}(V_k)^{(<k-1)}$$

is a Hecke-equivariant isomorphism.

An important obstacle in the efficient calculation of the p -adic L -function is that symbols in $\mathrm{Symb}_{\Gamma_0(N)}(V_k)$ only integrate polynomials of small degree. Thus integration of locally analytic functions involves taking Riemann sums with many sample points. On the other hand, symbols in $\mathrm{Symb}_{\Gamma_0(N)}(\mathcal{D}_k(\mathbb{Z}_p))$ integrate polynomials of arbitrary degree, and are thus well-suited for integrating locally analytic functions. Theorem 5.7 is essential since it ensures that the modular symbol φ_f attached to a weight k cusp form f can be lifted to an overconvergent modular symbol which produces the same integrals.

5.8.2 Solving the Manin relations

The next step is to describe an algorithm for lifting φ_f from $\text{Symb}_{\Gamma_0(N)}(V_k)$ to $\text{Symb}_{\Gamma_0(N)}(\mathcal{D}_k(\mathbb{Z}_p))$. To do so, we will continue with the ideas from section 3.2. To construct an overconvergent modular symbol, we need to solve the Manin relations in $\mathcal{D}_k(\mathbb{Z}_p)$. Recall the definition of a fundamental domain (section 2.2.1). An explicit description of Δ_0 as a $\Gamma_0(N)$ -module can be computed from a fundamental domain for $\Gamma_0(N)$. The complete description depends on the torsion elements in $\Gamma_0(N)$. For example, if $\Gamma_0(N)$ has no torsion, then Δ_0 has an especially simple presentation: the module Δ_0 is generated by a finite set of divisors:

$$D_1, \dots, D_t \in \Delta_0,$$

and there are matrices

$$\gamma_i \in \Gamma_0(N)$$

such that the only relation among the divisors is

$$\left(\left[\begin{array}{cc} 1 & -1 \\ 0 & 1 \end{array} \right] - 1 \right) D_\infty = \sum_{i=1}^t (1 - \gamma_i^{-1}) D_i.$$

The generators D_i correspond to the exterior edges of the fundamental domain, and the relationship among them is obtained by summing around the boundary. When $\Gamma_0(N)$ has torsion, the presentation for Δ_0 is slightly more complicated; details can be found in §2 and §3 of [19]. Once we have an explicit description of Δ_0 as a $\Gamma_0(N)$ -module, it becomes relatively simple to construct a symbol $\phi \in \text{Symb}_{\Gamma_0(N)}(V)$ for

any right $\mathbb{Z}_p[\Gamma_0(N)]$ -module V . We simply need to solve

$$v_\infty|\Delta = \sum_{i=1}^t v_i|(1 - \gamma_i),$$

with

$$\Delta = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} - 1.$$

Given such a solution, a symbol in $\text{Symb}_{\Gamma_0(N)}(V)$ is obtained simply by setting $\phi(D_i) = v_i$. Thus the only potential difficulty is in solving the “difference equation” $v_\infty|\Delta = w$. After that, it is simple to see that the equation relating the divisors is mapped to 0 by ϕ .

As for solving the difference equations in V , things work out well in the case of $\mathcal{D}_k(\mathbb{Z}_p)$. The space $\mathcal{D}_k(\mathbb{Z}_p)$ of locally analytic distributions has the nice property that an element is determined by its moments (that is, the values of the symbol at functions of the form z^j). This is true since the maps z^j (for non-negative integers j) span a dense subset of the space of locally analytic functions. So distributions in $\mathcal{D}_k(\mathbb{Z}_p)$ can be approximated by sums of elements of the form

$$\nu_j(z^r) := \begin{cases} 0 & \text{if } j \neq r \\ 1 & \text{if } j = r. \end{cases}$$

Fortunately, there is an explicit solution to the difference equation for the distributions ν_j : if we let

$$\eta_j(z^r) = \binom{r}{j} b_{r-j}$$

(with b_n being the n th Bernoulli number), then we get that

$$\frac{\eta_j|\Delta}{j+1} = \nu_{j+1}.$$

5.9 Computing the p -adic L -function

Now suppose f is an eigenform of non-critical slope (that is, slope $< k - 1$). The modular symbol $\phi_f \in \text{Symb}_{\Gamma_0(N)}(V_k)$ can be computed with linear algebra (as in [5]). Then we can take an arbitrary lift of ϕ_f to $\Psi \in \text{Symb}_{\Gamma_0(N)}(\mathcal{D}_k(\mathbb{Z}_p))$. Ideally the lift Ψ would be an eigensymbol, but this is unlikely to be the case. So we consider the sequence

$$\Psi_n := \frac{\Psi|U_p^n}{\lambda^n}$$

where λ is the U_p -eigenvalue of f . It is clear that Ψ_n also lifts $\phi_f \in \text{Symb}_{\Gamma_0(N)}(V_k)$ since the specialization map is Hecke-equivariant. The sequence of Ψ_n can be shown to converge, and the limit Φ of this sequence will have eigenvalue λ . Now in light of theorem 5.7, and since $\Phi|U_p \in \text{Symb}_{\Gamma_0(N)}(\mathcal{D}_k(\mathbb{Z}_p))^{(<k-1)}$ (since Φ has the same U_p -eigenvalue as f), Φ must be the form we are looking for. The L -function of f is then simply

$$L_p(f, s) = \Phi(\{\infty\} - \{0\})(\langle x \rangle^{s-1}).$$

The advantage of Pollack and Stevens's method is that is that the value of Φ on polynomials is explicitly computed. Thus locally analytic functions can be quickly integrated. With the Riemann sum method, the symbol ϕ_f had to be computed at many sample points, so the process takes many computations at each step. Furthermore, to increase precision, many times more sample points are needed. With

overconvergent modular symbols, computing Φ to more precision takes only slightly more time, but adds a few digits of precision to the answer.

CHAPTER 6

The Mazur-Kitagawa p -adic L -function

This chapter will outline the construction of a two variable p -adic L -function. This L -function was defined by Kitagawa [14] as a generalization of a construction of Mazur. The construction presented here is based on the approach of Greenberg and Stevens [10].

