p-adic L-functions

&

Overconvergent Modular Symbols

by

Berke Noyan Karagöz

A Dissertation Submitted to the
Graduate School of Sciences and Engineering
in Partial Fulfillment of the Requirements for
the Degree of

Master of Science

in

Mathematics

KOÇ UNIVERSITY

August 5, 2017

p-adic L-functions

&

Overconvergent Modular Symbols

Koç University

Graduate School of Sciences and Engineering

This is to certify that I have examined this copy of a master's thesis by

Berke Noyan Karagöz

and have found that it is complete and satisfactory in all respects,

and that any and all revisions required by the final

examining committee have been made.

Committee Members:

Assoc. Prof. Kâzım Büyükboduk

Prof. Varga K. Kalantarov

Prof. K. İlhan İkeda

Date:

To life

ABSTRACT

In *Chapter 1*, we introduce the p-adic L-function of *Amice & Velu* and *Vishik* associated to an eigenform f. We give an explicit construction of the underlying h-admissible distribution and discuss in detail the analyticity and interpolation properties the L-function satisfies. We then study *Stevens'* space of overconvergent modular symbols in *Chapter 2* and ultimately link the two discussions together via a theorem in the final section.

ÖZETÇE

Bölüm 1'de, *Amice & Velu* ve *Vishik*'in bir özform f ile ilişkili p-adik L-fonksiyonunu tanıttık. Altta yatan h-kabul edilebilir dağılımı açıkça yapılandırdık ve L-fonksiyonunun tatmin ettiği analitiklik ve enterpolasyon özelliklerini ayrıntılı olarak tartıştık. Daha sonra *Bölüm 2*'de, *Stevens*'ın aşırı yakınsak modüler sembolleri alanına geçtik ve sonunda iki tartışmayı son altbölümde bir teorem aracılığıyla birleştirdik.

ACKNOWLEDGMENTS

I thank with utmost gratitude to my advisor Kâzım Büyükboduk – none of this would have existed without him. His willingness in sharing his passion and his confidence in vesting his trust have been paramount throughout my journey. I am thankful and forever indebted.

I feel deeply grateful towards all past and present members of the Koç mathematics faculty for the altruism they showed in dedicating their time and support. The value and extent of their contributions cannot ever be overstated.

I wish to thank everybody at Koç for making me feel at home during all the times home felt like an emotion nowhere else to be found within a thousand miles. I have nothing but the best feelings for all of them.

To my entire family I thank from the deepest depths of my heart, for their unconditional love and selfless efforts are on what I today exist. Without them, I would have been nowhere.

To friends, past and present: For all the timeless memories, I am thankful.

To Enis, for his companionship throughout my graduate years at Koç: Thank you.

To Ian, for his invaluable counsel, and to Leo, for his everlasting aid: Thank you.

To Sven, in whose mere existence I find joy and solace: Zhank you.

TABLE OF CONTENTS

Chapter 0

Introduction

Conjecture 0.1. ($\mathbf{BSD}_\infty$) *Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$. Let r_{an} denote the order of vanishing of the complex L-series of E at $s = 1$ and r_{alg} the $\mathbb{Z}$-rank of $E(\mathbb{Q})$. Then,*

(i) $r_{an} = r_{alg}$

(ii) $L^*_\infty(E, s) = \dfrac{\prod_v c_v \cdot \Omega_E \cdot \#\text{Ш}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tor})^2} \cdot \mathrm{Reg}_\infty(E/\mathbb{Q})$

where $L^*_\infty(E, s)$ is the leading non-zero coefficient of $L_\infty(E, s)$ expanded at $s = 1$.

This is the *Birch and Swinnerton-Dyer Conjecture*, as formulated by *Tate.* The conjecture relates arithmetic invariants of an elliptic curve $E/\mathbb{Q}$ to its complex-analytic *Hasse-Weil* L-function $L_\infty(E, s)$ and a p-adic analogue in the same spirit had been long sought after, beginning with *Mazur, Tate and Teitelbaum.* A naïve yet inviting attempt at formulating a p-adic version of the conjecture would be to replace all complex analytic objects appearing in the statement with avatars of their putative counterparts living in the p-adic realm, which would look like:

pseudo-Conjecture 0.2. (**pseudo-BSD**$_p$) *Let $E/\mathbb{Q}$ be an elliptic curve and p a prime. Let r_{an} denote the order of vanishing of the p-adic L-series of E at $s = 1$ and r_{alg} the $\mathbb{Z}$-rank of $E(\mathbb{Q})$. Then,*

(i) $r_{an} = r_{alg}$

(ii) $L^*_p(E, s) = \dfrac{\prod_v c_v \cdot \Omega_E \cdot \#\text{Ш}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tor})^2} \cdot \mathrm{Reg}_p(E/\mathbb{Q})$

where $L_p^*(E,s)$ *is the leading non-zero coefficient of* $L_p(E,s)$ *expanded at* $s=1$.

Voila! A p-adic version of the conjecture $\boldsymbol{BSD}_\infty$, albeit with a caveat: It makes no-sense; *a priori*. The p-adic L-function L_p is *non-défini*, so is the p-adic regulator Reg_p. A long list of virtuoso mathematicians have been involved in the quest of rigorously defining these objects, with an essential history of:

- *Mazur & Swinnerton-Dyer* defined the p-adic L-function L_p for a good ordinary prime p. [MSD74]

- *Amice & Velu* and *Vishik* extended the definition of the p-adic L-function to supersingular primes. [AV75] & [Vis76]

- *Mazur, Tate & Teitelbaum* gave a definition for the p-adic regulator R_p for an ordinary prime p. [MTT86]

- *Perrin-Riou, Bernardi & Perrin-Riou* extended the definition of the p-adic regulator to supersingular primes. [BPR93] & [PR93]

These efforts culminate in the following precise statement of a *bona fide* p-adic BSD conjecture:

Conjecture 0.3. $\left(\mathbf{BSD}_p\right)$ *(Mazur, Tate and Teitelbaum, Bernardi and Perrin-Riou) Let* $E/\mathbb{Q}$ *be an elliptic curve and* p *a prime of good reduction. Let* r_{an} *denote the order of vanishing of* $L_{p,\alpha}(E,s)$ *at* $s=1$ *and* r_{alg} *the* $\mathbb{Z}$*-rank of* $E(\mathbb{Q})$*. Then,*

(i) $r_{an} = r_{alg}$

(ii) $L_{p,\alpha}^*(E,s) = \epsilon_{p,\alpha} \cdot \dfrac{\prod_v c_v \cdot \#Ш(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tor})^2} \cdot \mathrm{Reg}_{p,\alpha}(E/\mathbb{Q})$

where $L_{p,\alpha}^*(E,s)$ *is the leading non-zero coefficient of* $L_{p,\alpha}(E,s)$*,* α *an 'allowable root' and* $\epsilon_{p,\alpha} = \left(1-\alpha^{-1}\right)^2$.

Deja vu? It is deeply astonishing how closely a true formulation of $\mathbf{BSD}_p$ resembles the pseudo version forged out of thin air. Even the period Ω_E is in fact not missing but covertly embedded in $L^*_{p,\alpha}(E, s)$.

The history given above is slightly misleading without a mention of the *Modularity Theorem*: In truth, *Mazur & Swinnerton-Dyer* construct p-adic L-functions for p-ordinary weight 2 eigenforms and define the p-adic L-function of a *modular* elliptic curve $E/\mathbb{Q}$ to be that of the corresponding eigenform. *Amice & Velu* and *Vishik* then extend this definition not only to encompass supersingular primes but also arbitrary weight eigenforms. Succinctly speaking, the p-adic L-function they associate to an eigenform f is integration against an *h-admissible distribution* $\mu_{f,\alpha}$ attached to f and an *allowable root* α. A proper construction of these distributions is essentially achieved through defining linear maps of certain growth on *locally polynomial functions* and extending these maps to a larger domain appropriately. The resulting p-adic L-functions are then shown to be *analytic* and satisfy a certain growth condition themselves. We offer an in-depth study of all these (and more) in *Chapter 1*.

An alternative approach to construct h-admissible distributions is through *Stevens'* overconvergent modular symbols. In particular, the p-adic L-function of an eigenform f with respect to an *allowable* α may be obtained in the following way: For f_α a p-stabilization of f, one constructs a pair of *modular symbols* $\varphi^{\pm}_{f_\alpha}$ and lifts them to overconvergent symbols $\Phi^{\pm}_{f_\alpha}$, whose values on a certain *divisor* are the underlying distributions $\mu^{\pm}_{f,\alpha}$. A thorough discussion of these objects and their theory is what we do in *Chapter 2*. The final theorem we state (and prove) will be:

$$\Phi^{\pm}_{f_\alpha}\left(\{0\} - \{\infty\}\right)\big|_{\mathbb{Z}_p^\times} = \mu^{\pm}_{f,\alpha}$$

.

We feel the need to express the severe injustice we did to p-adic L-functions by confining them to the context of a p-adic BSD in our introduction. These functions play a central role in *Iwasawa Theory* and constitute one half of the *Main Conjecture for Elliptic Curves.* For a wonderful exposition on the subject, we refer the reader to [Sp12].

$*$ ***The set-up***

Fix forever an *odd* prime p.

Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ in $\mathbb{C}$ and an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. Fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. Let $\mathbb{C}_p$ denote the completion of $\overline{\mathbb{Q}}_p$ and $|\cdot|$ the absolute value on $\mathbb{C}_p$ normalized so that $|p| = 1/p$. Denote the corresponding p-adic valuation on $\mathbb{C}_p$ by ord_p. Denote by $\log(\cdot)$ the p-adic logarithm on $\mathbb{C}_p^{\times}$ extended with $\log(p) = 0$ and by exp the p-adic exponential on $|z| < p^{-1/(p-1)}$.

Chapter 1

p-adic L-functions

Section 1.1 defines p-adic distributions in a general context detailing on [Lang]. Section 1.2 introduces h-admissible distributions on $\mathbb{Z}_p^\times$ following [Vis76]. Section 1.3 chiefly deals with p-adic characters and L-functions on the character group X_p. Section 1.4 is largely based on [Pol03] and studies p-adic L-functions of modular forms. Section 1.5 specializes to elliptic curves and links p-adic L-functions to arithmetic data. Main references for the chapter are [Vis76], [MTT86] and [Pol03].

1.1 p-adic Distributions

Let $\{X_n\}$ be a sequence of finite sets and $\pi_{n+1} : X_{n+1} \to X_n$ a family of surjective maps such that (X_n, π_n) forms a projective system

$$\dots\ X_{n+1} \xrightarrow{\pi_{n+1}} X_n \xrightarrow{\pi_n} X_{n-1} \xrightarrow{\pi_{n-1}} \dots$$

Let $X = \varprojlim X_n$ be the projective limit, and for each n, let $r_n : X \to X_n$ denote the natural projection map onto X_n. X is naturally a compact topological space equipped with the projective limit topology, for which a basis of neighborhoods is given by $\{r_n^{-1}(x) : x \in X_n\}$.

Fix a complete local field K and let $\{\mu_n : X_n \to K\}$ be a collection of maps satisfying the following compatibility condition:

$$\sum_{y \in \pi_{n+1}^{-1}(x)} \mu_{n+1}(y) = \mu_n(x)$$

A function $g : X \to K$ is called *locally constant* if there exists some n such that the value $g(x)$ depends only on $r_n(x)$. We may then consider g as a function on X_n

simply by choosing a representative in X for each element of X_n. In such a case, we use the terminology *g factors through X_n*. Clearly, if $g : X \to K$ factors through X_n, then it also factors through X_m for $m \geq n$. Let us denote the space of locally constant functions $g : X \to K$ by $C^0(X)$. For $g \in C^0(X)$, let n_g refer to the smallest integer n such that g factors through X_n.

Lemma 1.1. *If $g \in C^0(X)$ factors through X_n, then for $m \geq n$,*

$$\sum_{x \in X_m} g(x)\mu_m(x) = \sum_{x \in X_n} g(x)\mu_n(X)$$

Proof. It is obviously enough to prove for $m = n+1$, which we do by suitably grouping the terms appearing in the sum and using the compatibility condition on $\{\mu_n\}$:

$$\sum_{x \in X_{n+1}} g(x)\mu_{n+1}(x) = \sum_{x \in X_n} \sum_{y \in \pi_{n+1}^{-1}(x)} g(y)\mu_{n+1}(y)$$

$$= \sum_{x \in X_n} g(x) \sum_{y \in \pi_{n+1}^{-1}(x)} \mu_{n+1}(y) = \sum_{x \in X_n} g(x)\mu_n(x)$$

□

Proposition 1.2. *A compatible family $\{\mu_n\}$ defines a K-linear functional $\mu : C^0(X) \to K$ given by*

$$\mu(g) = \sum_{x \in X_{n_g}} g(x)\mu_{n_g}(x)$$

Proof. We will simultaneously show that μ is well-defined and additive. For $g_1, g_2 \in C^0(X)$, let $n := max\{n_{g_1}, n_{g_2}\}$. Then g_1, g_2 and $g_1 + g_2$ all factor through X_n and the lemma above implies

$$\sum_{x \in X_{n_{g_i}}} g_i(x)\mu_{n_{g_i}}(x) = \sum_{x \in X_n} g_i(x)\mu_n(x)$$

Thus;

$$\mu(g_1 + g_2) = \sum_{x \in X_n} (g_1 + g_2)(x)\mu_n(x)$$

$$= \sum_{x \in X_n} g_1(x)\mu_n(x) + \sum_{x \in X_n} g_2(x)\mu_n(x) = \mu(g_1) + \mu(g_2)$$

□

Definition 1.3. *We call μ a* distribution *on X and use the notation*

$$\mu(g) =: \int g \, d\mu$$

We now have a well defined notion of integration on $C^0(X)$, which we wish to extend to larger spaces of functions. In the case that the values $\mu_n(x)$ are all bounded above, we will be able to do so all the way up to the space of continuous K-valued functions on X, which we denote by $C(X)$. We remark that locally constant functions $X \to K$ are continuous, and in fact, the space of all such functions $C^0(X)$ is dense in $C(X)$. Let us start with a couple of lemmas.

Lemma 1.4. *For $g \in C^0(X)$,*

$$\left| \int g \, d\mu \right| \leq \|g\| \cdot \|\mu\|$$

where $\|\cdot\|$ denotes the sup norm and $\|\mu\|$ means $\sup_n\{\|\mu_n\|\}$.

Proof. As g is in $C^0(X)$, it must factor through X_n for some n. We then have

$$\left| \int g \, d\mu \right| = \left| \sum_{x \in X_n} g(x)\mu_n(x) \right| \leq \max_{x \in X_n} |g(x)| \cdot |\mu_n(x)| \leq \|g\| \cdot \|\mu\|$$

where the first inequality follows from the ultra-metric property of K.

□

Lemma 1.5. *Every continuous function $g \in C(X)$ can be uniformly approximated by a sequence of locally constant functions, i.e. there exists a sequence $\{g_n\} \subset C^0(X)$ such that $\|g - g_n\| \to 0$.*

Definition 1.6. *A distribution μ is called a* measure *if $\|\mu\| < \infty$*

Proposition 1.7. *A measure μ uniquely extends to a K-linear functional $\mu : C(X) \to K$ given by*

$$\mu(g) = \lim_{n\to\infty} \int g_n \, d\mu$$

where $g \in C(X)$ and $\{g_j\} \subset C^0(X)$ uniformly approximate g.

Proof. Uniqueness follows directly from the definition. For the existence part, we need to show that $\left|\int g_n \, d\mu - \int g_m \, d\mu\right| \to 0$. But

$$\left|\int g_n \, d\mu - \int g_m \, d\mu\right| = \left|\int g_n - g_m \, d\mu\right| \leq \|g_n - g_m\| \cdot \|\mu\|$$

where the inequality relation is given by the above lemma. Since we know that $\|g_n - g_m\| \to 0$ and by assumption $\|\mu\| < \infty$, we get the desired result.

□

Definition 1.8. *For μ a measure on X and $g \in C(X)$, define*

$$\int g \, d\mu := \mu(g)$$

Later on, we will attach p-adic distributions to modular forms and construct p-adic L-functions via integrating against these distributions. For a modular form f that is ordinary at p, the resulting distribution will be a measure and the theory of integration presented above will be adequate. However; when f is supersingular at p, our construction will yield an unbounded distribution, against which we still wish to integrate functions that are not necessarily locally constant. To develop a suitable concept of integration, from now on we narrow our focus down to the case $X = \mathbb{Z}_p^\times$ and follow *Amice & Velu* [AV75] and *Vishik* [Vis76] in introducing h-admissible distributions. Before doing so, we slightly adjust our notation and present a useful lemma for constructing distributions on $\mathbb{Z}_p^\times$:

Notation: For μ a distribution on $\mathbb{Z}_p^\times$,

$$\mu(a + p^n\mathbb{Z}_p) := \mu(\chi_{a+p^n\mathbb{Z}_p})$$

$$\mu(g,\ a + p^n\mathbb{Z}_p) := \mu(g \cdot \chi_{a+p^n\mathbb{Z}_p})$$

Lemma 1.9. *Let $\mathcal{I}$ denote the collection of subsets of $\mathbb{Z}_p^\times$ that are of the form $a+p^n\mathbb{Z}_p$ and let $\mu : \mathcal{I} \to \mathbb{C}_p$ be a map satisfying the compatibility condition*

$$\mu(a + p^n\mathbb{Z}_p) = \sum_{b=0}^{p-1} \mu(a + bp^n + p^{n+1}\mathbb{Z}_p)$$

Then μ uniquely extends to a p-adic distribution on $\mathbb{Z}_p^\times$.

Proof. Adapt Proposition 1.2 to the notation above or see [Kob].

□

1.2 h-admissible Distributions

For a non-negative real number h, let $\mathcal{C}^h(\mathbb{Z}_p^\times)$ denote the space of $\mathbb{C}_p$-valued functions on $\mathbb{Z}_p^\times$ which are locally given by polynomials of degree less than or equal to h. For example, consistent with our earlier notation, $C^0(\mathbb{Z}_p^\times)$ describes locally constant $\mathbb{C}_p$-functions on $\mathbb{Z}_p^\times$. For U an open compact subset of $\mathbb{Z}_p^\times$, let χ_U denote the set characteristic function of U. In what follows, both an element $a \in \mathbb{Z}_p^\times$ and its projection on $\mathbb{Z}/p^n\mathbb{Z}$ will be denoted by a.

Definition 1.10. *An* h-admissible distribution *on* $\mathbb{Z}_p^\times$ *is a* $\mathbb{C}_p$*-linear map* $\mu : \mathcal{C}^h(\mathbb{Z}_p^\times) \to \mathbb{C}_p$ *which satisfies the following growth condition:*

$$\forall i,\ 0 \leq i \leq h,\ \sup_{a \in \mathbb{Z}_p^\times} \left| \int_{a+p^n\mathbb{Z}_p} (x-a)^i d\mu \right| = O(p^{n(h-i)}) \text{ as } n \to \infty$$

where $\int_{a+p^n\mathbb{Z}_p} (x-a)^i d\mu := \mu((x-a)^i \cdot \chi_{a+p^n\mathbb{Z}_p})$.

In the case of measures, we were able to extend μ to a linear functional on the space of continuous functions, whereas for an h-admissible distribution, the relevant domain of extension will be locally analytic functions, which we now define.

Definition 1.11. *Let* Y *be an open compact subset of* $\mathbb{Z}_p$*. A function* $F : Y \to \mathbb{C}_p$ *is said to be* locally analytic *if there exists a covering* $\mathcal{U}$ *of* Y *by sets of the form* $U = a + p^m\mathbb{Z}_p$ *such that* F *is representable as a convergent power series*

$$F(z) = \sum_{n=0}^{\infty} c_n (x-a)^n$$

on every $U = a + p^m\mathbb{Z}_p \in \mathcal{U}$ *with* $c_n \in \mathbb{C}_p$*. We denote the* $\mathbb{Z}_p$*-module of all* $\mathbb{C}_p$*-valued locally analytic functions on* Y *by* $C^{la}(Y)$*.*

The condition $U = a+p^m\mathbb{Z}_p$ is non-restrictive as sets of this form constitute a basis for $\mathbb{Z}_p$. We remark that by the compactness assumption on the subset Y, a locally analytic function $F \in C^{la}(Y)$ is representable by finitely many power series. Note that convergence of a power series $\sum c_n(x-a)^n$ on $a + p^m\mathbb{Z}_p$ is characterized by the criterion $|c_n| \cdot p^{-mn} \to 0$ as $n \to \infty$. Finally, let us record the following relationship between functions $\mathbb{Z}_p^\times \to \mathbb{C}_p$:

$$C^0(\mathbb{Z}_p^\times) \subset \dots C^h(\mathbb{Z}_p^\times) \subset \dots \subset C^{la}(\mathbb{Z}_p^\times) \subset C(\mathbb{Z}_p^\times)$$

Theorem 1.12. (Vishik) *An h-admissible distribution μ on $\mathbb{Z}_p^\times$ extends to a linear map $\mu : C^{la}(\mathbb{Z}_p^\times) \to \mathbb{C}_p$.*

Proof. Below we present the main argument of the proof as found in [Vis76] and in doing so, we concretely define $\mu(F)$ for a locally analytic function F and an h-admissible distribution μ. For details, see Lemma 1.5 and 1.6 in [Vis76] .
Let $F \in C^{la}(\mathbb{Z}_p^\times)$, $h' = [h]$ and choose a system of representatives Λ_m of $\mathbb{Z}_p^\times$ mod p^m. Consider the sums of the form

$$S_m(F) := \sum_{b \in \Lambda_m} \int_{b+p^m\mathbb{Z}_p} \sum_{i=0}^{h'} \frac{F^{(i)}(b)}{i!}(x-b)^i d\mu$$

obtained by using the first h' terms of the power series expansions of F. The limit $\lim_{m\to\infty} S_m(F)$ exists and is independent of the choice of representatives Λ_m. Set $\mu(F) := \lim_{m\to\infty} S_m(F)$.

□

Definition 1.13. *For $F \in C^{la}(\mathbb{Z}_p^\times)$ and μ an h-admissible distribution, define*

$$\int_{\mathbb{Z}_p^\times} F \, d\mu := \mu(F)$$

1.3 p-adic Characters and L-functions

Our primary interest is to integrate a particular class of locally analytic functions, namely the p-adic characters of $\mathbb{Z}_p^\times$, against h-admissible distributions. Let X_p be the group of continuous homomorphisms $\mathbb{Z}_p^\times \to \mathbb{C}_p^\times$, i.e.

$$X_p := Hom_{cont}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times)$$

We have the decomposition

$$\mathbb{Z}_p^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \oplus (1 + p\mathbb{Z}_p)$$

which in turn decomposes X_p into

$$X_p \simeq X((\mathbb{Z}/p\mathbb{Z})^\times) \oplus X(1+p\mathbb{Z}_p)$$

where $X(\cdot) := Hom_{cont}(\,\cdot\,, \mathbb{C}_p^\times)$. We call the characters in the component $X((\mathbb{Z}/p\mathbb{Z})^\times)$ *tame* and those in $X(1+p\mathbb{Z}_p)$ *wild.* As is clear from the above decomposition, every character $\chi \in X_p$ can be uniquely written as a product of a tame and a wild character.

Below are two examples of p-adic characters that will be of particular interest:

- For an integer $j \geq 0$ and a finite order character φ of p-power conductor, characters of the form
$$x^j \varphi(x)$$
- For $s \in \mathbb{Z}_p$ and $x \in \mathbb{Z}_p^\times$,
$$\langle x\rangle^s := exp(s \ \log\langle x\rangle) := \sum_{r=0}^{\infty} \frac{s^r}{r!}(\log\langle x\rangle)^r$$
where $\langle x\rangle := \dfrac{x}{\omega(x)} \in 1+p\mathbb{Z}_p$ with ω denoting the Teichmüller character.

We may also view Dirichlet characters of p-power conductor as p-adic characters in a natural way. Indeed, for $\chi : \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times \to \mathbb{C}^\times$, the following composition yields an element of X_p :

$$\mathbb{Z}_p^\times \twoheadrightarrow \ \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times \xrightarrow{\chi} \overline{\mathbb{Q}}^\times \hookrightarrow \mathbb{C}_p^\times$$

The character group X_p admits a natural identification with $p-1$ copies of the open unit disc of $\mathbb{C}_p$, upon which it acquires an analytic structure for which the map $\chi \mapsto \int_{\mathbb{Z}_p^\times} \chi \, d\mu$ is locally analytic. Below we describe this identification in detail.