Suppose E is an elliptic curve, with f being the corresponding newform via the modularity theorem. The first part of this chapter will outline a construction of Hida that attaches to E a so called Λ -adic modular form; this is a formal power series expansion whose coefficients are p -adic analytic functions. At an integer value $k \geq 2$ which is p -adically close to the central point 2, the Hida family specializes to a cusp form of weight k , and at weight 2 we recover f . The L -functions of these specializations can be combined into a two variable p -adic L -function, called the Mazur-Kitagawa p -adic L -function. The ideas from the previous chapter can be adapted to provide an algorithm for calculating values of the Mazur-Kitagawa p -adic L -function.

The case of interest in this section corresponds to elliptic curves E of conductor $N = Mp$, with $\gcd(M, p) = 1$ (so E has multiplicative reduction at p). Recall from section 5.7 that the Birch and Swinnerton-Dyer conjecture for the Mazur-Swinnerton-Dyer p -adic L -function has an added complication in the so called “exceptional case”; that is, the order of vanishing is one more than the rank of the curve, and the leading

coefficient has an extra factor. Greenberg and Stevens [10] successfully used properties of the two variable L -function to prove results concerning this phenomenon. Namely, they proved the “exceptional zero conjecture” of Mazur, Tate and Teitelbaum.

In the paper “Hida families and rational points on elliptic curves” by Massimo Bertolini and Henri Darmon [3], the authors prove a result about an analogue of the Birch and Swinnerton-Dyer conjecture for the Mazur-Kitagawa p -adic L -function. Specifically, in the “exceptional case”, they give a formula for the leading coefficient of the L -function along the central line, in the case where the L -function does not vanish identically on the central line. Their formula holds for quadratic twists of the Mazur-Kitagawa p -adic L -function as well, but the method of proof does not have any obvious generalizations to twists by higher order characters. In this chapter, the results about the Mazur-Kitagawa p -adic L -function function will be summarized, and we will look at possible generalizations of the results of Bertolini and Darmon to twists by Dirichlet characters of order greater than 2.

6.1 Iwasawa algebras

Let

$$\tilde{\Lambda}(R) = R[[\mathbb{Z}_p^\times]] := \varprojlim R[(\mathbb{Z}/p^n\mathbb{Z})^\times], \quad \Lambda(R) = R[[(1 + p\mathbb{Z}_p)^\times]]$$

for a \mathbb{Z}_p -subalgebra $R \subseteq \mathbb{C}_p$. These are the *Iwasawa algebras*. The ring $\tilde{\Lambda}(R)$ can be described explicitly by

$$\tilde{\Lambda}(R) = \left\{ \sum_{u \in \mathbb{Z}_p^\times} c_u [u] \mid c_u \in R, \text{ with } \sum_{u \in \mathbb{Z}_p^\times} c_u \text{ convergent} \right\}.$$

Here convergence of

$$\sum_{u \in \mathbb{Z}_p^\times} c_u$$

is equivalent to the finiteness of $\{u : \nu(c_u) < K\}$ for all positive K (where ν is the additive p -adic valuation). The ring $\Lambda(R)$ embeds into $\tilde{\Lambda}(R)$ in the obvious way. When R is omitted, it is taken to be \mathbb{Z}_p by default; note then that $\tilde{\Lambda}(R) \cong \tilde{\Lambda} \otimes_{\mathbb{Z}_p} R$ and $\Lambda(R) \cong \Lambda \otimes_{\mathbb{Z}_p} R$.

We define the space

$$\mathcal{X} := \text{Hom}_{\text{cont}}(\tilde{\Lambda}, \mathbb{Z}_p) = \text{Hom}_{\text{group}}(\mathbb{Z}_p^\times, \mathbb{Z}_p^\times) \cong \frac{\mathbb{Z}}{(p-1)\mathbb{Z}} \times \mathbb{Z}_p.$$

The isomorphism here is given by associating to

$$s = (s_0, s_p) \in \frac{\mathbb{Z}}{(p-1)\mathbb{Z}} \times \mathbb{Z}_p$$

the homomorphism $x_s : \mathbb{Z}_p^\times \rightarrow \mathbb{Z}_p^\times$, given by

$$u \mapsto u^{s-2} := \omega(u)^{s_0-2} \langle u \rangle^{s_p-2}$$

where ω is the Teichmüller character and $\langle \cdot \rangle : \mathbb{Z}_p^\times \rightarrow 1 + p\mathbb{Z}_p$ is the projection to the principal units. The space \mathcal{X} is given the product topology, with $\frac{\mathbb{Z}}{(p-1)\mathbb{Z}}$ discrete. The set \mathbb{Z} of integers corresponds to a dense subset of \mathcal{X} by identifying $k \in \mathbb{Z}$ with (k, k) in the product; the corresponding homomorphism x_k is then given by $[t] \mapsto t^{k-2}$ for $t \in \mathbb{Z}_p^\times$. The map x_k on $\tilde{\Lambda}(\mathbb{Z}_p)$ (or more generally its extension to $\tilde{\Lambda}(R)$) will be referred to as the *weight k specialization map*.

The algebra $\tilde{\Lambda}(R)$ imbeds into the space of R -valued functions on \mathcal{X} in the natural way; associate to $\lambda \in \tilde{\Lambda}(\mathbb{Z}_p)$ the map $x \mapsto x(\lambda)$ for $x \in \mathcal{X}$ and extend the

constants to R . Explicitly,

$$c = \sum_{u \in \mathbb{Z}_p^\times} c_u [u] \in \tilde{\Lambda}(R)$$

gives rise to the function

$$s \mapsto x_s(c) = \sum_{u \in \mathbb{Z}_p^\times} c_u u^{s-2}$$

for $s \in \mathcal{X}$.