Let $\mathcal{T} := \{u \in \mathbb{C}_p^\times : |u-1| < 1\}$ denote the open unit disc of $\mathbb{C}_p$ and let γ be a topological generator of $1+p\mathbb{Z}_p$, e.g. $\gamma = 1+p$. For each $u \in \mathcal{T}$, define a particular wild character $\chi_u \in X(1+p\mathbb{Z}_p)$ via

$$\begin{aligned} \chi_u : 1+p\mathbb{Z}_p &\longrightarrow \mathbb{C}_p^\times \\ \gamma &\longmapsto u \end{aligned}$$

By continuity of the characters, for any $\chi \in X(1+p\mathbb{Z}_p)$ we have $\big|\chi(\gamma)-1\big| < 1$. Thus $\{\chi_u\}_{u\in\mathcal{T}}$ accounts for all the possible wild characters and the injective map

$$\begin{aligned} \varphi : \mathcal{T} &\xrightarrow{\sim} X(1+p\mathbb{Z}_p) \\ u &\longmapsto \chi_u \end{aligned}$$

is surjective. Using the isomorphism φ, we may identify the group of characters $\chi \in X_p$ of trivial tame part with $\mathcal{T}$ and carry the analytic group structure of $\mathcal{T}$ onto $X(1+p\mathbb{Z}_p)$. We can then naturally extend this identification to whole of X_p via translating the $\mathcal{T}$-structure to each of the $p-1$ components:

$$X_p \simeq \bigsqcup_{i=1}^{p-1} \mathcal{T}$$

Using the above identification, we say that a function $F : X_p \to \mathbb{C}_p$ is analytic if, when restricted to each one of the $p-1$ components, F is given by an analytic function $\mathcal{T} \to \mathbb{C}_p$. In other words, $F : X_p \to \mathbb{C}_p$ is analytic if on each component of X_p, F is representable by a power series $\Sigma c_n(u-1)^n$ which converges on $\mathcal{T}$ with $c_n \in \mathbb{C}_p$. If $F : X_p \to \mathbb{C}_p$ and $G : X_p \to \mathbb{C}_p$ are two analytic functions, then the notation $F = O(G)$ means that on each component of X_p the following holds:

$$\sup_{|u-1|<r} |F(u)| = O\left(sup_{|u-1|<r} |G(u)| \right) \quad as \;\; r \to 1^-$$

Theorem 1.14. *(Amice and Velu, Vishik) For a fixed h-admissible distribution μ, define a map*

$$L(\,\cdot\,,\mu) : X_p \longrightarrow \mathbb{C}_p$$

via

$$L(\chi,\mu) = \int_{\mathbb{Z}_p^\times} \chi \, d\mu$$

Then $L(\,\cdot\,,\mu) : X_p \to \mathbb{C}_p^\times$ is analytic in u and is $O(\log^h(\cdot))$

Proof. See [Vis76] Theorem 2.3.

□

Let us discuss the theorem above a bit more concretely. Let K be a finite extension of $\mathbb{Q}_p$ and suppose all the values the h-admissible distribution μ assumes are contained in K. Fix a topological generator γ of $1 + p\mathbb{Z}_p$. The first part of the theorem then says, for each tame character $\psi \in X_p$, there exists a power series $g_{\mu,\psi} \in K[[T]]$ such that, if $\chi \in X_p$ has tame part ψ and wild part χ_u, then

$$L(\chi,\mu) = g_{\mu,\psi}(\chi_u(\gamma) - 1) = g_{\mu,\psi}(u-1) = \sum_{n \geq 0} a_{\mu,\psi,n}(u-1)^n$$

The second part, namely the growth condition on $L(\,\cdot\,,\mu)$, is characterized by the property that each power series $g_{\mu,\psi} = \sum a_{\mu,\psi,n} T^n$ satisfies $\left|a_{\mu,\psi,n}\right| = O(n^h)$.

Definition 1.15. *Let $L(\mu,\psi,T) := g_{\mu,\psi}(T)$ where ψ is a tame character and $g_{\mu,\psi}$ is as described above.*

Remark 1.16. $L(\mu,\psi,T)$ depends on the choice of a generator γ, but since the dependence is light, we omit γ from our notation.

1.4 p-adic L-functions of Modular Forms

Let $f \in S_k(N,\epsilon)$ be a normalized cusp form of weight k, level N prime to p and character ϵ. Assume that f is a Hecke eigenform with $T_n f = a_n f$ and let K_f be the number field generated by a_n together with the values of ϵ. Let $\mathcal{O}_f = \mathcal{O}_{K_f}$ be the ring of integers of K_f. Denote by α_1 and α_2 the roots of the Hecke polynomial of f at p, i.e.

$$x^2 - a_p x + \epsilon(p)p^{k-1} = (x - \alpha_1)(x - \alpha_2)$$

We call α_i an *allowable root* if $ord_p(\alpha_i) < k-1$. Note that there always exists at least one allowable root as $ord_p(\alpha_1\alpha_2) = p^{k-1}$.

Now fix an allowable root $\alpha \in \{\alpha_1, \alpha_2\}$. We will construct a pair of h-admissible distributions $\mu^{\pm}_{f,\alpha}$ using the period integrals

$$\Phi(f, P, r) := 2\pi i \int_{i\infty}^{r} f(z)P(z)dz$$

where $r \in \mathbb{Q}$ and $P \in \mathbb{Z}[T]$ of degree $\leq k-2$. To this end, let

$$\eta(f, P; a, m) := \Phi\left(f, P(-mz + a), \frac{a}{m}\right)$$

and fix $\pm$-parts of η by setting

$$\eta^{\pm}(f, P; a, m) := \frac{\eta(f, P; a, m) \pm \eta(f, P; a, -m)}{2}$$

Theorem 1.17. *(Manin) There exist two non-zero complex numbers Ω_f^+ and Ω_f^- such that*

$$\frac{\eta^{\pm}(f, P; a, m)}{\Omega_f^{\pm}} \in \mathcal{O}_f$$

for all $a,\ m \in \mathbb{Z}$ and $P \in \mathbb{Z}[T]$ of degree $\leq k-2$.

Definition 1.18. *With everything as above, define*

$$\lambda^{\pm}(f, P; a, m) := \frac{\eta^{\pm}(f, P; a, m)}{\Omega_f^{\pm}} \in \mathcal{O}_f$$

Before going any further, let us shed some light on our motivations behind introducing $\lambda^{\pm}$. Recall that our intent is to attach a certain pair of p-adic h-admissible distributions $\mu^{\pm}_{f,\alpha}$ to our cuspidal eigenform f depending on the allowable root α. As it often is the case in literature, we could have defined a working distribution $\mu_{f,\alpha}$ using the map η instead of obtaining a pair $\mu^{\pm}_{f,\alpha}$ via $\lambda^{\pm}$, albeit with a compromise: that distribution would not be guaranteed to take values in $\mathbb{C}_p$ since η does not necessarily assume algebraic values. At this point, this would merely trigger a practical inconvenience rather than a theoretical obstacle: As implied by the above theorem due to *Manin*, η takes values in an at most 2-dimensional vector space over $\mathbb{C}_p$ under our fixed embedding $\overline{Q} \hookrightarrow \overline{\mathbb{Q}}_p$, and [Vis76] in fact defines h-admissible distributions in a way to perfectly accommodate such a case. We instead follow [Pol03] and obtain two distributions $\mu^{\pm}_{f,\alpha}$ through the maps $\lambda^{\pm}$. Although we do not have an Iwasawa theoretic focus, our preference to do so will become fruitful when we present an alternative construction of $\mu^{\pm}_{f,\alpha}$ using *'overconvergent modular symbols'*, but for now, let us just return to our freshly defined maps $\lambda^{\pm}$.

Proposition 1.19. *$\lambda^{\pm}(f, P; a, m)$ depends only on a mod m for a fixed P.*

Proof. Observe that it suffices to prove the statement for η. For $b \in \mathbb{Z}$,

$$\begin{aligned}\eta(f, P; a + bm, m) &= \Phi\left(f(z), P(-mz + a + bm), \frac{a + bm}{m}\right)\\ &= 2\pi i \int_{i\infty}^{\frac{a+bm}{m}} f(z)P(-mz + a + bm)dz\end{aligned}$$

Following a change of variables $z \mapsto z + b$, we find

$$\begin{aligned}\eta(f, P; a + bm, m) &= 2\pi i \int_{i\infty}^{a/m} f(z + b)P(-mz + a)dz\\ &= 2\pi i \int_{i\infty}^{a/m} f(z)P(-mz + a)dz = \eta(f, P; a, m)\end{aligned}$$

$\square$

We are now ready to define the pair of distributions $\mu^{\pm}_{f,\alpha}$. Let v be the prime of K_f lying over p and denote by K the completion of K_f at v. Note that $\lambda^{\pm}$ take values in K under our fixed embedding $\overline{Q} \hookrightarrow \overline{\mathbb{Q}}_p$.

Definition 1.20. *For $a + p^n\mathbb{Z}_p \subset \mathbb{Z}_p^{\times}$ and P of degree $\leq k-2$, set*

$$\mu^{\pm}_{f,\alpha}(P,\ a + p^n\mathbb{Z}_p) = \frac{\lambda^{\pm}(f, P; a, p^n)}{\alpha^n} - \frac{\epsilon(p)p^{k-2}\lambda^{\pm}(f, P; a, p^{n-1})}{\alpha^{n+1}} \in K(\alpha)$$

Lemma 1.21. *$\mu^{\pm}_{f,\alpha}$ defines a distribution on $\mathbb{Z}_p^{\times}$.*

Proof. The fact that $\mu^{\pm}_{f,\alpha}$ is well-defined follows at once from the previous proposition. To see that $\mu^{\pm}_{f,\alpha}$ does indeed define a distribution, observe that the compatibility relation

$$\mu^{\pm}_{f,\alpha}(P, a + p^n\mathbb{Z}_p) = \sum_{b=0}^{p-1} \mu^{\pm}_{f,\alpha}(P, a + bp^n + p^{n+1}\mathbb{Z}_p)$$

is satisfied as f is assumed to be an eigenform for T_p and then use the lemma given at the end of Section 1.1.

□

If p is ordinary for f, then $ord_p(a_p) = 0$ by definition and there is a unique allowable root α that is necessarily a p-adic unit. Hence the distribution $\mu^{\pm}_{f,\alpha}$ is bounded and defines a measure. If, however, f is supersingular at p, that is $p \mid a_p$, then both α_1 and α_2 are allowable non-unit roots and $\mu^{\pm}_{f,\alpha}$ is not p-adically bounded.

Proposition 1.22. *$\mu^{\pm}_{f,\alpha}$ is h-admissible for $h = ord_p(\alpha) < k-1$.*

Proof. See Lemma 3.8 in [Vis76].

□

By the proposition above and Theorem 1.12, we may integrate locally analytic $\mathbb{C}_p$-functions on $\mathbb{Z}_p^{\times}$ against $\mu^{\pm}_{f,\alpha}$. The integral $\int (\cdot)\, d\mu^{\pm}_{f,\alpha} : C^{la}(\mathbb{Z}_p^{\times}) \to \mathbb{C}_p$ thus defined satisfies the following:

Proposition 1.23. *Assume that $F \in C^{la}(\mathbb{Z}_p^\times)$ is given by a convergent power series $\sum_n c_n(x-a)^n$ on $a + p^m\mathbb{Z}_p$. Then,*

$$\int_{a+p^m\mathbb{Z}_p} F\, d\mu_{f,\alpha}^{\pm} = \sum_n c_n \int_{a+p^m\mathbb{Z}_p} (x-a)^n d\mu_{f,\alpha}^{\pm}$$

Proof. See (IV) of the theorem in §11 [MTT86].

□

In particular, as p-adic characters are locally analytic, we may view $\int (\cdot)\, d\mu_{f,\alpha}^{\pm}$ as a $\mathbb{C}_p$-functional on $X_p = Hom_{cont}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times)$ and define an L-function as in Section 1.3 depending on f and α.

Definition 1.24. *With everything as above, the p-adic L-function of f with respect to α, $L_p(f, \alpha, \cdot) : X_p \to \mathbb{C}_p$ is defined to be*

$$L_p(f, \alpha, \chi) := L(\chi, \mu_{f,\alpha}^{sgn(\chi)}) = \int_{\mathbb{Z}_p^\times} \chi\, d\mu_{f,\alpha}^{sgn(\chi)}$$

Remark 1.25. $L_p(f, \alpha, \cdot)$ depends on the choice of the periods $\Omega_f^{\pm}$, which are only defined up to an element of $\mathcal{O}_f$.

By Theorem 1.14, $L_p(f, \alpha, \cdot)$ is analytic on X_p and thence given by a convergent power series $L_p(f, \alpha, \psi, T)$ on each component, where $L_p(f, \alpha, \psi, T)$ is as described in Definition 1.15 and the preceding discussion. Hence

$$L_p(f, \alpha, \psi\chi_u) = L_p(f, \alpha, \psi, u-1)$$

The following proposition characterizes $L_p(f, \alpha, \cdot)$ through an interpolation property and a growth condition.

Proposition 1.26. *$L_p(f,\alpha,\cdot)$ is the unique analytic $O(\log^h)$ map $X_p \to \mathbb{C}_p$ satisfying*

$$L_p(f,\alpha,x^j\varphi) = \frac{1}{\alpha^n}\cdot\frac{p^{n(j+1)}}{(-2\pi i)^j}\cdot\frac{j!}{\tau(\varphi^{-1})}\cdot\frac{L(f,\varphi^{-1},j+1)}{\Omega_f^{\pm}}$$

for every character $x^j\varphi(x) \in X_p$, where φ is of finite order with conductor p^n, j is an integer with $0 \le j \le k-2$, $h = ord_p(\alpha)$, τ denotes the Gauss sum and $L(f,\varphi^{-1},s)$ is the complex L-function of f twisted by φ^{-1}.