Let $\Lambda^\dagger(R)$ denote the set of power series in $s_p - 2$ with coefficients in a \mathbb{Z}_p -algebra R , which converge for s_p in some neighbourhood U around 2; here 2 is viewed as an element of \mathbb{Z}_p , which is identified with the slice $\{2\} \times \mathbb{Z}_p \subset \mathcal{X}$. The algebra $\Lambda(\mathbb{C}_p)$ imbeds into $\Lambda^\dagger(\mathbb{C}_p)$ by the rule $s \mapsto x_s$, since

$$\begin{aligned} \sum_{u \in 1+p\mathbb{Z}_p} c_u u^{s-2} &= \sum_{u \in 1+p\mathbb{Z}_p} c_u \exp((s_p - 2) \log_p(u)) \\ &= \sum_{u \in 1+p\mathbb{Z}_p} c_u \sum_{n \geq 0} \frac{(s_p - 2)^n \log_p(u)^n}{n!} \\ &= \sum_{n \geq 0} \left(\sum_{u \in 1+p\mathbb{Z}_p} c_u \log_p(u)^n \right) \frac{(s_p - 2)^n}{n!} \end{aligned}$$

which is convergent in a neighbourhood of 2 by basic estimates of the coefficients. Note that there is an analogous map $\tilde{\Lambda}(\mathbb{C}_p) \rightarrow \Lambda^\dagger(\mathbb{C}_p)$ as well, but it is not injective. For $k \in U$, we can define the map x_k on $\Lambda^\dagger(\mathbb{C}_p)$, which simply evaluates the series at $s_p - 2 = k - 2$; this is consistent with the map x_k that was defined on Λ , and will also be referred to as the weight k specialization map. For each ring introduced in this section, the kernel of the weight two specialization map x_2 will be referred to as the *augmentation ideal*. The following lemma gives an explicit generator for the augmentation ideal in $\Lambda(R)$:

Lemma 6.1. *Let $\lambda_k := [\gamma] - \gamma^{k-2}$, with γ a topological generator for $1 + p\mathbb{Z}_p$ (generally, γ will be taken to be $1 + p$). The following is an exact sequence of R -algebras:*

$$0 \rightarrow \Lambda(R) \xrightarrow{\lambda_k} \Lambda(R) \xrightarrow{x_k} R \rightarrow 0,$$

Proof. Take R to be \mathbb{Z}_p . There is no loss of generality since the above sequence can then be obtained by tensoring by R , which is flat. The inclusion $\Lambda(R) \hookrightarrow \Lambda^\dagger(\mathbb{C}_p)$ tells us that $\Lambda(R)$ is an integral domain, so λ_k is injective. The specialization map x_k is clearly surjective since $\Lambda(R)$ contains R . The composition $x_k \circ \lambda_k$ is zero since $x_k(\lambda_k) = \gamma^{k-2} - \gamma^{k-2} = 0$ and x_k is multiplicative. All that is left to show is that $\ker(x_k)$ is contained in the image of λ_k . Suppose $c \in \ker(x_k)$. Consider the reduction c_n of c to $R[1 + p(\mathbb{Z}/p^n\mathbb{Z})]$. The reduction γ_n of γ to $1 + p(\mathbb{Z}/p^n\mathbb{Z})$ generates this group, so

$$c_n = \sum_{e \bmod p^{n-1}} c_e [\gamma_n^e], \quad c_e \in R.$$

The element c is in the kernel of x_k , so

$$\sum_{e \bmod p^{n-1}} c_e \gamma^{e(k-2)} \equiv x_k(c) \equiv 0 \pmod{p^n},$$

so

$$c_n \equiv \sum_{e \bmod p^{n-1}} c_e ([\gamma_n]^e - \gamma^{e(k-2)}) \pmod{p^n}$$

and clearly $[\gamma_n] - \gamma^{k-2}$ divides each term in this sum modulo p^n . It then follows by a simple limit argument that λ_k divides c . \square

The motivation for working with Λ^\dagger is that it is *Henselian*; that is, the following version of Hensel's lemma holds:

Theorem 6.2 (Hensel's Lemma). *Take $g(x) \in \Lambda^\dagger[x]$, and let $g_2(x) \in \mathbb{C}_p[x]$ be its reduction via x_2 . For a simple root α_2 of $g_2(x)$ (i.e. with multiplicity 1), there exists a unique root $\alpha \in \Lambda^\dagger$ of $g(x)$ with $x_2(\alpha) = \alpha_2$.*

Proof. The fact that a root can be uniquely lifted to the ring of power series follows from the fact that the power series ring is a complete local ring. Thus all that is left to show is that the resulting lift has a positive radius of convergence. This fact follows from standard local analysis, and can be found in theorem 45.5 of [18]. \square

6.2 Hida family

The constructions in this section are based on the work of Hida [13]. They are outlined by Greenberg and Stevens in [10].

Theorem 6.3. *Given a normalized newform f of weight 2, there exists a unique formal expansion*

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

such that:

- Each $a_n(k)$ is an analytic function in a neighborhood U of $2 \in \mathcal{X}$ (which does not depend on n).
- $a_1(k) \equiv 1$
- For any positive integer $k \geq 2$ in U , the evaluation f_k of f_∞ at k is an eigenform of weight k .
- $f_2 = f$

The formal expansion f_∞ is called the Hida family attached to f .

See §2 of [10] for a more detailed description. The main construction of this chapter, namely the Mazur-Kitagawa p -adic L -function, is an L -function attached to the Hida family. The Mazur-Kitagawa p -adic L -function interpolates the Mazur-Swinnerton-Dyer p -adic L -function of the modular forms f_k for integers $k \geq 2$.

Recall from section 2.5 that the Hecke structure on the space of modular forms gives an alternate way of looking at modular forms. Given a space of cusp forms, the integration pairing map gives a Hecke-equivariant duality with a homology group. Thus, we could have simply looked at the Hecke operators acting on the homology, then *defined* an eigenform to be a formal q -expansion which encode the eigenvalues for an eigensymbol. The main idea in the construction of the Mazur-Kitagawa p -adic L -function is somewhat analogous, and will be outlined in this section.

In constructing the Hida family, a Λ -module on which the Hecke operators act Λ -linearly is defined. This Λ -module has the property that when taking the quotient with the subspace corresponding to the augmentation ideal, the result is a \mathbb{Z}_p -space that is Hecke-equivalent to a space of cusp forms. This allows us to lift a p -adic newform to a Λ -adic newform (though coefficients may need to be extended to Λ^\dagger first.)

The Λ -module is constructed as the homology of a projective system of Riemann surfaces. The resulting homology space is infinite dimensional, so a finite dimensional submodule is cut out first using Hida's projector to the ordinary part:

$$e_{\text{ord}} := \lim_{n \rightarrow \infty} U_p^{n!}.$$

(Recall the construction of §2.8 which used this operator.) Hida's projector will be essential to describing the L -function explicitly.

6.3 Measure-valued modular symbols

Let $L_* := \mathbb{Z}_p^2$, and let L'_* denote the vectors in L_* not divisible by p (the *primitive vectors*). Let $\mathfrak{C} = C(L'_*, \mathbb{C}_p)$ denote the space of continuous \mathbb{C}_p -valued functions on L'_* , with the sup norm. The group \mathbb{Z}_p^\times acts on L'_* by multiplication, which gives rise to an action on \mathfrak{C} :

$$[\lambda]F(x, y) := F(\lambda x, \lambda y)$$

which can be linearly extended to an action of $\tilde{\Lambda}$.

Let \mathbb{D}_* denote the \mathbb{C}_p -continuous dual of \mathfrak{C} ; this is the set of continuous homomorphisms from \mathfrak{C} to \mathbb{C}_p and is called the space of *measures* on \mathfrak{C} . For $F \in \mathfrak{C}$ and $\mu \in \mathbb{D}_*$, the value of μ at F is denoted

$$\int F d\mu.$$

Endow \mathbb{D}_* with the action of $\tilde{\Lambda}$ dual to the action on \mathfrak{C} . Explicitly,

$$\int F(x, y) d([\lambda]\mu) := \int F(\lambda x, \lambda y) d\mu.$$

For a subset $X \subseteq L'_*$ which is closed under multiplication by \mathbb{Z}_p^\times , let $\mathbf{1}_X$ denote the characteristic function of X . Then we define:

$$\int_X F d\mu := \int F \cdot \mathbf{1}_X d\mu.$$

There is a right action of $\mathrm{GL}_2(\mathbb{Z}_p)$ on \mathbb{D}_* defined by

$$\int Fd(\mu|\gamma) := \int F|\tilde{\gamma} d\mu,$$

so that

$$\int_X Fd(\mu|\gamma) = \int_{\tilde{\gamma}^{-1}X} F|\tilde{\gamma} d\mu = \int_{\gamma X} F|\tilde{\gamma} d\mu.$$

(The last line follows from the fact that X is closed under the action of \mathbb{Z}_p^\times , since $\tilde{\gamma}^{-1} = \det(\gamma)^{-1}\gamma$.) It is easy to check that the action of $\mathrm{GL}_2(\mathbb{Z}_p)$ commutes with that of $\tilde{\Lambda}$. The action of $\mathrm{GL}_2(\mathbb{Z}_p)$ also gives rise to an action of the Hecke operators, where for ℓ prime, T_ℓ acts as

$$\sum_{a \bmod \ell} \gamma_a + \chi(\ell)\gamma_\infty, \quad \gamma_a = \begin{bmatrix} 1 & a \\ 0 & \ell \end{bmatrix} \quad \text{for } a \in \mathbb{Z}, \quad \gamma_\infty = \begin{bmatrix} \ell & 0 \\ 0 & 1 \end{bmatrix},$$

with $\chi(\ell)$ being the trivial character modulo N .

6.3.1 Specialization maps

Recall that $V_k(\mathbb{C}_p)$ is defined to be the \mathbb{C}_p -dual to the space $\mathfrak{P}_k(\mathbb{C}_p)$ of homogeneous polynomials of degree $k - 2$ over \mathbb{C}_p . The homomorphism $x_k : \Lambda \rightarrow \mathbb{Z}_p$, $[u] \mapsto u^{k-2}$ defined in section 6.1 gives $V_k(\mathbb{C}_p)$ a Λ -module structure. Now define

$$\rho_k : \mathbb{D}_* \rightarrow V_k(\mathbb{C}_p)$$

by

$$\rho_k(\mu)(P) := \int_{\mathbb{Z}_p \times \mathbb{Z}_p^\times} P(x, y) d\mu(x, y).$$

This gives rise to a Λ -homomorphism

$$\rho_{k,*} : \text{Symb}_{\Gamma_0(M)}(\mathbb{D}_*) \rightarrow \text{Symb}_{\Gamma_0(N)}(V_k(\mathbb{C}_p))$$

by composition (i.e. $\rho_{k,*}(\phi) := \rho_k \circ \phi$). Notice that the level increases from M to N here (i.e. by a factor of p); thus the codomain is invariant under *fewer* matrices. The invariance under $\Gamma_0(N)$ is proven in the corollary to the following lemma. Let $\Gamma_0(\mathbb{Z}_p)$ denote the set of matrices in $\text{GL}_2(p\mathbb{Z}_p)$ that are upper triangular modulo p . The following lemma also implies that the specialization map is Hecke-equivariant; this is clear since the matrices used to define the Hecke operators are upper triangular.

Lemma 6.4. *The map $\rho_{k,*}$ is $\Gamma_0(\mathbb{Z}_p)$ -equivariant. That is,*

$$\rho_{k,*}(\phi|\gamma) = \rho_{k,*}(\phi)|\gamma$$

for $\phi \in \text{Symb}_{\Gamma_0(M)}(\mathbb{D}_*)$ and $\gamma \in \Gamma_0(p\mathbb{Z}_p)$.