Proof. See §14 of [MTT86] .

□

Remark 1.27. The proposition above may be interpreted as follows: For characters of the form $\chi = x^j\varphi(x)$ with $\varphi \in X_p$ of finite order and p-power conductor, $0 \le j \le k-2$, the values $L_p(f,\alpha,x^j\varphi)$ can be obtained by evaluating the power series $L_p(f,\alpha,\psi,T)$ at $T = \gamma^j\zeta_{p^n} - 1$, where ζ_{p^n} is a p^n-th root of unity satisfying $x^j\varphi(x) = \psi\chi_{\gamma^j\zeta_{p^n}}$ and ψ is appropriately chosen. Proposition 1.26 then says that as χ runs along all such characters, the values $L_p(f,\alpha,\psi,\gamma^j\zeta_{p^n}-1)$ agree with the right hand side of the equality given in the statement, i.e. $L_p(f,\alpha,\cdot)$ satisfies an interpolation property. Furthermore, this interpolation property uniquely determines $L_p(f,\alpha,\cdot)$ with the added condition that the interpolating function is $O(\log(1+T)^h)$ for $h = ord_p(\alpha)$.

1.5 p-adic L-functions of Elliptic Curves

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and let $f = f_E$ be the modular form associated to E by the Modularity Theorem ([Wi95], [TW95], [BCDT01]) so that f is a cuspidal normalized eigenform on $\Gamma_0(N)$ of weight 2 with $K_f = \mathbb{Q}$. Assume that E has good reduction at the prime p. Further assume that if p is supersingular for E, then $a_p = 0$. Note that this last assumption is automatically satisfied for all primes > 3 by Hasse's bound.

Let $\alpha_1,\ \alpha_2$ be the roots of the Hecke polynomial of E at p so that

$$x^2 - a_p x + p = (x-\alpha_1)(x-\alpha_2)$$

Then $\alpha \in \{\alpha_1, \alpha_2\}$ is an allowable root if $ord_p(\alpha) < 1$. If p is ordinary for E, $ord_p(a_p) = 0$ and there is a unique allowable α, which is a p-adic unit. If p supersingular for E, bearing in mind our assumption $a_p = 0$, we get $\alpha_1 = -\alpha_2$ with each root having p-adic order $1/2$ and thence two choices for an allowable α.

We define the p-adic L-function of E with respect to an allowable root α to be the p-adic L- function of f with respect to the same allowable root, i.e.

$$L_{p,\alpha}(E,\chi) := L_p(f,\alpha,\chi)$$

Observe that in the $k = 2$ case, we may considerably simplify the notation we introduced in Section 1.4 in the process of defining $\mu^{\pm}_{f,\alpha}$. Indeed, as the polynomial P appearing in $\lambda^{\pm}$ and $\mu^{\pm}_{f,\alpha}$ was of degree $\leq k-2$, we may discard the P component and adopt the following notation:

$$\Phi_f(r) := 2\pi i \int_{i\infty}^{r} f(z)dz$$

$$\left[\frac{a}{m}\right]^{\pm} := \lambda^{\pm}(f,1,a,m) = \frac{\Phi_f(r) \pm \Phi_f(-r)}{2} \cdot \frac{1}{\Omega_E} \in \frac{1}{c} \cdot \mathbb{Z}$$

Remark 1.28. The reason for the appearance of $\frac{1}{c}$ factor is that the period Ω_E does not necessarily satisfy Theorem 1.17. However, denominators of $\left[\frac{a}{m}\right]^{\pm}$ remain bounded as a and m vary in $\mathbb{Z}$. See [Man72].

With this new notation, the pair of distributions attached to E are given as

$$\mu^{\pm}_{E,\alpha}(a+p^n\mathbb{Z}_p) := \frac{1}{\alpha^n}\left[\frac{a}{p^n}\right]^{\pm} - \frac{1}{\alpha^{n+1}}\left[\frac{a}{p^{n-1}}\right]^{\pm} \in \mathbb{Q}_p(\alpha)$$

and the p-adic L-function of E with respect to α is

$$L_{p,\alpha}(E,\chi) := L(\mu^{sgn(\chi)}_{E,\alpha},\chi)$$

By Theorem 1.14, $L_{p,\alpha}(E,\cdot)$ is analytic in u upon identifying X_p with $\bigsqcup\limits_{i=1}^{p-1}\mathcal{T}$. Thus, as in Definition 1.15, $L_{p,\alpha}(E,\chi)$ is given by a power series $L_{p,\alpha}(E,\psi,T)\in Q_p(\alpha)[[T]]$ depending on the tame part ψ of χ. We henceforth denote $L_{p,\alpha}(E,\psi,T)$ by $L_{p,\alpha}(E,T)$ for ψ trivial.

Proposition 1.29. *$L_{p,\alpha}(E,T)$ satisfies the interpolation properties*

$$L_{p,\alpha}(E,\zeta_{p^n}-1) = \frac{1}{\alpha^{n+1}}\cdot\frac{p^{n+1}}{\tau(\chi^{-1}_{\zeta_{p^n}})}\cdot\frac{L(E,\chi^{-1}_{\zeta_{p^n}},1)}{\Omega_E}$$

$$L_{p,\alpha}(E,0) = \left(1-\frac{1}{\alpha}\right)^2\cdot\frac{L(E,1)}{\Omega_E}$$

where $L(E,\chi^{-1}_{\zeta_{p^n}},s)$ is the L-function of E twisted by $\chi^{-1}_{\zeta_{p^n}}$, ζ_{p^n} is a primitive p^n-th root of unity and $\chi_{\zeta_{p^n}}$ is as defined in Section 1.3.

Proof. See Proposition 1.26 and Remark 1.27. See also [MTT86] and [Sp15].

□

Remark 1.30. The reason $n+1$ instead of n appears in the powers of α and p on the right hand side is that $\chi_{\zeta_{p^n}}$ is considered as a character of $\mathbb{Z}/p^n\mathbb{Z}$ and as such has conductor p^{n+1}.

In literature, one often encounters $L_{p,\alpha}(E,T)$ expressed (and sometimes constructed) in the s variable (e.g. [MTT86], [SW13]), a formulation we may obtain through a variable change $T = \gamma^{s-1} - 1$. More precisely, recall the p-adic character $\langle\cdot\rangle^s : \mathbb{Z}_p^\times \to \mathbb{C}_p^\times$ given in Section 1.3 via

$$\langle x\rangle^s = \exp(s\log\langle x\rangle)$$

for $s \in \mathbb{Z}_p$ and define

$$L_{p,\alpha}(E,s) := \int_{\mathbb{Z}_p^\times} \langle x\rangle^{s-1} d\mu_{E,\alpha}(x)$$

where $\mu_{E,\alpha} = \mu_{f,\alpha}^+$ and the notation $d\mu_{E,\alpha}(x)$ is to signify the variable we are integrating against.

The character $\langle x\rangle^{s-1}$ clearly has trivial tame part, so it must be of the form χ_u for some $u \in \mathcal{T} = \{z \in \mathbb{C}_p^\times : |z-1| < 1\}$. Furthermore, once we determine u for $\langle x\rangle^{s-1}$, we know that $L_{p,\alpha}(E,s)$ is given by a power series expression of the form $\sum a_n(u-1)^n$. To this end, let γ be a topological generator of $1+p\mathbb{Z}_p$. Recall that the character χ_u is characterized by the property $\chi_u(\gamma) = u$. Correspondingly, for $\langle\cdot\rangle^{s-1} : \mathbb{Z}_p^\times \to \mathbb{C}_p^\times$ we have

$$\langle\gamma\rangle^{s-1} = \exp\big((s-1)\log\gamma\big)$$

and thus $L_{p,\alpha}(E,s)$ is given by

$$L_{p,\alpha}(E,s) = \sum_{n\geq 0} a_n \Big(\exp\big((s-1)\log\gamma\big) - 1\Big)^n$$

where a_n are the coefficients of $L_{p,\alpha}(E,T)$, i.e. $\sum_n a_n T^n = L_{p,\alpha}(E,T)$. To ease the notation, we write A^B for $\exp(B\log A)$. The power series expansion for $L_{p,\alpha}(E,s)$ then reads $\sum a_n(\gamma^{s-1}-1)^n$.

Remark 1.31. The two constructions are indeed equivalent: As explained above, $\langle\cdot\rangle^{s-1}$ is merely another way of writing $\chi_{\gamma^{s-1}}$ and every $u \in \mathcal{T}$ may be represented as γ^{s-1} for a unique $s \in \mathbb{Z}_p$. Thus switching between the two expressions of the p-adic L-function amounts to a variable change $T = \gamma^{s-1} - 1$.

Proposition 1.32. *$L_{p,\alpha}(E,s)$ is analytic in s,*

$$L_{p,\alpha}(E,s) = \sum_{n=0}^{\infty} b_n (s-1)^n$$

and the coefficients b_n are given by

$$b_n = \frac{1}{n!} \int_{\mathbb{Z}_p^\times} \big(\log\langle x\rangle\big)^n \, d\mu_{E,\alpha}$$

Proof. See §11 and §13 in [MTT86].

□

Apart from p-adically interpolating the special values of the Hasse-Weil L-series, the p-adic L-function encodes intrinsic arithmetic data about the elliptic curve E. Indeed, the leading non-zero coefficient of $L_{p,\alpha}(E,T)$ relates closely to algebraic invariants of E via the *p-adic BSD conjecture.*

Conjecture 1.33. $\big(\mathbf{BSD}_p\big)$ *(Mazur, Tate and Teitelbaum, Bernardi and Perrin-Riou) Let $E/\mathbb{Q}$ be an elliptic curve and assume E has good reduction at p. Let r_{an} denote the order of vanishing of $L_{p,\alpha}(E,T)$ at $T=0$ and r_{alg} the $\mathbb{Z}$-rank of $E(\mathbb{Q})$. Then,*

(i) $r_{an} = r_{alg}$

(ii) $L^*_{p,\alpha}(E,T) = \left(1 - \dfrac{1}{\alpha}\right)^2 \cdot \dfrac{\prod_v c_v \cdot \#\text{Ш}(E/\mathbb{Q})}{(\#E(\mathbb{Q})/tor)^2} \cdot \mathrm{Reg}_{\frac{1}{\beta}}(E,\mathbb{Q})$

where $L^*_{p,\alpha}(E,T)$ is the leading non-zero coefficient of $L_{p,\alpha}(E,T)$, α an allowable root (unique if p is ordinary) and $\beta = \dfrac{p}{\alpha}$.

Remark 1.34. The version of the *p-adic BSD* given above is as formulated in [Col04] and [Sp15]. For the individual treatments of ordinary and supersingular cases, see [MTT86] and [BPR93]. For definitions of the arithmetic quantities appearing on the right hand side, see [Silv]. For $\mathrm{Reg}_{\frac{1}{\beta}}(E/\mathbb{Q})$, see [PR03] and [SW13]. For a detailed exposition, see [BMS12], [Sp15] and [Sp17].

In the p-supersingular case (and under certain hypotheses detailed in the statement of the theorem below), the existence of two separate p-adic L-functions $L_{p,\alpha}(E,s)$ and $L_{p,\beta}(E,s)$ allows one to construct global non-torsion points on E as suggested by *Perrin-Riou* in [PR93].

Theorem 1.35. *(Büyükboduk) Let $E/\mathbb{Q}$ be an elliptic curve of square free conductor N and assume that E has good supersingular reduction at p. Further assume that the residual representation $\overline{\rho}_E : G_{\mathbb{Q},S} \to Aut(E[p])$ is surjective, where S is the set of all rational primes dividing Np and the Archimedean place. Then,*

$$P := \exp_V \left(\omega^* \cdot \sqrt{\delta_E \cdot \left((1-1/\alpha)^{-2} \cdot L'_{p,\alpha}(E,s)\big|_{s=1} - (1-1/\beta)^{-2} \cdot L'_{p,\beta}(E,s)\big|_{s=1} \right)} \right)$$

is a $\mathbb{Q}$-rational point on E of infinite order.

Proof. For a proof and descriptions of the terms appearing in the formula, see [Büy15]. □

Remark 1.36. A similar formula is proved in [KP07] assuming the conjecture $\boldsymbol{BSD}_p$. The result above is unconditional.

We will not discuss any further instances where the p-adic L-functions come into play but let us just say that they are plentiful in the realm of Iwasawa theory. The upshot for us is the following: Knowledge about $L_{p,\alpha}(E,T)$ translates into knowledge about E.