Corollary 6.5. *For $\phi \in \text{Symb}_{\Gamma_0(M)}(\mathbb{D}_*)$ and $\gamma \in \Gamma_0(N)$,*

$$\rho_{k,*}(\phi)|\gamma = \rho_{k,*}(\phi).$$

Proof. for $\gamma \in \text{GL}_2(\mathbb{Z}_p)$ and $\phi \in \text{Symb}_{\Gamma_0(M)}(\mathbb{D}_*)$, we calculate:

$$\begin{aligned} \rho_k(\phi|\gamma)\{r \rightarrow s\}(P) &= \int_{\mathbb{Z}_p \times \mathbb{Z}_p^\times} Pd(\phi|\gamma)\{r \rightarrow s\} \\ &= \int_{\mathbb{Z}_p \times \mathbb{Z}_p^\times} Pd((\phi\{\gamma r \rightarrow \gamma s\})|\gamma) \\ &= \int_{\gamma(\mathbb{Z}_p \times \mathbb{Z}_p^\times)} P|\tilde{\gamma} d\phi\{\gamma r \rightarrow \gamma s\} \end{aligned}$$

and

$$(\rho_k(\phi)|\gamma)\{r \rightarrow s\}(P) = \int_{\mathbb{Z}_p \times \mathbb{Z}_p^\times} P|\tilde{\gamma} d\phi\{\gamma r \rightarrow \gamma s\}$$

so the desired equality follows from the fact that $\gamma(\mathbb{Z}_p \times \mathbb{Z}_p^\times) = \mathbb{Z}_p \times \mathbb{Z}_p^\times$ if γ is upper triangular modulo p . The corollary follows since $\Gamma_0(M) \cap \Gamma_0(p\mathbb{Z}_p) = \Gamma_0(N)$. \square

6.4 Defining properties

This section will outline the properties characterizing a measure used to define the Mazur-Kitagawa p -adic L -function. Define

$$\mathbb{D}_*^\dagger := \mathbb{D}_* \otimes_{\Lambda(\mathbb{C}_p)} \Lambda^\dagger$$

For $\mu = \lambda_1\mu_1 + \dots + \lambda_t\mu_t \in \mathbb{D}_*^\dagger$, with $\lambda_j \in \Lambda^\dagger$ and $\mu_j \in \mathbb{D}_*$, we say U_μ is a *neighbourhood of regularity* for μ if all the λ_j converge on U_μ . Let $\Lambda^\dagger(U)$ be the submodule of Λ^\dagger which converges on U . Define

$$\mathbb{D}_*^\dagger(U) := \mathbb{D}_* \otimes_{\Lambda(\mathbb{C}_p)} \Lambda^\dagger(U)$$

to be the $\Lambda(\mathbb{C}_p)$ -submodule of \mathbb{D}_*^\dagger for which U is a neighbourhood of regularity.

For an integer k , let \mathfrak{C}_k denote the $\Lambda(\mathbb{C}_p)$ -submodule of \mathfrak{C} on which $\Lambda(\mathbb{C}_p)$ acts via x_k (this is equivalently defined as the space of homogeneous functions of degree $k - 2$). Note that \mathfrak{P}_k imbeds into \mathfrak{C}_k . If k is in U , we can integrate functions in \mathfrak{C}_k against an element of $\mathbb{D}_*^\dagger(U)$; this integration map is obtained by tensoring the integration map $\int : \mathbb{D}_* \rightarrow \text{Hom}_{cont}(\mathfrak{C}_k, \mathbb{C}_p)$ with the map x_k . Explicitly,

$$\int_X F d\mu = \lambda_1(k) \int_X F d\mu_1 + \dots + \lambda_t(k) \int_X F d\mu_t$$

for $\mu = \lambda_1\mu_1 + \dots + \lambda_t\mu_t$, with $\lambda_j \in \Lambda^\dagger$, $\mu_j \in \mathbb{D}_*$ and $F \in \mathfrak{C}_k$. Note that the codomain of this integration map is $\mathbb{C}_p \otimes_{\Lambda(\mathbb{C}_p)} \mathbb{C}_p$ which is canonically isomorphic to \mathbb{C}_p .

Now we define

$$\mathrm{Symb}_{\Gamma_0(M)}(\mathbb{D}_*)^\dagger := \mathrm{Symb}_{\Gamma_0(M)}(\mathbb{D}_*) \otimes_{\Lambda(\mathbb{C}_p)} \Lambda^\dagger$$

Again, the specialization maps extend:

$$\rho_{k,*}^\dagger := \rho_{k,*} \otimes x_k$$

and the codomain of this map is canonically isomorphic to $\mathrm{Symb}_{\Gamma_0(N)}(V_k(\mathbb{C}_p))$. When there is no danger of confusion, ρ_k , $\rho_{k,*}$ and $\rho_{k,*}^\dagger$ will all be denoted ρ_k .

6.4.1 Ordinary part

The space $\mathrm{Symb}_{\Gamma_0(M)}(\mathbb{D}_*)$ is possibly infinite dimensional as a Λ -module. It is useful here, as in the construction of the Hida family, to restrict our attention to a finite dimensional subspace. We use the same operator (Hida's projector to the ordinary part):

$$e_{\mathrm{ord}} = \lim_{n \rightarrow \infty} U_p^{n!}$$

to define

$$\mathrm{Symb}_{\Gamma_0(M)}^{\mathrm{ord}}(\mathbb{D}_*) := e_{\mathrm{ord}} \mathrm{Symb}_{\Gamma_0(M)}(\mathbb{D}_*).$$

It follows from proposition 6.1 of [10] that this is a free module of finite rank over Λ .

Recall section 2.8; we will now consider the space

$$\mathrm{Symb}_{\Gamma_0(N)}^{\mathrm{ord}}(V_k(\mathbb{C}_p)) = e_{\mathrm{ord}} \mathrm{Symb}_{\Gamma_0(N)}(V_k(\mathbb{C}_p)).$$

The following theorem (corollary 3.7.3 in [11]) gives a property that we will use to lift an ordinary symbol from $\text{Symb}_{\Gamma_0(N)}(V_k(\mathbb{C}_p))$ to $\text{Symb}_{\Gamma_0(M)}(\mathbb{D}_*)$ via ρ_k . Take a topological generator γ of \mathbb{Z}_p^\times . Let $\pi_k := [\gamma] - \gamma^{k-2} \in \tilde{\Lambda}$; this element is a topological generator for the kernel of x_k .

Theorem 6.6. *The sequence*

$$0 \rightarrow \text{Symb}_{\Gamma_0(M)}^{\text{ord}}(\mathbb{D}_*) \xrightarrow{\pi_k} \text{Symb}_{\Gamma_0(M)}^{\text{ord}}(\mathbb{D}_*) \xrightarrow{\rho_{k,*}} \text{Symb}_{\Gamma_0(N)}^{\text{ord}}(V_k(\mathbb{C}_p)) \rightarrow 0$$

is exact.

Now consider the action of the element $[\zeta]$ on $\text{Symb}_{\Gamma_0(M)}^{\text{ord}}(\mathbb{D}_*)$, where $\zeta \in \mathbb{Z}_p^\times$ is a primitive $(p-1)$ st root of unity. For r modulo $p-1$, take $\text{Symb}_{\Gamma_0(M)}^{\text{ord}}(\mathbb{D}_*)_r$ to be the ζ^r -eigensubmodule of $\text{Symb}_{\Gamma_0(M)}^{\text{ord}}(\mathbb{D}_*)$. The previous theorem is then made more specific, with $\lambda_k := [1+p] - (1+p)^{k-2}$ (note that $1+p$ could be replaced with any topological generator for $1+p\mathbb{Z}_p$):

Theorem 6.7. *The sequence of Λ -modules*

$$0 \rightarrow \text{Symb}_{\Gamma_0(M)}^{\text{ord}}(\mathbb{D}_*)_{k-2} \xrightarrow{\lambda_k} \text{Symb}_{\Gamma_0(M)}^{\text{ord}}(\mathbb{D}_*)_{k-2} \xrightarrow{\rho_{k,*}} \text{Symb}_{\Gamma_0(N)}^{\text{ord}}(V_k(\mathbb{C}_p)) \rightarrow 0$$

is exact. In particular $\text{Symb}_{\Gamma_0(M)}^{\text{ord}}(\mathbb{D}_)_{k-2}$ is a free Λ -module of rank equal to the \mathbb{Z}_p rank of $\text{Symb}_{\Gamma_0(N)}^{\text{ord}}(V_k(\mathbb{C}_p))$.*

This is corollary 3.7.4 of the same paper. Compare this to lemma 6.1. We can already use this to lift ϕ_f to $\text{Symb}_{\Gamma_0(M)}^{\text{ord}}(\mathbb{D}_*)$, but the resulting lift is not necessarily an eigensymbol for the Hecke operators. The space

$$\text{Symb}_{\Gamma_0(M)}^{\text{ord}}(\mathbb{D}_*)^\dagger := \text{Symb}_{\Gamma_0(M)}^{\text{ord}}(\mathbb{D}_*) \otimes_{\Lambda(\mathbb{C}_p)} \Lambda^\dagger$$

will allow us to find an eigensymbol lifting ϕ_f .

6.4.2 The symbol μ_*

The next step in defining the Mazur-Kitagawa p -adic L -function is to lift the eigensymbol ϕ_f to an eigensymbol in $\text{Symb}_{\Gamma_0(M)}^{\text{ord}}(\mathbb{D}_*)_{k-2}$. Consider the Hecke $\Lambda(\mathbb{C}_p)$ -algebra $\mathbb{T}_{*,k-2}^{\text{ord}}$ generated by the Hecke operators acting on $\text{Symb}_{\Gamma_0(M)}^{\text{ord}}(\mathbb{D}_*)_{k-2}$. From theorem 6.7, the quotient of $\mathbb{T}_{*,k-2}^{\text{ord}}$ by $\lambda_k \mathbb{T}_{*,k-2}^{\text{ord}}$ gives the \mathbb{C}_p -Hecke algebra acting on $\text{Symb}_{\Gamma_0(N)}^{\text{ord}}(V_k(\mathbb{C}_p))$ (denoted $\mathbb{T}_{k-2}^{\text{ord}}$). Now take an eigensymbol $g \in \text{Symb}_{\Gamma_0(N)}^{\text{ord}}(V_k(\mathbb{C}_p))$. This gives a homomorphism $\eta : \mathbb{T}_{k-2}^{\text{ord}} \rightarrow \mathbb{C}_p$ which is defined by $T_n \mapsto a_n(g)$. We would like to lift η to a homomorphism $\mathbb{T}_{*,k-2}^{\text{ord}} \rightarrow \Lambda(\mathbb{C}_p)$. Unfortunately, this might not be possible, but if we first tensor the sequence in theorem 6.7 by Λ^\dagger , we can use the Henselian property (theorem 6.2) to get the desired result. That is, we can lift $\eta : \mathbb{T}_{k-2}^{\text{ord}} \rightarrow \mathbb{C}_p$ to a map $\eta_\infty : \mathbb{T}_{*,k-2}^{\text{ord}}{}^\dagger \rightarrow \Lambda^\dagger$. In fact, this is the Hida family attached to g ; that is, the Hida family is the formal expansion

$$\sum_{n \geq 1} \eta_\infty(T_n) q^n.$$

Furthermore, $\mathbb{T}_{*,k-2}^{\text{ord}}{}^\dagger$ is the Hecke algebra acting on $\text{Symb}_{\Gamma_0(M)}^{\text{ord}}(\mathbb{D}_*)^\dagger$, and we can find an eigensymbol corresponding to this homomorphism η_∞ . This discussion gives the following essential result:

Theorem 6.8. *There exists a neighborhood U of $2 \in \mathcal{X}$ and a measure-valued symbol $\mu_* \in \text{Symb}_{\Gamma_0(M)}^{\text{ord}}(\mathbb{D}_*)^\dagger$ which is regular on U , and for all $k \in U \cap \mathbb{Z}^{\geq 2}$, there exists a scalar $\lambda(k) \in \mathbb{C}_p$ such that*

$$\rho_k(\mu_*) = \lambda(k) \phi_{f_k}$$

with $\lambda(2) = 1$, so in particular,

$$\rho_2(\mu_*) = \phi_f.$$

Further, μ_* is a Hecke-eigensymbol.