To determine $L_{p,\alpha}(E,T)$, *Stein* and *Wuthrich* provide the following algorithm in [SW13]: Pick $\gamma = p+1$ as the topological generator of $1+p\mathbb{Z}_p$ and for each $n \geq 1$, define a polynomial

$$P_n(T) = \sum_{a=1}^{p-1} \left(\sum_{j=0}^{p^{n-1}-1} \mu_{E,\alpha} \left(\omega(a)(1+p)^j + p^n\mathbb{Z}_p \right) \cdot (1+T)^j \right) \in \mathbb{Q}_p(\alpha)[T]$$

where ω denotes the Teichmüller character. Write $\sum_j a_{n,j} T^j$ for $P_n(T)$ and $\sum_j a_j T^j$ for $L_{p,\alpha}(E, T)$. Then $\lim_{n\to\infty} a_{n,j} = a_j$.

As can be observed from the way polynomials P_n are constructed, the algorithm above is exponential in p, which renders computations to a high p-adic accuracy infeasible in practice. As an alternative, one might attempt to use Proposition 1.32 and compute the values $\mu_{E,\alpha}(x^n)$, which, however, would require constructing Riemann sums as in the proof of Theorem 1.12 and thus would yield an algorithm which is as well exponential in p.

A different approach is to use *overconvergent modular symbols* to compute the values $\mu_{E,\alpha}(x^n)$, as has been done in [DP06], [KP07] and [PS11]. A careful study of these objects leads to an algorithm that is polynomial in p, which is thence very effective in carrying out computations in practice to a high p-adic accuracy. Computational complexities involving such calculations are discussed in detail in [DP06].

An in-depth study of *overconvergent modular symbols* not only enables an efficient algorithm for carrying out calculations but also presents a truly elegant way of constructing p-adic L-functions of *Amice & Velu* and *Vishik*. In the next chapter, we leave aside computational concerns and focus on the theoretical side of these objects as first introduced by *Stevens* in [Ste94] and later refined in [PS11].

Chapter 2

Overconvergent Modular Symbols

Section 2.1 is introductory and follows closely [Pol11]. In Section 2.2, classical modular symbols are presented and a particular pair $\varphi_f^{\pm}$ are attached to a cusp form f. Overconvergent modular symbols are introduced in Section 2.3. Section 2.4 establishes links between the two types of objects and studies the lifts of modular symbols to overconvergent symbols. In Section 2.5, $\mu_{f,\alpha}^{\pm}$ is realized as the value of the overconvergent symbol $\Phi_{f_\alpha}^{\pm}$ lifting $\varphi_{f_\alpha}^{\pm}$. Main references for the chapter are [Ste94] and [PS11].

2.1 Eichler-Shimura Relation

Let $\Delta_0 := Div^0(\mathbb{P}^1(\mathbb{Q}))$ be the group of degree 0 divisors on $\mathbb{P}^1(\mathbb{Q})$, Γ a congruence subgroup of level N and f a weight 2 cusp form on Γ. Define a map Ψ_f on divisors of the form $\{s\} - \{r\}$ to $\mathbb{C}$ via

$$\{s\} - \{r\} \longmapsto 2\pi i \int_r^s f(z)\, dz$$

and extend to whole Δ_0 appropriately using Cauchy's Theorem. In this way, f gives rise to a map $\Psi_f \in Hom(\Delta_0, \mathbb{C})$.

Δ_0 has a natural left $\mathbb{Z}[GL_2(\mathbb{Q})]$-module structure where $GL_2(\mathbb{Q})$ acts via linear fractional transformations on a divisor D. For example, if $D = \{s\} - \{r\}$ and $\gamma \in \Gamma$, then $\gamma D = \{\gamma s\} - \{\gamma r\}$. Correspondingly, we define an action of Γ on $Hom(\Delta_0, \mathbb{C})$ as follows: For $\varphi \in Hom(\Delta_0, \mathbb{C})$, set $(\varphi \mid \gamma) := \varphi(\gamma D)$. In particular, for Ψ_f we have,

$$(\Psi_f \mid \gamma)(D) = \Psi_f(\gamma D) = 2\pi i \int_{\gamma r}^{\gamma s} f(z)\, dz$$

$$= 2\pi i \int_{\gamma r}^{\gamma s} (cz+d)^{-2} f(\gamma z)\, dz = 2\pi i \int_{r}^{s} f(z)\, dz = \Psi_f(D)$$

so that Ψ_f is invariant under the action of Γ. To indicate this invariance, we write $\Psi_f \in Symb_\Gamma(\mathbb{C})$, where

$$Symb_\Gamma(\mathbb{C}) := \{\varphi \in Hom(\Delta_0, \mathbb{C}) : \varphi \mid \gamma = \varphi \quad \text{for all} \;\; \gamma \in \Gamma\}$$

is what we call the space of $\mathbb{C}$-*valued modular symbols on* Γ.

By our above construction of Ψ_f out of a weight 2 cusp form on Γ, it is evident that $S_2(\Gamma, \mathbb{C}) \hookrightarrow Symb_\Gamma(\mathbb{C})$. *Eichler-Shimura* theory yields a much finer result:

Theorem 2.1. *(Eichler-Shimura) Let* $\Gamma = \Gamma_1(N)$ *for some* N. *Then*

$$Symb_\Gamma(\mathbb{C}) \simeq S_2(\Gamma, \mathbb{C}) \oplus M_2(\Gamma, \mathbb{C})$$

In fact, there is a good deal more we can say about the *Eichler-Shimura* isomorphism above. But before doing so, let us extend our notion of a modular symbol slightly to encompass those arising from higher weight cusp forms.

Let $V_g(\mathbb{C}) := Sym^g(\mathbb{C}^2)$ be the space of homogeneous polynomials of degree g in $\mathbb{C}[X, Y]$ and let $S := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) : ad - bc \neq 0\}$ denote the semigroup of 2×2 matrices with integer entries and non-zero determinant. We endow $V_g(\mathbb{C})$ with a right action of S by setting

$$(P \mid \gamma)(X, Y) := P((X, Y) \mid \gamma^*) := P(dX - CY, -bX + aY)$$

where $P \in V_g(\mathbb{C})$, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in S$ and $\gamma^* = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Now let $f \in S_{k+2}(\Gamma, \mathbb{C})$ be a cusp form of an arbitrary weight $k+2$ on a congruence subgroup Γ and, in an analogous fashion to weight 2 case, define

$$\Psi_f(\{s\} - \{r\}) = 2\pi i \int_r^s f(z)(zX+Y)^k dz \in V_k(\mathbb{C})$$

for a divisor $\{s\}-\{r\} \in \Delta_0$ and extend Ψ_f appropriately to an element of $Hom(\Delta_0, V_k(\mathbb{C}))$. The action of the semigroup S on $V_k(\mathbb{C})$ induces a right action $Hom(\Delta_0, V_k(\mathbb{C}))$ given by

$$(\varphi \mid \gamma)(D) := \varphi(\gamma D) \mid \gamma$$

for $\varphi \in Hom(\Delta_0, V_k(\mathbb{C}))$ and $\gamma \in S$. Note that in particular, any congruence subgroup $\subset SL_2(\mathbb{Z})$ acts on $Hom(\Delta_0, V_k(\mathbb{C}))$ through the action of S as defined above. We then define the space of $V_k(\mathbb{C})$ *valued modular symbols on* Γ to be

$$Symb_\Gamma(V_k(\mathbb{C})) := \{\varphi \in Hom(\Delta_0, V_k(\mathbb{C})) : \varphi \mid \gamma = \varphi \text{ for all } \gamma \in \Gamma\}$$

Let us show that $\Psi_f \in Symb_\Gamma(V_k(\mathbb{C}))$. We have

$$\begin{aligned}
\Psi_f(\gamma D) &= 2\pi i \int_{\gamma r}^{\gamma s} (zX+Y)^k f(z) dz \\
&= 2\pi i \int_r^s ((az+b)X + (cz+d)Y)^k f(z) dz \\
&= \Psi_f(D) \mid \gamma^{-1}
\end{aligned}$$

and thus $\Psi_f \mid \gamma = \Psi_f$ for any $\gamma \in \Gamma$.

The seemingly peculiar action we introduced on the polynomial spaces $V_g(\mathbb{C})$ is characterized by the property that the association $f \mapsto \Psi_f$ is S-equivariant, where S acts on f via the standard action of $GL_2(\mathbb{Q})$ on modular forms. We wish to translate this fact into a Hecke equivariance property between the two spaces. To this end, through the action of S on $V_k(\mathbb{C})$, we bestow a Hecke-action on $Symb_\Gamma(V_k(\mathbb{C}))$ with the operator T_ℓ being defined by the action of the double coset $\Gamma\begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}\Gamma$ for each prime ℓ. Invoking *Eichler-Shimura* theory now gives the following delicate result:

Theorem 2.2. *(Eichler-Shimura) Let $\Gamma = \Gamma_1(N)$ for some N. Then there is a Hecke equivariant isomorphism*

$$Symb_\Gamma(V_k(\mathbb{C})) \simeq S_{k+2}(\Gamma, \mathbb{C}) \oplus M_{k+2}(\Gamma, \mathbb{C})$$

2.2 Classical Modular Symbols

We now switch to a p-adic setting and define *classical modular symbols* within this context. Define a semigroup $\Sigma_0(p) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_p) : (a,p) = 1, c \in p\mathbb{Z}_p, ad - bc \neq 0\}$ and let V be a right $\mathbb{Z}_p[\Sigma_0(p)]$ module. $\Sigma_0(p)$ induces an action on $Hom(\Delta_0, V)$ given by

$$(\varphi \mid \gamma)(D) = \varphi(\gamma D) \mid \gamma$$

for $\varphi \in Hom(\Delta_0, V)$, $D \in \Delta_0$ and $\gamma \in \Sigma_0(p)$. Let $\Gamma \subset \Gamma_0(p) \cap \Gamma_1(N)$ be a congruence subgroup of level Np with $(N,p) = 1$ and observe that Γ has a right action on V and $Hom(\Delta_0, V)$ inherited from $\Sigma_0(p)$. We define the space of *V-valued modular symbols on* Γ to be

$$Symb_\Gamma(V) := \{\varphi \in Hom(\Delta_0, V) : \varphi \mid \gamma = \varphi \text{ for all } \gamma \in \Gamma\}$$

Note that the matrix $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in \Sigma_0(p)$ acts as an involution on $Symb_\Gamma(V)$ and decomposes $Symb_\Gamma(V)$ into ± 1-eigenspaces

$$Symb_\Gamma(V) \simeq Symb_\Gamma(V)^+ \oplus Symb_\Gamma(V)^-$$

Hypothesis: We henceforth keep the assumption $\Gamma \subset \Gamma_0(p) \cap \Gamma_1(N)$ for any congruence subgroup we denote by Γ.

Through the action of $\Sigma_0(p)$ on V, we may define a Hecke-action on $Symb_\Gamma(V)$ with T_ℓ acting via the double coset $\Gamma\begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}\Gamma$ for a prime ℓ. We adopt the standard nomenclature for the Hecke operators so that the operator T_q is to be renamed U_q if q divides the level of Γ. We then have,

$$\varphi \mid T_\ell = \varphi \mid \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} + \sum_{a=0}^{\ell-1} \varphi \mid \begin{pmatrix} 1 & a \\ 0 & \ell \end{pmatrix}$$

$$\varphi \mid U_q = \sum_{a=0}^{q-1} \varphi \mid \begin{pmatrix} 1 & a \\ 0 & q \end{pmatrix}$$

for all $\varphi \in Symb_\Gamma(V)$.

For the most part, we will involve ourselves with two very specific right $\mathbb{Z}_p[\Sigma_0(p)]$-modules, namely $V = V_k(\mathbb{Q}_p)$ and $V = \mathcal{D}_k$, both of which are yet to be defined. In what follows, we introduce $V_k(\mathbb{Q}_p)$ & $\mathcal{D}_k$, the dual objects $Symb_\Gamma(V_k(\mathbb{Q}_p))$ & $Symb_\Gamma(\mathcal{D}_k)$ and discuss in detail how they relate to one another.

We let $V_k := V_k(\mathbb{Q}_p) := Sym^k(\mathbb{Q}_p^2)$ denote the space of homogeneous polynomials of degree k in $\mathbb{Q}_p[X, Y]$. $\Sigma_0(p)$ acts on V_k on the right via

$$(P \mid \gamma)(X, Y) := P(dX - cY, -bX + aY)$$

for $P \in V_k$ and $\gamma \in \Sigma_0(p)$. In essentially the same way $V_k(\mathbb{C})$ is related to cusp forms on $\mathbb{C}$, $V_k(\mathbb{Q}_p)$ is related to cusp forms on $\mathbb{Q}_p$ as made precise below.