6.5 The Mazur-Kitagawa p -adic L -function

Given a primitive Dirichlet character χ of conductor m , set the sign at infinity w_∞ to $\chi(-1)$, and define the Mazur-Kitagawa p -adic L -function to be:

$$L_p(f_\infty, \chi, k, s) = \sum_{a=1}^m \chi(ap) \int_{\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times} \left(x - \frac{pa}{m}y\right)^{s-1} y^{k-s-1} d\mu_* \left\{ \infty \rightarrow \frac{pa}{m} \right\} \quad (6.1)$$

for $(k, s) \in U \times \mathcal{X}$, where U is the neighborhood of 2 over which μ_* is defined. The Mazur-Kitagawa p -adic L -function satisfies the following properties:

Theorem 6.9. *The weight k specialization of the Mazur-Kitagawa p -adic L -function is*

$$L_p(f_\infty, \chi, k, s) = \lambda(k) L_p(f_k, \chi, s).$$

Theorem 6.10. *Suppose c is the w_N -eigenvalue of f , and take χ to be a primitive Dirichlet character satisfying $\chi(-1) = w_\infty$. Suppose further that $(p, N) = 1$. Then the Mazur-Kitagawa p -adic L -function satisfies the following functional equation:*

$$L_p(f_\infty, \chi, k, s) = -c \chi^{-1}(-N) \langle -N \rangle^{\frac{k}{2}-s} L_p(f_\infty, \chi^{-1}, k, k-s),$$

where $\langle a \rangle = \omega(a)^{-1}a$.

Proof. This follows from theorem 5.17 of [10]. □

6.6 The exceptional zero conjecture

Suppose the elliptic curve E has split multiplicative reduction at p . Recall then, from theorem 5.5, that we are in the “exceptional case” of Mazur, Tate and Teitelbaum [17]. In this case, the sign ϵ_p in the functional equation for $L_p(E, s)$ is the opposite of the sign ϵ_∞ in the functional equation for $L(E, s)$; thus the orders of vanishing have different parity. The p -adic Birch and Swinnerton-Dyer conjecture (conjecture 5.6) predicts that the order of vanishing of the Mazur-Swinnerton-Dyer p -adic L -function at the central point will be one greater than the rank of E . Furthermore, Mazur, Tate and Teitelbaum empirically conjectured that when E has rank 0,

$$\frac{d}{ds}L_p(E, s)_{s=1} = \mathcal{L}_p \cdot \frac{L(E, 1)}{\Omega_E}, \quad (6.2)$$

with

$$\mathcal{L}_p = \frac{\log_p(q)}{\text{ord}_p(q)}$$

and with q being the Tate period of E . Greenberg and Stevens found an elegant proof of this “exceptional zero conjecture”, which appears in [10]. Their proof relies on properties of the Mazur-Kitagawa p -adic L -function, and will be outlined here. First suppose that $\epsilon_\infty = -1$. Then the functional equation implies that $L(E, 1) = 0$. Also, $\epsilon_p = 1$, so $L_p(E, 1)$ vanishes to even order. But the interpolation formulas imply that $L_p(E, 1) = 0$, so the order of vanishing is at least 2; thus both sides of equation (6.2) are 0. In the case $\epsilon_\infty = 1$, we have $\epsilon_p = -1$, so the Mazur-Kitagawa p -adic L -function $L(E, k, s)$ vanishes identically along the central line $s = \frac{k}{2}$. Thus

$$\frac{\partial}{\partial s}L_p(E, 2, 1) = -2\frac{\partial}{\partial k}L_p(E, 2, 1).$$

This equation allows us to study the leading term of the one variable L -function by analyzing the behavior of the two variable L -function restricted to the line $s = 1$. The authors then use a factorization formula for the restriction $L_p(E, k, 1)$ to establish the exceptional zero conjecture.

6.7 The Birch and Swinnerton-Dyer conjecture in two variables

Suppose E is an elliptic curve of conductor N , with $p \parallel N$ so that E has multiplicative reduction at p . Suppose χ is a quadratic Dirichlet character of conductor m . Suppose $\chi(p) = a_p$, so that there is an exceptional zero. Now we restrict our attention to the critical line $s = \frac{k}{2}$. There are two cases, corresponding to the sign ϵ_∞ of the functional equation for the classical L -function. Since we are in the exceptional case, the sign in the functional equation for the p -adic L -functions is $-\epsilon_\infty$. So if $\epsilon_\infty = -1$, the classical L -function has odd order of vanishing at the central point, so $L(E, 1) = 0$, and thus the classical Birch and Swinnerton-Dyer conjecture predicts the existence of a point of infinite order on $E(\mathbb{Q})$. Also, in the case $\epsilon_\infty = -1$, the functional equation for $L_p(E, k, s)$ has sign 1, so this p -adic L -function need not vanish on the central line. Greenberg and Stevens [10] show that $L_p(E, k, k/2)$ vanishes to order at least 2 at $k = 2$ in this non-vanishing case. Thus it is of interest to look at the “leading term”; that is, the value of the second derivative of $L_p(E, k, k/2)$ at $k = 2$. Bertolini and Darmon [3] proved that

Theorem 6.11. *There is a point P on $E(\mathbb{Q}) \otimes \mathbb{Q}$ and a rational number $l \in \mathbb{Q}^\times$ such that*

$$\frac{d^2}{dk^2} L_p(E, k, k/2)_{k=2} = l \cdot \log_E(P)^2.$$

Where \log_E is the linear extension of the formal group logarithm of E . Furthermore, the authors proved the following more general case:

Theorem 6.12. *Suppose that E is a rational elliptic curve of conductor N , and χ is a quadratic Dirichlet character of conductor D prime to N . Assume that $\chi(p) = a_p$, so that we are in the case of an exceptional zero. Assume further that $\chi(-N) = w_N$, where w_N is the eigenvalue of the newform associated to E under the Atkin-Lehner operator. Lastly, assume that E has two distinct primes of semistable reduction. Then*

- $L_p(E, \chi, k, \frac{k}{2})$ vanishes to order at least 2 at $k = 2$.
- There is a point P in $(E(\mathbb{Q}(\sqrt{D})) \otimes \mathbb{Q})^\times$ and a rational number $\ell \in \mathbb{Q}^\times$ such that

$$\frac{d^2}{dk^2} L_p(E, \chi, k, k/2)_{k=2} = \ell \cdot \log_E(P)^2.$$

Following the form of the theorem 6.12, and considering the form of the twisted Birch and Swinnerton-Dyer conjectures (see §4.7), I conjecture:

Conjecture 6.13. *Suppose χ is a cubic Dirichlet character with conductor m such that $\chi(p) = a_p = 1$, so that there is an exceptional zero. Suppose further that the order of vanishing of $L_p(E, \chi, k, k/2)$ at $k = 2$ is at least 2. Let F denote the cubic subfield of $\mathbb{Q}(\zeta_m)$ cut out by $\ker(\chi)$. Then there is a point P on $(E(\mathbb{Q}(F)) \otimes \mathbb{Q}(\chi))^\times$ and $\ell \in \mathbb{Q}(\chi)^\times$ such that*

$$\frac{d^2}{dk^2} L_p(E, \chi, k, k/2)_{k=2} = \ell \cdot \log_E(P) \cdot \log_E(\bar{P}),$$

where \bar{P} denotes the image of P under complex conjugation on the $\mathbb{Q}(\chi)$ -coefficients.

Note that $\bar{P} \in (E(\mathbb{Q}(F)) \otimes \mathbb{Q}(\chi))^{x^{-1}}$. The motivation for including this second point in this statement comes from the functional equation:

$$L_p(f_\infty, \chi, k, k/2) = -c \chi^{-1}(-N) L_p(f_\infty, \chi^{-1}, k, k/2).$$

By comparing leading terms in the expansion around $k = 2$, it seems most natural that the form of conjecture 6.13 should be symmetric in P and \bar{P} .

6.8 Continuing work

The methods of section 5.8 are well suited for doing the calculations with the Mazur-Kitagawa p -adic L -function. It would be interesting to implement the ideas of this section on a computer to test Conjecture 6.13. If numerical computations supported Conjecture 6.13, then it would be interesting to generalize the conjecture in a direction similar to the conjectures of Kisilevsky and Fearnley [8].

References

- [1] Y. Amice and J. Velu. Distributions p -adiques associees aux series de Hecke. *Asterisque*, 24/25:119–131, 1975.
- [2] A.O.L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Mathematische Annalen*, 185:134–160, 1970.
- [3] M. Bertolini and H. Darmon. Hida families and rational points on elliptic curves. *Inventiones Mathematicae*, 168:371–431, 2007.
- [4] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over \mathbb{Q} : Wild 3-adic exercises. *Journal of the American Mathematical Society*, 14(4):843–939, 2001.
- [5] J. E. Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, 1997.
- [6] H. Darmon. A proof of the full Shimura-Taniyama-Weil conjecture is announced. *Notices of the AMS*, 46:1397–1401, 11.
- [7] F. Diamond and J. Shurman. *A First Course in Modular Forms*. Springer, 2005.
- [8] J. Fearnley and H. Kisilevsky. Critical values of derivatives of twisted elliptic L -functions. To appear in *Experimental Mathematics*.
- [9] J. Fearnley and H. Kisilevsky. Critical values of higher derivatives of twisted elliptic L -functions. Preprint.
- [10] R. Greenberg and G. Stevens. p -adic L -functions and p -adic periods of modular forms. *Inventiones Mathematicae*, 111:407–447, 1993.
- [11] R. Greenberg and G. Stevens. On the conjecture of Mazur, Tate, and Teitelbaum. *Contemporary Mathematics*, 165:183–211, 1994.
- [12] K. Hatada. Periods of primitive forms. *Proc. Japan Acad.*, 53(A), 1977.

- [13] H. Hida. Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms. *Inventiones Mathematicae*, 85:545–613, 1986.
- [14] K. Kitagawa. On standard p -adic L -functions of families of elliptic cusp forms. In *p -adic monodromy and the Birch and Swinnerton-Dyer conjecture*, pages 81–110. American Mathematical Society, 1994.
- [15] A. W. Knapp. *Elliptic Curves*. Princeton University Press, 1992.
- [16] B. Mazur and P. Swinnerton-Dyer. Arithmetic of weil curves. *Inventiones Mathematicae*, 25:1–61, 1974.
- [17] B. Mazur, J. Tate, and J. Teitelbaum. On p -adic analogues of the conjectures of Birch and Swinnerton-Dyer. *Inventiones Mathematicae*, 84:1–48, 1986.
- [18] M. Nagata. *Local Rings*. John Wiley & Sons, 1962.
- [19] R. Pollack and G. Stevens. Overconvergent modular symbols and p -adic L -functions. preprint, available at: <http://math.bu.edu/people/rpollack>.
- [20] J. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, 1994.
- [21] J. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 2009.
- [22] W. Stein and C. Wüthrich. Computations about Tate-Shafarevich groups using Iwasawa theory.
- [23] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *The Annals of Mathematics*, 141:553–572, 1995.
- [24] M. Vishik. Nonarchimedean measures connected with Dirichlet series. *Math. USSR Sb.*, 28:216–228, 1976.
- [25] L. C. Washington. *Introduction to Cyclotomic Fields*. Springer-Verlag, 1982.
- [26] A. Wiles. The Birch and Swinnerton-Dyer conjecture. The Clay Mathematics Institute’s official millennium problem description.
- [27] A. Wiles. Modular elliptic curves and Fermat’s Last Theorem. *Annals of Mathematics*, 141:443–551, 1995.

- [28] D. Zagier. Elliptic modular forms and their applications. In *The 1-2-3 of Modular Forms*.