Let $S_{k+2}(\Gamma, \mathbb{Q})$ denote the space of weight $k+2$ cusp forms in $S_{k+2}(\Gamma, \mathbb{C})$ whose q-expansions at ∞ have all rational coefficients. As is well known, there exists an isomorphism $S_{k+2}(\Gamma, \mathbb{C}) \simeq S_{k+2}(\Gamma, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C}$ since $S_{k+2}(\Gamma, \mathbb{C})$ admits a basis consisting of cusp forms contained in $S_{k+2}(\Gamma, \mathbb{Q})$. Analogously, for any $\mathbb{Q}$-algebra R, we define $S_{k+2}(\Gamma, R)$ to be $S_{k+2}(\Gamma, \mathbb{Q}) \otimes_{\mathbb{Q}} R$.

To a cusp form $f \in S_{k+2}(\Gamma, \overline{\mathbb{Q}}_p)$, we attach a pair of modular symbols $\varphi_f^\pm \in Symb_\Gamma(V_k)^\pm \otimes \overline{\mathbb{Q}}_p$ by setting

$$\varphi_f^\pm(\{s\} - \{r\}) = \frac{\pi i}{\Omega_f^\pm} \left(\int_r^s f(z)\,(zX + Y)^k\, dz \pm (-1)^k \int_{-r}^{-s} f(z)\,(zX - Y)^k\, dz \right)$$

where the periods $\Omega_f^{\pm}$ are chosen so that $\varphi_f^{\pm}$ take only integral values and at least one unit value. Note that if $f \in S_{k+2}(\Gamma, \mathbb{C})$ is an eigenform for the full Hecke-algebra, then f sits inside $S_{k+2}(\Gamma, \overline{\mathbb{Q}})$ and we may view f as an element of $S_{k+2}(\Gamma, \overline{\mathbb{Q}}_p)$ under our fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. In that case, f and $\varphi_f^{\pm}$ share the same system of eigenvalues, and in fact, $\varphi_f^{\pm}$ generates the f-isotypic subspace of $Symb_{\Gamma}(V_k)^{\pm} \otimes \overline{\mathbb{Q}}_p$. We highlight the fact that $\varphi_f^{\pm}$ are essentially the $\pm$ parts of $2\pi i \int f(z)(zX+Y)^k dz$ normalized with respect to $\Omega_f^{\pm}$.

2.3 Overconvergent Modular Symbols

We now set out to construct what we call the space of locally analytic distributions on $\mathbb{Z}_p$, which we denote by $\mathcal{D}$. We realize $\mathcal{D}$ as the continuous dual of locally analytic functions on $\mathbb{Z}_p$ after suitably topologizing the latter space. As a first step in our construction, for each $r \in |\mathbb{C}_p^{\times}|$, we set

$$B[\mathbb{Z}_p, r] := \{z \in \mathbb{C}_p : \exists a \in \mathbb{Z}_p \text{ with } |z-a| \leq r\}$$

For example we have,

$$\begin{aligned} r \geq 1 &\implies B[\mathbb{Z}_p, r] \text{ is the closed disc in } \mathbb{C}_p \text{ of radius } r \text{ around } 0 \\ r = 1/p &\implies B[\mathbb{Z}_p, r] \text{ is the disjoint union of } p \text{ discs of radius } 1/p \\ &\qquad \text{around the points } 0, 1, ..., p-1 \end{aligned}$$

Let $\mathbf{A}[r]$ denote the $\mathbb{Q}_p$-algebra of rigid analytic functions on $B[\mathbb{Z}_p, r]$.

$$\begin{aligned} r \geq 1 &\implies \mathbf{A}[r] = \{F(z) = \Sigma a_n z^n \ \in \mathbb{Q}_p[[z]] : |a_n| \cdot r^n \to 0\} \\ r = 1/p &\implies \mathbf{A}[r] = \{\text{functions on } B[\mathbb{Z}_p, r] \text{ which are analytic} \\ &\qquad \text{on each of the } p \text{ discs of radius } 1/p\} \end{aligned}$$

Each $\mathbf{A}[r]$ is a Banach algebra under the sup norm $\|F\|_r = \sup_{z \in B[\mathbb{Z}_p, r]} |F(z)|$ and for $r_1 > r_2$, there is a continuous injection $\mathbf{A}[r_1] \hookrightarrow \mathbf{A}[r_2]$.

Now let $\mathcal{A}$ denote the set of locally analytic $\mathbb{Q}_p$ valued functions on $\mathbb{Z}_p$. As $\mathbb{Z}_p \subset B[\mathbb{Z}_p, r]$ for any $r > 0$, we have restriction maps $\mathbf{A}[r] \to \mathcal{A}$. Since $\mathbb{Z}_p$ is compact, any element of $\mathcal{A}$ is representable by finitely many power series and any such power series must be in the image of $\mathbf{A}[r]$ in $\mathcal{A}$ for some r. Thus

$$\mathcal{A} = \varinjlim_{r>0} \mathbf{A}[r]$$

We endow $\mathcal{A}$ with the inductive limit topology, the strongest topology for which all inclusions $\mathbf{A}[r] \hookrightarrow \mathcal{A}$ are continuous, and set

$$\mathcal{D} := Hom_{cont}(\mathcal{A}, \mathbb{Q}_p)$$

to be the space of *locally analytic distributions*. Equivalently, if we define $\mathbf{D}[r] := Hom_{cont}(\mathbf{A}[r], \mathbb{Q}_p)$ to be the continuous $\mathbb{Q}_p$-dual of $\mathbf{A}[r]$, we can realize $\mathcal{D}$ as

$$\mathcal{D} = \varprojlim_{r>0} \mathbf{D}[r]$$

equipped with the projective limit topology. Note that we have natural continuous injections

$$\mathbf{A}[r] \hookrightarrow \mathcal{A} \quad \text{and} \quad \mathcal{D} \hookrightarrow \mathbf{D}[r]$$

for any $r > 0$. Further note that $\mathbf{D}[r]$ is a Banach space under the norm

$$\|\mu\|_r = \sup_{F \in \mathbf{A}[r],\, F \neq 0} \frac{|\mu(F)|}{\|F\|}$$

We henceforth denote $\mathbf{A}[1]$ and $\mathbf{D}[1]$ by $\mathbf{A}$ and $\mathbf{D}$ respectively.

The distribution spaces $\mathcal{D}$ and $\mathbf{D}$ admit a right action of the semigroup $\Sigma_0(p)$. Indeed, for each $k \geq 0$, $\Sigma_0(p)$ has a weight k left action on $\mathcal{A}$ (resp. $\mathbf{A}$) given by

$$(\gamma \mid_k F)(z) = (a+cz)^k F\left(\frac{b+dz}{a+cz}\right)$$

which induces a right action on $\mathcal{D}$ (resp. $\mathbf{D}$) via

$$(\mu \mid_k \gamma)(F) = \mu(\gamma \mid_k F)$$

We write $\mathcal{D}_k$ and $\mathbf{D}_k$ to incorporate the weight k action of $\Sigma_0(p)$ into our notation. When thought together with this action, $\mathcal{D}_k$ and $\mathbf{D}_k$ assume a right $\mathbb{Z}_p[\Sigma_0(p)]$-module structure.

Definition 2.3. *The space $Symb_\Gamma(D_k)$ is a space of* overconvergent modular symbols *of level Γ considered together with the weight k action of $\Sigma_0(p)$ for $D_k = \mathcal{D}_k$ or $\boldsymbol{D}_k$.*

Let us elaborate on the Hecke structure on $Symb_\Gamma(\mathcal{D}_k)$. Due to our running hypothesis $\Gamma \subset \Gamma_0(p) \cap \Gamma_1(N)$, the p-th Hecke operator on $Symb_\Gamma(\mathcal{D}_k)$ is given by the action of U_p. Let us denote the matrix $\begin{pmatrix} 1 & a \\ 0 & p^n \end{pmatrix}$ by $\gamma(a,p^n)$ and let $\Phi \in Symb_\Gamma(V)$ be a U_p-eigensymbol with eigenvalue λ. We then have

$$\begin{aligned}\Phi(D) &= \lambda^{-n}(\Phi \mid U_p^n)(D) \\ &= \lambda^{-n}\sum_{a=0}^{p^n-1} \Phi\big(\gamma(a,p^n)D\big) \mid \gamma(a,p^n)\end{aligned}$$

Now, each $\Phi\big(\gamma(a,p^n)D\big)$ defines a distribution in $\mathcal{D}$. For an arbitrary $\mu \in \mathcal{D}$ and $F \in \mathcal{A}$,

$$\begin{aligned}\big(\mu \mid \gamma(a,p^n)\big)(F) &= \mu\big(F(a+p^n z)\big) \\ &= \big(\mu \mid \gamma(a,p^n)\big)(F \cdot \chi_{a+p^n\mathbb{Z}_p})\end{aligned}$$

so that $\mu \mid \gamma(a, p^n)$ is zero on F outside of $a + p^n\mathbb{Z}_p$, i.e.

$$\mu \mid \gamma(a, p^n)(F) = \mu \mid \gamma(a, p^n)\big|_{a+p^n\mathbb{Z}_p}(F)$$

By a slight abuse of language, we say that μ *has support contained in* $a + p^n\mathbb{Z}_p$. Thus, if $\Phi \in Symb_\Gamma(\mathcal{D}_k)$ is a U_p-eigensymbol, then the operator U_p^n breaks $\Phi(D)$ into p^n distributions each essentially operating on a disc of the form $a + p^n\mathbb{Z}_p$. Denoting $\Phi(\gamma(a, p^n)D) \mid \gamma(a, p^n)$ by $\Phi_{a,n}(D_n)$ for notational simplicity, we get

$$\Phi(D)(f) = \lambda^{-n} \sum_{a=0}^{p^n-1} \Phi_{a,n}(D_n)(f \cdot \chi_{a+p^n\mathbb{Z}_p}) = \lambda^{-n} \sum_{a=0}^{p^n-1} \Phi_{a,n}(D_n)(f)$$

2.4 The Specialization Map

We now proceed to establish a link between the spaces of overconvergent modular symbols $Symb_\Gamma(\mathcal{D}_k)$ and classical modular symbols $Symb_\Gamma(V_k)$ as introduced in Section 2.2. More specifically, we will construct a Hecke equivariant map ρ_k^* called *the specialization map*, which restricts to an isomorphism between certain well-behaved subspaces.

Theorem 2.4. *Let* $D_k = \mathcal{D}_k$ *or* $\boldsymbol{D}_k$. *Then the map*

$$\begin{aligned} \rho_k : D_k &\longrightarrow V_k(\mathbb{Q}_p) \\ \mu &\longmapsto \int (Y - zX)^k d\mu \end{aligned}$$

is $\Sigma_0(p)$*-equivariant, where the integration takes place with respect to* z *and the variables* X *&* Y *are treated as coefficients.*

Proof. Let us verify for the $k = 2$ case via explicit calculations. For $\mu \in D_2$ and $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Sigma_0(p)$ we have;

$$\begin{aligned}
&\rho_2\left(\mu \,|_2 \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right) \\
&= \int (Y - zX)^2 \, d\left(\mu \,|_2 \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right) \\
&= \sum_{j=0}^{2} (-1)^j \binom{2}{j} \mu\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) |_2 \, z^j\right) X^j \, Y^{2-j} \\
&= \mu\left((a + cz)^2\right) Y^2 - 2\mu\left((b + dz)(a + cz)\right) XY + \mu\left((b + dz)^2\right) X^2 \\
&= \mu(1)(-bX + aY)^2 - 2\mu(z)(dX - cY)(-bX + aY) + \mu(z^2)(dX - cY)^2 \\
&= \rho_2(\mu) \mid \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)
\end{aligned}$$

The general proof follows from obvious modifications to the case we considered above.

□

Remark 2.5. As can be observed in the calculations above, the expression $\mu(z^j)$ appears within the coefficient of the $X^j Y^{k-j}$ term for $0 \le j \le k$. Also, recall that the modular symbols in V_k correspond to modular forms of weight $k + 2$. Further, recall our running hypothesis $\Gamma \subset \Gamma_0(p) \cap \Gamma_1(N)$.

Theorem 2.6. *ρ_k induces a surjective Hecke equivariant map*

$$\rho_k^* : Symb_\Gamma(\boldsymbol{D}_k) \longrightarrow \; Symb_\Gamma(V_k)$$

via

$$\rho_k^*\left(\Phi\right)\left(D\right) = \rho_k\left(\Phi(D)\right)$$

Proof. Hecke equivariance follows at once from the $\Sigma_0(p)$-equivariance of ρ_k and remains true if we replace $\mathbf{D}_k$ with $\mathcal{D}_k$ since $\mathcal{D}_k \hookrightarrow \mathbf{D}_k$. For surjectivity, see [PS11] Theorem 5.1 and Corollary 5.4.

□

The map ρ_k^* is what we refer to as *the specialization map* and it enables us to view the space of classical modular symbols as a quotient of overconvergent modular symbols. We highlight the fact that ρ_k^* maps an infinite dimensional space to a finite dimensional one and thence has an infinite dimensional kernel. In what follows, we describe $ker(\rho_k^*)$ in terms of the operator U_p.

Definition 2.7. *Let f be an eigenform of weight $k+2$ on Γ, φ an eigensymbol in $Symb_\Gamma(V_k)$, Φ an overconvergent eigensymbol in $Symb_\Gamma(\mathcal{D}_k)$ or $Symb_\Gamma(\boldsymbol{D}_k)$. We define the slope of θ at p to be the valuation of its U_p-eigenvalue for $\theta = f, \varphi, \Phi$.*

Lemma 2.8. *Slope of a weight $k+2$ eigenform f on Γ is at most $k+1$.*

Proof. Let $\alpha = a_p(f)$ be the U_p-eigenvalue of f. If f is new at p, then $\alpha = \pm p^{k/2}$ and thus f has slope $k/2$. If f is old at p, then α, viewed as an element of $\overline{\mathbb{Q}}$, satisfies $\alpha\overline{\alpha} = p^{k+1}$ and hence $0 \leq ord_p(\alpha) \leq k+1$. As such, slope of f (at p) is at most $k+1$ as claimed.

□

Now, the specialization map $\rho_k^* : Symb_\Gamma(\mathbf{D}_k) \to Symb_\Gamma(V_k)$ is Hecke equivariant and U_p acts on the image with slope at most $k+1$. Thus the entire subspace of $Symb_\Gamma(\mathbf{D}_k)$ of slope $> k+1$ must be in the kernel of ρ_k^*. The following control theorem due to Stevens extends this simple observation and gives an isomorphism result between small slope subspaces. We adopt the notation that if V is a $\mathbb{Z}_p[\Gamma]$-module endowed with a Hecke action, $V^{(<h)}$ refers to the subspace obtained by taking a direct sum over the generalized U_p-eigenspaces of V on which U_p acts with slope strictly less than h.

Theorem 2.9. *(Stevens) ρ_k^* restricted to slope $< k+1$ subspace of $Symb_\Gamma(\boldsymbol{D}_k)$*

$$Symb_\Gamma(\boldsymbol{D}_k)^{(<k+1)} \xrightarrow{\rho_k^*} Symb_\Gamma(V_k)^{(<k+1)}$$

is a Hecke equivariant isomorphism.

Proof. See [PS11] Theorem 5.12

□

Recall that the space of locally analytic distributions $\mathcal{D}_k$ injects into $\mathbf{D}_k$, which lends itself to an inclusion $Symb_\Gamma(\mathcal{D}_k) \hookrightarrow Symb_\Gamma(\mathbf{D}_k)$. Focusing instead on the finite slope subspaces, we now establish an isomorphism relation.

Theorem 2.10. *For any $h < \infty$, the inclusion*

$$Symb_\Gamma(\mathcal{D}_k)^{(<h)} \hookrightarrow Symb_\Gamma(\boldsymbol{D}_k)^{(<h)}$$

is an isomorphism.

Proof. Let $\Phi \in Symb_\Gamma(\mathbf{D}_k)^{(<h)}$. We will show that for any divisor $D \in \Delta_0$, $\Phi(D)$ defines a locally analytic distribution in $\mathcal{D}$, i.e. $\Phi(D) \in \mathcal{D}$ and hence $\Phi \in Symb_\Gamma(\mathcal{D}_k)$. Since $h < \infty$, the linear operator U_p is injective on both spaces and as the spaces are finite dimensional, U_p is an automorphism of both. Therefore, Φ must be in the image of U_p^n for all n. Let $\Psi \in Symb_\Gamma(\mathbf{D}_k)$ be such that $\Psi \mid U_p^n = \Phi$ and let $\gamma(a,p^n)$ denote the matrix $\begin{pmatrix} 1 & a \\ 0 & p^n \end{pmatrix} \in \Sigma_0(p)$. Then, for any divisor $D \in \Delta_0$ we have

$$\begin{aligned} \Phi(D)(F) = (\Psi \mid U_p^n)(D)(F) = &= \sum_{a=0}^{p^n-1} \left(\Psi \mid \gamma(a,p^n)\right)(D)(F) \\ &= \sum_{a=0}^{p^n-1} \Big(\Psi\left(\gamma(a,p^n)D\right) \mid \gamma(a,p^n)\Big)(F) \\ &= \sum_{a=0}^{p^n-1} \Psi\left(\gamma(a,p^n)D\right)\left(\gamma(a,p^n) \mid F\right) \end{aligned}$$

Now, for any function $F \in \mathbf{A}[p^{-n}]$, the translation $\gamma(a,p^n) \mid F$ lands in $\mathbf{A}[1] = \mathbf{A}$ and thus the distributions $\Psi\big(\gamma(a,p^n)D\big) \in \mathbf{D}$ can be evaluated at $\gamma(a,p^n) \mid g$. Therefore, $\Phi(D)$ naturally extends to a distribution in $\mathbf{D}[p^{-n}]$ through our calculations above. Since n was arbitrary and $\mathcal{D}$ is given by the limit $\varprojlim_{r>0} \mathbf{D}[r]$, we get $\Phi(D) \in \mathcal{D}$.

□

The following then is an immediate consequence of the two preceding theorems:

Corollary 2.11. *The composition*

$$Symb_\Gamma(\mathcal{D}_k)^{(<k+1)} \xrightarrow{\sim} Symb_\Gamma(\boldsymbol{D}_k)^{(<k+1)} \xrightarrow[\rho_k^*]{\sim} Symb_\Gamma(V_k)^{(<k+1)}$$

defines a Hecke equivariant isomorphism.

The corollary above is the main result we have been after. It says that if φ is a small slope U_p-eigensymbol in $Symb_\Gamma(V_k)$, then there is a unique overconvergent U_p-eigensymbol Φ in $Symb_\Gamma(\mathcal{D}_k)$ lifting φ with the same U_p-eigenvalue as φ.

2.5 p-adic L-functions via Overconvergent Modular Symbols

Recall that the space of analytic distributions $\mathcal{D}$ injects into $\mathbf{D}[r]$ for every $r > 0$. Further recall that each $\mathbf{D}[r]$ is a Banach space under the norm

$$\|\mu\|_r = \sup_{F \in \mathbf{A}[r],\, F \neq 0} \frac{\big|\mu(F)\big|}{\|F\|}$$

The two together imply that $\mathcal{D}$ is naturally equipped with a family of norms $\{\|\cdot\|_r\}_{r>0}$ satisfying $\|\mu\|_{r_1} \geq \|\mu\|_{r_2}$ for $r_1 \leq r_2$.

Proposition 2.12. *Let $\Phi \in Symb_\Gamma(\mathcal{D}_k)$ be a U_p-eigensymbol of slope h. Then for any $D \in \Delta_0$, the distribution $\Phi(D)$ satisfies $\big\|\Phi(D)\big\|_r = O(r^{-h})$ as $r \to 0^+$.*

Proof. See Definition 6.1 and Lemma 6.2 of [PS11].

□

Corollary 2.13. *For Φ as above and $D \in \Delta_0$ arbitrary, restriction of $\Phi(D)$ to $\mathbb{Z}_p^\times$ is h-admissible.*

Proof. After rewriting the growth condition given in Definition 1.10 as

$$\sup_{a \in \mathbb{Z}_p^\times} \frac{\left|\mu\left((x-a)^i \cdot \chi_{a+p^n\mathbb{Z}_p}\right)\right|}{\left\|(x-a)^i \cdot \chi_{a+p^n\mathbb{Z}_p}\right\|} = O(p^{nh}) \text{ as } n \to \infty$$

the corollary follows at once from the proposition above.

□

Let $f \in S_{k+2}(N, \epsilon)$ be a cuspidal normalized eigenform of weight $k+2$, level N with $(N,p) = 1$ and character ϵ as in Section 1.4. Fix a choice of periods $\Omega_f^\pm$ satisfying Theorem 1.17 and let α_1 and α_2 denote the roots of the Hecke polynomial $x^2 - a_p(f)x + \epsilon(p)p^k$. Recall that α_i is called allowable if $ord_p(\alpha_i) < k+1$. Fix an allowable root $\alpha \in \{\alpha_1, \alpha_2\}$ and call the other root β. Set

$$f_\alpha(z) = f(z) - \beta f(pz)$$

Then f_α is a weight $k+2$ eigenform on a congruence subgroup $\Gamma \subset \Gamma_1(N) \cap \Gamma_0(p)$ with the same Hecke eigenvalues as f away from p and U_p-eigenvalue α. We note that Γ satisfies our running hypothesis on congruence subgroups.

Recall that the h-admissible distributions $\mu_{f,\alpha}^\pm$ attached to f with respect to the allowable root α are explicitly given by

$$\mu_{f,\alpha}^\pm(P,\ a + p^n\mathbb{Z}_p) = \frac{\lambda^\pm(f, P; a, p^n)}{\alpha^n} - \frac{\epsilon(p)p^k\lambda^\pm(f, P; a, p^{n-1})}{\alpha^{n+1}} \in K(\alpha)$$

where P is a polynomial of degree $\leq k$ and $\lambda^\pm$ are as defined in Section 1.4.

Proposition 2.14. *With f and f_α as above,*

$$\mu_{f,\alpha}^\pm(P,\ a + p^n\mathbb{Z}_p) = \frac{\lambda^\pm(f_\alpha, P; a, p^n)}{\alpha^n}$$

Proof. As $f_\alpha(z) = f(z) - \beta f(pz)$,

$$\begin{aligned}
&\alpha^{-n}\lambda^{\pm}(f_\alpha, P; a, p^n) \\
&= \alpha^{-n}\left(\int_{i\infty}^{a/p^n} P(-p^n z + a) f_\alpha(z) dz \pm \int_{i\infty}^{-a/p^n} P(p^n z + a) f_\alpha(z) dz\right)\frac{\pi i}{\Omega_f^{\pm}} \\
&= \alpha^{-n}\left(A^{\pm} - B^{\pm}\right)\frac{\pi i}{\Omega_f^{\pm}}
\end{aligned}$$

where $A^{\pm}$ and $B^{\pm}$ are

$$A^{\pm} = \int_{i\infty}^{a/p^n} P(-p^n z + a) f(z) dz \pm \int_{i\infty}^{-a/p^n} P(p^n z + a) f(z) dz$$

$$B^{\pm} = \int_{i\infty}^{a/p^n} P(-p^n z + a)\beta f(pz) dz \pm \int_{i\infty}^{-a/p^n} P(p^n z + a)\beta f(pz) dz$$

Performing a change of variables $pz \mapsto z$ in $B^{\pm}$ and using $\alpha\beta = \epsilon(p)p^k$ we find

$$\frac{\lambda^{\pm}(f_\alpha, P; a, p^n)}{\alpha^n} = \frac{\lambda^{\pm}(f, P; a, p^n)}{\alpha^n} - \frac{\epsilon(p)p^{k-2}\lambda^{\pm}(f, P; a, p^{n-1})}{\alpha^{n+1}}$$

□

As f_α is an eigenform the full Hecke algebra, it lies inside the subspace $S_{k+2}(\Gamma, \overline{\mathbb{Q}})$. Viewing then f_α as an element of $S_{k+2}(\Gamma, \overline{\mathbb{Q}}_p)$ under our fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, denote by $\varphi_{f_\alpha}^{\pm}$ the associated modular symbol in $Symb_\Gamma(V_k(\mathbb{Q}_p))^{\pm} \otimes \overline{\mathbb{Q}}_p$ as defined in Section 2.2. Explicitly,

$$\varphi_{f_\alpha}^{\pm}\left(\{s\} - \{r\}\right) = \frac{\pi i}{\Omega_f^{\pm}}\left(\int_r^s f_\alpha(z)\,(zX + Y)^k\,dz \pm (-1)^k \int_{-r}^{-s} f_\alpha(z)\,(zX - Y)^k\,dz\right)$$

Since f_α and $\varphi_{f_\alpha}^{\pm}$ share the same system of eigenvalues and α is allowable, $\varphi_{f_\alpha}^{\pm}$ is of slope $< k + 1$. By Corollary 2.11, there exists a unique overconvergent modular symbol $\Phi_{f_\alpha}^{\pm} \in Symb_\Gamma(\mathcal{D}_k)^{\pm} \otimes \overline{\mathbb{Q}}_p$ lifting $\varphi_{f_\alpha}^{\pm}$, i.e. $\Phi_{f_\alpha}^{\pm}$ satisfies $\rho_k^*(\Phi_{f_\alpha}^{\pm}) = \varphi_{f_\alpha}^{\pm}$. Since the specialization map ρ_k^* is Hecke equivariant and $\varphi_{f_\alpha}^{\pm}$ is a U_p-eigensymbol with eigenvalue α, $\Phi_{f_\alpha}^{\pm}$ also must be a U_p-eigensymbol with the same U_p-eigenvalue.

Theorem 2.15. *Restriction of* $\Phi^{\pm}_{f_\alpha}\big(\{0\}-\{\infty\}\big)$ *to* $\mathbb{Z}_p^\times$ *is the* p*-adic distribution* $\mu^{\pm}_{f,\alpha}$ *attached to* f*, or in no words,*

$$\Phi^{\pm}_{f_\alpha}\big(\{0\}-\{\infty\}\big)\big|_{\mathbb{Z}_p^\times} = \mu^{\pm}_{f,\alpha}$$

Proof. Let $h = ord_p(\alpha)$. Then $\Phi^{\pm}_{f_\alpha}\big(\{0\}-\{\infty\}\big)$ and $\mu^{\pm}_{f,\alpha}$ are both h-admissible by Corollary 2.13 and Proposition 1.22 respectively. Therefore it suffices to establish equality whenever the two distributions are evaluated on $C^h(\mathbb{Z}_p^\times)$. As functions in $C^h(\mathbb{Z}_p^\times)$ are locally given by polynomials of degree $\leq h < k+1$ and distributions are additive, we may further reduce to the case of showing equality for functions that are of the form $z^j \cdot \chi_{a+p^n\mathbb{Z}_p}$ for $0 \leq j \leq k$.

Now, the overconvergent modular symbol $\Phi^{\pm}_{f_\alpha}$ is a U_p-eigensymbol with eigenvalue α. Therefore,

$$\begin{aligned}\Phi^{\pm}_{f_\alpha}\big(\{0\}-\{\infty\}\big) &= \alpha^{-n}\left(\Phi^{\pm}_{f_\alpha} \mid U_p^n\right)\big(\{0\}-\{\infty\}\big)\\ &= \alpha^{-n}\left(\sum_{a=0}^{p^n-1}\Phi^{\pm}_{f_\alpha}\big(\{a/p^n\}-\{\infty\}\big) \mid \gamma(a,p^n)\right)\end{aligned}$$

As discussed after Definition 2.3, the distributions $\Phi^{\pm}_{f_\alpha}\big(\{a/p^n\}-\{\infty\}\big) \mid \gamma(a,p^n)$ appearing in the above sum have support fully contained in $a+p^n\mathbb{Z}_p$ for $a = 0,\ldots,p^{n-1}$. Thus, for $z^j \cdot \chi_{a+p^n\mathbb{Z}_p} \in C^h(\mathbb{Z}_p^\times)$,

$$\begin{aligned}&\Phi^{\pm}_{f_\alpha}\big(\{0\}-\{\infty\}\big)\left(z^j \cdot \chi_{a+p^n\mathbb{Z}_p}\right) \qquad (*)\\ &= \alpha^{-n}\left(\Phi^{\pm}_{f_\alpha}\big(\{a/p^n\}-\{\infty\}\big) \mid \gamma(a,p^n)\right)\left(z^j \cdot \chi_{a+p^n\mathbb{Z}_p}\right)\\ &= \alpha^{-n}\,\Phi^{\pm}_{f_\alpha}\big(\{a/p^n\}-\{\infty\}\big)\left(\,(p^n z + a)^j\,\right)\end{aligned}$$

We may now use the specialization map ρ_k^* to make explicit that final line above. By definition of ρ_k^*,

$$\rho_k^*(\Phi^{\pm}_{f_\alpha})(\{a/p^n\}-\{\infty\}) = \rho_k\left(\Phi^{\pm}_{f_\alpha}\big(\{a/p^n\}-\{\infty\}\big)\right)$$

The right hand side of the above equality reads

$$\begin{aligned} &\rho_k\left(\Phi^{\pm}_{f_\alpha}\left(\{a/p^n\}-\{\infty\}\right)\right) \\ &= \int (Y-zX)^k \, d\Phi^{\pm}_{f_\alpha}\left(\{a/p^n\}-\{\infty\}\right) \end{aligned} \tag{A}$$

while the left hand side is given by

$$\begin{aligned} &\rho_k^*(\Phi^{\pm}_{f_\alpha})\left(\{a/p^n\}-\{\infty\}\right) \\ &= \varphi^{\pm}_{f_\alpha}\left(\{a/p^n\}-\{\infty\}\right) \\ &= \frac{\pi i}{\Omega_f^{\pm}}\left(\int_{i\infty}^{a/p^n} f_\alpha(z)\,(zX+Y)^k\,dz \pm (-1)^k \int_{i\infty}^{-a/p^n} f_\alpha(z)\,(zX-Y)^k\,dz\right) \end{aligned} \tag{B}$$

so the two expressions labeled (A) and (B) must match coefficient by coefficient. For example, the coefficient in front of the Y^k term in (A) is $\Phi^{\pm}_{f_\alpha}\left(\{a/p^n\}-\{\infty\}\right)(1)$ and is $\int_{i\infty}^{a/p^n} f_\alpha(z)\,dz \pm \int_{i\infty}^{-a/p^n} f_\alpha(z)\,dz$ in (B). Accordingly, we must have

$$\Phi^{\pm}_{f_\alpha}\left(\{a/p^n\}-\{\infty\}\right)(1) = \frac{\pi i}{\Omega_f^{\pm}}\left(\int_{i\infty}^{a/p^n} f_\alpha(z)\,dz \pm \int_{i\infty}^{-a/p^n} f_\alpha(z)\,dz\right)$$

Similarly, equating the coefficients appearing in front of the XY^{k-1} terms, we find

$$\Phi^{\pm}_{f_\alpha}\left(\{a/p^n\}-\{\infty\}\right)(z) = \frac{\pi i}{\Omega_f^{\pm}}\left(\int_{i\infty}^{a/p^n} (-z) f_\alpha(z)\,dz \pm \int_{i\infty}^{-a/p^n} z\, f_\alpha(z)\,dz\right)$$

Continuing in this way, we extract the values $\Phi^{\pm}_{f_\alpha}\left(\{a/p^n\}-\{\infty\}\right)(z^j)$ for $0 \le j \le k$ and using linearity of $\Phi^{\pm}_{f_\alpha}\left(\{a/p^n\}-\{\infty\}\right)$, we arrive at the following: For a polynomial Q of degree $\le k$;

$$\Phi^{\pm}_{f_\alpha}\left(\{a/p^n\}-\{\infty\}\right)\left(\,Q(z)\,\right) = \frac{\pi i}{\Omega_f^{\pm}}\left(\int_{i\infty}^{a/p^n} Q(-z)\, f_\alpha(z)\,dz \pm \int_{i\infty}^{-a/p^n} Q(z)\, f_\alpha(z)\,dz\right)$$

In particular, assigning $(p^n z + a)^j$ to $Q(z)$ and substituting in $(*)$ we get,

$$\begin{aligned}
&\Phi^{\pm}_{f_\alpha}\left(\{0\} - \{\infty\}\right)(z^j \cdot \chi_{a+p^n\mathbb{Z}_p}) \\
&= \alpha^{-n}\, \Phi^{\pm}_{f_\alpha}\left(\{a/p^n\} - \{\infty\}\right)(\ (p^n z + a)^j\ ) \\
&= \alpha^{-n} \frac{\pi i}{\Omega^{\pm}_f}\left(\int_{i\infty}^{a/p^n} (-p^n z + a)^j\ f_\alpha(z)\ dz \pm \int_{i\infty}^{-a/p^n} (p^n z + a)^j\ f_\alpha(z)\ dz\right)
\end{aligned}$$

where the last line precisely is $\alpha^{-n}\lambda^{\pm}(f_\alpha, z^j; a, p^n)$. But by Proposition 2.14,

$$\frac{\lambda^{\pm}(f_\alpha, z^j; a, p^n)}{\alpha^n} \ = \ \mu^{\pm}_{f,\alpha}(z^j \cdot \chi_{a+p^n\mathbb{Z}_p})$$

and therefore $\Phi^{\pm}_{f_\alpha}\left(\{0\} - \{\infty\}\right)\big|_{\mathbb{Z}_p^\times}$ and $\mu^{\pm}_{f,\alpha}$ agree on all of $C^h(\mathbb{Z}_p^\times)$ by linearity. Both distributions being h-admissible then implies that they are one and the same.

$\square$

BIBLIOGRAPHY

[AV75] Y. Amice, J. Vélu: *Distributions p-adiques associées aux séries de Hecke*, in Journées Arithmétiques de Bordeaux (Bordeaux, 1974), Astérisque **24-25**, Société Mathématique de France, Montrogue, 1975, 119-131.

[BCDT01] 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** (2001), 843-939.

[BMS12] J. Balakrishnan, J. Müller, W. Stein: *A p-adic analogue of the conjecture of Birch and Swinnerton-Dyer for modular abelian varieties*, Mathematics of Computation, **85** (2016), 983-1016.

[BPR93] D. Bernardi, B. Perrin-Riou: *Variante p-adique de la conjecture de Birch et Swinnerton-Dyer (le cas supersingulier)*, Comptes Rendus de l'Académie des Sciences. Paris Série I Mathématique **317** (1993), no. 3, 227-232.

[Büy15] K. Büyükboduk: *Beilinson-Kato and Beilinson-Flach elements, Coleman-Rubin-Stark classes, Heegner points and the Perrin-Riou Conjecture*, arXiv:1511.06131

[Col04] P. Colmez: *La conjecture de Birch et Swinnerton-Dyer p-adique*, Astérisque **294, ix** (2004), 251-319.

[DP06] H. Darmon, R. Pollack *The efficient calculation of Stark-Heegner points via overconvergent modular symbols*, Israel Journal of Mathematics **153** (2006), 319-354.

[Kob] N. Koblitz : *p-adic numbers, p-adic analysis, and zeta-functions.* Second edition. Graduate Texts in Mathematics, 58. (1984) Springer-Verlag, New York.

[KP07] M. Kurihara, R. Pollack: *Two p-adic L-functions and rational points on elliptic curves with supersingular reduction*, L-functions and Galois representations, 300-332.

[Lang] S. Lang : *Cyclotomic fields I and II. Combined second edition. With an appendix by Karl Rubin.* (1990) Springer-Verlag, New York.

[Man72] J. Manin: *Parabolic points and zeta functions of modular curves*, Izvestiya Akademii Nauk SSSR. Seriya Matematičeskaya **36** (1972), 19-66.

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

[MTT86] B. Mazur, J. Tate, and J. Teitelbaum: *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), 1-48.

[Pol03] R. Pollack: *The p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), no. 1, 1-36.

[Pol11] R. Pollack: Overconvergent modular symbols. Lecture Notes from the Arizona Winter School, 2011.

[PR93] B. Perrin-Riou: *Fonctions L p-adiques d'une courbe elliptique et points rationnels* Annales de l'Institute Fourier, **43**, no.4 (1993), pp. 945–995.

[PR03] B. Perrin-Riou: *Arithmétique des courbes elliptiques à réduction supersingulière.* Experiment. Math. **12** (2003), 155-186.

[PS11] R. Pollack and G. Stevens, *Overconvergent modular symbols and p-adic L-functions*, Ann. Sci. Éc. Norm. Supér. (4) **44** (2011), no. 1, 1–42.

[Silv] J. Silverman: *The arithmetic of elliptic curves*, Second Edition, Graduate Texts in Mathematics **106** (2009), Springer, New York.

[Sp12] F. Sprung: *The p-parts of Tate-Shafarevich groups of elliptic curves*, RIMS Bessatsu **6** (2012).

[Sp15] F. Sprung: *A formulation of p-adic versions of the Birch and Swinnerton-Dyer conjectures in the supersingular case*, Research in Number Theory, **1** (2015) no.1

[Sp17] F. Sprung: *On pairs of p-adic L-functions for weight two modular forms*, Alg. Number Th. **11** (2017) **885-928**

[Ste94] G. Stevens, *Rigid analytic modular symbols*, 1994, Available at http://math.bu.edu/people/ghs/research.html.

[SW13] W. Stein, C. Wuthrich: *Algorithms for the Arithmetic of Elliptic Curves using Iwasawa Theory*, Mathematics of Computation, **82** (2013), 1757-1792.

[TW95] R. Taylor and A. Wiles: *Ring-Theoretic Properties of Certain Hecke Algebras*, Ann. Math. **141** (1995), 553-572

[Vis76] M. M. Višik: *Nonarchimedean measures associated with Dirichlet series*, Math. Sbornik **99 (141)**, no. 2 (1976), pp. 248-260.

[Wi95] A. Wiles: *Modular elliptic curves and Fermat's last theorem*, Annals of Mathematics **(2) 141** (1995), 443-551.